Contents

Abstract

A pair of Lucas sequences $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ and $V_n = \alpha^n + \beta^n$ is famously associated with each polynomial $x^2 - Px + Q \in \mathbb{Z}[x]$ with roots α and β. It is the purpose of this paper to show that when the root field of $x^2 - Px + Q$ is either $\mathbb{Q}(i)$, or $\mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/6}$, there are respectively two and four other second-order integral recurring sequences of characteristic polynomial $x^2 - Px + Q$ that are of the same kinship as the U and V Lucas sequences. These are, when $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(i)$, the G and the H sequences with

$$G_n = [(1-i)\alpha^n + (1+i)\bar{\alpha}^n]/2, \quad H_n = [(1+i)\alpha^n + (1-i)\bar{\alpha}^n]/2,$$

and, when $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\omega)$, the S, T, Y and Z sequences given by

$$\begin{aligned} S_n &= (\omega\alpha^n - \bar{\omega}\bar{\alpha}^n)/\sqrt{-3}, \\ T_n &= (\omega^2\alpha^n - \bar{\omega}^2\bar{\alpha}^n)/\sqrt{-3}, \\ Y_n &= \bar{\omega}\alpha^n + \omega\bar{\alpha}^n, \\ Z_n &= \omega\alpha^n + \bar{\omega}\bar{\alpha}^n, \end{aligned}$$

where $\bar{\alpha} = \beta$ and $\bar{\omega} = e^{-2\pi i/6}$. Several themes of the theory of Lucas sequences have been selected and studied to support the claim that the six sequences G, H, S, T, Y and Z ought to be viewed as Lucas sequences.

Acknowledgments. I am very thankful to Hugh Williams for remembering his relevant paper [29] and mentioning it to me. I also thank an anonymous referee for his appreciative comments.

2010 *Mathematics Subject Classification*: 11B39, 11B83, 11A07, 11B05.

Key words and phrases: Lucas sequences, identities, laws of appearance and repetition, congruences, Wolstenholme congruence, divisibility, prime density.

Received 13.8.2012; revised version 21.3.2013.

Dedicated to
John Brillhart and Hugh Williams

1. Introduction

We begin by recalling in some detail the definition of Lucas sequences. To a monic quadratic polynomial $x^2 - Px + Q$, where P and Q are rational integers, Q non-zero, we associate a pair of Lucas sequences $U = (U_n)_{n\geq 0}$ and $V = (V_n)_{n\geq 0}$. Both sequences satisfy the binary recursion

$$X_{n+2} = PX_{n+1} - QX_n \quad \text{for } n \geq 0. \tag{1.1}$$

Their respective initial values are

$$U_0 = 0,\ U_1 = 1 \quad \text{and} \quad V_0 = 2,\ V_1 = P. \tag{1.2}$$

Note that recursion (1.1) and the initial conditions (1.2) do define the two sequences U and V and that their terms are integral.

If the discriminant $D = P^2 - 4Q$ is non-zero and the complex roots of $x^2 - Px + Q$ are denoted by α and β, then any recurring sequence $X = (X_n)_{n\geq 0}$ of complex numbers with characteristic polynomial $x^2 - Px + Q$, that is, satisfying recursion (1.1), has closed form

$$X_n = c_1\alpha^n + c_2\beta^n,$$

for some complex numbers c_1 and c_2.

It is straightforward to compute the closed form, the so-called Binet form, of our Lucas sequences,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n. \tag{1.3}$$

If D is zero, then the double root α is the integer $P/2$. The closed form of any recurring sequence of complex numbers satisfying (1.1) is then of type $(c_1 + c_2 n)\alpha^n$. For the U and V sequences, we find

$$U_n = n\alpha^{n-1} \quad \text{and} \quad V_n = 2\alpha^n. \tag{1.4}$$

Alternatively, we may obtain (1.4) using the Binet form (1.3) for U_n and V_n. Note that $U_n = \sum_{k=0}^{n-1} \alpha^{n-1-k}\beta^k$, so that taking the limits $\lim_{\beta\to\alpha} U_n$ and $\lim_{\beta\to\alpha} V_n$ in (1.3) yields (1.4).

The classical theory of Lucas sequences [16, 17, 5, 21, 30] deals with identities involving the terms of the U and/or the V sequences, their arithmetic properties and many arithmetic applications such as the solving of some Diophantine equations and the primality testing of certain types of numbers.

As Lucas [16] himself pointed out it may be observed that the U_n and V_n functions form a discrete version of the sine and cosine functions. Indeed, there is a one-to-one correspondence between Lucas identities and sine and cosine identities. The (*fundamental*)

Lucas sequence (U_n), being a difference of two exponential functions, acts as the sine function, whereas the (*companion*, or *associate*) Lucas sequence (V_n), being the sum of two exponentials, acts as the cosine.

Many mathematically inclined people are familiar with some aspects of Lucas sequences, either special identities, or special arithmetic properties, sometimes more so for particular pairs (U_n, V_n). One of the most studied and known pair is that of the Fibonacci and Lucas numbers (F_n, L_n) that corresponds to $(P, Q) = (1, -1)$. The purpose of this paper is to show that, for some pairs (P, Q) with special discriminants D, there are simply more than two Lucas sequences. In poetic, or silly, or preposterous terms, if one is to compare each recursion (1.1) with a solar system, where, say, (U_n) is the star around which some planets revolve, i.e., the companion Lucas sequences, it may happen that more than one planet, besides the V sequence, orbits around its star. Such a claim would seem to require a formal definition of what is a Lucasian sequence; however, we will not attempt to define what we mean by a Lucas sequence. Of course, it has to be, at least, a second order recurring sequence $X = (X_n)$ satisfying (1.1) and it has to have integral terms for all $n \geq 0$. Also, it should satisfy some addition and multiplication formulas, i.e., identities of the type $X_{m+n} = \cdots$ and $X_{mn} = \cdots$, where the right-hand sides should be polynomial expressions in the mth and nth terms of such Lucasian sequences. Indeed, addition and, most of all, multiplication formulas are fundamental to the theory of Lucas sequences. Defined additively, these sequences, nevertheless, satisfy numerous divisibility properties that are linked to cyclotomy. In fact, this long paper is written so as to convince the readers that the few sequences that are studied herein are indeed of the same kinship as the U and the V Lucas sequences.

It should be clear from what we just wrote that this paper is not about elaborating a new generalization of Lucas sequences. It is about studying very basic objects mostly with the classical and elementary tools from the traditional theory of Lucas sequences.

The next paragraph is meant to introduce and motivate within this introduction and with some precision, albeit from one chosen perspective, these other Lucasian sequences.

Given a prime number p not dividing Q, we denote by $\rho = \rho(p)$ the rank of appearance of p in the U sequence. That is, ρ is the smallest positive index t such that $p \,|\, U_t$. Any prime not dividing Q has a well defined rank. In fact, it is well known that, if p does not divide $2Q$, then ρ is a divisor of $p - \epsilon_p$, where throughout the paper ϵ_p will denote the Legendre character $(D \,|\, p)$, which is 0 or ± 1 according as, respectively, p divides D, D is a non-zero square modulo p or D is not a square modulo p. This rank property is called the *law of appearance* for primes. The rank is said to be *maximal* whenever it is $p - \epsilon_p$. The *law of repetition* states that p divides U_n if and only if n is a multiple of ρ, provided p does not divide Q. However, if we consider the V sequence, then, generally, primes that do not divide any term of that sequence make up a positive proportion of the set of primes. For a prime p which divides terms of the V sequence, we will denote by $\rho_V = \rho_V(p)$ the least positive integer t such that p divides V_t. Thus, ρ_V is the rank of appearance of p in the V sequence. The law of appearance for primes in the V sequence basically says that ρ_V exists if and only if ρ is even, in which case $\rho_V = \rho/2$. We may say that the V sequence 'captures' all primes of even rank. Given a prime p with rank ρ_V,

the law of repetition with respect to the V sequence says that p divides V_n if and only if n is of the form $\rho_V + k\rho = (2k+1)\rho_V$, where k is an integer. Thus, any prime p of maximal rank, not a factor of $2QD$, divides all terms V_n with n congruent to $(p-\epsilon_p)/2$ modulo $p-\epsilon_p$. Indeed, $p-\epsilon_p$ is even for odd primes not dividing D.

The object of this paper is to demonstrate that when the discriminant $D = P^2 - 4Q$ of the characteristic polynomial $x^2 - Px + Q$ is minus a square, or minus three times a square, i.e., $D = -E^2$, or $D = -3F^2$, where E and F are non-zero integers, then the theory of Lucas sequences is even richer than usual. Indeed in these cases, there are, besides the V sequence, other integral *companion* sequences all satisfying recursion (1.1) that lead to yet more identities, arithmetic properties and applications of the Lucas type.

When D is of the form $-E^2$, that is, when the root field of $x^2 - Px + Q$ is the cyclotomic field $\mathbb{Q}(i)$, where i designates as usual the complex number of norm one and argument $\pi/2$, then there are two additional special sequences, denoted throughout by $G = (G_n)_{n\geq 0}$ and $H = (H_n)_{n\geq 0}$. See equations (2.15) and (2.16) for the definitions of the G and the H sequences. A peculiarity of recursions with root field $\mathbb{Q}(i)$ is that, for all primes p not dividing $2E$, $p-\epsilon_p$ is not only even, but divisible by four. The G and the H sequences share the same prime factors and these primes are exactly the primes whose rank is divisible by 4. In fact, we will prove, among other items, that p divides G_n if and only if n is of the form $\rho_G + k\rho$, where ρ_G is either $\rho/4$ or $3\rho/4$ and k is any integer. The same result holds for H with ρ_H replacing ρ_G and $\rho_H + \rho_G = \rho$.

When the discriminant D is of the form $-3F^2$, F a non-zero integer, that is, when the associated root field is the cyclotomic field $\mathbb{Q}(\omega)$, ω being the complex number $e^{2\pi i/6}$, there are, besides the classical U and V Lucas sequences, four additional sequences that ought to be viewed as Lucas sequences. They are the $S = (S_n)_{n\geq 0}$ and the $T = (T_n)_{n\geq 0}$ sequences on one hand, and the $Y = (Y_n)_{n\geq 0}$ and the $Z = (Z_n)_{n\geq 0}$ sequences on the other. See (2.37), (2.39), (2.41), (2.43) for their exact definitions. Note that when the root field of $x^2 - Px + Q$ is $\mathbb{Q}(\omega)$, the quantity $p-\epsilon_p$ for primes p not dividing $6F$ is always a multiple of 6. Each of the two sequences S and T capture all primes of rank a multiple of 3, whereas the sequences Y and Z, each individually, capture all primes whose rank is a multiple of 6.

If $\Phi_n(x,y)$ denotes the nth homogeneous cyclotomic polynomial, then $\Phi_1(\alpha^n, \beta^n)$ is, up to the constant $\alpha - \beta$, equal to U_n, while V_n, which is U_{2n}/U_n, is $\Phi_2(\alpha^n, \beta^n)$. Thus, the U and the V sequences are respectively connected to Φ_1 and Φ_2. The fourth polynomial Φ_4 is also connected, that way, to a second order recurring sequence, namely (V_{2n}). Indeed, $\Phi_4(x,y) = (x^4 - y^4)/(x^2 - y^2) = x^2 + y^2$ and $U_{4n}/U_{2n} = V_{2n}$. But, unless $(P,Q) = (-1,1)$ or $(2,1)$, the sequence (V_{2n}) satisfies a distinct recursion, namely

$$X_{n+2} = V_2 X_{n+1} - Q^2 X_n.$$

What is remarkable about recursions with a discriminant of the form $-E^2$ is that $V_{2n} = 2G_n H_n$, where G and H are both integral second order recurrences that follow the same recursion as U and V.

In general, $\Phi_3(\alpha^n, \beta^n) = \alpha^{2n} + (\alpha\beta)^n + \beta^{2n}$ and $\Phi_6(\alpha^n, \beta^n) = \alpha^{2n} - (\alpha\beta)^n + \beta^{2n}$ will be third order recurring sequences. However, for recursions with a discriminant of the

form $-3F^2$, we have the conspicuous fact that

$$\Phi_3(\alpha^n,\beta^n)=\frac{\alpha^{3n}-\beta^{3n}}{\alpha^n-\beta^n}=\frac{U_{3n}}{U_n}=3S_nT_n,$$
$$\Phi_6(\alpha^n,\beta^n)=\frac{(\alpha^{6n}-\beta^{6n})(\alpha^n-\beta^n)}{(\alpha^{3n}-\beta^{3n})(\alpha^{2n}-\beta^{2n})}=\frac{U_{6n}U_n}{U_{3n}U_{2n}}=\frac{V_{3n}}{V_n}=Y_nZ_n,$$

where all four sequences S, T, Y and Z are integral second order recurring sequences satisfying the same recursion as the U and the V sequences.

It may be noted that these Lucasian sequences all come in pairs either (G,H), or (S,T) and (Y,Z). Returning to our grand comparison, we may think of each pair as being a pair of planets sharing the same orbit, but diametrically opposed to each other at all times! No doubt, an implausible curiosity of astronomy. In earnest, the symmetry of each pair is best expressed algebraically by the formulas

$$Q^nG_{-n}=H_n,\quad Q^nS_{-n}=T_n\quad\text{and}\quad Q^nY_{-n}=Z_n,$$

which hold for all $n\in\mathbb{Z}$. Indeed, since Q is non-zero, recursion (1.1) may be run backward, and we may consider our sequences as indexed over $\mathbb{Z}$ with, possibly, non-integral rational terms for $n<0$.

Besides this introductory chapter, the paper is divided into five chapters. Each chapter deals with one theme in the theory of Lucas sequences. Chapters 2 and 3 deal with basic classical aspects of Lucas theory, while the last three, Chapters 4, 5 and 6, deal with themes that are less often visited. The structure of each chapter is invariably the same: we begin by reviewing the properties exhibited by the U and the V Lucas sequences with respect to the chapter's theme, we then move to a section on recursions of discriminant $D=-E^2$ establishing corresponding results for the G and the H sequences and, finally, treat the case of $-3F^2$ recursions and prove theorems for the four sequences, first for the S and the T, and secondly for the Y and Z sequences. The case $D=-E^2$ is comparatively simpler than that of $D=-3F^2$ in that precisely there are only two sequences instead of four to study.

Except for Theorems 3.16 and 3.25 which are extended Euler criteria for Lucas sequences and are based on higher reciprocity laws that require a smattering of algebraic number theory, the first three chapters require no more than number theory knowledge found in an introduction to elementary number theory such as Fermat's little theorem, or the law of quadratic reciprocity. That is also nearly true of Chapter 5, except that again the three lemmas 5.11, 5.20 and 5.27, use elementary notions of algebraic number theory. The last chapter, Chapter 6, uses basic notions of algebraic number theory in a more extensive way and, on a few occasions, familiarity with basic analytic number theoretic notation and manipulation.

Chapter 2 is devoted to defining the 'new' sequences and listing identities. We made a small selection of classical U and V identities that includes addition and multiplication formulas in Section 2.1. In Section 2.2, we list identities for the G and H sequences in a way that respects the order in which U and V identities were listed in Section 2.1 so as to ease comparison. The same is then done for the four sequences S, T, Y and Z that are defined for $-3F^2$ discriminants in a third section. Many identities listed will also be useful at some point in the paper.

In Chapter 3, we chose to study how some arithmetic properties of the U and V Lucas sequences extend, or generalize, to the other six sequences to which this paper is dedicated. The chapter is divided into four sections each corresponding to a distinct arithmetic property. Of course, each section then splits into three subsections following the usual order of study, i.e., general recursions, $-E^2$ recursions and $-3F^2$ recursions. Arithmetic properties of the Lucas functions $U_n(P,Q)$ and $V_n(P,Q)$ are often developed with the assumption that $\gcd(P,Q)=1$. We do not generally make this assumption. In fact, *special* primes, i.e., primes that divide both P and Q, play an important role in Chapter 5.

Section 3.1, thus, is placed first because it deals with lemmas that assert that, with scarce exception, if the nth terms of two of the four, or the six sequences at hand, are divisible by some prime q, then q must be special. These lemmas will be useful throughout the paper.

The second section, Section 3.2, examines how the classical laws of appearance and repetition of primes in the U and V sequences adjust to the six sequences under study. We already provided partial answers to the question within this introduction since we motivated this study through the respective rank properties of prime divisors. Proposition 3.11, which is a repetition law, and Theorem 3.12, known as Euler's criterion for Lucas sequences, have taken place within Subsection 3.2.1 since they relate to the notion of the rank of a prime and to the law of repetition in the U sequence. Proposition 3.11 will be used many times. Thus, two proofs are given for each of the three theorems that, respectively, state the law of repetition of primes in the G and H sequences (Theorem 3.14), the law of repetition in the S and T sequences (Theorem 3.20) and the law of repetition in the Y and the Z sequences (Theorem 3.23). One proof uses Lucasian identities and the other Proposition 3.11. Again we do so to promote comparisons and for the pleasure of seeing analogies both in the statement of results and in their proof(s). Theorem 3.12 is the so-called Euler criterion for Lucas sequences, and analogous theorems are stated for the other sequences.

In Section 3.3, we derive a congruence formula that yields for all primes p the value of $X_p \pmod p$, where X stands for any of the two, four or six sequences at hand, depending on whether no condition is imposed on D, $D=-E^2$ or $D=-3F^2$. In fact, this congruence is not specific to our sequences, but holds for all integral sequences satisfying (1.1) at least for all odd primes. Still giving explicit versions of this congruence for our various Lucasian sequences highlights the interplay in between each of the three pairs (G,H), (S,T) and (Y,Z). Also, our eight sequences have this in common that the congruence for $X_p \pmod p$ may be derived from multiplication formulas.

Suppose p is a prime that does not divide Q. Then arbitrarily large powers of p will divide some U terms. In fact, if p does not divide 6 and p divides some X terms, where X stands for anyone of our eight Lucasian sequences, then arbitrarily large powers of p will also divide some X terms. The situation is different, say for $X=V$ and $p=2$, where some V terms may be even, yet the highest power of 2 dividing V terms be bounded. In Section 3.4, we examine the question of whether arbitrarily large powers of 2 and 3 divide the sequences herein studied. As might be expected, the role of 2 in V and the

role of 3 in S and T in this respect are analogous. Here as in earlier sections theorems and, occasionally, their several proofs are arranged so as to enhance the twin-character of the properties satisfied by our sequences.

Today the theory of Lucas sequences is still a lively field of mathematics if one judges from the numerous publications that have appeared since, say, the year 1998. The 1998 book [30] which we will refer to on several occasions in this paper contains much on Lucas sequences, in particular in relation to their use in primality testing, but also a whole chapter, Chapter 4, on their properties, and the identities they satisfy. In fact, a new cubic generalization, arguably more satisfactory that most past generalizations, was the object of Eric Roettger's 2009 thesis. A summary of the main features of this generalization appeared in [19]. The last three chapters of the present paper are each based on relatively recent papers on Lucas sequences. Chapter 4 attempts to discover new facets of a beautiful property of Lucas sequences discovered by William Kimball and William Webb in a 1999 publication [12]. Chapter 5 finds its motivation principally from a 2010 paper of Chris Smyth [25], while Chapter 6 has for main source the approaches to the prime density of the V companion Lucas sequences that were conducted in the 2008 paper by the author [2].

In an 1862 paper [31], Joseph Wolstenholme proved the congruence

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$$

for all prime $p \geq 5$. A rational number a/b, where a and b are coprime integers, is said to be divisible by the integer d if d is coprime to b and d divides a.

Several elementary generalizations of Wolstenholme's congruence soon appeared before and after 1900, but mostly around 1900 [9, Chapter 8]. Amusingly, the genuine elementary generalization in [12] took some hundred more years to find a discoverer. It involves sums of consecutive quotients V_n/U_n that are congruent to zero modulo the square of a prime ≥ 5.

In Chapter 4, Section 4.1, we begin by re-examining the theorem of [12] and giving it a slightly more general form. In Sections 4.2 and 4.3, we establish comparable theorems for sums of consecutive quotients of other pairs of sequences such as (G, H), (S, Z) or (T, Y). These theorems could actually all be given analogous proofs based on similar, yet different Lucasian identities each time. We wrote Chapter 4 by mostly and purposefully preserving the naive way the theorems came to us. However in Section 4.4 we added some comments and began addressing questions raised by the extreme similarity all these Wolstenholme-like, Lucas theory-based theorems share. For instance, do they all produce zero modulo p^2 in essentially the same way? Is there a hint that they are all instances of the same phenomenon and could all be proven at once?

Let X be one of the two Lucas sequences U or V. Suppose $\mathcal{N}_X$ denotes the set of integers n which divide X_n, where $n \geq 1$. Let $\Omega(\cdot)$ be the function that maps integers to the number of their prime factors. An integer b in $\mathcal{N}_X$ is said to be X-*basic* if either b is 1 or no divisor d of b with $\Omega(d) = \Omega(b) - 1$ lies in $\mathcal{N}_X$. In [25], completing the work of other authors, in particular that of Lawrence Somer, Smyth showed that $\mathcal{N}_X$ has at most two basic elements, either 1 and 6, or 1 and 12, or 1 only. Also, for n in $\mathcal{N}_X$ the sets $\mathcal{P}_{X,n}$

of primes p for which np is in $\mathcal{N}_X$ are fully characterized as all the prime factors of X_n (with possibly a few others we omit here). That enables one in theory to construct all integers n in $\mathcal{N}_X$ starting with an X-basic element b and multiplying it, one at a time, by $\Omega(n) - \Omega(b)$ prime factors p, where at each stage if m is already constructed the prime p is chosen in $\mathcal{P}_{X,m}$. Smyth adds that it would be interesting to see whether the analysis of his paper could be extended to other second-order recurrence sequences. This is what we have attempted to do in Chapter 5 for the sequences that are under scrutiny in this paper. As turns out, a comparable analysis, beautiful in its smoothness and its analogy with the study in [25], may be carried out provided we look at these sequences in pairs $\{X, X^*\}$ where $\{X, X^*\}$ stands for $\{G, H\}$, $\{S, T\}$ or $\{Y, Z\}$. Indeed, if n divides X_n and, omitting detail, if p divides X_n, then np divides either X_{np} or X^*_{np} according to whether respectively the Legendre character ϵ_p is ± 1.

A prime is said to divide a sequence X if it divides some term of X. The *prime density* of a sequence X is the limit, if it exists, of the ratio of the number of primes $\leq x$ that divide X to $\pi(x)$, the number of primes less than or equal to x, as x goes to ∞. All primes, but perhaps those dividing Q, divide a $U(P, Q)$ Lucas sequence so the prime density of all U sequences is 1. Several papers referenced in [2] have shown some V sequences to have a prime density of $2/3$. The object of [2] was two-fold. First to show heuristically why $2/3$ ought to be the expected prime density of most V Lucas sequences and then to prove that, in some definite sense indeed, almost all V sequences do have prime density $2/3$. The approach taken to prove the latter result was to consider all recursions $x^2 - Px + Q$, or all pairs of integers (P, Q) within a square box $|P| \leq x$ and $|Q| \leq x$, and show that the number of corresponding $V = V(P, Q)$ sequences not having prime density $2/3$ is $o(x^2)$ as x tends to ∞. In Chapter 6, we borrow notation and use the methods of [2] to establish comparable density results for both $-E^2$ recursions and $-3F^2$ recursions. In Section 6.1 we show that in some definite sense within the set of all $-E^2$ recursions almost all V and G sequences have prime densities $5/6$ and $2/3$ respectively. Note that, assuming existence, a G and an H sequences satisfying the same recursion share the same prime density. We then turn to $-3F^2$ recursions in Section 6.2 and establish that the prime densities of the V, the S (or the T) and the Y (or the Z) sequences associated with almost all $-3F^2$ recursions are respectively $2/3$, $3/4$ and $1/2$. The heuristics predicting the prime densities of Sections 6.1 and 6.2 are conducted in Section 6.3.

Some instances of the sequences defined in this paper have appeared here and there in the literature. Roger Laxton ([14], [15]) studied a group associated with each recursion $x^2 - Px + Q$. The elements of the group are equivalence classes of integral sequences that satisfy recursion (1.1), where two such sequences are in the same class if they are equal modulo a shift of index and a multiplication by a rational scalar. The class of the U sequence is the identity of the group, while the class of the V sequence is of order 2. For many recursions, these two classes are the only two of finite order in the group. It is easy to check that in a $-E^2$ recursion the successive powers of the class of G are respectively the classes of G, V, H and U so that, if the four classes are distinct, the class of G has order 4. Similarly, in a $-3F^2$ recursion the successive powers of the class of the Z sequence are respectively the classes of Z, T, V, S, Y and U so that, if all six classes

are distinct, the class of Z is of order 6. In [15, p. 178], Laxton considers as an example the recursion $x^2 - 5x + 7$ which has discriminant -3 and notes that the two sequences with initial terms 1 and 3, and 1 and 2, have classes of order 3. They are respectively an instance of an S and a T sequence if we assume F is 1. Thus, another common point of the sequences we study in this paper is that they are torsion elements of infinite groups with finite torsion subgroup.

The third sequence of which Jeffrey Lagarias computes the prime density in [13] is again the T sequence associated with $x^2 - 5x + 7$. Its prime density is $3/4$. As Chapter 6 further demonstrates, all our sequences lend themselves to unconditional prime density calculations, that is, to calculations that do not require generalized Riemann hypotheses, unlike most other second order recurring sequences.

The paper [3] studies three specific third-order recurring sequences that are associated with each cubic polynomial of the form $x^3 - 3m^2x^2 - 3\epsilon mx - 1$, where m is a non-zero integer and $\epsilon = \pm 1$. Their classes form a subgroup of order 3 in a group that generalizes the group of Laxton to higher order recurrences. These sequences also lent themselves to some unconditional density calculations. It was explicitly remarked [3, p. 276], alas with a few mistakes in the theorem that accompanied the remark, that they could be viewed as generalizing the triplet (U, S, T) of a $-3F^2$ quadratic recursion.

One paper [29] did entirely focus on the sequences U, S and T, and to a lesser degree also on the Y and Z sequences, which concerns us here. Although the upshot of the paper [29] was to develop necessary and sufficient primality tests for numbers of the form $2^m 3^n A - 1$, where $A < 2^{m+1}3^n - 1$, many identities and arithmetic properties that intersect and complete the corresponding sections of Chapters 2 and 3 of our paper may be found there. In fact, properties such as laws of appearance and repetition, are developed for general integers rather than just primes. However, this is done under the hypothesis that $\gcd(P, Q) = 1$ unlike the present paper. Notation differs: R_n, S_n, T_n, W_n, X_n and Y_n stand respectively for what we denote as T_n, $-S_n$, FU_n, V_n, Y_n and Z_n. In fact, the R_n, S_n and T_n sequences of Hugh Williams appeared earlier in [28], where formal identities and connections to Diophantine equations were developed [28, pp. 40–52]. The main object of the thesis [28] is to study three third order recurring sequences associated with a cubic integral monic polynomial. These were denoted by the letters W, V and U and they display properties analogous to a classical pair of Lucas sequences. Therefore, another letter than the letter U (namely T) had to be used to denote (up to a constant) the ordinary U Lucas sequence. Incidentally, we first developed this long paper without being aware of the earlier paper [29]. This raises the obvious question of whether one may, or may not, develop new primality tests based on the G and the H sequences, or find connections of these two sequences with some Diophantine equations.

No doubt, the sequences we study here must have occurred elsewhere, in places we are not aware of. What characterizes this paper, as well as the two earlier papers [29] and to some extent [15], is that their primary focus is on these particular sequences and their properties. The emphasis of the present paper is on showing that the six sequences G, H, S, T, Y and Z, that is, when they exist, are Lucas sequences. In fact, from the work of Laxton [14], [15], one may expect that, for some polynomials $x^2 - Px + Q$, other

such sequences are waiting to be studied and, perhaps, shown to be yet additional Lucas sequences. Indeed, if Q is a square, say R^2, then the two sequences with initial values 1 and $P + R$, and 1 and $P - R$, yield two order-two torsion sequences in the Laxton group. Thus, we may expect eight or twelve sequences with Lucasian properties when, in addition to Q being a square, the discriminant D is respectively of the form $-E^2$ or of the form $-3F^2$.

It is our fond hope that this work will spur people with an interest in Lucas theory to initiate further studies, either on aspects of the Lucas theory of the sequences studied herein, or with respect to yet other sequences.

2. Definition and identities

2.1. Some of the classical identities. We only select a few of the classical identities involving the U and the V sequences, but enough, we think, to convince one that the G and the H sequences for $-E^2$ discriminants, and the S, T, Y and Z sequences for $-3F^2$ discriminants, satisfy identities of a similar nature. Proofs of these classical identities can be found in [16] or [30].

Note that the Binet forms (1.3), (1.4), or running the recursion (1.1) backwards, allows us to view the U and the V sequences as defined for all $n \in \mathbb{Z}$. Of course, their negative terms are rational numbers whose denominators are powers of Q. We will, whenever convenient, also view the binary sequences defined in the next two sections as defined for all $n \in \mathbb{Z}$, although we still refer to the terms of index $n = 0$ and $n = 1$ as the initial values of the sequence. All identities are valid for all indices m and n in $\mathbb{Z}$. Note that the U and V identities listed below are valid with no restriction on D. In particular, D may be 0.

We begin by the formulas that relate the nth term to the $(-n)$th term,

$$Q^n U_{-n} = -U_n \quad \text{and} \quad Q^n V_{-n} = V_n. \tag{2.1}$$

Here is the Pythagorean formula akin to $\cos^2 x + \sin^2 x = 1$:

$$V_n^2 - DU_n^2 = 4Q^n. \tag{2.2}$$

We have the addition and subtraction formulas,

$$2U_{m+n} = U_m V_n + U_n V_m, \tag{2.3}$$

$$2Q^n U_{m-n} = U_m V_n - U_n V_m. \tag{2.4}$$

Subtracting (2.4) from (2.3) yields

$$U_{m+n} = V_m U_n + Q^n U_{m-n}. \tag{2.5}$$

We have more such formulas:

$$2V_{m+n} = V_m V_n + DU_m U_n, \tag{2.6}$$

$$2Q^n V_{m-n} = V_m V_n - DU_m U_n. \tag{2.7}$$

Subtracting (2.7) from (2.6) gives

$$V_{m+n} = DU_m U_n + Q^n V_{m-n}. \tag{2.8}$$

Some double-angle identities are easily obtained from the above formulas:

$$U_{2n} = U_n V_n, \tag{2.9}$$

$$V_{2n} = V_n^2 - 2Q^n = DU_n^2 + 2Q^n. \tag{2.10}$$

Replacing m by n and n by 1 in both (2.5) and (2.8) yields

$$U_{n+1} - QU_{n-1} = V_n \quad \text{and} \quad V_{n+1} - QV_{n-1} = DU_n. \tag{2.11}$$

Also we have

$$U_n^2 - U_{n-1}U_{n+1} = Q^{n-1} \quad \text{and} \quad V_n^2 - V_{n-1}V_{n+1} = -DQ^{n-1}. \tag{2.12}$$

Finally we give the multiplication formulas

$$2^{m-1}U_{mn} = \sum_{k=0}^{\lfloor (m-1)/2 \rfloor} \binom{m}{2k+1} D^k U_n^{2k+1} V_n^{m-2k-1}, \tag{2.13}$$

$$2^{m-1}V_{mn} = \sum_{k=0}^{\lfloor (m-1)/2 \rfloor} \binom{m}{2k} D^k U_n^{2k} V_n^{m-2k}. \tag{2.14}$$

2.2. Identities involving G_n and H_n. We assume that $D = P^2 - 4Q = -E^2$, where E is a non-zero integer. It may be convenient, but not necessary, given only the knowledge of P and Q in a recursion $x^2 - Px + Q$ with $D = -E^2$, to adopt the convention that $E > 0$ so as to lift any ambiguity about what the G and the H sequences are.

The roots α and $\bar{\alpha}$ of $x^2 - Px + Q$ are complex conjugate and by convention

$$\alpha = \frac{P + iE}{2} \quad \text{and} \quad \bar{\alpha} = \frac{P - iE}{2},$$

so that $\alpha - \bar{\alpha} = iE$.

Let us introduce the two new binary recurring sequences $G = (G_n)_{n \geq 0}$ and $H = (H_n)_{n \geq 0}$ both via their Binet form and via their initial values. For any $n \in \mathbb{Z}$, we define

$$G_n = \frac{1}{2}\big[(1-i)\alpha^n + (1+i)\bar{\alpha}^n\big] = \frac{\sqrt{2}}{2}\big[\bar{\zeta}_8\alpha^n + \zeta_8\bar{\alpha}^n\big], \tag{2.15}$$

with initial values $G_0 = 1$ and $G_1 = (P+E)/2$.

The nth term of the H sequence is

$$H_n = \frac{1}{2}\big[(1+i)\alpha^n + (1-i)\bar{\alpha}^n\big] = \frac{\sqrt{2}}{2}\big[\zeta_8\alpha^n + \bar{\zeta}_8\bar{\alpha}^n\big], \tag{2.16}$$

with initial values $H_0 = 1$ and $H_1 = (P-E)/2$.

Note that looking at the equation $P^2 + E^2 = 4Q$ modulo 4, we see that P and E are both even. Thus, G_1 and H_1 are indeed rational integers. Because both sequences (G_n) and (H_n) are linear combinations of the two sequences (α^n) and $(\bar{\alpha}^n)$, G and H both satisfy recursion (1.1).

The U_n and V_n Lucas functions, as Lucas mentioned in the first sentence of his memoir [16], are symmetric functions of the roots α and β as can be seen from their Binet form (1.3). Permuting the roots α and $\bar{\alpha}$ interchanges G_n and H_n. Since, up to powers of Q, G_n and H_{-n} are identical, we may say that G_n and H_n are nearly symmetric functions of the roots. Of course, $G_n H_n$ is. Note that permuting α and $\bar{\alpha}$ also corresponds

to changing the sign of E. It may be of interest to see the effect of changing the signs in both E and P as we do in the following lemma.

Given two even integers P and E, $E \neq 0$, we denote the nth term of a linear recurring sequence X satisfying (1.1) with $P = P$ and $Q = (P^2 + E^2)/4$ by $X_n(P, E)$. Then we have

LEMMA 2.1. *For all $n \geq 0$,*

$$G_n(P, -E) = H_n(P, E) \quad \textit{and} \quad G_n(-P, E) = (-1)^n H_n(P, E).$$

Proof. The two binary sequences $\big(G_n(P, -E)\big)$ and $\big(H_n(P, E)\big)$ have the same initial values 1 and $(P - E)/2$ and share the same recursion since Q is independent of the sign of E, so they must be the same sequences.

The sequences $\big(G_n(-P, E)\big)$ and $\big((-1)^n H_n(P, E)\big)$ are both equal to 1 for $n = 0$ and to $-(P - E)/2$ for $n = 1$. We then show that if they agree on two consecutive terms, n and $n + 1$, they agree on the next two, $n + 1$ and $n + 2$. Thus, equality of the two sequences will follow by induction. Indeed, assuming equality for n and $n + 1$ we have

$$\begin{aligned} G_{n+2}(-P, E) &= -PG_{n+1}(-P, E) - QG_n(-P, E) \\ &= -P(-1)^{n+1} H_{n+1}(P, E) - Q(-1)^n H_n(P, E) \\ &= (-1)^n \big[PH_{n+1}(P, E) - QH_n(P, E)\big] = (-1)^{n+2} H_{n+2}(P, E). \end{aligned}$$ ∎

We are about to list some selected identities involving the G and the H sequences. Besides some fundamental 'first degree' formulas such as

$$V_n = G_n + H_n \quad \text{and} \quad EU_n = G_n - H_n, \tag{2.17}$$

we have attempted to make a list that matches the order in which, in Section 2.1, we listed U, V-identities: Pythagorean, addition and subtraction, double-angle, and so on. These identities, valid for all integers m and n, can be obtained in various ways and often conveniently by the Binet forms for G_n and H_n. We list them below:

$$Q^n G_{-n} = H_n \quad \text{and} \quad Q^n H_{-n} = G_n, \tag{2.18}$$

$$G_n^2 + H_n^2 = 2Q^n, \tag{2.19}$$

$$EU_{m+n} = G_m G_n - H_m H_n, \tag{2.20}$$

$$V_{m+n} = G_m H_n + H_m G_n, \tag{2.21}$$

$$2G_{m+n} = G_m V_n + EH_m U_n, \tag{2.22}$$

$$2H_{m+n} = H_m V_n - EG_m U_n, \tag{2.23}$$

and a subtraction formula

$$EQ^n U_{m-n} = G_m H_n - G_n H_m. \tag{2.24}$$

Equation (2.22), for example, besides being easy to check via the Binet forms (1.3), (2.15) and (2.16) can be proved by fixing an arbitrary value of m. Then $2G_{m+n}$ and $G_m V_n + EH_m U_n$ being two second order recurring sequences in n satisfying (1.1), it is enough to verify their equality for two consecutive values of n. For $n = 0$, this is immediate, since $V_0 = 2$ and $U_0 = 0$. For $n = 1$, this boils down to checking that

$G_{m+1} - QG_{m-1} = EH_m$. Now both terms of this equation are second order recurring sequences in m that satisfy equation (1.1), and their equality holds for $m = 0$ and $m = 1$.

We have some useful double-angle identities. First,

$$V_{2n} = 2G_nH_n. \tag{2.25}$$

Putting $m = n$ in (2.22) and using both identities in (2.17) and the Pythagorean identity (2.19), we get the double-angle formula

$$G_{2n} = EU_nH_n + Q^n. \tag{2.26}$$

A similar calculation leads to

$$H_{2n} = -EU_nG_n + Q^n. \tag{2.27}$$

We also have the important formula

$$U_{4n} = U_{2n}V_{2n} = 2U_nV_nG_nH_n. \tag{2.28}$$

Combining identities (2.17) together with (2.11) leads to formulas between the G and the H sequences analogous to the classical formulas in (2.11) between the U and the V sequences, namely

$$G_{n+1} - QG_{n-1} = EH_n \quad \text{and} \quad H_{n+1} - QH_{n-1} = -EG_n. \tag{2.29}$$

Also we have analogs of (2.12),

$$G_n^2 - G_{n-1}G_{n+1} = E^2Q^{n-1}/2 = H_n^2 - H_{n-1}H_{n+1}. \tag{2.30}$$

Finally we give some multiplication formulas. We have respectively

$$G_n \pm iH_n = (\sqrt{2})^{-1}\big[(\bar{\zeta}_8 \pm i\zeta_8)\alpha^n + (\zeta_8 \pm i\bar{\zeta}_8)\bar{\alpha}^n\big],$$

so that, since $\bar{\zeta}_8 + i\zeta_8 = 0$ and $\zeta_8 + i\bar{\zeta}_8 = 2\zeta_8$, $G_n + iH_n = \sqrt{2}\,\zeta_8\bar{\alpha}^n$ and $G_n - iH_n = \sqrt{2}\,\bar{\zeta}_8\alpha^n$. Thus, adding the two expressions $G_n \pm iH_n$ each raised to the mth power, and expanding them by the binomial formula, yields

$$2\sum_{k\geq 0}\binom{m}{2k}(-1)^kG_n^{m-2k}H_n^{2k} = (\sqrt{2}\,\zeta_8)^m\bar{\alpha}^{mn} + (\sqrt{2}\,\bar{\zeta}_8)^m\alpha^{mn}. \tag{2.31}$$

Putting either $m = 1 + 4\ell$, or $-1 + 4\ell$, in (2.31) gives the multiplication formulas

$$\sum_{k\geq 0}\binom{m}{2k}(-1)^kG_n^{m-2k}H_n^{2k} = \begin{cases}(\sqrt{2})^{m-1}(-1)^\ell G_{mn} & \text{if } m = 1 + 4\ell,\\ (\sqrt{2})^{m-1}(-1)^\ell H_{mn} & \text{if } m = -1 + 4\ell.\end{cases} \tag{2.32}$$

We also have

$$\begin{aligned}(\sqrt{2}\,\zeta_8)^m\alpha^{mn} + (\sqrt{2}\,\bar{\zeta}_8)^m\bar{\alpha}^{mn} &= (H_n + iG_n)^m + (H_n - iG_n)^m\\ &= 2\sum_{k\geq 0}\binom{m}{2k}(-1)^kH_n^{m-2k}G_n^{2k},\end{aligned}$$

which leads to the formulas

$$\sum_{k\geq 0}\binom{m}{2k}(-1)^kH_n^{m-2k}G_n^{2k} = \begin{cases}(\sqrt{2})^{m-1}(-1)^\ell H_{mn} & \text{if } m = 1 + 4\ell,\\ (\sqrt{2})^{m-1}(-1)^\ell G_{mn} & \text{if } m = -1 + 4\ell.\end{cases} \tag{2.33}$$

We present two more multiplication formulas obtained in similar fashion:

$$2^{2m-1}EU_{4mn} = (-1)^m \sum_{k=0}^{2m-1} \binom{4m}{2k+1} (-1)^{k+1} H_n^{2k+1} G_n^{4m-2k-1}, \tag{2.34}$$

$$2^{2m-1}V_{4mn} = (-1)^m \sum_{k=0}^{2m} \binom{4m}{2k} (-1)^{k} H_n^{2k} G_n^{4m-2k}. \tag{2.35}$$

Identity (2.35), for instance, is obtained by expressing the integer $(G_n + iH_n)^{4m} + (G_n - iH_n)^{4m}$ in two ways. On one hand, the binomial formula yields a sum whose terms are even powers of H_n multiplied by even powers of G_n, where, in each term, the sum of the exponents is $4m$; on the other, noting that $G_n + iH_n$ is $(1+i)\bar{\alpha}^n$ and $G_n - iH_n$ is $(1-i)\alpha^n$, the sum of their $4m$th powers is $(-4)^m V_{4mn}$.

2.3. Identities involving S_n, T_n, Y_n and Z_n. We assume here that $D = P^2 - 4Q = -3F^2$, where F is a non-zero integer. Here again, unless stated otherwise, it may be convenient to assume F to be a natural number. Changing the sign of F interchanges the two sequences S and T, and interchanges Y and Z as well.

The roots α and $\bar{\alpha}$ of $x^2 - Px + Q$ are complex conjugate and by convention, we set $\sqrt{-3} = i\sqrt{3}$ and

$$\alpha = \frac{P + F\sqrt{-3}}{2} \quad \text{and} \quad \bar{\alpha} = \frac{P - F\sqrt{-3}}{2},$$

so that $\alpha - \bar{\alpha} = F\sqrt{-3}$. Also, throughout the paper, we denote the complex sixth root of unity $e^{2i\pi/6} = (1 + \sqrt{-3})/2$ by ω. In particular, $1 - \omega + \omega^2 = 0$.

Let us define the four sequences $S = (S_n)_{n\geq 0}$, $T = (T_n)_{n\geq 0}$, $Y = (Y_n)_{n\geq 0}$ and $Z = (Z_n)_{n\geq 0}$. They all satisfy the binary recursion (1.1), and thus are determined by their initial values. We also provide their Binet form.

The initial values of the S sequence are

$$S_0 = 1 \quad \text{and} \quad S_1 = (P + F)/2. \tag{2.36}$$

The Binet form of the nth term is, for any $n \in \mathbb{Z}$,

$$S_n = \frac{1}{\sqrt{-3}} \cdot (\omega\alpha^n - \bar{\omega}\bar{\alpha}^n) = F\frac{\omega\alpha^n - \bar{\omega}\bar{\alpha}^n}{\alpha - \bar{\alpha}}. \tag{2.37}$$

The T sequence has initial values

$$T_0 = 1 \quad \text{and} \quad T_1 = (P - F)/2, \tag{2.38}$$

and the Binet form for T_n, $n \in \mathbb{Z}$, is

$$T_n = \frac{\omega^2\alpha^n - \bar{\omega}^2\bar{\alpha}^n}{\sqrt{-3}} = F\frac{\omega\bar{\alpha}^n - \bar{\omega}\alpha^n}{\alpha - \bar{\alpha}}. \tag{2.39}$$

Initial values for the Y sequence are

$$Y_0 = 1 \quad \text{and} \quad Y_1 = (P + 3F)/2. \tag{2.40}$$

Finding the Binet form for Y_n, $n \in \mathbb{Z}$, gives

$$Y_n = \bar{\omega}\alpha^n + \omega\bar{\alpha}^n. \tag{2.41}$$

Finally, the Z sequence is defined via its initial values

$$Z_0 = 1 \quad \text{and} \quad Z_1 = (P - 3F)/2, \tag{2.42}$$

and its Binet form is, for all $n \in \mathbb{Z}$,

$$Z_n = \omega\alpha^n + \bar{\omega}\bar{\alpha}^n. \tag{2.43}$$

Note that since $P \equiv P^2 \equiv -3F^2 \equiv \pm F \equiv \pm 3F \pmod 2$, S_1, T_1, Y_1 and Z_1 are all rational integers. Thus, all terms with non-negative indices are integral. In particular, as is readily seen, all Binet forms are invariant by complex conjugation.

Unlike the U and the V sequences, the S, T, Y and Z are not exactly symmetric functions of the roots α and $\bar{\alpha}$, but, as for G and H, they have a form of near-symmetry. Permuting α and $\bar{\alpha}$ interchanges Y_n and Z_n, and changes S_n into $-T_n$ and T_n into $-S_n$ as can be seen from (2.41), (2.43), (2.37) and (2.39) ([1]). The near-symmetry comes from considering the upcoming identities (2.46). The products S_nT_n and Y_nZ_n are both symmetric functions of α and $\bar{\alpha}$.

As we did for $G = G(P, E)$ and $H = H(P, E)$, we say what the effect of changing the signs of P and F has on our sequences. Given two integers P and F of the same parity, where $F \neq 0$, we associate the recursion $x^2 - Px + Q$, where $Q = (P^2 + 3F^2)/4$. This recursion has discriminant $-3F^2$. We denote by $X_n(P, F)$ the nth term of a sequence satisfying (1.1) with $P = P$ and $Q = (P^2 + 3F^2)/4$.

We immediately see, on inspecting initial terms of our sequences and noticing that Q is independent of the sign of F, that, for all $n \geq 0$,

$$\begin{aligned} U_n(P, -F) &= U_n(P, F), \\ V_n(P, -F) &= V_n(P, F), \\ S_n(P, -F) &= T_n(P, F), \\ T_n(P, -F) &= S_n(P, F), \\ Z_n(P, -F) &= Y_n(P, F), \\ Y_n(P, -F) &= Z_n(P, F). \end{aligned} \tag{2.44}$$

Assuming X and X' are two sequences with nth terms $X_n = X_n(P, F)$ and $X'_n = X'_n(-P, F)$, where $X_0 = X'_0$ and $X_1 = -X'_1$, an induction will prove as in Lemma 2.1 that

$$X_n = (-1)^n X'_n \quad \text{for all } n \geq 0.$$

This explains the last three of the identities below:

$$\begin{aligned} U_n(P, F) &= (-1)^{n+1} U_n(-P, F), \\ V_n(P, F) &= (-1)^n V_n(-P, F), \\ S_n(P, F) &= (-1)^n T_n(-P, F), \\ Z_n(P, F) &= (-1)^n Y_n(-P, F). \end{aligned} \tag{2.45}$$

([1]) Had we chosen initial values for T_n equal to -1 and $(-P + F)/2$, then permuting the roots would also have interchanged S_n and T_n. Instead we chose each sequence to have 0th term equal to $+1$.

Looking at the Binet forms only, one might guess that the relationship between the S and the Z sequences on one hand, and the relationship between the T and the Y sequences on the other, might well bear resemblance with the relationship that exists between the U and the V sequences. Without further explicit mention, this intuition will be corroborated many times, both by analogy in identities and properties. For example, the Wolstenholme congruences satisfied by the quotients V_n/U_n have an analogue in terms of the quotients Z_n/S_n and another in terms of the quotients Y_n/T_n, as we will see in Chapter 4. The Pythagorean formula (2.2) between the V and the U sequences has analogues, as we will soon see, between the Z and the S sequences on one hand, and the Y and the T sequences on the other.

All our forthcoming identities can either be proved by using the Binet forms of our sequences, or by noting that both sides of the identity are recurring sequences sharing the same recursion of order k, in which case checking the identity on k consecutive terms proves the general identity, or by using identities already established, or any combination of the three methods.

We begin by the formulas that relate nth and $(-n)$th terms,

$$Q^nS_{-n} = T_n, \quad Q^nT_{-n} = S_n, \quad Q^nZ_{-n} = Y_n \quad \text{and} \quad Q^nY_{-n} = Z_n. \tag{2.46}$$

There are many 'first degree' simple identities such as

$$V_n = S_n + T_n \quad \text{and} \quad FU_n = S_n - T_n, \tag{2.47}$$

$$V_n = Y_n + Z_n \quad \text{and} \quad 3FU_n = Y_n - Z_n, \tag{2.48}$$

$$3S_n + Z_n = 2V_n = 3T_n + Y_n, \tag{2.49}$$

$$2S_n = T_n + Y_n \quad \text{and} \quad 2T_n = S_n + Z_n, \tag{2.50}$$

$$Z_n = T_n - FU_n \quad \text{and} \quad Y_n = S_n + FU_n. \tag{2.51}$$

Some Pythagorean identities are echoing identity (2.2), namely

$$S_nT_n + F^2U_n^2 = Q^n = Y_nZ_n + 3F^2U_n^2, \tag{2.52}$$

$$Z_n^2 + 3S_n^2 = 4Q^n = Y_n^2 + 3T_n^2. \tag{2.53}$$

There are analogues of the two double-angle formulas (2.9) and (2.10)

$$FU_{2n} = S_nY_n - Q^n = -T_nZ_n + Q^n, \tag{2.54}$$

$$V_{2n} = S_nZ_n + T_nY_n = 3S_nT_n - Q^n = Y_nZ_n + Q^n, \tag{2.55}$$

$$S_{2n} = T_nY_n \quad \text{and} \quad T_{2n} = S_nZ_n, \tag{2.56}$$

$$S_{2n} = S_nV_n - Q^n \quad \text{and} \quad T_{2n} = T_nV_n - Q^n, \tag{2.57}$$

$$Y_{2n} = Y_nV_n - Q^n = 3S_n^2 - 2Q^n = -Z_n^2 + 2Q^n, \tag{2.58}$$

$$Z_{2n} = Z_nV_n - Q^n = 3T_n^2 - 2Q^n = -Y_n^2 + 2Q^n. \tag{2.59}$$

One of these analogues is the important triple-angle formula

$$U_{3n} = 3U_nS_nT_n. \tag{2.60}$$

By (2.60), $U_{6n} = 3U_{2n}S_{2n}T_{2n}$ and, by identities (2.9) and (2.56), we get the sextuple angle formula

$$U_{6n} = 3U_nV_nS_nT_nY_nZ_n. \tag{2.61}$$

Since $U_{6n} = U_{3n}V_{3n} = 3U_nS_nT_nV_{3n}$, we deduce that

$$V_{3n} = V_nY_nZ_n. \tag{2.62}$$

We give triple-angle formulas for the S and the T sequences:

$$S_{3n} = V_nT_nY_n - Q^nS_n, \tag{2.63}$$

$$T_{3n} = V_nS_nZ_n - Q^nT_n. \tag{2.64}$$

Let us choose to quote some of the many summation formulas:

$$FU_{m+n} = S_mS_n - T_mT_n = T_mY_n - Z_mS_n, \tag{2.65}$$

$$U_{m+n} = S_mU_n + U_mT_n = Z_mU_n + U_mY_n, \tag{2.66}$$

$$2V_{m+n} = S_mZ_n + Z_mS_n + T_mY_n + Y_mT_n, \tag{2.67}$$

$$2S_{m+n} = T_mY_n + Y_mT_n \quad \text{and} \quad S_{m+n} = Y_mT_n - FQ^nU_{m-n}, \tag{2.68}$$

$$2Z_{m+n} = -Y_mY_n + 3T_mT_n, \tag{2.69}$$

$$2Y_{m+n} = -Z_mZ_n + 3S_mS_n, \tag{2.70}$$

$$Y_{m+n} = 3S_mS_n - Q^nV_{m-n} = -Z_mZ_n + Q^nV_{m-n}. \tag{2.71}$$

Replacing n by $-n$ in (2.66) and using (2.47) yields the two subtraction formulas

$$Q^nU_{m-n} = U_mS_n - U_nS_m = U_mT_n - U_nT_m. \tag{2.72}$$

There are some analogues of (2.12), i.e.,

$$S_n^2 - S_{n-1}S_{n+1} = F^2Q^{n-1} = T_n^2 - T_{n-1}T_{n+1}, \tag{2.73}$$

$$Y_n^2 - Y_{n-1}Y_{n+1} = 3F^2Q^{n-1} = Z_n^2 - Z_{n-1}Z_{n+1}. \tag{2.74}$$

Let us now give some multiplication formulas in the same vein as identities (2.13) and (2.14). Thus, expanding by the binomial formula the left-hand sides of the two equations $(Z_n + \sqrt{-3}\,S_n)^m = 2^m\omega^m\alpha^{mn}$ and $(Z_n - \sqrt{-3}\,S_n)^m = 2^m\bar{\omega}^m\bar{\alpha}^{mn}$ and subtracting them yields

$$\sum_{k\geq 0}\binom{m}{2k+1}(-3)^kZ_n^{m-2k-1}S_n^{2k+1} = \begin{cases} 2^{m-1}S_{mn} & \text{if } m \equiv 1 \pmod 6, \\ -2^{m-1}T_{mn} & \text{if } m \equiv -1 \pmod 6. \end{cases} \tag{2.75}$$

If instead of subtracting the two equations we add them, we get

$$\sum_{k\geq 0}\binom{m}{2k}(-3)^kZ_n^{m-2k}S_n^{2k} = \begin{cases} 2^{m-1}Z_{mn} & \text{if } m \equiv 1 \pmod 6, \\ 2^{m-1}Y_{mn} & \text{if } m \equiv -1 \pmod 6. \end{cases} \tag{2.76}$$

Subtracting the two expressions $(Y_n \pm \sqrt{-3}\,T_n)^m$ yields the multiplication formulas

$$\sum_{k\geq 0}\binom{m}{2k+1}(-3)^kY_n^{m-2k-1}T_n^{2k+1} = \begin{cases} 2^{m-1}T_{mn} & \text{if } m \equiv 1 \pmod 6, \\ -2^{m-1}S_{mn} & \text{if } m \equiv -1 \pmod 6. \end{cases} \tag{2.77}$$

Adding them gives

$$\sum_{k\geq 0}\binom{m}{2k}(-3)^kY_n^{m-2k}T_n^{2k} = \begin{cases} 2^{m-1}Y_{mn} & \text{if } m \equiv 1 \pmod 6, \\ 2^{m-1}Z_{mn} & \text{if } m \equiv -1 \pmod 6. \end{cases} \tag{2.78}$$

We give yet a few other multiplication formulas either not covered, or not exactly covered, by the previous formulas:

$$2^{3m}Z_{(3m+1)n} = (-1)^m \sum_{k=0}^{\lfloor \frac{3m+1}{2} \rfloor} \binom{3m+1}{2k} (-3)^k S_n^{2k} Z_n^{3m+1-2k}, \tag{2.79}$$

$$2^{3m}S_{(3m+1)n} = (-1)^m \sum_{k=0}^{\lfloor \frac{3m}{2} \rfloor} \binom{3m+1}{2k+1} (-3)^k S_n^{2k+1} Z_n^{3m-2k}, \tag{2.80}$$

$$2^{3m-1}V_{3mn} = (-1)^m \sum_{k=0}^{\lfloor \frac{3m}{2} \rfloor} \binom{3m}{2k} (-3)^k S_n^{2k} Z_n^{3m-2k}, \tag{2.81}$$

$$2^{3m-1}FU_{3mn} = (-1)^m \sum_{k=0}^{\lfloor \frac{3m-1}{2} \rfloor} \binom{3m}{2k+1} (-3)^k S_n^{2k+1} Z_n^{3m-2k-1}. \tag{2.82}$$

There are identities reminiscent of (2.32), (2.33) and (2.35). Indeed, taking advantage of the identity $\omega^4 S_m + \omega^2 T_m = -\alpha^m$ and its conjugate identity, as was done in the proof of Theorem 5 in [29], we may derive the multiplication identities

$$\begin{aligned} S_{mn} &= (-1)^{n-1} \sum_{k=0}^{n} \binom{n}{k} \mu_{n,k} S_m^k T_m^{n-k}, \\ &= (-1)^{n-1} \sum_{k=0}^{n} \binom{n}{k} \mu_{n,n-k} S_m^{n-k} T_m^k, \end{aligned} \tag{2.83}$$

where $\mu_{n,k}$ is -1, 0 or 1, and $\mu_{n,k} \equiv (n-1 \,|\, 3) + (k \,|\, 3) \pmod 3$, with $(x \,|\, 3)$ standing for the Legendre character of $x \pmod 3$.

Changing F into $-F$ and using the third and fourth identities in (2.44) yields

$$\begin{aligned} T_{mn} &= (-1)^{n-1} \sum_{k=0}^{n} \binom{n}{k} \mu_{n,k} T_m^k S_m^{n-k}, \\ &= (-1)^{n-1} \sum_{k=0}^{n} \binom{n}{k} \mu_{n,n-k} T_m^{n-k} S_m^k. \end{aligned} \tag{2.84}$$

Summing, say, identities (2.83) and (2.84) term by term yields

$$V_{mn} = (-1)^{n-1} \sum_{k=0}^{n} \binom{n}{k} \nu_{n,k} S_m^k T_m^{n-k}, \tag{2.85}$$

where

$$\nu_{n,k} = \begin{cases} -2 & \text{if } 3 \,|\, n+k, \\ 1 & \text{otherwise.} \end{cases}$$

We end this section with a beautiful identity

$$Q^n V_n = S_n^3 + T_n^3. \tag{2.86}$$

It has the associated identity

$$9FQ^n U_n = Y_n^3 - Z_n^3. \tag{2.87}$$

3. Arithmetic properties

This chapter is divided into four sections. Each section is devoted to one arithmetic property. This arithmetic property is studied in three subsections. The first subsection deals with the U and V sequences when P and Q are arbitrary, the second treats the case of the G and the H sequences for $-E^2$ discriminants, and the third looks at the S and the T sequences, as well as the Y and the Z sequences that are defined when the recursion has a discriminant of the form $-3F^2$. This organization allows for a clear view on the analogies that these sequences or their properties share both with the U and the V sequences and among themselves.

We begin with a small section. The lemmas that it contains will be used many times in the next sections as well as in Chapter 5.

3.1. Special primes and $\gcd(X_n, X_n^*)$**.** Recall here that a prime is said to be *special* with respect to $x^2 - Px + Q$ if and only if it divides both P and Q.

3.1.1. General recursions. Given a quadratic polynomial $x^2 - Px + Q$ in $\mathbb{Z}[x]$, $Q \neq 0$, we prove one lemma.

LEMMA 3.1. *If a prime q divides both U_n and V_n for some $n \geq 1$, then q is a special prime, unless $q = 2$ and Q is odd.*

Proof. By the Pythagorean identity (2.2), $V_n^2 - DU_n^2 = 4Q^n$ so that q divides $2Q$. If $q \mid Q$, then as $V_1 = P$ and $V_{k+1} \equiv PV_k \pmod{q}$ an induction yields $V_n \equiv P^n \pmod{q}$. Hence q also divides P, and thus q is special.

Using recursion (1.1) modulo 2, one sees that if P is even and Q is odd, then $2 \mid \gcd(U_n, V_n)$ whenever n is even. If P and Q are odd, then $2 \mid \gcd(U_n, V_n)$ iff 3 divides n. Hence, if $q = 2$ and Q is odd, 2 will divide both U_n and V_n for some positive indices n. Yet 2 is not special. ∎

3.1.2. Recursions with $D = -E^2$

LEMMA 3.2. *Let q be a prime, and X and X^* be any two of the four sequences U, V, G and H. If q divides both X_n and X_n^* for some $n \geq 1$, then q is special, except in the case where the sequences X and X^* are the U and V sequences and q is 2, Q is odd and n is even.*

Proof. We first look at the case $\{X, X^*\} = \{G, H\}$. If $q \mid \gcd(G_n, H_n)$, then $q^2 \mid G_n^2 + H_n^2$. However, $G_n^2 + H_n^2 = 2Q^n$, so $q \mid Q$. Since $V_n = G_n + H_n$, we have $q \mid V_n$. Hence, $V_n \equiv P^n \pmod{q}$. Therefore, $q \mid P$ and we conclude that q is a special prime.

If, say, X is the V sequence and X^* is either G or H, then, as $V_n = G_n + H_n$, $q \mid \gcd(G_n, H_n)$. Hence, q is special.

Similarly, if, say, X is U and X^* is either G or H, then, because $EU_n = G_n - H_n$, $q \mid \gcd(G_n, H_n)$. Thus, q is special.

By Lemma 3.1, if X and X^* are U and V, then q is special, unless Q is odd and $q = 2$. Note that Q may indeed be odd when $D = -E^2$ as we may witness from, say, the recursion $x^2 - 4x + 5$ of discriminant -4. However, recursions with discriminant $-E^2$ have even P's, so that, when Q is odd, we see from the proof of Lemma 3.1 that $2 \mid \gcd(U_n, V_n)$ iff n is even. ∎

3.1.3. Recursions with $D = -3F^2$. We first prove two useful lemmas: one about common prime factors of S_n and T_n, and another about common prime factors of Y_n and Z_n.

LEMMA 3.3. *Let q be a prime dividing both S_n and T_n, for some $n \geq 1$. Then q is a special prime.*

Proof. We have the two identities

$$S_n - T_n = FU_n \quad \text{and} \quad S_n T_n = Q^n - F^2 U_n^2. \tag{3.1}$$

By the first identity in (3.1), $q \mid FU_n$. By the second, $q^2 \mid Q^n$, and thus $q \mid Q$. Now $V_n \equiv P^n \pmod{q}$ for $n \geq 1$ and $V_n = S_n + T_n \equiv 0 \pmod{q}$. So $q \mid P$. Hence q is a special prime. ∎

LEMMA 3.4. *Let q be a prime. If q divides both Y_n and Z_n for some $n \geq 1$, then q is special.*

Proof. By the two identities

$$Y_n - Z_n = 3FU_n \quad \text{and} \quad Y_n Z_n + 3F^2 U_n^2 = Q^n,$$

we find that $q \mid Q$. Thus, $V_n \equiv P^n \pmod{q}$, for any $n \geq 1$. But $V_n = Y_n + Z_n$ is divisible by q. Hence, $q \mid P$ and q is indeed special. ∎

We prove a lemma comparable to that of the previous section.

LEMMA 3.5. *Let X, X^* be two of the six sequences U, V, S, T, Y and Z. Let q be a prime that divides both X_n and X_n^* for some $n \geq 1$, then q is special, unless q is 2, Q is odd and the pair $\{X, X^*\}$ is one of the three pairs $\{U, V\}$, $\{S, Z\}$ or $\{T, Y\}$.*

Proof. There are fifteen possible pairs $\{X, X^*\}$, but three have their case already settled by the three Lemmas 3.1, 3.3 and 3.4.

So suppose, say, X is U or V, and X^* is one of the four sequences S, T, Y or Z. Then, by the identities $FU_n = S_n - T_n$ and $3FU_n = Y_n - Z_n$, or by the identities $V_n = S_n + T_n = Y_n + Z_n$, and by the Lemmas 3.3 and 3.4, q is special.

If the pair $\{X, X^*\}$ is either $\{S, Y\}$, or $\{T, Z\}$, then by the identities $2S_n = T_n + Y_n$ and $2T_n = S_n + Z_n$, q divides S_n and T_n. Hence, q is special by Lemma 3.3. For the two remaining cases, i.e., $\{X, X^*\}$ is either $\{S, Z\}$ or $\{T, Y\}$, then the same two identities $2S_n = T_n + Y_n$ and $2T_n = S_n + Z_n$ and Lemma 3.3 lead to the conclusion that q is special, provided q is odd. One can easily check that for all n, $S_n \equiv Z_n \pmod{2}$, and that $T_n \equiv Y_n \pmod{2}$, and that infinitely many terms S_n and Z_n, or infinitely many terms

T_n and Y_n, will be even iff P and Q are odd (see the proof of Remark 5.22). If Q is even, then, by Lemma 5.18, P is even. Thus, in that case, $q = 2$ is special. ∎

3.2. Laws of appearance and repetition. This second section of Chapter 3 deals with the classical laws of appearance and repetition that reflect an important characteristic of the Lucas functions U and V. Their generalizations to other sequences will be studied here.

3.2.1. Laws of appearance and repetition for U and V. Proofs of these classical U and V laws can be found in various places in the literature such as, for instance, [5], [16] or [30]. They are often established with the assumption that $\gcd(P, Q) = 1$. This assumption is not always necessary. Comments on proofs will exclusively refer to the proofs given in [30, Chapter 4], where most of these properties appear in concise and rigorous form.

DEFINITION 1. Let $f(x) = x^2 - Px + Q$ and $X = (X_n)_{n\geq 0}$ be a sequence that satisfies the recursion (1.1). Let m be a positive integer. If m divides some term X_n, $n \geq 1$, then we define $\rho_X(m)$, the *rank* of m in X, as the smallest positive integer t such that m divides X_t. When writing $\rho(m)$ without reference to a sequence X, it is understood that we refer to the rank, $\rho_U(m)$, of m in U. The rank ρ of m relative to U is also referred to as the rank of the integer m *relative* to f ([1]).

The first theorem is to be read with the convention that for the prime $p = 2$, the symbol ϵ_p is defined by

$$\epsilon_2 = \begin{cases} 0 & \text{if } 2 \mid P \text{ (i.e., if } 2 \mid D), \\ -1 & \text{otherwise.} \end{cases} \tag{3.2}$$

THEOREM 3.6 (Law of appearance of primes). *Let p be a prime not dividing Q. Then p has a rank ρ such that*

$$\rho \text{ divides } p - \epsilon_p.$$

Proof. Most of the argument for proving Theorem 3.6 may be found in [30, p. 84]. The missing cases $p = 2$ and $p \mid D$ are easily completed. Do it! ∎

THEOREM 3.7 (Law of repetition). *Let p be a prime not dividing Q. Then p has a rank ρ and, for all $n \in \mathbb{Z}$, we have*

$$p \text{ divides } U_n \;\Leftrightarrow\; \rho \text{ divides } n.$$

Proof. Theorem 3.7 extends to any positive integer m prime to Q. The forward implication ($\Rightarrow$) of the extended theorem corresponds to Theorem 4.3.4, p. 87, of [30], but it is proved with the (unnecessary) assumption that $\gcd(P, Q) = 1$. If $\gcd(P, Q) = 1$, then $\gcd(U_k, V_k)$ is, for each k, either 1 or 2. If no assumption is made on $\gcd(P, Q)$, then $\gcd(U_k, V_k)$ divides $2Q^k$. However, the hypothesis that $\gcd(m, Q) = 1$ is enough for the

([1]) It may be convenient to adopt the convention that $\rho_U(m) = \infty$ together with the obvious properties of ∞, whenever this rank does not exist. However, we will only do so when explicitly mentioned.

proof of Theorem 4.3.4 of [30] to remain valid. The reverse direction is trivially seen to hold because $U_\rho \,|\, U_n$. ∎

THEOREM 3.8 (Law of appearance of prime powers). *Let p be a prime not dividing $2Q$ of rank ρ. Assume that $p^a \,\|\, U_\rho$ for some integer $a \geq 1$ ([2]). Let b be an integer ≥ 0. Then the rank of p^{a+b} is $p^b\rho$ and*

$$n \text{ is of the form } kp^b\rho \;\Leftrightarrow\; \nu_p(U_n) = a + b,$$

where k is an integer prime to p.

Proof. The direct implication in Theorem 3.8 corresponds to Theorem 4.3.6 of [30], where it is proved with the assumption that $\gcd(P, Q) = 1$. This assumption implies that for any two non-negative integers m and n, $\gcd(U_m, U_n)$ is $|U_d|$, where $d = \gcd(m, n)$. This property does not hold in general, but in the proof of Theorem 4.3.6 of [30] it can conveniently be replaced by the fact that, since $p \nmid Q$, $\nu_p(\gcd(U_m, U_n)) = \nu_p(U_d)$. (Put $\ell = \nu_p\big(\gcd(U_m, U_n)\big)$ and $k = \nu_p(U_d)$. Then $k \leq \ell$ because U_d divides both U_m and U_n, and $\ell \leq k$ because the rank of p^ℓ divides both m and n. Therefore, $\rho(p^\ell)$ divides d and p^ℓ divides U_d.)

The reverse implication is easy. By Theorem 3.7, n must be of the form $kp^c\rho$, where $c \geq 0$ and k is prime to p. But, by the direct implication ($\Rightarrow$) of Theorem 3.8, $\nu_p(U_n) = a + c$. Thus, we have $b = c$ and $n = kp^b\rho$. ∎

THEOREM 3.9 (Law of appearance for primes in (V_n)). *Let p be a prime not dividing $2Q$ of rank ρ. Then*

$$2 \text{ divides } \rho \;\Leftrightarrow\; \text{the rank } \rho_V \text{ exists,}$$

and, in case of existence, $\rho_V = \rho/2$. Moreover, V_{ρ_V} has the same p-adic valuation as U_ρ.

Proof. Since $p \nmid 2Q$ and since $V_n^2 - DU_n^2 = 4Q^n$, p does not divide $\gcd(V_n, U_n)$, for any $n \geq 0$. Suppose ρ is even and write $\rho = 2\rho^*$. By the identity $U_\rho = U_{\rho^*}V_{\rho^*}$ and the definition of ρ, we find that $p \,|\, V_{\rho^*}$. Thus, ρ_V exists and is $\leq \rho^*$. But $p \,|\, V_{\rho_V} \Rightarrow p \,|\, U_{2\rho_V}$. Hence, $\rho = 2\rho^* \leq 2\rho_V$. Therefore, $\rho_V = \rho/2$. Also, $\nu_p(V_{\rho_V}) = \nu_p(U_\rho)$, since $p \nmid U_{\rho_V}$. Conversely, if ρ_V exists, then $p \,|\, U_{2\rho_V}$. Hence, $\rho \mid 2\rho_V$, but $p \nmid U_{\rho_V}$ so that ρ is even. ∎

THEOREM 3.10 (Law of repetition for primes in (V_n)). *Let p be a prime not dividing $2Q$ whose rank ρ is even. Then*

$$p \text{ divides } V_n \;\Leftrightarrow\; n \text{ is of the form } \rho_V + k\rho,\ k \in \mathbb{Z}.$$

Proof. After reading the proof of Theorem 3.9, one can easily see that $p \,|\, V_n$ iff $p \,|\, U_{2n}$ and $p \nmid U_n$, which, by Theorem 3.7, holds iff $\rho \,|\, 2n$ and $\rho \nmid n$, that is, if and only if $\rho_V \,|\, n$, but $2\rho_V \nmid n$, or n is an odd multiple of ρ_V. ∎

We now give a less fundamental, but handy result we will use many times, which is the observation that a sequence (X_n) satisfying recursion (1.1), which, modulo an integer $d > 1$, takes on the successive values 0 and c, where c is an integer prime to d, is, modulo d, identical to the sequence (cU_n), where (U_n) is the associated Lucas U sequence. We chose

([2]) If $x^2 - Px + Q$ has two roots whose ratio is a root of unity, then it may happen that $U_\rho = 0$. Then a does not exist and the theorem is void.

a condition, imposed on the initial values of (X_n), that guarantees that, if d divides some term X_{n_0}, then X_{n_0+1} is prime to d.

PROPOSITION 3.11. *Let P and Q be integers, with Q non-zero. Assume $(X_n)_{n\in\mathbb{Z}}$ is a sequence of rational numbers, with integral coprime initial values X_0 and X_1, that satisfies recursion* (1.1)*, i.e.,*

$$X_{n+2} = PX_{n+1} - QX_n \quad \text{for all } n \in \mathbb{Z}.$$

Suppose $d \geq 2$ is an integer prime to Q that divides some term X_{n_0}, $n_0 \in \mathbb{Z}$. Then, for $n \in \mathbb{Z}$, we have

$$d \,|\, X_n \;\Leftrightarrow\; n = n_0 + k\rho \text{ for some } k \in \mathbb{Z},$$

where ρ is the rank of d relative to $f(x) = x^2 - Px + Q$.

Proof. The extended version of Theorem 3.7, mentioned in the proof of Theorem 3.7, implies the existence of the rank $\rho = \rho(d)$, as d is prime to Q. Let $c \in \mathbb{Z}$ be such that $X_{n_0+1} \equiv c \pmod{d}$. Note that c must exist, because X_{n_0+1} is, possibly up to a power of Q, integral and d is prime to Q. Then $X_{n_0} \equiv cU_0 \pmod{d}$ and $X_{n_0+1} \equiv cU_1 \pmod{d}$. Running recursion (1.1) forward we get through induction that

$$X_{n_0+m} \equiv cU_m \pmod{d}, \qquad \forall m \geq 0.$$

Since d is prime to Q, both (X_n) and (U_n) satisfy the backward recursion

$$x_{n-2} = Q^{-1}(Px_{n-1} - x_n),$$

and this recursion is well defined modulo d. Thus, we also have $X_{n_0+m} \equiv cU_m \pmod{d}$ for all $m < 0$. Therefore, if $\gcd(c, d) > 1$, then all X_n, $n \in \mathbb{Z}$, are multiples of the non-trivial factor $\gcd(c, d)$. But this contradicts the hypothesis $\gcd(X_0, X_1) = 1$. Hence, $\gcd(c, d) = 1$, and thus $d \,|\, X_n = X_{n_0+(n-n_0)}$ if and only if $d \,|\, U_{n-n_0}$. Now, applying the extended version of Theorem 3.7 yields our result. ∎

By Theorem 3.6, if p is an odd prime that does not divide QD, then p divides the even-indexed U term, $U_{p-\epsilon_p}$. Since $U_{2n} = U_nV_n$, it may be interesting to decide which of $U_{(p-\epsilon_p)/2}$ or $V_{(p-\epsilon_p)/2}$ is divisible by p. There is a criterion, called *Euler's Criterion for Lucas sequences*, that yields a simple answer which we state as the last result of this subsection, since we will be referring to it a few times throughout the paper. A proof of this criterion and historical comments may be found in [30, pp. 84–85].

THEOREM 3.12. *Let p be a prime not dividing $2QD$. Then*

$$\begin{aligned} p \,|\, U_{(p-\epsilon_p)/2} \quad &\text{iff} \quad (Q \,|\, p) = 1, \text{ and thus} \\ p \,|\, V_{(p-\epsilon_p)/2} \quad &\text{iff} \quad (Q \,|\, p) = -1, \end{aligned}$$

where $(Q \,|\, p)$ is the Legendre character of $Q \pmod{p}$.

3.2.2. Laws of appearance and repetition for G and H

THEOREM 3.13 (Law of appearance for primes in (G_n) and (H_n)). *Let p be a prime not dividing $2Q$ of rank ρ. Then*

$$4 \text{ divides } \rho \;\Leftrightarrow\; \text{the ranks } \rho_G \text{ and } \rho_H \text{ exist,}$$

and, in case of existence, $\rho_G + \rho_H = \rho$ *and* $\{\rho_G, \rho_H\} = \{\rho/4, 3\rho/4\}$. *In addition,* G_{ρ_G} *and* H_{ρ_H} *have the same p-adic valuation as* U_ρ, *unless* $p = 3$ *and* $\rho_X = 3\rho/4$, *where* X *is* G *or* H, *in which case* $\nu_3(X_{\rho_X}) = 1 + \nu_3(U_\rho)$.

Proof. Assume $\rho = 4m$. Then $p \,|\, U_{4m}$ and $p \nmid U_{2m}$. Since $U_{4m} = U_{2m}V_{2m}$, we have $p \,|\, V_{2m}$. By (2.25), $V_{2m} = 2G_mH_m$ and, since $p \neq 2$, $p \,|\, G_mH_m$. Suppose $p \,|\, G_m$. Then, by (2.28), $p \nmid G_n$, for any n, $1 \leq n < m$, or else p would divide U_{4n}, contradicting $\rho = 4m$. Thus, $\rho_G = m$. Putting $n = 2m$ in identity (2.23) yields $2H_{3m} = H_mV_{2m} - EG_mU_{2m}$ from which we get that p divides H_{3m}. If p divided some H_n for some positive $n < 3m$, then, by (2.28), p would divide U_{4n}. Hence, we would have $4m \,|\, 4n$ and n would either be m or $2m$. Note that p does not divide E. For if $p \,|\, E$, then $\epsilon_p = 0$ and $\rho \,|\, p$. This would mean that 4 divides p, which is absurd. Now since $EU_m = G_m - H_m$ and $p \nmid EU_m$, p does not divide H_m. Putting $n = 2m$ in identity (2.20) yields $EU_{3m} = G_mG_{2m} - H_mH_{2m}$. So p cannot divide H_{2m}, since this would entail that $p \,|\, U_{3m}$. Thus $\rho_G = \rho/4$ and $\rho_H = 3\rho/4$. The case 'p divides H_m' would lead, through similar arguments, to the reverse situation, i.e., $\rho_H = \rho/4$ and $\rho_G = 3\rho/4$.

To prove the converse, put $\rho_G = n$. Since $U_{4n} = 2U_nV_nG_nH_n$, p divides U_{4n}. Hence, $\rho \,|\, 4n$. Since $V_{2n} = 2G_nH_n$ and $p \nmid 2Q$, p does not divide U_{2n} by (2.2). Thus, $\rho \nmid 2n$. Therefore, $4n/\rho$ is an odd integer and 4 divides ρ.

Finally, consider the identity $U_{4n} = 2U_{2n}G_nH_n$ and put $n = \rho_G$. Without loss of generality, we may assume that $\rho_G < \rho_H$ (if not, put $n = \rho_H$, and reason on H rather than on G). Thus, we have $\rho = 4n$ and, as we just saw, $p \nmid H_n$, $p \,|\, V_{2n}$ and $p \nmid U_{2n}$. So $\nu_p(U_{4n}) = \nu_p(G_{\rho_G})$. Now $\rho_H = 3n$ and $U_{4\rho_H} = 2U_{2\rho_H}G_{\rho_H}H_{\rho_H}$. Since $4\rho_H = 3\rho$, but $\rho \nmid 2\rho_H$, we find that $\nu_p(H_{\rho_H}) = \nu_p(U_{3\rho})$, which, by Theorem 3.8, is $\nu_p(U_\rho)$, if $p \neq 3$, and is $1 + \nu_3(U_\rho)$, if $p = 3$. ∎

Remark. The cases where, in Theorem 3.13, either $\nu_3(G_{\rho_G})$, or $\nu_3(H_{\rho_H})$, equals $1 + \nu_3(U_\rho)$, do occur. In fact, as soon as $3 \nmid PQE$, we have $\rho(3) = 4$ and so this phenomenon occurs. For instance, for $P = 2$, $Q = 5$ and $E = 4$, we have $\rho(3) = 4$, with $U_4 = -12$, $G_1 = 3$ and $H_3 = -9$. Also, note that, to show that $\nu_p(H_{\rho_H}) = 1 + \nu_3(U_\rho)$ (when $\rho_H = 3\rho_G$), instead of using Theorem 3.8, one may use identities (2.23) and (2.20) (putting $m = n$), to get $2H_{3n} = (2H_n^2 - EU_{2n})G_n = (3H_n^2 - G_n^2)G_n$. Hence, if $3 \nmid Q$ and $3 \,|\, G_n$, then $\nu_3(H_{3n}) = \nu_3(G_n) + 1$.

Theorem 3.14 (Law of repetition for primes in (G_n) and (H_n)). *Let* p *be a prime not dividing* Q *whose rank* ρ *is a multiple of* 4. *Then* ρ_G *and* ρ_H *exist, and*

$$p \text{ divides } G_n \;\Leftrightarrow\; n \text{ is of the form } \rho_G + k\rho,\ k \in \mathbb{Z},$$
$$p \text{ divides } H_n \;\Leftrightarrow\; n \text{ is of the form } \rho_H + k\rho,\ k \in \mathbb{Z}.$$

We give two proofs of the theorem.

Proof 1. Let us show the first equivalence, since the second one may be shown in similar manner. Note first that $p \nmid 2E$, because 2 has a rank at most 3 and, if $p \,|\, E$, then $\rho(p)$ is p, which is not a multiple of 4. Assume n to be of the form $\rho_G + k\rho$ for some k and put $m = \rho_H$. By Theorem 3.13, $m + n = (k + 1)\rho$. Thus p divides U_{m+n}. But $EU_{m+n} = G_mG_n - H_mH_n$. Thus, p divides G_mG_n. Since $p \nmid 2Q$, identity (2.19) implies

that $p \nmid G_m$. Hence p divides G_n. Conversely, by (2.24), $Q^m E U_{n-m} = G_n H_m - H_n G_m$. If p divides G_n and $m = \rho_G$, then p must divide U_{n-m}. But, by Theorem 3.7, $\rho \,|\, n-m$, i.e., n is of the form $\rho_G + k\rho$. ∎

Proof 2. Since the rank of 2 cannot exceed 3, p is not 2. Thus, by Theorem 3.13, ρ_G exists. Since $\gcd(G_0, G_1) = 1$, applying Proposition 3.11 with $d = \rho_G$ yields the theorem. ∎

COROLLARY 3.15. *Let p be a prime not dividing Q with rank ρ divisible by 4. Then either $\rho_G = \rho/4$ and*

$$\rho_G < \rho_V = \rho/2 < \rho_H = 3\rho/4 < \rho,$$

or $\rho_G = 3\rho/4$ and

$$\rho_H = \rho/4 < \rho_V = \rho/2 < \rho_G = 3\rho/4 < \rho.$$

Proof. This is an immediate consequence of Theorems 3.9 and 3.13. ∎

Given a prime of rank a multiple of 4, we may, in some cases, tell which of ρ_G or ρ_H is $\rho/4$ by using an extension of Theorem 3.12 that includes the G and the H sequences.

THEOREM 3.16. *Assume $D = -E^2$. Let p be a prime not dividing QE. If $p \equiv 1 \pmod 4$, then*

$$\begin{aligned} p \,|\, U_{(p-1)/4} \quad &\text{iff} \quad (Q\alpha^2 \,|\, \pi)_4 = 1, \\ p \,|\, V_{(p-1)/4} \quad &\text{iff} \quad (Q\alpha^2 \,|\, \pi)_4 = -1, \\ p \,|\, G_{(p-1)/4} \quad &\text{iff} \quad (Q\alpha^2 \,|\, \pi)_4 = i, \\ p \,|\, H_{(p-1)/4} \quad &\text{iff} \quad (Q\alpha^2 \,|\, \pi)_4 = -i. \end{aligned}$$

If $p \equiv 3 \pmod 4$, then

$$\begin{aligned} p \,|\, U_{(p+1)/4} \quad &\text{iff} \quad (\alpha \,|\, \pi)_4 = 1, \\ p \,|\, V_{(p+1)/4} \quad &\text{iff} \quad (\alpha \,|\, \pi)_4 = -1, \\ p \,|\, G_{(p+1)/4} \quad &\text{iff} \quad (\alpha \,|\, \pi)_4 = i, \\ p \,|\, H_{(p+1)/4} \quad &\text{iff} \quad (\alpha \,|\, \pi)_4 = -i. \end{aligned}$$

In the above two statements π is a prime ideal above p in $\mathbb{Q}(i)$, which is primary, that is, $\pi \equiv 1 \pmod{2+2i}$ in $\mathbb{Z}[i]$, and $(x \,|\, \pi)_4$ is the biquadratic Legendre character i^{η_p} of x, i.e., $x^{(N(\pi)-1)/4} \equiv i^{\eta_p} \pmod \pi$ in $\mathbb{Z}[i]$, $\eta_p = 0$, 1, 2 or 3, and $N(\pi)$ is the norm of the ideal π.

Proof. Assume $p \equiv 1 \pmod 4$, i.e., $\epsilon_p = 1$ and $N(\pi) = p$. As $p \nmid Q$, $\alpha^{p-1} \equiv \bar{\alpha}^{p-1} \equiv 1 \pmod \pi$. By definition of $(\alpha^2 Q \,|\, \pi)_4$, we have $i^{\eta_p} \equiv (\alpha^2 Q)^{\frac{p-1}{4}} \equiv \alpha^{3\frac{p-1}{4}} (\bar{\alpha})^{\frac{p-1}{4}} \pmod \pi$. Thus, $(\bar{\alpha})^{\frac{p-1}{4}} \equiv i^{\eta_p} \alpha^{\frac{p-1}{4}} \pmod \pi$, which using the Binet formulas (1.3), (2.15) and (2.16) yields, for $\eta_p = 0$, 1, 2 and 3, the announced results.

Suppose now $p \equiv 3 \pmod 4$, i.e., $\epsilon_p = -1$ and $N(\pi) = p^2$. Then $\pi = -p$ and $\alpha^p \equiv \bar{\alpha} \pmod \pi$. We have

$$(\alpha \,|\, \pi)_4 = i^{\eta_p} \equiv \alpha^{\frac{p^2-1}{4}} = (\alpha^{p-1})^{\frac{p+1}{4}} = (\alpha^p/\alpha)^{\frac{p+1}{4}} \equiv (\bar{\alpha}/\alpha)^{\frac{p+1}{4}} \pmod p,$$

which using the Binet forms (1.3), (2.15) and (2.16) implies that p divides $X_{\frac{p+1}{4}}$ iff the pair (X, η_p) is one of the four pairs $(U, 0)$, $(V, 2)$, $(G, 1)$ or $(H, 3)$. ∎

We illustrate the use of Theorem 3.16 with two small primes $p = 13$ and $p = 7$ and the recursion $x^2 - 4x + 5$, where $P = 4$, $Q = 5$ and $E = 2$. Then $\alpha = 2 + i$. Note that α is not a primary prime of the ring $\mathbb{Z}[i]$, but that the associate prime $i\alpha = -1 + 2i$ is primary.

Let us first consider $p = 13$. We have $\rho(13) = 12$ so that 13 divides either G_3 or H_3. Using Theorem 3.16 with the primary prime $\pi = 3 + 2i$, we have

$$\begin{aligned}(Q\alpha^2 \,|\, \pi)_4 &= [(i \,|\, \pi)_4]^2[(i\alpha \,|\, \pi)_4]^3(-i\bar{\alpha} \,|\, \pi)_4 \\ &= \big(i^{\frac{13-1}{4}}\big)^2[(\pi \,|\, i\alpha)_4]^3(\pi \,|\, -i\bar{\alpha})_4 \\ &= (-1)[(-1 \,|\, i\alpha)_4]^3(i \,|\, -i\bar{\alpha})_4 = (-1)(-1)^3 i = i.\end{aligned}$$

In the above calculation, we used the law of biquadratic reciprocity (see Theorem 4.21, p. 82 of [6]) and the identities $\pi = 3+2i = -2i(-1+2i)-1$ and $\pi = (-1+i)(-1-2i)+i$. Therefore, 13 must divide G_3. In fact, $G_3 = 13$.

We now turn to $p = 7$. The rank of 7 is 8 so either 7 divides G_2 or H_2. Theorem 3.16 may be used as a tool for deciding the case. We compute $(\alpha \,|\, 7)_4$. Noting that -7 is the primary prime associate to 7, we use biquadratic reciprocity and the identity $7 = (-1 + 2i)(-1 - 3i) - i$ to obtain

$$(i\alpha \,|\, -7)_4 = (-7 \,|\, i\alpha)_4 = -(7 \,|\, i\alpha)_4 = -(-i)^{\frac{5-1}{4}} = i.$$

Therefore, $i = (i\alpha \,|\, -7)_4 = (i\alpha \,|\, 7)_4 = (i \,|\, 7)_4(\alpha \,|\, 7)_4$. But $(i \,|\, 7)_4 = i^{\frac{49-1}{4}} = 1$. Thus, $(\alpha \,|\, 7)_4 = i$, that is, $\eta_7 = 1$ and 7 divides $G_{\frac{7+1}{4}}$. In fact, $G_2 = 7$.

3.2.3. Laws of appearance and repetition for S, T, Y and Z. Throughout Subsection 3.2.3 it is assumed that $D = -3F^2$, $F \geq 1$. The notation is borrowed from Subsection 2.3.

LEMMA 3.17. *Let p be a prime not dividing $2Q$ and a be either an integer ≥ 1 or ∞. Then*

$$\begin{aligned}p^a \parallel S_n \quad &\text{if and only if} \quad p^a \parallel T_{2n} \text{ and } p \nmid Z_n, \\ p^a \parallel T_n \quad &\text{if and only if} \quad p^a \parallel S_{2n} \text{ and } p \nmid Y_n.\end{aligned}$$

Proof. The first statement follows from the identity $Z_n^2 + 3S_n^2 = 4Q^n$ and the formula $T_{2n} = S_n Z_n$, whereas the second follows from $Y_n^2 + 3T_n^2 = 4Q^n$ and $S_{2n} = T_n Y_n$. ∎

LEMMA 3.18. *Suppose p is a prime that does not divide $3Q$ and p divides X_n, where X stands for either S or T. Then $\nu_p(U_{3n}) = \nu_p(X_n)$.*

Proof. Since $p \nmid Q$, p is not special. Thus, by Lemma 3.5, $p \nmid U_n X_n^*$, where

$$X^* = \begin{cases} T & \text{if } X = S, \\ S & \text{if } X = T. \end{cases}$$

But $p \neq 3$ and $U_{3n} = 3U_n X_n X_n^*$, so $\nu_p(U_{3n}) = \nu_p(X_n)$. ∎

THEOREM 3.19 (Law of appearance for primes in (S_n) and (T_n)). *Let p be a prime not dividing $3Q$ of rank ρ. Then*

$$3 \text{ divides } \rho \;\Leftrightarrow\; \text{the ranks } \rho_S \text{ and } \rho_T \text{ exist},$$

where, in case of existence, $\rho_S + \rho_T = \rho$ *and* $\{\rho_S, \rho_T\} = \{\rho/3, 2\rho/3\}$. *Moreover,* S_{ρ_S} *and* T_{ρ_T} *have the same p-adic valuation as* U_ρ, *unless* $p = 2$ *and* ρ_S, *or* ρ_T, *is* 2.

Proof. Assume first that 3 divides ρ. Then $p \nmid F$. Otherwise $\rho(p)$ is p, by Theorem 3.6, forcing p to be 3, which would contradict the hypothesis. Put $\rho = 3m$. By identity (2.60), we have $U_{3m} = 3U_m S_m T_m$. Since p divides U_{3m}, but not U_m, and $p \neq 3$, p divides $S_m T_m$. Suppose $p \mid S_m$. Then by identity (2.60) and the definition of $\rho = 3m$, p does not divide any S_n with $1 \leq n < m$. Thus ρ_S is m. By Lemma 3.17, p divides T_{2m}. Assume p divides some T_k, with $1 \leq k < 2m$. Then again, by identity (2.60), p would divide U_{3k}. This would mean that $3m \mid 3k$, and hence $k = m$. But p cannot divide S_m and T_m, or, by Lemma 3.3, p would be a special prime and divide Q, yielding a contradiction. Thus, $\rho_T = 2m$ and $\rho_S + \rho_T = m + 2m = \rho$. The argument is entirely similar if $p \mid T_m$, leading instead to $\rho_T = m$ and $\rho_S = 2m$.

For the converse, put $\rho_S = n$. By identity (2.60), we have that $p \mid U_{3n}$, so that ρ divides $3n$. Note that $p \nmid U_n$, or else p would divide S_n and U_n, which, by Lemma 3.5, would imply that $p \mid Q$. Thus, $\rho \mid 3n$ and $\rho \nmid n$, which implies that $3 \mid \rho$.

We now compare the p-adic values of U_ρ, S_{ρ_S} and T_{ρ_T}. Say $m = \rho_S = \rho/3$; the case $m = \rho_T$ would be treated identically. Applying Lemma 3.18 with $n = \rho/3$ yields $\nu_p(U_\rho) = \nu_p(S_{\rho_S})$. By Lemma 3.17, if $p \neq 2$, then T_{2m} and S_m also have the same p-adic valuation. The claim follows as $2m = \rho_T$. ∎

Theorem 3.20 (Law of repetition for primes in (S_n) and (T_n)). *Let* p *be a prime not dividing* $3Q$ *whose rank* ρ *is a multiple of* 3. *Then*

$$p \text{ divides } S_n \;\Leftrightarrow\; n \text{ is of the form } \rho_S + k\rho,\ k \in \mathbb{Z},$$
$$p \text{ divides } T_n \;\Leftrightarrow\; n \text{ is of the form } \rho_T + k\rho,\ k \in \mathbb{Z}.$$

As for Theorem 3.14 we may give two proofs, a direct one using Lucasian identities, and one that uses Proposition 3.11.

Proof 1. We only write a proof for the first equivalence, but the second one can be handled by similar means. Assume $n = \rho_S + k\rho$, for some $k \in \mathbb{Z}$, and put $m = \rho_T$. By Theorem 3.19, $m + n = (k+1)\rho$, so that $p \mid U_{m+n}$ and $p \mid T_m$. By (2.66), $U_{m+n} = T_m U_n + U_m S_n$, so p divides $U_m S_n$. But $p \nmid U_m$. Hence, $p \mid S_n$. For the converse, assume that p divides some term S_n. By (2.72), we have $Q^{\rho_S} U_{n-\rho_S} = U_n S_{\rho_S} - S_n U_{\rho_S}$. Hence, p must divide $Q^{\rho_S} U_{n-\rho_S}$. Since $p \nmid Q$, we deduce that p divides $U_{n-\rho_S}$. Therefore, ρ divides $n - \rho_S$, which implies that n is of the form $\rho_S + k\rho$, for some $k \in \mathbb{Z}$. ∎

Proof 2. By Theorem 3.19, the ranks ρ_S and ρ_T exist. So the theorem follows by applying Proposition 3.11 with $d = \rho_S$ for the S sequence, and with $d = \rho_T$ for the T sequence. ∎

There are comparable theorems for the Y and the Z sequences.

Lemma 3.21. *Suppose* p *is a prime, not a factor of* $2Q$, *which divides* X_n, *where* X *stands for either* Y *or* Z. *Then* $\nu_p(U_{6n}) = \nu_p(X_n)$.

Proof. By Lemma 3.5, $p \nmid V_n X_n^*$, where X^* denotes Z if $X = Y$, and Y if $X = Z$. As $V_{3n} = V_n Y_n Z_n$, $\nu_p(V_{3n}) = \nu_p(X_n)$. But $U_{6n} = U_{3n} V_{3n}$ and, by Lemma 3.1, $p \nmid U_{3n}$. Thus, $\nu_p(U_{6n}) = \nu_p(X_n)$. ∎

THEOREM 3.22 (Law of appearance for primes in (Y_n) and (Z_n)). *Let p be a prime not dividing $2Q$ of rank ρ. Then*

$$6 \text{ divides } \rho \;\Leftrightarrow\; \text{the ranks } \rho_Y \text{ and } \rho_Z \text{ exist,}$$

and, in case of existence, $\rho_Y + \rho_Z = \rho$ with $\{\rho_Y, \rho_Z\} = \{\rho/6, 5\rho/6\}$. Moreover, Y_{ρ_Y} and Z_{ρ_Z} have the same p-adic valuation as U_ρ, unless $p = 5$ and $\rho_X = 5\rho/6$ (X being either Y or Z), in which case $\nu_5(X_{\rho_X}) = \nu_5(U_\rho) + 1$.

Proof. Assume first that ρ is of the form $6m$ with $m \geq 1$. Note that $p \neq 3$, as $\rho(3) \leq 4$. By Theorem 3.19, p divides $S_{2m}T_{2m}$. Suppose $p \,|\, S_{2m}$. That is, by Theorem 3.19, $\rho_S = 2m$ and $\rho_T = 4m$. Since m is not of the form $4m + 6km$, $k \in \mathbb{Z}$, p does not divide T_m by Theorem 3.20. But $S_{2m} = T_m Y_m$, so p divides Y_m. By (2.61), if p divides Y_n, $1 \leq n < m$, then p divides U_{6n}, which contradicts $\rho = 6m$. Hence ρ_Y exists and is $\rho/6$.

By Theorem 3.20, $p \nmid S_{5m}S_{10m}$. Also $p \nmid U_{10m}$. Thus $U_{5\rho} = 3U_{10m}S_{10m}T_{10m}$ implies that p divides T_{10m}. Because $T_{10m} = S_{5m}Z_{5m}$, we find that p divides Z_{5m}. Suppose $p \,|\, Z_n$, for some n, $1 \leq n < 5m$, then by (2.61), $p \,|\, U_{6n}$. Thus, by Theorem 3.7, m must divide n, so that $n \in \{m, 2m, 3m, 4m\}$. Since $T_{2n} = S_n Z_n$, p divides T_{2n}. Hence $2n$ is of the form $\rho_T + k\rho = 4m + 6km$. This occurs only for $n = 2m$. However, $p \,|\, S_{2m}$. So, by Lemma 3.5, $p \nmid Z_{2m}$. Hence ρ_Z exists and is $5\rho/6$. The case $p \,|\, T_{2m}$ is handled similarly leading to $\rho_Y = 5\rho/6$ and $\rho_Z = \rho/6$.

Conversely, put $n = \rho_Y$. By (2.61), $p \,|\, U_{6n}$ so that $\rho \,|\, 6n$. Also, $V_{3n} = V_n Y_n Z_n$ implies that p divides V_{3n}, which by Theorem 3.9, says that ρ is even. We next show that p cannot divide U_{2n}. For contradiction suppose $p \,|\, U_{2n}$. Since $FU_{2n} = S_{2n} - T_{2n} = T_n Y_n - S_n Z_n$, we have $p \,|\, S_n Z_n$. But $V_{2n} = S_n Z_n + T_n Y_n$. Hence p divides $\gcd(V_{2n}, U_{2n})$, which, by Lemma 3.1, implies that p divides $2Q$, a contradiction. Now $\rho \nmid 2n$ and $\rho \mid 6n \Rightarrow 3 \,|\, \rho$. Hence, $6 \,|\, \rho$.

Suppose $\rho = 6n$ with $n = \rho_Y$. By Lemma 3.21, $\nu_p(U_\rho) = \nu_p(\rho_Y)$. As $\rho_Z = 5n$, the same lemma yields $\nu_p(U_{5\rho}) = \nu_p(Z_{\rho_Z})$. By Theorem 3.8, $\nu_p(U_{5\rho}) = \nu_p(U_\rho)$, if $p \neq 5$, and $\nu_p(U_{5\rho}) = 1 + \nu_p(U_\rho)$, if $p = 5$. Hence, the claims on the p-adic valuations of U_ρ, Y_{ρ_Y} and Z_{ρ_Z} hold. The case $n = \rho_Z$ is handled similarly. ∎

REMARK. Note that if $5 \nmid FQ$, then $\epsilon_5 = (-3F^2|5) = -1$ and $\rho(5)$ divides 6. So, if in addition $5 \nmid P = U_2$ and $(Q \,|\, 5) = -1$, then, using Euler's criterion for Lucas sequences, i.e., Theorem 3.12, $\rho(5) = 6$. For instance, for $P = 1$, $Q = 7$ and $F = 3$, we have $\rho(5) = 6$ with $U_6 = 120$, $Y_1 = 5$ and $Z_5 = -25$. The 5-valuation of Z_5 is indeed one more than that of U_ρ and $Y_{\rho/6}$. Amusingly, one may show directly that $\nu_5(Z_5) = 1 + \nu_5(Y_1)$, when $5 \,|\, Y_1$, using appropriate identities, that is, without resorting to Theorem 3.8. Indeed, by (2.69), $Z_5 = xY_1$, with $x = -Y_4 + 3T_1^2 Z_2$. Using (2.58), (2.53) and (2.59) modulo 25, one finds that $x \equiv 10Q^2 \pmod{25}$.

THEOREM 3.23 (Law of repetition for primes in (Y_n) and (Z_n)). *Let p be a prime not dividing Q whose rank ρ is a multiple of 6. Then*

$$p \text{ divides } Y_n \;\Leftrightarrow\; n \text{ is of the form } \rho_Y + k\rho,\ k \in \mathbb{Z},$$
$$p \text{ divides } Z_n \;\Leftrightarrow\; n \text{ is of the form } \rho_Z + k\rho,\ k \in \mathbb{Z}.$$

Proof. As for Theorem 3.20, these statements can be proved either by application of Proposition 3.11, or by direct use of Lucas-like identities. Here, we choose to write down an identity-based proof only for the first equivalence. Note first that $p \nmid 6$ since the ranks of either 2, or 3 cannot be multiples of 6. By Theorem 3.22, ρ_Y and ρ_Z exist. So, assume $n = \rho_Y + k\rho$ for some k in $\mathbb{Z}$ and put $m = \rho_Z$. Use the identity $U_{m+n} = Z_m U_n + Y_n U_m$ to deduce that p divides Y_n. For the converse, use instead the identity $Q^n U_{m-n} = U_m Y_n - Y_m U_n$ to write that $Q^{\rho_Y} U_{n-\rho_Y} = U_n Y_{\rho_Y} - Y_n U_{\rho_Y}$. If p divides Y_n, then p divides $U_{n-\rho_Y}$. Thus, by Theorem 3.7, n is of the form $\rho_Y + k\rho$. ∎

Corollary 3.24. *Let p be a prime not dividing Q with rank ρ divisible by 6. Then either $\rho_Z = \rho/6$ and*

$$\rho_Z < \rho_T = \rho/3 < \rho_V = \rho/2 < \rho_S = 2\rho/3 < \rho_Y = 5\rho/6,$$

or $\rho_Z = 5\rho/6$ and

$$\rho_Y = \rho/6 < \rho_S = \rho/3 < \rho_V = \rho/2 < \rho_T = 2\rho/3 < \rho_Z.$$

Proof. By Theorems 3.9, 3.19 and 3.22, the ranks of p in V, S, T, Y and Z all exist and $\rho_V = \rho/2$, $\{\rho_S, \rho_T\} = \{\rho/3, 2\rho/3\}$ and $\{\rho_Y, \rho_Z\} = \{\rho/6, 5\rho/6\}$. Since $T_{2n} = S_n Z_n$, if ρ_Z is $\rho/6$, then ρ_T is $\rho/3$. But then ρ_Y is $5\rho/6$ and ρ_S is $2\rho/3$. If ρ_Z is $5\rho/6$, then ρ_Y is $\rho/6$ and we conclude using the identity $S_{2n} = T_n Y_n$. ∎

Corollary 3.24 leaves open the question of deciding which of the two possibilities actually takes place for a given prime p. This question was considered in the paper [29]. An analogue for the S and T sequences of Theorem 3.12, i.e., of the classical Euler criterion for Lucas sequences, will help settle the matter in some cases.

Theorem 3.25. *Assume $D = -3F^2$. Let p be a prime not dividing $6QF$. Then*

$$\begin{aligned} p \,|\, U_{(p-\epsilon_p)/3} \quad &\text{iff} \quad (Q\alpha \,|\, \pi)_3 = 1, \quad \text{and thus} \\ p \,|\, S_{(p-\epsilon_p)/3} T_{(p-\epsilon_p)/3} \quad &\text{iff} \quad (Q\alpha \,|\, \pi)_3 \neq 1, \end{aligned}$$

with $p \,|\, S_{(p-\epsilon_p)/3}$ iff $\eta_p = 1$, where π is a primary prime ideal above p in $\mathbb{Q}(\omega)$, that is, $\pi \equiv \pm 1 \pmod 3$ in $\mathbb{Z}[\omega]$, and $(Q\alpha \,|\, \pi)_3$ is the cubic Legendre character $\omega^{2\eta_p}$, where $(Q\alpha)^{(N(\pi)-1)/3} \equiv \omega^{2\eta_p} \pmod \pi$ in $\mathbb{Z}[\omega]$, $\eta_p = 0$, 1 or 2, and $N(\pi)$ is the norm of the ideal π.

Proof. See Theorem 6 in [29]. ∎

Suppose p is a prime of rank ρ equal to $p - \epsilon_p$ with $\epsilon_p \neq 0$. Clearly, p satisfies the conditions of Corollary 3.24. Also, by Theorem 3.25, $\eta_p \neq 0$. Furthermore, if $\eta_p = 1$, then p divides $S_{\rho/3}$. Therefore, $\rho_S = \rho/3$ and $\rho_T = 2\rho_S$, that is, we are in the second case of Corollary 3.24. If $\eta_p = 2$, then we are in the first case.

We illustrate the use of Theorem 3.25 with a simple computational example. Take $x^2 - Px + Q = x^2 + x + 7$, that is, $P = -1$, $Q = 7$ and $F = 3$. Then $\alpha = 1 + 3\omega^2$, which happens to be a primary prime of the ring $\mathbb{Z}[\omega]$. We have $\rho(11) = 12$. Let us compute η_{11}. We have

$$(Q\alpha \,|\, 11)_3 = (7 \,|\, 11)_3 \times (\alpha \,|\, 11)_3 = 1 \times (11 \,|\, \alpha)_3.$$

Indeed, any integer, not a multiple of 11, is a cubic residue modulo 11. Note that 11 is also a primary prime of $\mathbb{Z}[\omega]$ and that we used cubic reciprocity. (See for instance [6, p. 79]). Now $11 = \alpha\bar{\alpha} + 4 \equiv 2^2 \pmod{\alpha}$. But

$$(2 \mid \alpha)_3 \equiv 2^{(7-1)/3} = 4 \equiv -3 = -\omega^4(1 + 3\omega^2) + \omega^4 \equiv \omega^4 \pmod{\alpha}.$$

Thus, $(11 \mid \alpha)_3 = (\omega^4)^2 = \omega^2$, that is, $\eta_{11} = 1$. Indeed, 11 divides $S_4 = 55$ and $Y_2 = -11$.

3.3. Values of $X_p \pmod{p}$

3.3.1. Values of U_p and $V_p \pmod{p}$. We are interested in a classical theorem ([30, p. 84]) that states that, for any odd prime p, we have

$$U_p \equiv \epsilon_p \pmod{p}, \qquad V_p \equiv P \pmod{p}.$$

In fact, for $p = 2$, we also have $U_2 \equiv \epsilon_2 \pmod{2}$ and $V_2 \equiv P \pmod{2}$, provided we agree, as in Theorem 3.6, that ϵ_2 is 0 or -1 according as, respectively, D is even or odd. Convention (3.2) is actually adopted throughout the paper.

We will provide extensions of this theorem to the G, H, S, T, Y and Z sequences. To this end, it is convenient to give it a less explicit, but more uniform expression, susceptible of generalization. Note that in the theorem below the discriminant D may, or may not, be 0.

THEOREM 3.26. *For all primes p, we have*

$$X_p \equiv Q^{(1-\epsilon_p)/2} X_{\epsilon_p} \pmod{p}, \tag{3.3}$$

where (X_n) is either one of the two Lucas sequences (U_n) or (V_n), and, by convention, we agree that, if p divides D, then the chosen square root of $Q \pmod{p}$ is $P/2$, when p is odd, and Q, when p is 2.

In particular (3.3) *implies that*

$$U_2 \equiv V_2 \equiv P \pmod{2}.$$

Proof. Suppose p is odd. Then the classical elementary proofs use the multiplication formulas (2.13) and (2.14) with $m = p$ and $n = 1$. To obtain the congruence involving, say, U_p, note that, in (2.13), all binomial coefficients, but the last, are divisible by p. This yields $2^{p-1}U_p \equiv D^{(p-1)/2} \pmod{p}$, or $U_p \equiv \epsilon_p \pmod{p}$. The reformulation (3.3) is valid. Indeed, that $\epsilon_p \equiv Q^{(1-\epsilon_p)/2} U_{\epsilon_p} \pmod{p}$ is immediate, since $U_1 = 1$, $QU_{-1} = -U_1 = -1$ and $U_0 = 0$. Also, $P \equiv Q^{(1-\epsilon_p)/2} V_{\epsilon_p} \pmod{p}$ holds because $V_1 = P$, $V_{-1} = P/Q$ and $V_0 = 2$. Suppose $p = 2$. Then $U_2 = P$ and $V_2 = P^2 - 2Q \equiv P \pmod{2}$. Note that if P is even, then $Q^{(1-\epsilon_2)/2} X_{\epsilon_2} = QX_0$, which for either $X = U$ or $X = V$ is even, as it is respectively 0 and $2Q$. If P is odd, then $Q^{(1-\epsilon_2)/2} X_{\epsilon_2} = QX_{-1}$, which is either $-U_1 = -1$, or $V_1 = P$ depending on whether X is U or V. ∎

COROLLARY 3.27. *For all integral sequences $X = (X_n)_{n \geq 0}$ satisfying* (1.1) *and all odd primes p, we have*

$$X_p \equiv Q^{(1-\epsilon_p)/2} X_{\epsilon_p} \pmod{p},$$

where the conventions for $Q^{1/2} \pmod{p}$ and primes dividing D are those of Theorem 3.26.

Proof. For all $n \geq 0$, we have $X_n = aU_n + bV_n$, with $a = X_1 - PX_0/2$ and $b = X_0/2$. Thus, a and b are well defined modulo any odd prime. Therefore, by Theorem 3.26 and for all odd primes p, we have

$$X_p = aU_p + bV_p \equiv Q^{(1-\epsilon_p)/2}(aU_{\epsilon_p} + bV_{\epsilon_p}) = Q^{(1-\epsilon_p)/2}X_{\epsilon_p} \pmod p. \ \blacksquare$$

3.3.2. Values of G_p and $H_p \pmod p$. Here, we deal with recursions of discriminant $-E^2$, where E is a non-zero integer, and propose a theorem that extends Theorem 3.26 to the G and H sequences.

THEOREM 3.28. *For all primes p, we have*

$$X_p \equiv Q^{(1-\epsilon_p)/2}X_{\epsilon_p} \pmod p,$$

where X, besides U or V, may stand for either G or H. Here, we adopt the convention of Theorem 3.26*, which is that, for primes p dividing E, the chosen square root of $Q \pmod p$ is $P/2$ when p is odd, and Q when p is* 2.

More explicitly, we have modulo p,

$$\begin{cases} G_p \equiv G_1 \text{ and } H_p \equiv H_1 & \text{if } p \equiv 1 \pmod 4, \\ G_p \equiv H_1 \text{ and } H_p \equiv G_1 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

The primes p dividing E, which always include $p = 2$, satisfy both of the above congruences. But we also have

$$\begin{cases} G_p \equiv H_p \equiv P/2 \pmod p & \text{for } p \text{ odd}, \\ G_2 \equiv H_2 \equiv Q \pmod 2 & \text{for } p = 2. \end{cases}$$

Proof. For odd primes we apply Corollary 3.27.

For odd primes p dividing E, we get $G_p \equiv H_p \equiv P/2 \pmod p$. But for such primes $G_1 \equiv H_1 \equiv P/2 \pmod p$, so we also have $G_p \equiv G_1 \equiv H_1 \pmod p$ and $H_p \equiv H_1 \equiv G_1 \pmod p$.

Suppose $p = 2$. Since $4Q = P^2 + E^2$, P and E must both be even. Thus, $G_2 = PG_1 - QG_0 \equiv Q \pmod 2$. Similarly, $H_2 \equiv Q \pmod 2$. Also, $Q = (P/2)^2 + (E/2)^2 \equiv (P/2) + (E/2) \equiv (P/2) - (E/2) \pmod 2$. Therefore, the five integers Q, G_2, H_2, G_1 and H_1 all have the same parity. $\blacksquare$

REMARK. One can obtain an alternative elementary proof of Theorem 3.28 for odd primes in line with the classical proof of Theorem 3.26. We do so here for the G sequence. Suppose first that $p = 4\ell + 1$, $\ell \geq 1$. Replacing m by p and n by 1 in (2.32), we get, since all binomial coefficients are divisible by p except the first, $2^{(p-1)/2}(-1)^{(p-1)/4}G_p \equiv G_1^p \pmod p$. If p is 1 (mod 8), then $(2 \,|\, p) = 1$ so that, by Euler's criterion, $2^{(p-1)/2} \equiv 1 \pmod p$ and $(-1)^{(p-1)/4} = 1$. Thus, $G_p \equiv G_1 \pmod p$. If $p \equiv 5 \pmod 8$, then $(2 \,|\, p) = -1$ and $(-1)^{(p-1)/4} = -1$. Again we get $G_p \equiv G_1 \pmod p$. For primes p of the form $-1 + 4\ell$, use the second identity in (2.33) modulo p with $m = p$ and $n = 1$, to get $G_p \equiv H_1 \pmod p$. Note that one can also use the second identity of (2.32) with $m = p$ and $n = -1$. Assuming $p = -1 + 4\ell$ does not divide Q, this leads to $H_{-p} \equiv G_{-1} \pmod p$. But then $G_p = Q^p H_{-p} \equiv QG_{-1} = H_1 \pmod p$. Then we would have to look at the case where $p = -1 + 4\ell$ divides Q. Since $4Q = P^2 + E^2$ there are no such primes, if $p \nmid P$. If p divides P, then $p \,|\, G_n$ and $p \,|\, H_n$, for all $n \geq 1$. Thus $G_p \equiv H_1 \equiv 0 \pmod p$.

REMARK. In the development of Chapter 5, stronger congruence results that imply the odd prime case of Theorem 3.28 will appear in Lemma 5.11.

3.3.3. Values of S_p, T_p, Y_p and Z_p (mod p). We now provide a theorem, which, for all recursions of discriminant $-3F^2$, extends Theorem 3.26 to the S, T, Y and Z sequences.

THEOREM 3.29. *For all primes p, we have*

$$X_p \equiv Q^{(1-\epsilon_p)/2} X_{\epsilon_p} \pmod{p}, \tag{3.4}$$

where X, besides U or V, may stand for S, T, Y or Z. As in Theorems 3.26 *and* 3.28, *we agree that modulo p,*

$$Q^{1/2} = \begin{cases} P/2 & \text{if } p \text{ is odd and } p \mid D, \\ Q & \text{if } p \text{ is } 2 \text{ and } p \mid D. \end{cases}$$

More explicitly, if p is congruent to 1 (mod 6), *then*

$$S_p \equiv S_1,\ T_p \equiv T_1,\ Y_p \equiv Y_1,\ Z_p \equiv Z_1 \pmod{p}. \tag{3.5}$$

If p is congruent to -1 (mod 3), *then*

$$S_p \equiv T_1,\ T_p \equiv S_1,\ Y_p \equiv Z_1,\ Z_p \equiv Y_1 \pmod{p}. \tag{3.6}$$

For primes dividing $3F$, we also have

$$S_p \equiv T_p \equiv Y_p \equiv Z_p \equiv \begin{cases} P/2 & \text{if } p \text{ is odd,} \\ Q & \text{if } p = 2, \end{cases} \pmod{p}.$$

That is, primes p dividing $3F$ satisfy both (3.5) *and* (3.6), *unless X is S or T, $p = 3$ and $3 \nmid F$, in which case S_3 and T_3 are congruent neither to S_1, nor to T_1* (mod 3).

Proof. Congruence (3.4) holds for all odd primes by Corollary 3.27. In particular, for odd primes p dividing $3F$, we have, by (3.4), $X_p \equiv P/2 \pmod{p}$, since $\epsilon_p = 0$ and $X_0 = 1$, for any choice of X among S, T, Y or Z. Now, S_1, T_1, Y_1, Z_1 being equal to $(P \pm F)/2$ or $(P \pm 3F)/2$ are all congruent to $P/2 \pmod{p}$ and to each other, unless $p = 3$ and $3 \nmid F$. In this latter case, only Y_3 and Z_3 satisfy the congruences (3.5) and (3.6), not S_3 or T_3, for which neither congruence is satisfied, since, for instance, $S_3 \equiv P/2 \not\equiv (P \pm F)/2 \pmod{3}$.

Suppose $p = 2$. Since $S_1 - Z_1 = 2F = Y_1 - T_1$, we have $S_1 \equiv Z_1 \pmod{2}$ and $T_1 \equiv Y_1 \pmod{2}$. Now, by (2.56), $S_2 = T_1 Y_1$. Hence, $S_2 \equiv T_1^2 \equiv T_1 \pmod{2}$. Also, $T_2 = S_1 Z_1$ so that $T_2 \equiv S_1 \pmod{2}$. The two identities (2.53) with $n = 2$ yield $Z_2 \equiv S_2 \pmod{2}$ and $Y_2 \equiv T_2 \pmod{2}$. Thus, $Z_2 \equiv T_1 \equiv Y_1 \pmod{2}$ and $Y_2 \equiv S_1 \equiv Z_1 \pmod{2}$. Hence, 2 obeys congruence (3.6) as do primes $-1 \pmod{6}$.

However, if 2 divides F, then since the differences $S_1 - T_1 = F$, $Y_1 - Z_1 = 3F$ and $S_1 - Z_1 = 2F$ are all even, we deduce that S_1, T_1, Y_1 and Z_1 have the same parity. Thus, 2 follows both congruences (3.5) and (3.6), and $S_2 \equiv T_2 \equiv Y_2 \equiv Z_2 \equiv Q \pmod{2}$, since $S_2 = PS_1 - QS_0 \equiv Q \pmod{2}$ as P and F have the same parity.

One easily checks that congruence (3.4) predicts the correct answer when p is 2. Say F is odd. Then $Q^{(1-\epsilon_2)/2} X_{\epsilon_2} = QX_{-1} = X_1^*$, where the pair $\{X, X^*\}$ is either $\{S, T\}$, or $\{Y, Z\}$. If F is even, then $Q^{(1-\epsilon_2)/2} X_{\epsilon_2} = QX_0$, which equals Q, for X any of the four sequences S, T, Y or Z. ∎

REMARK. One may provide elementary proofs of Theorem 3.29 for primes not dividing 6, which, as in the classical proof of Theorem 3.26 or in the remark that follows Theorem 3.28, use appropriate multiplication identities. For instance, to prove that $Z_p \equiv Z_1 \pmod{p}$ for primes $p \equiv 1 \pmod 6$, we may use (2.76) with $p = m$ and $n = 1$. Since all binomial coefficients, but the first, are divisible by p, one gets $2^{p-1}Z_p \equiv S_1^0 Z_1^p \equiv Z_1 \pmod{p}$, yielding our congruence.

REMARK. Lemmas 5.20 and 5.27 of Chapter 5 contain congruences that are, at least for all primes not 2 or 3, more potent than those of Theorem 3.29.

3.4. Powers of 2 and 3 in X. Given a sequence X satisfying recursion (1.1) and a prime p, we will say that *powers of p in X are bounded* if there exists an integer $b \geq 1$ such that $\nu_p(X_n) \leq b$, for all $n \in \mathbb{Z}$.

Suppose p is a prime not dividing Q. If p is odd, then, given an arbitrarily large power of p, Theorem 3.8 guarantees that this power will divide some terms of the U sequence. In fact, if $p = 2$ and Q is odd, powers of p in U are also unbounded ([30, Theorem 4.3.2]). The situation for the V sequence is slightly different. All odd primes, not dividing Q, with even rank, will have unbounded powers in V. Indeed, if $p \nmid 2Q$, then, by (2.2), $p \nmid \gcd(U_n, V_n)$. If b is an arbitrary integer ≥ 1, then, by Theorem 3.10, p divides $V_{p^b\rho_V}$. By the identity $U_{2n} = U_n V_n$ and as $p \nmid U_{p^b\rho_V}$, $\nu_2(U_{p^b\rho}) = \nu_2(V_{p^b\rho_V})$. But, by Theorem 3.8, $\nu_2(U_{p^b\rho}) > b$, thereby proving our claim. However, powers of 2 in the V sequence are bounded, that is, when Q is odd and $P(P^2 - 3Q) \neq 0$. This is true in spite of the existence of even V terms. We have already observed the special role of the integer 2 with respect to the V sequence, and hinted at the analogous role the prime 3 plays with respect to the S and the T sequences. In this section, we study the boundedness and/or the distribution of powers of 2 and 3 in our various sequences.

We first state a useful observation. Suppose $X = (X_n)$ is a sequence that satisfies (1.1). Then the terms of $X = (X_n)$ whose indices lie in an arithmetic progression $n_0 + mx$ satisfy the recursion

$$X_{n_0+m(n+2)} = V_m X_{n_0+m(n+1)} - Q^m X_{n_0+mn}, \tag{3.7}$$

where n_0 and m are two fixed integers with $m \geq 1$, and $n \in \mathbb{Z}$.

Given a prime p and two rational numbers x and y, the notation $x \sim_p y$ means that the p-adic valuations $\nu_p(x)$ and $\nu_p(y)$ are the same.

3.4.1. Powers of 2 in V. Here we provide two proofs of the fact that, generally, powers of 2 are bounded in the V sequence. A similar result will be shown for powers of 3 in S and T with two comparable proofs.

THEOREM 3.30. *Let $x^2 - Px + Q$ be in $\mathbb{Z}[x]$ with Q odd. If P is even, then*

$$V_n \sim_2 \begin{cases} 2 & \text{if } n \text{ is even,} \\ P & \text{if } n \text{ is odd,} \end{cases} \qquad (n \in \mathbb{Z}).$$

If P is odd, then, for all n in $\mathbb{Z}$,

$$2 \,|\, V_n \;\Leftrightarrow\; 3 \,|\, n,$$

and $V_{3n} \sim_2 2$ *whenever* $Q \equiv 1 \pmod 4$, *whereas, for* $Q \equiv 3 \pmod 4$, $V_{6n} \sim_2 2$ *and* $V_{6n+3} \sim_2 V_3 \sim_2 P^2 - 3Q$ *with* 4 *dividing* V_3.

Proof 1. We first treat the case of non-negative indices n.

If Q is odd and P is even, then, as $V_0 = 2$ and $V_1 = P$ are even integers, all V terms are even. Thus, if $\nu_2(V_{2n}) = 1$, then $\nu_2(V_{2n+2}) = 1$ as well since $V_{2n+2} = PV_{2n+1} - QV_{2n}$ and $\nu_2(PV_{2n+1}) \geq 2$. Also, if $\nu_2(V_{2n+1}) = \nu_2(P)$, then, as $\nu_2(PV_{2n+2}) > \nu_2(P)$, we get $\nu_2(V_{2n+3}) = \nu_2(P)$. Thus, the result will follow by induction.

So we assume P and Q are both odd. Then looking at $V_n \pmod 2$, we find, using the recursion (1.1), the values $0, 1, 1, 0, 1, 1, \cdots$. Therefore, $2 \mid V_n$ iff $3 \mid n$. Now $V_3 = P(P^2 - 3Q)$. Suppose $Q \equiv 1 \pmod 4$. Then $P^2 - 3Q \equiv 2 \pmod 4$. Thus, $V_3 \sim_2 2$. By (2.10), $V_6 = V_3^2 - 2Q^3 \sim_2 2$. By (3.7) with $X = V$, $n_0 = 0$ and $m = 3$, we have $V_{3n+6} = V_3V_{3n+3} - Q^3V_{3n}$. Thus, if $\nu_2(V_{3n}) = \nu_2(V_{3n+3}) = 1$, then $\nu_2(V_{3n+6}) = \nu_2(V_{3n}) = 1$. As $\nu_2(V_0) = \nu_2(V_3) = 1$, induction yields that $V_{3n} \sim_2 2$, for any $n \geq 0$. Assume $Q \equiv 3 \pmod 4$. Then $4 \mid V_3$. Using again the identity $V_{3n+6} = V_3V_{3n+3} - Q^3V_{3n}$, we find that if $V_{3n} \sim_2 2$, then $V_{3n+6} \sim_2 2$, and if $V_{3n} \sim_2 V_3$, then $V_{3n+6} \sim_2 V_3$, since $2 \mid V_{3n+3}$. Hence, the result follows by induction.

If $n < 0$, then, as $Q^nV_{-n} = V_n$ and Q is odd, we have $V_{-n} \sim_2 V_n$, from which one easily sees that the theorem holds for negative indices. ∎

We give a second proof of Theorem 3.30 in the case where P and Q are both odd, which, unlike the first proof, relies on Proposition 3.11.

Proof 2. Assume P and Q are odd integers. Then $2 \nmid U_2 = P$ and $2 \mid U_3 = P^2 - Q$, so $\rho(2) = 3$. Since $V_0 = 2$ and $V_1 = P$ are coprime, we may apply Proposition 3.11 with $X = V$, $d = 2$ and $n_0 = 0$, and obtain that $2 \mid V_n$ iff $3 \mid n$. If $Q \equiv 1 \pmod 4$, then $4 \mid U_3$. Hence, $\rho(2) = \rho(4) = 3$. Thus, if 4 divided some V_{3n}, $n \in \mathbb{Z}$, then Proposition 3.11 (with $d = 4$) would imply that $4 \mid V_0$, a contradiction. Therefore, $V_{3n} \sim_2 2$, for all $n \in \mathbb{Z}$. If $Q \equiv 3 \pmod 4$, then $V_3 = P(P^2 - 3Q)$ is divisible by 4, but $2^1 \parallel U_3$. Suppose $2^a \parallel V_3$ with a an integer ≥ 2. Then since $U_6 = U_3V_3$, we have $\rho(4) = \rho(2^a) = \rho(2^{a+1}) = 6$. Therefore, by Proposition 3.11, if $4 \mid V_{6n}$ for some n, then $4 \mid V_0$, a contradiction. Thus, $V_{6n} \sim_2 2$. Applying Proposition 3.11 with $d = 2^a$ and $n_0 = 3$ yields $2^a \mid V_{6n+3}$ for all $n \in \mathbb{Z}$. By the same theorem, if 2^{a+1} divided some V_{6n+3}, then 2^{a+1} would divide V_3, since $\rho(2^{a+1}) = 6$. As a result, $2^a \parallel V_{6n+3}$ for all $n \in \mathbb{Z}$. If $V_3 = 0$, then $2^b \mid V_3$ for all integers $b \geq 2$. Hence, $\rho(2^b) = 6$ for any $b \geq 2$, which, by Proposition 3.11, implies that each term V_{6n+3} is divisible by arbitrarily large powers of 2. That is, $V_{6n+3} = 0$. Thus, $V_{6n+3} \sim_2 V_3$ holds in this case as well. ∎

3.4.2. Powers of 2 in G and H. Here the assumption is that $D = -E^2 \neq 0$ and that $2 \nmid Q$. We prove that not only powers of 2 in G and H are bounded, but actually all terms of these two sequences are odd.

THEOREM 3.31. *Let* $x^2 - Px + Q$ *in* $\mathbb{Z}[x]$ *have a non-zero discriminant of the form* $-E^2$ *with* Q *odd. Then all terms in* G *and* H *are odd.*

Proof. Recall that for such recursions P is even. Thus, by Theorem 3.30, for all $n \in \mathbb{Z}$, $\nu_2(V_{2n}) = 1$. From the identity $V_{2n} = 2G_nH_n$, valid for all integers n, we deduce that G_n and H_n are odd. ∎

3.4.3. Powers of 2 and 3 in S, T, Y and Z. It should be noted here that the question of the powers of 3 in the S and T sequences had been addressed in [29, Lemma 3], under the assumption that $\gcd(P, Q) = 1$. But there too, the law of appearance of prime powers in U and the identity (2.60) had been the main ingredients.

Showing that, in general, powers of 3 in S and T are bounded can be done briefly.

THEOREM 3.32. *Suppose $x^2 - Px + Q$ in $\mathbb{Z}[x]$ has a non-zero discriminant of the form $-3F^2$ and Q is not a multiple of 3. Assume U_3 is not zero and 3^a is the exact power of 3 in U_3, then the set of 3-adic valuations of S_n and T_n as n varies over $\mathbb{Z}$ is bounded above by $a - 1$.*

Proof. Note that, as $3 \nmid Q$ and $3 \mid D$, we have $\rho(3) = 3$, by Theorem 3.6. Let us reason by contradiction and assume some term S_n, $n \geq 1$, is divisible by 3^a. As $U_{3n} = 3U_nS_nT_n$, 3^{a+1} divides U_{3n}. By Theorem 3.8, $3\rho(3)$ must divide $3n$. But $\rho(3) \mid n$ says that $3^a \mid U_n$. Therefore, 3^a divides both U_n and S_n, which, as $3 \nmid Q$, contradicts Lemma 3.5. The same argument would show that 3^a cannot divide any T_n with $n \geq 1$. Because $Q^nS_{-n} = T_n$, $Q^nT_{-n} = S_n$ and $S_0 = T_0 = 1$, the claim holds for all integers n. ∎

The upshot, however, is to prove Theorem 3.37, a theorem comparable to Theorem 3.30 in that it states precisely how powers of 3 in the S and T sequences are distributed.

We first prove a few lemmas that will help establish one of the proofs of Theorem 3.37.

LEMMA 3.33. *In any recursion $x^2 - Px + Q$ of discriminant $D = -3F^2$, where 3 does not divide Q, we have that $P \equiv \pm 1 \pmod 3$, $Q \equiv 1 \pmod 3$, $Y_1 \equiv Z_1 \equiv -P \pmod 3$, $V_3 \equiv P \pmod 3$ and $S_3 \equiv T_3 \equiv -P \pmod 3$.*

Proof. Because 3 divides $D = P^2 - 4Q$ and $3 \nmid Q$, 3 cannot divide P. Thus, $P \equiv \pm 1 \pmod 3$. Also, $D \equiv P^2 - Q \equiv 0 \pmod 3$, so that $Q \equiv 1 \pmod 3$. Clearly, $Y_1 \equiv Z_1 \equiv P/2 \equiv -P \pmod 3$. By (2.62), $V_3 = V_1Y_1Z_1$. Thus, $V_3 \equiv P(-P)^2 \equiv P \pmod 3$. Finally, $S_3 = PS_2 - QS_1 = PY_1T_1 - QS_1 \equiv -(T_1 + S_1) \equiv -P \pmod 3$ and $T_3 = PT_2 - QT_1 = PZ_1S_1 - QT_1 \equiv -(S_1 + T_1) \equiv -P \pmod 3$. ∎

LEMMA 3.34. *Suppose $D = -3F^2$, $F \neq 0$, and Q is not divisible by 3. Let λ_n be defined by $S_{1+3n} = \lambda_nS_1$. Then, for all $n \geq 0$, λ_n is an integer. For $n < 0$, λ_n belongs to $\mathbb{Z}/Q^{3n}$. For all n in $\mathbb{Z}$, we have, modulo 3, the congruences*

$$\lambda_n \equiv \begin{cases} 1 & \text{if } n \text{ is even,} \\ -P & \text{if } n \text{ is odd.} \end{cases} \tag{3.8}$$

Proof. Congruence (3.8) holds trivially for $n = 0$. Using (3.7) with $X = S$, $n_0 = 1$ and $m = 3$, yields $S_4 = V_3S_1 - Q^3S_{-2} = V_3S_1 - QT_2 = (V_3 - QZ_1)S_1$, since $T_2 = Z_1S_1$. Therefore, S_1 divides S_4 and $\lambda_1 = V_3 - QZ_1$. By Lemma 3.33, we have $\lambda_1 \equiv -P \pmod 3$. Thus, our congruence holds for $n = 1$. Assume congruence (3.8) holds for two consecutive values n and $n + 1$. Then, by (3.7) again, we have $S_{1+3(n+2)} = V_3S_{1+3(n+1)} - Q^3S_{1+3n} = (V_3\lambda_{n+1} - Q^3\lambda_n)S_1$. Thus, S_1 divides $S_{1+3(n+2)}$ and $\lambda_{n+2} = V_3\lambda_{n+1} - Q^3\lambda_n$. By Lemma 3.33, $\lambda_{n+2} \equiv P\lambda_{n+1} - \lambda_n \pmod 3$. If n is even, then $\lambda_{n+2} \equiv P(-P) - 1 \equiv 1 \pmod 3$, whereas, if n is odd, then $\lambda_{n+2} \equiv P - (-P) \equiv -P \pmod 3$. Hence, the result follows

for $n \geq 0$ by induction. For $n < 0$, the result follows also by induction on observing that $S_{1+3n} = Q^{-3}[V_3 S_{1+3(n+1)} - S_{1+3(n+2)}]$. Note that since $Q \equiv 1 \pmod 3$ the congruence $\lambda_{n+2} \equiv P\lambda_{n+1} - \lambda_n \pmod 3$ holds backwards as well, i.e., $\lambda_n \equiv P\lambda_{n+1} - \lambda_{n+2} \pmod 3$. ∎

LEMMA 3.35. *Suppose $D = -3F^2$, $F \neq 0$, and Q is not divisible by 3. Let μ_n be defined by $S_{2+3n} = \mu_n T_1$. Then, for all $n \geq 0$, μ_n is an integer. For $n < 0$, μ_n is in $\mathbb{Z}/Q^{3n}$. In addition, we have, modulo 3, the congruences*

$$\mu_n \equiv \begin{cases} -P & \text{if } n \text{ is even,} \\ 1 & \text{if } n \text{ is odd.} \end{cases}$$

Proof. One may proceed by induction as in the proof of Lemma 3.34, using (3.7) with $n_0 = 2$ and $m = 3$. The basis of the induction is easily established since $S_2 = Y_1 T_1$ and $S_5 = V_3 S_2 - Q^3 S_{-1} = V_3 S_2 - Q^2 T_1$. By Lemma 3.33, we have $\mu_0 = Y_1 \equiv -P \pmod 3$ and $\mu_1 = V_3 Y_1 - Q^2 \equiv -P^2 - 1 \equiv 1 \pmod 3$. ∎

LEMMA 3.36. *Suppose $D = -3F^2$, $F \neq 0$, and Q is not divisible by 3. Then for all integers n,*

$$S_{3n} \equiv (-P)^n \equiv T_{3n} \pmod 3.$$

Proof. We have $S_0 = 1$ and, by Lemma 3.33, $S_3 \equiv -P \pmod 3$. Using the recursion (3.7) with $n_0 = 0$ and $m = 3$, one finds that $S_{3n} \equiv (-P)^n \pmod 3$, for all $n \geq 0$, by induction. Indeed,

$$\begin{aligned} S_{3(n+2)} &= V_3 S_{3(n+1)} - Q^3 S_{3n} \equiv P S_{3(n+1)} - S_{3n} \quad \text{(by Lemma 3.33)} \\ &\equiv \begin{cases} P(-P) - 1 \equiv 1 \pmod 3 & \text{if } n \text{ is even,} \\ P \cdot 1 - (-P) \equiv -P \pmod 3 & \text{if } n \text{ is odd.} \end{cases} \end{aligned}$$

But since for all $n \in \mathbb{Z}$, we have $S_{3n} \equiv P S_{3(n+1)} - S_{3(n+2)} \pmod 3$, we may run an induction backwards and obtain $S_{3n} \equiv (-P)^n \pmod 3$ for all $n \in \mathbb{Z}$. Now, for $n \in \mathbb{Z}$, $Q^{3n} S_{-3n} = T_{3n}$ so that $T_{3n} \equiv S_{-3n} \equiv (-P)^{-3n} \equiv (-P)^{3n} \pmod 3$, as $P \equiv \pm 1 \pmod 3$ and $Q \equiv 1 \pmod 3$. ∎

THEOREM 3.37. *Let $x^2 - Px + Q$ in $\mathbb{Z}[x]$ have a non-zero discriminant of the form $-3F^2$ and assume that 3 does not divide Q.*

If 3 does not divide $P \pm F$, then no term S_n, or T_n, for n in $\mathbb{Z}$, is divisible by 3.

Suppose 3 divides $P + F$. Then 3 divides S_n if and only if $n \equiv 1 \pmod 3$, and 3 divides T_n if and only if $n \equiv 2 \pmod 3$. Moreover, $S_{1+3k} \sim_3 S_1 \sim_3 T_2 \sim_3 T_{2+3\ell}$ for all k and ℓ in $\mathbb{Z}$.

Suppose 3 divides $P - F$. Then 3 divides S_n if and only if $n \equiv 2 \pmod 3$, and 3 divides T_n if and only if $n \equiv 1 \pmod 3$. In addition, $S_{2+3k} \sim_3 S_2 \sim_3 T_1 \sim_3 T_{1+3\ell}$ for all k and ℓ in $\mathbb{Z}$.

Proof 1. If $P \pm F$ are not multiples of 3, then neither S_1, nor T_1 is divisible by 3. Hence, by Lemmas 3.34–3.36, no term of S is divisible by 3. Since $T_n = Q^n S_{-n}$, the same is true of the terms of T.

If $3 \mid P + F$, then $3 \mid S_1$ and, by Lemma 3.34, $S_{1+3k} \sim_3 S_1$ for all $k \in \mathbb{Z}$. Since $T_2 = S_1 Z_1$ and, by Lemma 3.33, $3 \nmid Z_1$, we have $T_2 \sim_3 S_1$. Hence, it remains to show

that $T_{2+3\ell} \sim_3 S_1$ for all ℓ. Because $3 \nmid Q$ and $Q^n T_{-n} = S_n$ for all $n \in \mathbb{Z}$, we have $T_{-n} \sim_3 S_n$. Since $2 + 3\ell = -(1 + 3k)$ with $k = -1 - \ell$, we find that $T_{2+3\ell} \sim_3 S_{1+3k}$.

Suppose $3 \mid P - F$. Since changing the sign of F exchanges the roles of S and T, we directly deduce the claim of the theorem for that case. ∎

We offer a second proof of Theorem 3.37, which does not use Lemmas 3.34–3.36, but instead, much like the second proof of Theorem 3.30, is mostly based on Proposition 3.11.

Proof 2. Note that $U_1 = 1$, $U_2 = P$ and $U_3 = P^2 - Q$ so that, by Lemma 3.33, $3 \mid U_3$ and thus $\rho(3) = 3$. By Proposition 3.11, $3 \mid X_n$ iff there is an ℓ, $0 \le \ell \le 2$, $3 \mid X_\ell$ and $n \equiv \ell \pmod 3$, where X stands for either S or T. If $P \pm F$ are not multiples of 3, then $3 \nmid X_0 X_1 X_2$ so no term of X is divisible by 3, where, again, X stands for either sequence S or T.

If $3 \mid P + F$, then $3 \mid S_1$. Suppose $S_1 \neq 0$ and $3^a \parallel S_1$, $a \ge 1$. Since $U_3 = 3U_1 S_1 T_1 = 3S_1 T_1$, we have $\rho(3^a) = \rho(3^{a+1}) = 3$. Hence applying Proposition 3.11 with $X = S$, $d = 3^a$ and $n_0 = 1$ yields $3^a \mid S_{1+3k}$ for all $k \in \mathbb{Z}$. Suppose 3^{a+1} divided S_{1+3k} for some k. Then, since $\rho(3^{a+1}) = 3$, applying Proposition 3.11 with $X = S$, $d = 3^{a+1}$ and $n_0 = 1+3k$ would lead to the conclusion that 3^{a+1} divides S_1, which is not true. Hence, $S_{1+3k} \sim_3 S_1$ for all $k \in \mathbb{Z}$. If $S_1 = 0$, then putting $m = k$ and $n = 1$ in (2.80) gives $S_{1+3k} = 0$ for all k. Therefore, it remains true that $S_{1+3k} \sim_3 S_1$. That terms $T_{2+3\ell}$ have the same 3-adic value as S_1 is most easily obtained, as in Proof 1, using $T_n \sim_3 S_{-n}$.

Since changing F into $-F$ interchanges the roles of S and T, we readily obtain the result claimed in the case $3 \mid P - F$, as $P - F = P + (-F)$. ∎

Thus, we have shown that if Q is odd and $V_3 \neq 0$, then powers of 2 in the V sequence are bounded, and that, when $3 \nmid QD$, $\rho(3)$ is even and powers of 3 in V are unbounded. In analogy, we have, for non-zero discriminants of the form $-3F^2$, that, when $3 \nmid Q$ and $S_1 T_1 \neq 0$, powers of 3 in the S and the T sequences are bounded. To complete the analogy, we verify that, if some S or T terms are divisible by 2, then powers of 2 in S and T are unbounded. This is the object of the next theorem.

THEOREM 3.38. *Let $x^2 - Px + Q$ in $\mathbb{Z}[x]$ have a non-zero discriminant of the form $-3F^2$ with Q odd. Let X stand for either the S or the T sequence. Then 2 divides some X terms if and only if P is odd, and, if P is odd, then powers of 2 in X are unbounded.*

Proof. If P is even, then $\rho(2) = 2$. Since $Q = (P/2)^2 + 3(F/2)^2$ is odd, $P/2$ and $F/2$ have distinct parities. Therefore, X_1 is odd. By Proposition 3.11, as $2 \nmid X_0 X_1$, no X term is even. On the other hand, if P is odd, then $\rho(2) = 3$. Say $2^a \parallel U_3$. Then, by Theorem 4.3.2, [30], $2^{a+b} \mid U_{3n}$, where $n = 2^b$ and b is an arbitrary integer ≥ 1. By Theorem 3.7, $2 \nmid U_n$. As $U_{3n} = 3U_n S_n T_n$, we have $2^{a+b} \mid S_n T_n$. By Lemma 3.3, 2 cannot divide both S_n and T_n. Hence, since Q is odd and $Q^n S_{-n} = T_n$, $2^{a+b} \mid X_m$ with either $m = n$ or $m = -n$. ∎

The primes 2 and 3, as seen earlier, play a special role in both the Y and the Z sequences, so we do expect, generally, their powers to be bounded in these two sequences. The next theorem settles this question.

THEOREM 3.39. *Let $x^2 - Px + Q$ in $\mathbb{Z}[x]$ have a non-zero discriminant of the form $-3F^2$ with Q prime to 6. If $U_6 \neq 0$, then powers of 2 and powers of 3 are bounded in the Y and the Z sequences. In fact, no term of the Y or the Z sequences is divisible by 3.*

Proof. By (2.61), $U_6 = 3V_1S_1T_1Y_1Z_1$. Thus, $V_3 = V_1Y_1Z_1$ and S_1T_1 are not zero. Hence, by Theorems 3.30 and 3.37, powers of 2 in V are bounded and powers of 3 in S and T are bounded. Consequently, since $V_{3n} = V_nY_nZ_n$ for all n, powers of 2 in Y and Z have to be bounded. Likewise, since $S_{2n} = T_nY_n$ and $T_{2n} = S_nZ_n$ hold for all n, powers of 3 in both Y and Z must be bounded.

That no Y or Z term is divisible by 3 can be shown in at least three ways. One way is to use the identities $S_{2n} = T_nY_n$ and $T_{2n} = S_nZ_n$ together with Theorem 3.37, which, for example, shows that whenever $3 \mid S_{2n}$ then $3 \mid T_n$ and $\nu_3(T_n) = \nu_3(S_{2n})$. Another is to observe that $Y_0Y_1Y_2 \equiv (-P)(-P^2 - Q) \equiv -P \not\equiv 0 \pmod 3$, by Lemma 3.33. Because $\rho(3) = 3$ and $3 \nmid Q$, we conclude by Proposition 3.11. A third method is to use an induction and the recursion $Y_{6n+6} = V_3Y_{6n+3} - Q^3Y_{3n} \pmod 3$, and, for the last two methods, proceed similarly for the Z sequence. ∎

4. On a Lucasian generalization of a theorem of Wolstenholme

Our congruences will either take place in $\mathbb{Z}$, or in the ring A_p of p-integers. The ring A_p is the localization of $\mathbb{Z}$ at $(\mathbb{Z} \setminus p\mathbb{Z})$ ([11, Ch. 1]). It is the subring of the rationals with p-adic valuation ≥ 0. Thus, if p is a prime and a an integer ≥ 1, x and y are in A_p, then the congruence $x \equiv y \pmod{p^a}$ means that $x - y \in p^a A_p$. Such congruences generalize and are compatible with ordinary modulo p^a congruences in $\mathbb{Z}$, since $p^a A_p \cap \mathbb{Z} = p^a\mathbb{Z}$. In fact, the map $m + p^a\mathbb{Z} \mapsto m + p^a A_p$ for $m \in \mathbb{Z}$ is a ring isomorphism from $\mathbb{Z}/p^a\mathbb{Z}$ onto $A_p/p^a A_p$.

Our theorems will all be conditional on the fact that p has maximal rank $p - \epsilon_p$. This condition is akin to requiring that a prime p has a given integer a as a primitive root. Hooley [10] proved conditionally to some Riemann hypotheses that this set of primes has a positive natural density within the set of primes, that is, if a is neither the square of an integer, nor -1. For many a's this density is close to $3/8$. So we are confident that these theorems apply to a positive proportion of the set of all primes, as long as Q is not the square of an integer. Indeed, by Euler's criterion for Lucas sequences (Theorem 3.12), if Q is a square, then p divides $U_{(p-\epsilon_p)/2}$, so $\rho(p)$ is at most $(p - \epsilon_p)/2$, for all odd primes p not dividing QD.

Throughout this chapter, we assume complete familiarity with the theorems of Section 3.2, which most of the time will be used without mention.

4.1. On former Wolstenholme congruences. Wolstenholme's theorem [31] is a classical result of elementary number theory which states that for any prime $p \geq 5$, the sum

$$\sum_{n=1}^{p-1} \frac{1}{n}$$

is congruent to 0 (mod p^2). Several pages of [9] are devoted to this theorem. The authors of [12] discovered an analogous phenomenon which involves sums of consecutive terms of the type V_n/U_n. Their result may be viewed as a generalization of Wolstenholme's theorem as we will later remark.

In this section and the next two, we present as many as seven new Wolstenholme congruences, in the vein of the result of [12], involving ratios of our special binary recurring sequences. Interestingly in all cases there is a proof that closely follows the proof in [12]. But we will only develop such a proof for the ratios G_n/H_n and the ratios Z_n/S_n. For the ratios U_n/V_n, H_n/G_n, Y_n/T_n, S_n/Z_n and T_n/Y_n, we provide shorter proofs that make the results appear as corollaries of the congruences initially established.

We begin by outlining a simple proof of the classical theorem of Wolstenholme that differs from the one in [9], but resembles the proof used in [12].

Recall that the sum of the squares of the first n natural numbers is equal to $n(n+1)(2n+1)/6$. Therefore the sum $\sum_{k=1}^{p-1} k^2$ is congruent to 0 (mod p) for any prime p at least 5. In particular, the sum of all quadratic residues is zero modulo p for any $p \geq 5$.

Let $w = \sum_{n=1}^{p-1} 1/n$, where p is a prime ≥ 5. Then

$$2w = \sum_{n=1}^{p-1} \left(\frac{1}{n} + \frac{1}{p-n} \right) = p \sum_{n=1}^{p-1} \frac{1}{n(p-n)}.$$

But

$$\sum_{n=1}^{p-1} \frac{1}{n(p-n)} \equiv -\sum_{n=1}^{p-1} \frac{1}{n^2} \equiv -\sum_{n=1}^{p-1} n^2 \equiv 0 \pmod{p},$$

since $p \geq 5$. Hence, $w \equiv 0 \pmod{p^2}$.

Kimball and Webb [12] essentially showed that for any prime p of rank ρ, $\rho = p - \epsilon_p$, $\epsilon_p = \pm 1$, $p > 3$, the sum $\sum_{n=1}^{\rho-1}(V_n/U_n)$ is congruent to 0 (mod p^2). We next reprove their theorem. Actually, we prove, using the same technique, a broader theorem, valid not only for $\epsilon_p = \pm 1$, but also for $\epsilon_p = 0$, and not only on the interval $(0, \rho) \cap \mathbb{N}$, but on any interval $I_k(U)$ of the form $(k\rho, (k+1)\rho) \cap \mathbb{Z}$, $k \in \mathbb{Z}$. The observation that the congruence holds for primes dividing D is a marginal improvement, but to realize that it holds on any $I_k(U)$ will prove to be crucial in deriving concise proofs for other Wolstenholme congruences. Also we point out that it is not necessary to differentiate the case $D = 0$ from the case $D \neq 0$ in proving the theorem, as was done in [12]. The identities below and the ensuing theorem hold in particular for $D = 0$.

We restate here some of the classical identities mentioned in Section 2.1. They hold for all integers m and n:

$$2U_{m+n} = U_m V_n + U_n V_m, \tag{4.1}$$

$$2V_{m+n} = V_m V_n + D U_m U_n, \tag{4.2}$$

$$V_n^2 - D U_n^2 = 4Q^n. \tag{4.3}$$

It is easy to deduce from (4.1) and the relations $Q^n V_{-n} = V_n$, $Q^n U_{-n} = -U_n$ that

$$2Q^n U_{m-n} = U_m V_n - U_n V_m. \tag{4.4}$$

Let p be a prime not a factor of $2Q$ of rank ρ. By (4.4) the ratios V_n/U_n are pairwise incongruent modulo p, for $n = 1 + k\rho, 2 + k\rho, \ldots, \rho - 1 + k\rho$, k a fixed integer. Also if n is not a multiple of ρ, then from (4.3) we see that the square of the ratio V_n/U_n is well-defined and not congruent to D (mod p).

THEOREM 4.1. *Let p be a prime at least 5 which is not a factor of Q. Assume the rank ρ of p is maximal, i.e., $\rho = p - \epsilon_p$. Then*

$$w_k(V, U) := \sum_{n \in I_k(U)} \frac{V_n}{U_n} \equiv 0 \pmod{p^2},$$

where $I_k(U)$ is the interval $\big(k\rho, (k+1)\rho\big) \cap \mathbb{Z}$, and k is an integer.

Proof. All sums appearing in the proof are taken over the interval $I_k(U)$, and thus contain precisely $\rho - 1$ terms. Denoting $(2k+1)\rho$ by a, we have by (4.1)

$$2w_k(V,U) = \sum\left(\frac{V_n}{U_n} + \frac{V_{a-n}}{U_{a-n}}\right) = 2\sum \frac{U_a}{U_n U_{a-n}},$$

so that to prove that $w_k(V,U)$ is divisible by p^2 it suffices to show that

$$w_1' = 2\sum \frac{V_a}{U_n U_{a-n}}$$

is divisible by p. Now, by (4.2), w_1' is equal to

$$\sum \frac{V_n V_{a-n}}{U_n U_{a-n}} + D(\rho - 1).$$

But

$$\sum \frac{V_n V_{a-n}}{U_n U_{a-n}} = \sum \frac{U_n U_{a-n} V_n V_{a-n}}{(U_n U_{a-n})^2} = \frac{1}{2}\sum \frac{(U_n V_{a-n} + U_{a-n} V_n)^2}{(U_n U_{a-n})^2} - \sum\left(\frac{V_n}{U_n}\right)^2.$$

In the above final expression, the numerators of the terms in the first sum are all equal to $4U_a^2$ by (4.1). Since p divides U_a, we find that p divides w_1' if and only if p divides

$$w_1^* = D(\rho - 1) - \sum\left(\frac{V_n}{U_n}\right)^2.$$

If ρ is $p+1$, then the sum $\sum (V_n/U_n)^2$ contains all quadratic residues modulo p, where 0 occurs once and non-zero quadratic residues occur twice. Indeed, by Theorems 3.9 and 3.10, for $n \in I_k(U)$, V_n/U_n is 0 (mod p) iff $n = \rho_V + k\rho$, where $\rho_V = (p+1)/2$. Thus, the sum $\sum (V_n/U_n)^2$ is 0 (mod p). If ρ is p, then the sum $\sum (V_n/U_n)^2$ contains all non-zero quadratic residues twice and p divides D so that p divides w_1^*. If ρ is $p-1$, then the sum $\sum (V_n/U_n)^2$ contains once 0 and twice every non-zero quadratic residue modulo p, but D, so this sum is $-2D$ (mod p). Hence $w_1^* \equiv D(\rho-1) + 2D \equiv 0 \pmod{p}$. ∎

Theorem 4.1 was further generalized [4] to all positive integers, not just primes, that have, in some generalized sense, a maximal rank.

Remark 4.2. Note that given $e \geq 0$, there is a k such that $w_k(U,V)$ is divisible by p^{e+2}. It is enough to choose k such that $2k+1$ equals p^e for then p^{e+1} divides U_a and, by the proof of Theorem 4.1, p^{e+2} divides $w_k(U,V)$.

Remark 4.3. The classical Wolstenholme congruence may be derived from Theorem 4.1. Choose the U and the V Lucas sequences associated with $f(x) = (x-1)^2$. Then we have $U_n = n$ and $V_n = 2$ for all n. Each prime p has maximal rank p. Thus, if $p \geq 5$, then $\sum_{n=1}^{p-1} 1/n = (1/2)\sum_{n=1}^{p-1} V_n/U_n \equiv 0 \pmod{p^2}$, by Theorem 4.1.

There is a 'conjugate' result to Theorem 4.1 that has not been observed yet, but which it is natural to think of once one has read the next two sections. The inverse quotients U_n/V_n do satisfy a similar Wolstenholme congruence for a prime p of maximal rank, provided the summation is made over a full interval of indices n, where p does not divide any V_n.

We make a theorem of this claim.

THEOREM 4.4. *Let p be a prime at least 5 which is not a factor of QD. Assume the rank ρ of p is maximal, i.e., $\rho = p - \epsilon_p$. Let k be an arbitrary integer and $I_k(V)$ be the interval $\big(\rho_V + (k-1)\rho, \rho_V + k\rho\big) \cap \mathbb{Z}$. Define $w_k(U,V)$ as the sum $\sum_{n\in I_k(V)}(U_n/V_n)$. Then*

$$D\, w_k(U,V) \equiv w_\ell(V,U) \equiv 0 \pmod{p^2},$$

where $\ell = k - (p+1)/2$.

Proof. Recall that $I_\ell(U) = \big(\ell\rho, (\ell+1)\rho\big)$. Note that ρ being even, ρ_V exists and is $\rho/2$. It is straightforward to check that $n + p\rho_V$ is in $I_k(V)$ if and only if n is in $I_\ell(U)$. Hence

$$w_k(U,V) = \sum_{n\in I_\ell(U)} \frac{U_{n+p\rho_V}}{V_{n+p\rho_V}}.$$

Thus, using both addition identities (4.1) and (4.2), we have

$$w_k(U,V) = \sum_{n\in I_\ell(U)} \frac{U_nV_{p\rho_V} + U_{p\rho_V}V_n}{V_nV_{p\rho_V} + DU_nU_{p\rho_V}}.$$

By Theorem 3.8, the law of appearance for prime powers, p^2 divides $U_{p\rho}$. Now $U_{p\rho} = U_{p\rho_V}V_{p\rho_V}$. Since $p \nmid U_{p\rho_V}$, $p^2 \mid V_{p\rho_V}$. Hence

$$w_k(U,V) \equiv \sum_{n\in I_\ell(U)} \frac{U_{p\rho_V}V_n}{DU_{p\rho_V}U_n} = \frac{1}{D} w_\ell(V,U) \pmod{p^2},$$

which, by Theorem 4.1, is 0 (mod p^2). ∎

We briefly outline a proof of Theorem 4.4 that follows the template seen in Theorem 4.1.

This proof uses the same basic identities used in proving Theorem 4.1, in the same order and with the same manipulations. Using identity (4.1), we deduce that twice $w_k(U,V)$ is the sum over all $n \in I_k(V)$ of the terms $2U_{2k\rho}/(V_nV_{2k\rho-n})$. Since p divides $U_{2k\rho}$ and does not divide $V_{2k\rho}$, it is sufficient to prove that the previous sum, with $U_{2k\rho}$ replaced by $V_{2k\rho}$, is 0 (mod p). One expands this sum using identity (4.2) to get $\rho - 1$ plus D times a secondary sum, which is shown to be equal modulo p to $-\sum(U_n/V_n)^2$. By identity (4.3), $(U_n/V_n)^2 \not\equiv 1/D \pmod{p}$ and one concludes that $\rho - 1 - D\sum_{n\in I_k(V)}(U_n/V_n)^2$ is divisible by p both for $\epsilon_p = \pm 1$, noting again by identity (4.4) that the ratios U_n/V_n are all distinct modulo p when n runs through $I_k(V)$.

REMARK 4.5. Note that for $k = 0$ the result of Theorem 4.4 is trivial since $w_0(U,V)$ is zero, so any power of p divides $w_0(U,V)$. Indeed, $I_0(V)$ is symmetric about 0 and $U_{-n}/V_{-n} = (Q^nU_{-n})/(Q^nV_{-n}) = -U_n/V_n$. But, note that no matter how large the natural number e may be, there is a non-zero k such that $w_k(U,V)$ is divisible by p^{e+2}. Indeed, if k is a multiple of p^e then p^{e+1} divides $U_{2k\rho}$ and, by the above outlined second proof of Theorem 4.4, p^{e+2} divides $w_k(U,V)$.

4.2. A Wolstenholme congruence for ratios G_n/H_n. Surprisingly, sums of consecutive quotients G_n/H_n over appropriate intervals of length $\rho - 1$, where p is a prime of maximal rank ρ, also satisfy a Wolstenholme congruence. The proof we will provide of this fact closely mimics the proof of Theorem 4.1.

Instead of the three identities (4.1), (4.2) and (4.3) we use the three corresponding identities, also valid for all integers m and n,

$$V_{m+n} = G_m H_n + H_m G_n, \tag{4.5}$$

$$EU_{m+n} = G_m G_n - H_m H_n, \tag{4.6}$$

$$H_n^2 + G_n^2 = 2Q^n. \tag{4.7}$$

Let p be a prime not a factor of $2QE$ of rank ρ. Replacing n by $-n$ in (4.6) and using the relations $Q^n G_{-n} = H_n$ and $Q^n H_{-n} = G_n$, we get

$$EQ^n U_{m-n} = G_m H_n - G_n H_m, \tag{4.8}$$

so that the ratios G_n/H_n are pairwise incongruent modulo p for n belonging to an interval of the type $\big(\rho_H + (k-1)\rho, \rho_H + k\rho\big) \cap \mathbb{Z}$, k a fixed integer. Also for n not congruent to ρ_H modulo ρ, we find, by (4.7), that the square of G_n/H_n is well-defined and not congruent to $-1 \pmod p$. Note that in the theorem below the case $\epsilon_p = 0$ does not occur since we need p to not divide E.

THEOREM 4.6. *Let p be a prime at least 5 which is not a factor of QE. Assume the rank ρ of p is maximal, i.e., $\rho = p - \epsilon_p$. Let k be an integer and $I_k(H)$ be the interval of consecutive integers $\big(\rho_H + (k-1)\rho, \rho_H + k\rho\big) \cap \mathbb{Z}$. Then*

$$w_k(G,H) := \sum_{n \in I_k(H)} \frac{G_n}{H_n} \equiv 0 \pmod{p^2}.$$

Proof. First note that 4 divides $\rho = p - \epsilon_p$ for any such prime p, so that ρ_H and $I_k(H)$ are well-defined. All sums being over all $\rho - 1$ indices n in $I_k(H)$, we do not indicate intervals of summation. For the sake of concision, we set $b = 2\rho_H + (2k-1)\rho$. By (4.5) we have

$$2w_k(G,H) = \sum \left(\frac{G_n}{H_n} + \frac{G_{b-n}}{H_{b-n}} \right) = 2 \sum \frac{V_b}{H_n H_{b-n}}.$$

Since $2\rho_H$ is either equal to ρ_V, or to $3\rho_V = \rho_V + \rho$, the index $b = 2\rho_H + (2k-1)\rho$ is of the form $\rho_V + \ell\rho$, ℓ an integer, so that p divides V_b. Hence, to prove that $w_k(G,H)$ is divisible by p^2 it suffices to show that

$$w_2' = \sum \frac{EU_b}{H_n H_{b-n}}$$

is divisible by p. Now, by (4.6), w_2' is equal to

$$\sum \frac{G_n G_{b-n}}{H_n H_{b-n}} - (\rho - 1).$$

But

$$\sum \frac{G_n G_{b-n}}{H_n H_{b-n}} = \frac{1}{2} \sum \frac{(G_n H_{b-n} + G_{b-n} H_n)^2}{(H_n H_{b-n})^2} - \sum \left(\frac{G_n}{H_n} \right)^2.$$

The numerators of the terms in the first sum of the right-hand side of the above equation being all equal to V_b^2, which is divisible by p^2, we deduce that p divides w_2' if and only if p divides

$$w_2^* = \sum \left(\frac{G_n}{H_n} \right)^2 + (\rho - 1).$$

If ρ is $p+1$, then the ratios G_n/H_n appearing in the sum $\sum(G_n/H_n)^2$ being all distinct modulo p, we find that $\sum(G_n/H_n)^2$ is congruent to $\sum_{j=0}^{p-1} j^2$, which is 0 (mod p) since $p>3$. Hence p divides w_2^*. If ρ is $p-1$, then the sum $\sum(G_n/H_n)^2$ contains $p-2$ terms, which (mod p) are 0 and twice each of the $(p-3)/2$ non-zero quadratic residues, except -1 (by 4.7), so this sum is 2 (mod p). Hence $w_2^* \equiv 2+(\rho-1) \equiv 0 \pmod{p}$. ∎

THEOREM 4.7. *Let p be a prime at least 5 which is not a factor of QE. Assume the rank ρ of p is maximal, i.e., $\rho = p-\epsilon_p$. Let k be an integer and $I_k(G)$ be the interval $\big(\rho_G+(k-1)\rho, \rho_G+k\rho\big)\cap\mathbb{Z}$. Then*

$$w_k(H,G) := \sum_{n\in I_k(G)} \frac{H_n}{G_n} = w_{-k}(G,H) \equiv 0 \pmod{p^2}.$$

Proof. When n runs through $I_k(G)$, then $-n$ runs through $\big(-\rho_G-k\rho, -\rho_G-(k-1)\rho\big)\cap\mathbb{Z}$, which, since $\rho_G+\rho_H=\rho$, is $\big(\rho_H-(k+1)\rho, \rho_H-k\rho\big)\cap\mathbb{Z}$. That is, $-n$ runs through $I_{-k}(H)$.

But since $Q^n H_{-n} = G_n$ and $Q^n G_{-n} = H_n$, we have

$$w_k(H,G) = \sum_{n\in I_{-k}(H)} \frac{H_{-n}}{G_{-n}} = \sum_{n\in I_{-k}(H)} \frac{G_n}{H_n} = w_{-k}(G,H),$$

which is congruent to 0 (mod p^2) by Theorem 4.6. ∎

4.3. Wolstenholme congruences when $D=-3F^2$. For such discriminants, besides the quotients V_n/U_n and U_n/V_n, the quotients Z_n/S_n, Y_n/T_n, S_n/Z_n and T_n/Y_n, for primes of maximal rank, all satisfy some Wolstenholme congruences. For quotients Z_n/S_n, we chose again a proof that follows the template of Theorems 4.1 and 4.6, whereas for other quotients we chose instead to deduce in sequence the congruences starting from the theorem involving the ratios Z_n/S_n. That is, we follow the path indicated below:

$$\frac{Z_n}{S_n} \to \frac{Y_n}{T_n} \to \frac{S_n}{Z_n} \to \frac{T_n}{Y_n}.$$

Thus, let us start with the quotients Z_n/S_n. We consider the four identities, valid for all integral values of m and n,

$$2Q^n F U_{m-n} = S_m Z_n - S_n Z_m, \tag{4.9}$$

$$2T_{m+n} = S_m Z_n + S_n Z_m, \tag{4.10}$$

$$2Y_{m+n} = -Z_m Z_n + 3S_m S_n, \tag{4.11}$$

$$Z_n^2 + 3S_n^2 = 4Q^n. \tag{4.12}$$

Let p be a prime not a factor of $2QF$ of rank ρ. By identity (4.9), if $m \not\equiv n \pmod{\rho}$ and p does not divide $S_m S_n$, then the ratios Z_m/S_m and Z_n/S_n are well-defined modulo p and not congruent to each other modulo p. In particular, the ratios Z_n/S_n are pairwise incongruent modulo p for n belonging to an interval of the type $\big(\rho_S+(k-1)\rho, \rho_S+k\rho\big)\cap\mathbb{Z}$, k a fixed integer. Also for n not congruent to ρ_S modulo ρ, we conclude, by (4.12), that the square of Z_n/S_n is well-defined and not congruent to -3 (mod p).

THEOREM 4.8. *Let p be a prime at least 5 which is not a factor of QF. Assume the rank ρ of p is maximal, i.e., $\rho = p-\epsilon_p$. Let k be an integer and $I_k(S)$ be the interval*

$(\rho_S + (k-1)\rho, \rho_S + k\rho) \cap \mathbb{Z}$. *Then*

$$w_k(Z,S) := \sum_{n \in I_k(S)} \frac{Z_n}{S_n} \equiv 0 \pmod{p^2}.$$

Proof. First note that 3 divides $\rho = p - \epsilon_p$ for any such prime p, so that ρ_S and $I_k(S)$ are well-defined. All sums being over all $\rho - 1$ indices n in $I_k(S)$, we do not indicate intervals of summation. For the sake of concision, we set $c = 2\rho_S + (2k-1)\rho$. By (4.10) we have

$$2w_k(Z,S) = \sum \left(\frac{Z_n}{S_n} + \frac{Z_{c-n}}{S_{c-n}} \right) = 2 \sum \frac{T_c}{S_n S_{c-n}}.$$

Since $2\rho_S$ is either equal to ρ_T, or equal to $4\rho_T$ $(= \rho_T + \rho)$, the index $c = 2\rho_S + (2k-1)\rho$ is of the form $\rho_T + \ell\rho$, ℓ an integer, so that p divides T_c. By (2.53), $p \nmid Y_c$. Hence, showing that $w_k(Z,S)$ is divisible by p^2 amounts to showing that

$$w_3' = \sum \frac{2Y_c}{S_n S_{c-n}}$$

is divisible by p. Now, by (4.11), w_3' is equal to

$$-\sum \frac{Z_n Z_{c-n}}{S_n S_{c-n}} + 3(\rho - 1).$$

But

$$\sum \frac{Z_n Z_{c-n}}{S_n S_{c-n}} = \frac{1}{2} \sum \frac{(Z_n S_{c-n} + Z_{c-n} S_n)^2}{(S_n S_{c-n})^2} - \sum \left(\frac{Z_n}{S_n} \right)^2.$$

Since $(Z_n S_{c-n} + Z_{c-n} S_n)^2$ is $4T_c^2$, the first sum of the right-hand side of the above equation is 0 (mod p^2), and so p divides w_3' if and only if p divides

$$w_3^* = \sum \left(\frac{Z_n}{S_n} \right)^2 + 3(\rho - 1).$$

If ρ is $p+1$, then the ratios Z_n/S_n appearing in the sum $\sum (Z_n/S_n)^2$ being all distinct modulo p, we find that $\sum (Z_n/S_n)^2$ is congruent to $\sum_{j=0}^{p-1} j^2$, which is 0 (mod p) since $p > 3$. Hence p divides w_3^*. If ρ is $p-1$, then the sum $\sum (Z_n/S_n)^2$ contains $p-2$ terms, which modulo p are 0 and twice each of the $(p-3)/2$ non-zero quadratic residues, except -3 (by 4.12), so this sum is 6 (mod p). Hence $w_3^* \equiv 6 + 3(\rho - 1) \equiv 0 \pmod{p}$. ∎

THEOREM 4.9. *Let p be a prime not a factor of $6QF$. Assume the rank ρ of p is maximal, i.e., $\rho = p - \epsilon_p$. Let k be an integer and $I_k(T) := (\rho_T + (k-1)\rho, \rho_T + k\rho) \cap \mathbb{Z}$. Then*

$$w_k(Y,T) := \sum_{n \in I_k(T)} \frac{Y_n}{T_n} = w_{-k}(Z,S) \equiv 0 \pmod{p^2}.$$

Proof. As n runs through $I_k(T)$, $-n$ runs through $(-\rho_T - k\rho, -\rho_T - (k-1)\rho) \cap \mathbb{Z}$ and vice versa. But, since $\rho_T + \rho_S = \rho$, this last interval is $\big(\rho_S - (k+1)\rho, \rho_S - k\rho\big) \cap \mathbb{Z}$, which, using the notation of Theorem 4.8, is $I_{-k}(S)$.

Having in mind that $Q^n Y_{-n} = Z_n$ and $Q^n T_{-n} = S_n$, we find that

$$w_k(Y,T) = \sum_{n \in I_{-k}(S)} \frac{Y_{-n}}{T_{-n}} = \sum_{n \in I_{-k}(S)} \frac{Z_n}{S_n} = w_{-k}(Z,S),$$

which is congruent to 0 (mod p^2) by Theorem 4.8. ∎

For ratios S_n/Z_n, our proof will use the same technique used in Theorem 4.4, which enabled us to deduce the Wolstenholme congruences for ratios U_n/V_n from those involving the ratios V_n/U_n. First note that by replacing m and n respectively by $-m$ and $-n$ and using formulas (2.46), we can transform identities (4.10) and (4.11) into

$$2S_{m+n} = T_mY_n + T_nY_m, \tag{4.13}$$

$$2Z_{m+n} = -Y_mY_n + 3T_mT_n. \tag{4.14}$$

Let us state our result.

THEOREM 4.10. *Let p be a prime not dividing $6QF$. Assume the rank ρ of p is maximal, i.e., $\rho = p - \epsilon_p$. Let k be an arbitrary integer and $I_k(Z) := (\rho_Z + (k-1)\rho, \rho_Z + k\rho) \cap \mathbb{Z}$. Define $w_k(S,Z)$ as the sum $\sum_{n\in I_k(Z)}(S_n/Z_n)$. Then there is an integer ℓ such that*

$$3w_k(S,Z) \equiv w_\ell(Y,T) \pmod{p^3}. \tag{4.15}$$

Thus, $w_k(S,Z)$ is congruent to 0 (mod p^2).

Proof. Put $m = p^2\rho_Y$. Since p^2 is 1 (mod ρ), m is congruent to ρ_Y (mod ρ). Hence, by Theorem 3.23, Y_m is divisible by p, and, by lemma 3.21, $\nu_p(U_{6m}) = \nu_p(Y_m)$. But p^3 divides $U_{6p^2\rho_Y}$ so that p^3 also divides $Y_{p^2\rho_Y}$. Now $n + p^2\rho_Y \in I_k(Z)$ if and only if n belongs to the interval $\big(\rho_1 + (k-1)\rho, \rho_1 + k\rho\big)$ with $\rho_1 = \rho_Z - p^2\rho_Y$. Since $p^2 \equiv 1$ (mod ρ), $\rho_1 \equiv \rho_Z - \rho_Y$ (mod ρ). By Corollary 3.24, either ρ_Z is $\rho/6$ and ρ_T is $\rho/3$, in which case $\rho_1 \equiv \rho_Z - \rho_Y = -4\rho/6 = -\rho + \rho_T \equiv \rho_T$ (mod ρ), or ρ_Z is $5\rho/6$ and ρ_T is $2\rho/3$, and again $\rho_1 \equiv \rho_Z - \rho_Y = 4\rho/6 = \rho_T$ (mod ρ). Thus, there is an integer ℓ such that $n + p^2\rho_Y \in I_k(Z)$ if and only if n belongs to $I_\ell(T)$. Hence $w_k(S,Z)$ is equal to

$$\sum_{n\in I_\ell(T)} \frac{S_{n+p^2\rho_Y}}{Z_{n+p^2\rho_Y}},$$

which by identities (4.13) and (4.14) is also equal to

$$\sum_{n\in I_\ell(T)} \frac{Y_nT_{p^2\rho_Y} + Y_{p^2\rho_Y}T_n}{-Y_nY_{p^2\rho_Y} + 3T_nT_{p^2\rho_Y}}.$$

Now since $p^3 \mid Y_{p^2\rho_Y}$ and $p \nmid T_{p^2\rho_Y}$, the foregoing sum is congruent to

$$\frac{1}{3}\sum_{n\in I_\ell(T)} \frac{Y_n}{T_n} = \frac{1}{3}w_\ell(Y,T) \pmod{p^3}.$$

By Theorem 4.9, $w_\ell(Y,T)$ is 0 (mod p^2), so that $w_k(S,Z)$ is 0 (mod p^2). ∎

REMARK 4.11. We opted to prove congruence (4.15) with the modulus p^3. In fact, for any prime power p^e, $e \geq 2$ and any integer k, there is an integer ℓ for which the same congruence holds, albeit modulo p^e. Use $m = p^{e-1}\rho_Y$ for odd e, and $m = \epsilon_p p^{e-1}\rho_Y$ for even e, instead of $m = p^2\rho_Y$ in the proof of the theorem. Thus, we could have used $m = \epsilon_p p\rho_Y$ to obtain our Wolstenholme congruence modulo p^2. Indeed, for any prime p satisfying the hypotheses of the theorem, $\epsilon_p p$ is 1 (mod 6), so that, for even e, $m = \epsilon_p p^{e-1}\rho_Y \equiv p^{e-2}\rho_Y \equiv \rho_Y$ (mod ρ).

A now standard argument yields our last set of congruences.

THEOREM 4.12. *Let p be a prime not dividing $6QF$. Assume the rank ρ of p is maximal, i.e., $\rho = p - \epsilon_p$. Let k be an integer and $I_k(Y) := (\rho_Y + (k-1)\rho, \rho_Y + k\rho) \cap \mathbb{Z}$. Then*

$$w_k(T,Y) := \sum_{n \in I_k(Y)} \frac{T_n}{Y_n} = w_{-k}(S,Z) \equiv 0 \pmod{p^2}.$$

Proof. The two intervals $I_k(Y)$ and $I_{-k}(Z)$ are symmetric of each other about 0, since $-\rho_Y - k\rho = (\rho - \rho_Y) - (k+1)\rho = \rho_Z - (k+1)\rho$, i.e., minus the upper bound of $I_k(Y)$ is the lower bound of $I_{-k}(Z)$. Therefore, since $Q^n T_{-n}$ is S_n and $Q^n Y_{-n}$ is Z_n, we have

$$w_k(T,Y) = \sum_{-n \in I_k(Y)} \frac{T_{-n}}{Y_{-n}} = \sum_{n \in I_{-k}(Z)} \frac{S_n}{Z_n} = w_{-k}(S,Z),$$

which is congruent to 0 (mod p^2) by Theorem 4.10. ∎

4.4. Concluding comments, results and applications. We introduce for the sake of the upcoming discussion the set of pairs of sequences $\mathcal{W} := \{(V,U), (U,V), (G,H), (H,G), (Z,S), (Y,T), (S,Z), (T,Y)\}$. For each such pair, we have proved congruences of the Wolstenholme type. In addition, Theorems 4.4, 4.6–4.10 and 4.12 may all be established with proofs very similar to that of the Theorem of [12], or Theorem 4.1 of the present paper, but is it true that all sums $w_k(x,y)$, for any $k \in \mathbb{Z}$ and any $(x,y) \in \mathcal{W}$, are each simply related to a sum of the type $w_\ell(V,U) \pmod{p^2}$? That is, do the $p - \epsilon_p - 1$ terms they contain yield 0 (mod p^2) in essentially the same manner as the terms of a sum $w_\ell(V,U)$, for some integer ℓ?

The proof of Theorem 4.4 shows that the nth term ($n = 1, \ldots, \rho - 1$) of the sum $w_k(U,V)$ is equal modulo p^2 to $1/D$ times the nth term of the sum $w_\ell(V,U)$, where ℓ is $k - (p+1)/2$. The proof of Theorem 4.7 shows that the terms of $w_k(G,H)$ are the same rational terms as those of the sum $w_{-k}(H,G)$. Similarly, the proof of Theorem 4.9 shows that the sums $w_k(Z,S)$ and $w_{-k}(Y,T)$ have identical terms, but so do the sums $w_k(T,Y)$ and $w_{-k}(S,Z)$ by the proof of Theorem 4.12. Also the proof of Theorem 4.10 implies that multiplying by 3 the terms of any sum $w_k(S,Z)$ yields modulo p^2 the terms of a sum $w_\ell(Y,T)$, for an appropriate integer ℓ.

We summarize below with obvious meaning the above observations:

$$\frac{U}{V} \leftrightarrow \frac{1}{D} \times \frac{V}{U}, \quad \frac{G}{H} \leftrightarrow \frac{H}{G}, \quad \frac{Z}{S} \leftrightarrow \frac{Y}{T} \leftrightarrow 3 \times \frac{S}{Z} \quad \text{and} \quad \frac{S}{Z} \leftrightarrow \frac{T}{Y}.$$

Thus, we now ask the natural question of whether it is possible to relate the terms of any sum $w_k(x,y)$, $(x,y) \in \mathcal{W}$, to the terms of a sum $w_\ell(V,U)$. To address this question, all we need is relate the terms of the sums $w_k(S,Z)$ and the sums $w_k(H,G)$, say, to the terms of a sum of type $w_\ell(V,U)$.

Proving two more theorems based on yet other Lucas-like identities and the method of proof of Theorem 4.4 will be useful.

THEOREM 4.13. *Assume D is $-3F^2$, $F \geq 1$. Let p be a prime not dividing $6QF$ with rank ρ equal to $p - \epsilon_p$. For all integers k, the sums $Fw_k(S,Z)$ and $w_{k+\nu}(V,U)$, with $\nu = \epsilon_p \rho_T$, share the same nth term modulo p^2.*

Proof. Note that 3 divides ρ so that ρ_T is well-defined. Clearly $n \in I_{k-\nu}(S)$ if and only if $n + \nu\rho \in I_k(S)$, which, since $\rho_T + \rho_S = \rho$ and $I_k(S) = \big(\rho_S + (k-1)\rho, \rho_S + k\rho\big)$, holds whenever $n + \nu\rho + \rho_T \in I_k(U)$. Note that $p\nu - \rho_T = p\epsilon_p\rho_T - \rho_T = \epsilon_p\rho_T(p - \epsilon_p) = \nu\rho$ so that $p\nu = \nu\rho + \rho_T$.

Thus, as n runs through the interval $I_{k-\nu}(S)$, the ratios $V_{n+p\nu}/U_{n+p\nu}$ run through the terms of the sum $w_k(V, U)$.

By Theorem 3.19, p divides $T_{p\nu}$. In fact, since 3ν is either $\pm\rho$ or $\pm 2\rho$, we see, by Theorem 3.8, that p^2 divides $U_{3\nu p}$. By identity (2.60) and Lemma 3.5, p^2 divides $T_{p\nu}$. Hence, from the two identities,

$$2V_{m+n} = Z_m Y_n + DS_m T_n, \tag{4.16}$$

$$2FU_{m+n} = S_m Y_n - Z_m T_n, \tag{4.17}$$

valid for all integers m and n, we find that the nth term of the sum $w_k(V, U)$, i.e., $V_{n+p\nu}/U_{n+p\nu}$, satisfies

$$\frac{V_{n+p\nu}}{U_{n+p\nu}} = F\frac{Z_n Y_{p\nu} + DS_n T_{p\nu}}{S_n Y_{p\nu} - Z_n T_{p\nu}} \equiv F\frac{Z_n}{S_n} \pmod{p^2},$$

for any $n \in I_{k-\nu}(S)$. This proves the theorem. ∎

Using identities (2.20) and (2.21), one can establish in a similar way the following theorem.

THEOREM 4.14. *Assume D is $-E^2$, $E \geq 1$. Let p be a prime not dividing $6QE$ with rank ρ equal to $p - \epsilon_p$. For any integer k, the sums $Ew_k(H, G)$ and $w_{k+\nu}(V, U)$, where $\nu = \epsilon_p\rho_H$, share the same nth term modulo p^2.*

REMARK 4.15. The proofs of Theorems 4.13 and 4.14 could have served as alternative proofs for showing that the sums $w_k(S, Z)$ and $w_k(H, G)$ are congruent to 0 (mod p^2) for primes of maximal rank, since they readily imply that

$$Fw_k(S, Z) \equiv w_{k+\nu}(V, U) \pmod{p^2}, \quad \text{where } \nu = \epsilon_p\rho_T, \tag{4.18}$$

$$Ew_k(H, G) \equiv w_{k+\nu}(V, U) \pmod{p^2}, \quad \text{where } \nu = \epsilon_p\rho_H. \tag{4.19}$$

The proofs of the two previous theorems show that, indeed, the set of terms of a sum $w_k(S, Z)$ multiplied by F is, modulo p^2, identical to the set of terms of a sum $w_\ell(V, U)$, for an appropriate ℓ, and that the set of terms of a sum $w_k(H, G)$ multiplied by E is, modulo p^2, identical to the set of terms of another sum of type $w_\ell(V, U)$, for some ℓ. Thus, we have another theorem.

THEOREM 4.16. *Let D be either of the form $-E^2$, or $-3F^2$. Let p be a prime not dividing $6QD$ of maximal rank. Given an integer k and a pair $(x, y) \in \mathcal{W}$, there exist an integer ℓ and a rational constant c of p-adic value zero such that the nth term of the sum $w_k(x, y)$ is congruent to c times the nth term of the sum $w_\ell(V, U)$ (mod p^2), for $n = 1, \ldots, \rho - 1$.*

That is, all sums $w_k(x, y)$ are 0 (mod p^2) in essentially the same way, since these sums use the same sets of residues modulo p^2 up to a constant of p-adic value zero. Therefore, all our theorems on Wolstenholme-like congruences may be regarded as variations of the first theorem, Theorem 4.1.

Note that the terms of the sums $w_k(V,U)$, as k varies in $\mathbb{Z}$, can constitute no more than p distinct sets, when these terms are taken modulo p^2. Indeed, for $k = 0, 1, \ldots, p-1$, we have, using (4.1), (4.2) and $p^2 \mid U_{\lambda p\rho}$, λ an integer, and $n = 1, \ldots, \rho - 1$,

$$\frac{V_{(k+\lambda p)\rho+n}}{U_{(k+\lambda p)\rho+n}} \equiv \frac{V_{k\rho+n}}{U_{k\rho+n}} \pmod{p^2}.$$

That is, the nth term in $w_{k+\lambda p}(V,U)$ is equal modulo p^2 to the nth term in the sum $w_k(V,U)$. An example will show that the terms of, say, the sums $w_0(V,U)$ and $w_1(V,U)$ may indeed sum up to 0 (mod p^2) in distinct ways.

Example. Let us choose the characteristic polynomial $x^2 - x - 1$ for which the (U_n) and the (V_n) Lucas sequences are respectively the sequence (F_n) of Fibonacci numbers and the sequence (L_n) of Lucas numbers. For $p = 7$, we have $\rho = 8$. The terms L_n/F_n (mod 49) of the sum $w_0(L,F)$ are $\{1, 3, 2, 35, 12, 39, 6\}$, whereas the terms of $w_1(L,F)$ are $\{8, 45, 16, 7, 26, 32, 13\}$. Note that both sets sum up to 0 (mod 49), both reduce modulo 7 to the set $\{1, 3, 2, 0, 5, 4, 6\}$, and that no integer c (mod 49) exists such that multiplying the first set by c yields the second set.

We pursue this section by providing a general way of constructing sequences that behave, at least modulo the square of a fixed prime, as the sequences G and H, or as the S, T, Y and Z sequences, when the recursion associated with $x^2 - Px + Q$ does not have a discriminant of the required form. Briefly, we do so in the next remark followed by an illustrative example.

Remark 4.17. Suppose the characteristic polynomial $x^2 - Px + Q$ has a discriminant D neither of the form $-E^2$, nor $-3F^2$. Assume p is a prime such that either $\epsilon_p = (-1 \mid p)$, or $\epsilon_p = (-3 \mid p)$. In the first case, there is an integer E such that $D \equiv -E^2 \pmod{p^2}$, while in the second there is an integer F such that $D \equiv -3F^2 \pmod{p^2}$. It follows that, relative to the prime p, there are either G and H sequences, or sequences S, T, Y and Z, which, at least modulo p^2, act as the sequences we have studied. In particular, the Wolstenholme congruences hold.

Example. Let us illustrate the above remark with the recursion $x^2 - x - 1$. Suppose p is $\pm 1 \pmod 5$ and $\rho(p) = p - 1$. If, in addition p is 1 (mod 3), then there is an F such that $D = 5 \equiv -3F^2 \pmod{p^2}$. Indeed, by hypothesis, both 5 and -3 are quadratic residues modulo p. Hence, there is an integer f such that $5 \equiv -3f^2 \pmod p$. Putting $F = f + px$, we solve the congruence $5 \equiv -3F^2 \pmod{p^2}$. This yields $6fx + (5 + 3f^2)/p \equiv 0 \pmod p$, which has a solution since $p \nmid 6f$. For instance, for $p = 19$ where $\rho = 18$, we may choose $F = -31$. Thus, we have $\rho_Z = 3$, $\rho_S = 12$ and $w_0(Z,S) = \sum_{n=-5}^{11}(Z_n/S_n) \equiv 0 \pmod{19^2}$, where $Z_0 = 1$, $Z_1 = 47$, $S_0 = 1$, $S_1 = -15$, and Z and S have characteristic polynomial $x^2 - x - 1$.

Although this chapter fulfilled its duty, that is, by mixing the identities developed in Sections 2.2 and 2.3 with the arithmetic properties of Subsections 3.2.2 and 3.2.3, we were able to show that the pairs (G,H), (S,Z) and (T,Y) are analogues of the pair (U,V), at least with regard to the generalization of the classical congruence of Wolstenholme that Kimball and Webb discovered, it, arguably, raises numerous questions.

For one thing, considering how similar the proofs of our Wolstenholme congruences are from one pair of sequences to another, no doubt, there must be a common approach to proving all the corresponding theorems at once. In retrospect, or at least partly in retrospect, we see a common feature to all eight pairs in $\mathcal{W}$. This observation may well be key to bringing out an explanation of all our cases at once, and, in fact, to yielding other instances of pairs of sequences with similar modulo p^2 congruences. However, as going further in this direction would lead us astray from the theme of this paper, we will be content to state the aforementioned observation.

Observation 4.18. For all eight pairs (X, X^*) in $\mathcal{W}$, up to a constant, the sequences $V \oplus X$ and X^* are equal, where $\oplus$ is the binary operation of the Laxton semigroup associated with the recursion $x^2 - Px + Q$.

Besides reading the paper of Laxton [14], one may also consult [1, p. 15], where a brief description of this semigroup is outlined. In particular, we find there that given two sequences $x = (x_n)_{n\geq 0}$ and $y = (y_n)_{n\geq 0}$ that satisfy recursion (1.1), the sequence $z = x \oplus y$ also satisfies recursion (1.1), and thus is defined by its two initial terms, which are

$$z_0 = x_0y_1 + x_1y_0 - Px_0y_0,$$
$$z_1 = x_1y_1 - Qx_0y_0.$$

Thus, for instance, the two initial terms of $V \oplus G$ are $(P + E) + P - 2P = E$ and $P(P+E)/2-2Q = P(P+E)/2-(P^2+E^2)/2 = E(P-E)/2$, so we see that, up to the constant E, $V \oplus G$ is H. Also, one finds, say, that $V \oplus Z$ is $-3F$ times the sequence S.

5. On the set of indices n such that $n \mid X_n$

5.1. Introduction. In [25], Smyth gave an interesting general description of the set of positive integers n such that n divides X_n, where X is either a U, or a V Lucas sequence. His work was based on many earlier duly quoted observations and papers. But it was worth seeing a clear, nearly graph-theoretic, step by step construction of these sets emerge.

In this chapter, we will try to show that similar descriptions also exist, on the one hand, for the G and H sequences, and, on the other, for the S and T sequences and the Y and Z sequences.

NOTATION. Given a polynomial $x^2 - Px + Q \in \mathbb{Z}[x]$, if X denotes an integral-valued recurring sequence $(X_n)_{n\geq 0}$ satisfying $X_{n+2} = PX_{n+1} - QX_n$, then we define

$$\mathcal{N}_X = \{n \geq 1;\, n \mid X_n\}. \tag{5.1}$$

Although the notion of 'special' primes was used in various lemmas of Section 3.1, we remind ourselves that a prime is said to be *special* if it divides both P and Q. In the following, the integer 1 is considered as a product of special primes.

We restate the two main theorems, Theorems 1 and 12, of [25] that concern the sets $\mathcal{N}_U$ and $\mathcal{N}_V$ in the next two propositions. If X is a U or a V sequence and $n \in \mathcal{N}_X$, then the set of primes p such that np is in $\mathcal{N}_X$ is denoted by $\mathcal{P}_{X,n}$. An integer b in $\mathcal{N}_X$ is said to be *basic*, or X-*basic*, if it has no prime factor p such that b/p belongs to $\mathcal{N}_X$.

PROPOSITION 5.1. *Let $x^2 - Px + Q \in \mathbb{Z}[x]$ be a polynomial of discriminant D. If n divides U_n, then $\mathcal{P}_{U,n}$ is the set of primes that divide DU_n. Suppose n divides V_n. Then $\mathcal{P}_{V,n}$ is the set of odd primes that divide V_n, with the possible inclusion of $p = 2$, if n is a product of special primes and, either P is even, or P and Q are odd and 3 divides n.*

PROPOSITION 5.2. *Let P and Q be integers, $Q \neq 0$, and let $X = X(P, Q)$ be either the U or the V sequence associated with the parameters P and Q. Then every integer in $\mathcal{N}_X$ is equal to a product of the form $bp_1 \cdots p_k$, where b is an X-basic integer, p_i is prime and $bp_1 \cdots p_{i-1}$ belongs to $\mathcal{N}_X$, i.e., p_i is in $\mathcal{P}_{X,bp_1\cdots p_{i-1}}$, for $i = 1, \ldots, k$. The only X-basic elements are*

- 1 *and* 6, *if* $X = U$; 1 *only, if* $X = V$, *whenever* $P \equiv 3 \pmod 6$ *and* $Q \equiv \pm 1 \pmod 6$;
- 1 *and* 12 *for* $X = U$, 1 *and* 6 *for* $X = V$, *whenever* $P \equiv \pm 1 \pmod 6$ *and* $Q \equiv -1 \pmod 6$;
- 1 *only for* X *equal to either* U *or* V, *otherwise.*

We will look for comparable results when $D = -E^2$ and X is equal to G or H, and when $D = -3F^2$ and X is S, T, Y or Z. While the definition (5.1) of the sets $\mathcal{N}_X$ is maintained for the new sequences, the definition of the sets $\mathcal{P}_{X,n}$ will differ from those of X equal to U or V, because it seemed more natural to do so considering that these sequences appear in pairs. Nevertheless, it will be easy to get a description of the sets of primes p such that $np \mid X_{np}$ given that $n \mid X_n$, that is, of the sets $\mathcal{P}_{X,n}$ with their former definition, from our results. Suppose (X, X^*) denotes one of the six pairs (G, H), (H, G), (S, T), (T, S), (Y, Z) or (Z, Y). The definition of $\mathcal{P}_{X,n}$ we will work with is still that of the set of primes p such that $np \mid X_{np}$, but under the assumption that n belongs to $\mathcal{N}_X \cup \mathcal{N}_{X^*}$, rather than $\mathcal{N}_X$ only. We refer to the situation where $n \mid X_n$ and $np \mid X^*_{np}$, or $n \mid X^*_n$ and $np \mid X_{np}$, as the *cross-over* case.

The description of $\mathcal{N}_U$ given in [25] and stated in Propositions 5.1 and 5.2 above hinged on a 'descent' result of Somer ([23], Theorem 5(iv)), namely

LEMMA 5.3. *Let $U = U(P, Q)$ be any U Lucas sequence. Let $m = np$ be a positive integer with largest prime factor p. Suppose m belongs to $\mathcal{N}_U$. Then, unless P is odd and m is of the form $2^\ell \cdot 3$ with $\ell \geq 1$, n belongs to $\mathcal{N}_U$.*

Smyth [25, Proposition 4] completed the result for most remaining cases by establishing

LEMMA 5.4. *Let $U = U(P, Q)$ be any U Lucas sequence with P odd. Assume m is an integer of the form $2^\ell \cdot 3$, $\ell \geq 3$, which belongs to $\mathcal{N}_U$. Then $m/2$ belongs to $\mathcal{N}_U$.*

The description of $\mathcal{N}_V$, restated above, also hinged on another comparable 'descent' result for V sequences that appeared in Somer's paper [24], and which was also completed by Proposition 18 of Smyth's paper [25].

To obtain descriptions of the sets $\mathcal{N}_X$, for X equal to G, H, S, T, Y or Z, we will not establish corresponding 'descent' results for those X, but rather resort to using, in each case, the descent results for the U sequence, i.e., Lemmas 5.3 and 5.4.

Given the importance of Lemmas 5.3 and 5.4 in establishing the main results of this chapter, we will reprove them at the end of this introductory section. Smyth included himself in [25], at the bottom of p. 3, a brief idea as to why Lemma 5.3 actually holds. Our proof will differ and use a slightly modified version of Theorem 2 of [23].

Our intention is not only to show the sequences G, H, etc, behave as the U and V Lucas sequences, but also to establish the corresponding results by arguments that are themselves similar to those used for the U and V sequences. Thus, we restate and reprove some well known results concerning the U and the V sequences simply because similar statements will be made about our sequences, and so analogies will become obvious.

LEMMA 5.5. *Given a positive integer n and an odd prime p, we have*

$$U_n \mid U_{np} \quad \text{and, for } U_n \neq 0, \quad U_{np}/U_n \equiv \epsilon_p U_n^{p-1} \pmod{p}.$$

Proof. It is well known that if $m = kn$, then $U_n \mid U_m$. Indeed, if α is a double root, then, by (1.4), $U_n \neq 0$ and $U_m/U_n = (m\alpha^{m-1})/(n\alpha^{n-1}) = k(\alpha^n)^{k-1} = U_k(2\alpha^n, \alpha^{2n}) = U_k(V_n, Q^n) \in \mathbb{Z}$. Suppose the roots α and β are distinct. If $U_n \neq 0$, then $U_m/U_n =$

$(\alpha^{kn} - \beta^{kn})/(\alpha^n - \beta^n) = U_k(V_n, Q^n) \in \mathbb{Z}$. If $U_n = 0$, then $\alpha^n = \beta^n$, and thus $\alpha^{kn} = \beta^{kn}$. Hence, $U_{kn} = 0$, and it remains true that $U_n \mid U_{kn}$.

Assuming $U_n \neq 0$, we may put $m = p$ and $n = n$ in the multiplication identity (2.13), divide both sides by U_n and reduce modulo p. This yields the congruence of the lemma, since $\epsilon_p \equiv D^{(p-1)/2} \pmod{p}$. ∎

LEMMA 5.6. *Let n be a positive integer. If p is an odd prime, then*

$$V_n \mid V_{np} \quad \textit{and, for } V_n \neq 0, \quad V_{np}/V_n \equiv V_n^{p-1} \pmod{p}.$$

Proof. See [25, Lemma 21(ii)]. ∎

LEMMA 5.7. *If n is a product of special primes, then n divides Q^{n-1}.*

Proof. It suffices to show that, for each prime factor p of n, $p^{\nu_p(n)} \mid p^{n-1}$. But, on the one hand, $p^{n-1} \geq 2^{n-1} \geq n$ implies that $n > \log n/\log p$ and, on the other, $p^{\nu_p(n)} \leq n$ implies that $\nu_p(n) \leq \log n/\log p$. Hence $\nu_p(n) \leq n - 1$. ∎

We will use another small, but handy result, which is a particular case of Theorem 5(i) of [24], and which was reproved in [25] as Corollary 17, namely

LEMMA 5.8. *If $n \geq 1$ is a product of special primes then n divides V_n.*

That Lemma 5.8 holds when n is a square-free product of special primes is straightforward as it is easily seen that each special prime divides all V_k, $k \geq 1$. The case n is not square-free can be readily handled by using Proposition 5.1. That is, a proof by induction using Proposition 5.1 would be the shortest way of proving this lemma. However, Lemma 5.8 was instrumental in the proof of Proposition 5.1 in [25]. So we prefer an induction that does not use Proposition 5.1.

Proof of Lemma 5.8. We run an induction on $k = \Omega(n)$, the number of prime factors of n. The result holds trivially for $k = 0$, since $1 \mid V_1$. Suppose $k = 1$, i.e., n is a special prime p. Since $V_1 = P$, we have $p \mid V_1$. Suppose p is odd. Then, by Lemma 5.6, $V_1 \mid V_p$ so that $p \mid V_p$.

Note that if 2 is special, then since V_0 and V_1 are even, V_n is even for all $n \geq 0$, by recursion (1.1). Thus, if $p = 2$, then $2 \mid V_2$.

Let $k \geq 2$ and assume the inductive hypothesis holds up to $k-1$. Let m be a product of k special primes. If 2 is special and $2 \mid m$, then, writing $m = 2n$, we know by the inductive hypothesis that $n \mid V_n$. Also, we just saw that $2 \mid V_n$, and that $n \mid Q^{n-1}$ by Lemma 5.7. Hence, $V_{2n} = V_n^2 - 2Q^n$ is divisible by $2n$. So assume m is odd and write $m = np$, where p is a prime ≥ 3. By Lemma 5.6, possibly applied several times, we have $V_p \mid V_{np}$ and $V_n \mid V_{np}$. Thus, $n \mid V_{np}$ and $p \mid V_{np}$. Hence, $np \mid V_{np}$, if $p \nmid n$. If $p \mid n$ and $V_n \neq 0$, then, by the congruence in Lemma 5.6, $p \mid V_{np}/V_n$, so that pV_n and, in particular, pn divides V_{np}. If $p \mid n$ and $V_n = 0$, then, as $V_n \mid V_{np}$, $V_{np} = 0$ and np divides trivially V_{np}. ∎

In fact, we state and prove a lemma for the U sequence similar to Lemma 5.8, both to promote comparisons and to serve in proving the descent Lemmas 5.3 and 5.4.

LEMMA 5.9. *If $n \geq 1$ is a product of special primes then n divides U_n.*

Proof. Again we run an induction on $k = \Omega(n)$. The lemma holds for $k = 0$. Suppose p is an odd special prime. Then $p \mid D = P^2 - 4Q$. Hence, $\epsilon_p = 0$ and, for all $n \geq 1$, p divides U_{np}/U_n, by the congruence of Lemma 5.5. Thus, if $n \mid U_n$, then $np \mid U_{np}$. Therefore induction only needs to be checked for powers of 2. Say $m = 2^k$, $k \geq 1$, and put $m = 2n$, where 2 is assumed to be special. Then, by the inductive hypothesis, $n \mid U_n$, and $2 \mid V_n$, by the proof of Lemma 5.8. Hence, since $U_{2n} = U_n V_n$, m divides U_m. ∎

Theorem 2 in [23] states that, given a $U = U(P, Q)$ Lucas sequence and a positive integer n, we have that $n \mid U_n$ iff the rank of each prime divisor of n, not dividing the discriminant D, divides n. Somer points to the fact that this result was proved by Jarden, when U is the Fibonacci sequence, and later by André-Jeannin, when $\gcd(P, Q) = 1$. It appears to be slightly erroneous, as stated, though. For instance, if $U = U(5, 6)$, then $U_n = 3^n - 2^n$. If n is equal to 3^k, $k \geq 1$, then no prime divisor of n has a rank. Hence n satisfies the second statement, but not the first since 3 does not divide any U_m, $m \geq 1$. So we establish a replacement proposition that we will be using to prove both Lemmas 5.3 and 5.4.

We now adopt the convention that if a prime q has no rank, then $\rho(q) = \infty$ (see Definition 1).

PROPOSITION 5.10. *Let $U(P, Q)$ be a U Lucas sequence with parameters P and Q. Let m be an integer ≥ 1. Then $m \mid U_m$ if and only if for any prime divisor q of m which is not a special prime, the rank of q divides m.*

Proof. Suppose $m \mid U_m$. Let q be a non-special prime factor of m. If q divides Q, then q does not divide P. Thus, by recursion (1.1), we have $U_n \equiv P^{n-1} \not\equiv 0 \pmod{q}$ for any $n \geq 1$. This contradicts $q \mid U_m$. Hence, $q \nmid Q$. By Theorem 3.7, $\rho(q) \mid m$.

For the converse, suppose q is a prime factor of m and $q^k \parallel m$. We need to show that $q^k \mid U_m$. If q is special, then, by Lemma 5.9, $q^k \mid U_{q^k}$. Since $U_{q^k} \mid U_m$, we do have $q^k \mid U_m$. If q is non-special, then $q \nmid Q$. Otherwise, as we saw above, $q \nmid U_n$ for any $n \geq 1$, and thus $\rho(q) = \infty$, contradicting the fact that m is an integer. Thus, q has a finite rank. Assume $q^{a_q} \parallel U_{\rho(q)}$. By Theorem 3.6, $\rho(q)$ is either prime to q, if $q \nmid D$, or equal to q, if $q \mid D$. That is, we have $q^k \rho(q) \mid m$, if $q \nmid D$, or $q^{k-1}\rho(q) \mid m$, if $q \mid D$. Hence, by Theorem 3.8, $\nu_q(U_m) \geq k - 1 + a_q \geq k$, if q is odd. If Q is odd and $2^\ell \mid U_n$ for some $\ell \geq 1$, then $2^{\ell+1} \mid U_{2n}$. Indeed, by the identity $V_n^2 - DU_n^2 = 4Q^n$, $2^\ell \mid U_n$ implies $2 \mid V_n$ and, since $U_{2n} = U_n V_n$, $2^{\ell+1} \mid U_{2n}$. Therefore, if $q = 2$, then Q is odd and, from $2^{k-1}\rho(2) \mid m$ and $2 \mid U_{\rho(2)}$, we conclude by induction that $2^k \mid U_m$. ∎

Proposition 5.10 allows a proof of the two 'descent' results, Lemmas 5.3 and 5.4.

Proofs of Lemmas 5.3 and 5.4. Let $U(P, Q)$ be a U Lucas sequence. Consider a composite positive integer m satisfying $m \mid U_m$. We first write $m = np$, where p is the largest prime factor of m, and assume m is not of the form $2^\ell \cdot 3$, $\ell \geq 1$ in case P is odd. We seek to show that $n \mid U_n$ using the criterion of Proposition 5.10. Let q be a non-special prime factor of n. Note that $q \mid U_m$ so that, by the proof of Proposition 5.10, q does not divide Q. Suppose first $q < p$. Then $p \geq 3$. By Theorem 3.6 and because $\rho(2)$ is at most 3, we have $\rho(q) \leq q + 1 \leq p$, with $\rho(q) = p$ iff $q = 2$, $p = 3$ and $\rho(2) = 3$, i.e., iff $q = 2$, $p = 3$ and P is odd, since $U_2 = P$. If $\rho(q) < p$, then $\rho(q) \mid n$. Indeed, $q \mid U_m$ implies that $\rho(q) \mid m = np$,

and so $\rho(q) \mid n$. If, on the contrary, $\rho(q) = p$, i.e., $q = 2$, $p = 3$ and P is odd, then, since m is not of the form $2^\ell \cdot 3$, $\ell \geq 1$, $3^2 \mid m$. Hence, $3 = \rho(q) \mid n$. Suppose now $q = p$. If $\rho(p) = p$, then $\rho(p) \mid n$, since by hypothesis $q = p$ is a factor of n. If $\rho(p) \neq p$, then $\gcd(\rho(p), p) = 1$. But $\rho(p) \mid m = np$, so we get $\rho(p) \mid n$. Hence, by Proposition 5.10, $n \mid U_n$. Thus, Lemma 5.3 is proved.

Suppose P is odd and $m = 2^\ell \cdot 3$, $\ell \geq 3$. Write $m = 2n$. Let q be a non-special prime factor of n. Again $q \nmid Q$, or else $q \nmid P$ and q could not divide U_m. It follows, since q is either 2 or 3, that $\rho(q)$ is 2, 3 or 4. Thus, $\rho(q) \mid n$. Hence, by Proposition 5.10, $n \mid U_n$. So Lemma 5.4 is proved. ∎

5.2. Recursions of discriminant $-E^2$. Given a recursion defined by a characteristic polynomial $x^2 - Px + Q \in \mathbb{Z}[x]$ of discriminant $-E^2$, we study the sets $\mathcal{N}_G$ and $\mathcal{N}_H$ of the associated G and H sequences. We begin with an important result remindful of Lemmas 5.5 and 5.6.

LEMMA 5.11. *Let (X, X^*) stand for one of the two pairs (G, H), or (H, G). Let n be a positive integer and p be a prime. If $p \equiv 1 \pmod 4$, then*

(i) *$X_n \mid X_{np}$ and, if $X_n \neq 0$, $X_{np}/X_n \equiv X_n^{p-1} \pmod p$.*

If $p \equiv -1 \pmod 4$, then

(ii) *$X_n \mid X^*_{np}$ and, if $X_n \neq 0$, $X^*_{np}/X_n \equiv X_n^{p-1} \pmod p$.*

Proof. Suppose for instance that $p = -1 + 4\ell$ and we wish to show that H_n divides G_{np}. Noting that $\zeta_8^p = (-1)^\ell \bar{\zeta}_8$ and $(\bar{\zeta}_8)^p = (-1)^\ell \zeta_8$, we find that

$$G_{np} = \frac{\sqrt{2}}{2}\left[\bar{\zeta}_8 \alpha^{np} + \zeta_8 \bar{\alpha}^{np}\right] = (-1)^\ell \frac{\sqrt{2}}{2}\left[\zeta_8^p \alpha^{np} + (\bar{\zeta}_8)^p \bar{\alpha}^{np}\right] = (-1)^\ell H_n N,$$

where $N = \sum_{k=0}^{p-1} (-1)^k (\zeta_8 \alpha^n)^{p-1-k} (\bar{\zeta}_8 \bar{\alpha}^n)^k$ is a rational integer, since N is an algebraic integer of $\mathbb{Z}[\zeta_8]$ invariant under both complex conjugation and the automorphism that fixes i and sends $\sqrt{2}$ to $-\sqrt{2}$.

The congruences modulo p are obtained by putting $m = p$ in the four identities in (2.32) and (2.33). Staying with the case of G_{np} and $p = -1 + 4\ell$, we use the second identity of (2.33) with $m = p$ and get

$$2^{(p-1)/2}(-1)^\ell G_{np} = H_n \cdot \sum_{k \geq 0} \binom{p}{2k} H_n^{p-2k-1} G_n^{2k}.$$

Dividing through by H_n and reducing the integers on both sides of the resulting equation modulo p gives that $(2 \mid p)(-1)^\ell G_{np}/H_n \equiv H_n^{p-1} \pmod p$. If ℓ is odd, then $p \equiv 3 \pmod 8$ and both the Legendre character $(2 \mid p)$ and $(-1)^\ell$ are -1, whereas if ℓ is even, both are $+1$, yielding our congruence relation. The other cases are obtained through analogous reasoning. ∎

We define for a positive integer n in $\mathcal{N}_G \cup \mathcal{N}_H$ the two sets of primes $\mathcal{P}_{G,n}$ and $\mathcal{P}_{H,n}$ as

$$\mathcal{P}_{G,n} = \{p;\, np \in \mathcal{N}_G\}, \qquad \mathcal{P}_{H,n} = \{p;\, np \in \mathcal{N}_H\}.$$

An integer n in $\mathcal{N}_G \cup \mathcal{N}_H$ will be said to be *basic*, or *GH-basic*, if for any prime factor p of n, n/p is neither in $\mathcal{N}_G$, nor in $\mathcal{N}_H$.

The next theorem that concerns G and H plays the role that Proposition 5.1 played for U and V.

THEOREM 5.12. *Let (X, X^*) represent one of the two pairs of sequences (G, H) or (H, G). Suppose $n \geq 1$ divides X_n. Then for primes $p \equiv 1 \pmod 4$, we have*

- *$p \in \mathcal{P}_{X,n}$ if and only if $p \mid X_n$,*
- *$p \in \mathcal{P}_{X^*,n}$ if and only if $p \mid X_n^*$ and n is a product of special primes.*

For primes $p \equiv -1 \pmod 4$, we have

- *$p \in \mathcal{P}_{X,n}$ if and only if $p \mid X_n^*$ and n is a product of special primes,*
- *$p \in \mathcal{P}_{X^*,n}$ if and only if $p \mid X_n$.*

The prime 2 belongs to $\mathcal{P}_{X,n}$ if and only if $2n$ is a product of special primes, which also occurs if and only if 2 belongs to $\mathcal{P}_{X^*,n}$.

Proof. Assume $p \equiv 1 \pmod 4$. By the congruence in Lemma 5.11(i), if $p \mid X_n$ and $X_n \neq 0$, then pX_n and, a fortiori, np divides X_{np}. If $X_n = 0$, then, as $X_n \mid X_{np}$, $X_{np} = 0$ and, trivially, $np \mid X_{np}$. If $p \nmid X_n$, then $X_n \neq 0$. Thus, by the congruence of Lemma 5.11(i) again, $X_{np} \equiv X_n^p \equiv X_n \pmod p$, so $p \nmid X_{np}$, in particular, $np \nmid X_{np}$. Suppose now $np \mid X_{np}^*$. Since $n \mid X_n$ and $X_n \mid X_{np}$, we have $n \mid \gcd(X_{np}, X_{np}^*)$. Hence, by Lemma 3.2, n has to be a product of special primes. By Lemma 5.8, $n \mid V_n$. But $V_n = X_n + X_n^*$, so that $n \mid X_n^*$. But, by what we just proved, bearing in mind that X and X^* have a dual relationship, as $n \mid X_n^*$, $p \in \mathcal{P}_{X^*,n}$ iff $p \mid X_n^*$. Thus, $p \mid X_n^*$. Conversely, n being a product of special primes, $n \mid V_n$. Since $n \mid X_n$, we have $n \mid X_n^*$. We then use the equivalence $p \in \mathcal{P}_{X^*,n}$ iff $p \mid X_n^*$ in the backwards direction to conclude.

The proof for primes $p \equiv -1 \pmod 4$ is analogous, provided one uses Lemma 5.11(ii), so we turn to $p = 2$.

To fix ideas we assume $n \mid G_n$. The case $n \mid H_n$ can be treated similarly. We first show that $2 \in \mathcal{P}_{H,n}$ iff $2n$ is a product of special primes. Suppose first that $2 \in \mathcal{P}_{H,n}$. By the identity (2.27), we have

$$H_{2n} = -EU_nG_n + Q^n, \tag{5.2}$$

so that $n \mid Q^n$. Thus, every prime factor q of n divides Q. But then, using the recursion $G_{t+2} = PG_{t+1} - QG_t$, we have $G_n \equiv P^{n-1}G_1 \pmod q$. Since $q \mid G_n$, either $q \mid P$ and q is special, or $q \mid G_1$. If q is odd and $q \mid G_1$, then $P \equiv -E \pmod q$. But, since $q \mid Q$ and $4Q = P^2 + E^2 \equiv 2P^2 \pmod q$, $q \mid P$ and q is special. By (5.2), $2 \mid Q$ since $2 \mid H_{2n}$ and $2 \mid E$. Thus, P being an even integer, 2 is special. Hence, $2n$ must indeed be a product of special primes. But that condition also suffices to guarantee that $2 \in \mathcal{P}_{H,n}$. Indeed, by Lemma 5.7, $n \mid Q^{n-1}$. Hence, $2n \mid Q^n$. Also $2n \mid EG_n$. Thus, by (5.2), $2n \mid H_{2n}$.

Note that if $2n$ is a product of special primes, then $2n \mid V_{2n}$, by Lemma 5.8. Since, as we just proved, $2n$ divides H_{2n}, $2n$ also divides G_{2n}, which equals $V_{2n} - H_{2n}$. That is, $2 \in \mathcal{P}_{G,n}$.

Conversely, assume $2 \in \mathcal{P}_{G,n}$. Since $V_{2n} = 2G_nH_n$, $2n$ divides V_{2n}. Thus, $2n \mid H_{2n} = V_{2n} - G_{2n}$. That is, $2 \in \mathcal{P}_{H,n}$, and thus $2n$ is a product of special primes. ∎

At this point it is natural to ask whether, in general, every $n \in \mathcal{N}_G \cup \mathcal{N}_H$ may be constructed by starting from 1 and multiplying successively by primes in the sets $\mathcal{P}_{G,k}$ and $\mathcal{P}_{H,k}$, where $k \mid n$ and $k \in \mathcal{N}_G \cup \mathcal{N}_H$. To reach a conclusion and establish a theorem that completes Theorem 5.12, a few more lemmas are needed.

As seen in the proof of Lemma 5.5, any U Lucas sequence is a divisibility sequence in the sense that for positive integers m and n, we have $U_n \mid U_{mn}$. Any V Lucas sequence is nearly a divisibility sequence. That is, if $2 \nmid m$, then $V_n \mid V_{mn}$. The following lemma shows precisely what divisibility property the sequences G and H obey.

LEMMA 5.13. *If m and n are positive integers and m is odd, then G_nH_n divides $G_{mn}H_{mn}$. In fact, if m has k primes factors congruent to $-1 \pmod 4$, then*

$$\begin{aligned} &G_n \mid G_{mn} \text{ and } H_n \mid H_{mn} \quad \text{if } k \text{ is even,} \\ &G_n \mid H_{mn} \text{ and } H_n \mid G_{mn} \quad \text{if } k \text{ is odd.} \end{aligned}$$

Proof. It suffices to prove the lemma for m equal to a prime $p \equiv \pm 1 \pmod 4$. But, if $m = p$, it is a consequence of Lemma 5.11. ∎

LEMMA 5.14. *Suppose p is a special prime. Then p divides both G_n and H_n for any integer $n \geq 1$.*

Proof. Since p divides both P and Q, the recursion $X_{t+2} = PX_{t+1} - QX_t$ satisfied by both the G and the H sequences implies that $p \mid \gcd(G_n, H_n)$ for all $n \geq 2$. Since $P^2 - 4Q = -E^2$, $p \mid E$. Thus, if p is odd, clearly $p \mid \gcd(G_1, H_1)$. If $p = 2$ then Q is even. But $Q = (P/2)^2 + (E/2)^2$ so $P/2$ and $E/2$ must have the same parity. Therefore, $2 \mid \gcd(G_1, H_1)$. ∎

LEMMA 5.15. *If n is a product of special primes, then n divides both G_n and H_n.*

Proof. As in Lemmas 5.8 and 5.9, we proceed by induction on $k = \Omega(n)$. The result holds trivially for $k = 0$. So assume $k \geq 1$ and assume the inductive hypothesis holds for $k - 1$. Let m be a product of k special primes and write m as np with p prime. By the inductive hypothesis $n \mid \gcd(G_n, H_n)$. By Lemma 5.14, $p \mid \gcd(G_n, H_n)$. Thus, whether p is odd or $p = 2$, Theorem 5.12 says that $p \in \mathcal{P}_{G,n} \cap \mathcal{P}_{H,n}$. That is, $m \mid \gcd(G_m, H_m)$. ∎

LEMMA 5.16. *Assume that 2 is not a special prime, i.e., that Q is odd. Then all terms of the G and the H sequences are odd.*

Proof. Note that, since P is even, 2 is special iff Q is even. Suppose Q is odd. Then the conclusion is given by Theorem 3.31. ∎

We are now ready for our second theorem concerning $\mathcal{N}_G$ and $\mathcal{N}_H$, one which plays the role that Proposition 5.2 plays with respect to U and V.

THEOREM 5.17. *Let $m > 1$ be an integer in $\mathcal{N}_G \cup \mathcal{N}_H$. Then, we may write m as $p_1 \cdots p_k$, where, for each $i = 1, \ldots, k$, p_i is prime and $p_1 \cdots p_i$ belongs to $\mathcal{N}_G \cup \mathcal{N}_H$. In particular, 1 is the only GH-basic element.*

Proof. We assume that $m \mid G_m$ and write $m = np$, where p is the largest prime factor of m. To prove the theorem, it suffices to show that n is in $\mathcal{N}_G \cup \mathcal{N}_H$. Indeed, the case $m \mid H_m$ can be treated analogously.

If $p = 2$, then m is a power of 2, and hence G_m is even. By Lemma 5.16, Q must be even, so that 2 is special. Then n is a product of special primes and, by Lemma 5.15, n divides both G_n and H_n.

So we now assume that $p \geq 3$. By the identity (2.28), we have $U_{4m} = 2U_mV_mG_mH_m$. Hence, if 2 divides $U_mV_mH_m$, then $4m$ divides U_{4m}. But P being even, all terms of the V sequence are even. So $4m \mid U_{4m}$, which, by Lemma 5.3, as P is even, implies that $4n \mid U_{4n}$. That is, $2n \mid U_nV_nG_nH_n$. Let n_s be the largest product of special primes which divides n and write $n = n_s \cdot n_t$.

We claim that $n_s \mid \gcd(G_n, H_n)$. By Lemma 5.15, $n_s \mid \gcd(G_{n_s}, H_{n_s})$. Note that n_t must be odd. Otherwise, G_m is even and, by Lemma 5.16, 2 is special and cannot divide n_t. So since n_t is odd, Lemma 5.13 says that $G_{n_s} \mid G_n$ and $H_{n_s} \mid H_n$, or $G_{n_s} \mid H_n$ and $H_{n_s} \mid G_n$. Hence, $n_s \mid \gcd(G_n, H_n)$.

We next show that $n_t \mid G_nH_n$. We have $n_t \mid U_nV_nG_nH_n$. Let q be a prime factor of n_t. Then $q \mid G_m$. If q divided U_n, then q would divide U_m and thus be special by Lemma 3.2. But n_t is free of special primes. Similarly, V_n divides V_m since $p = m/n$ is odd. So q cannot divide V_n, or else q would divide $\gcd(G_m, V_m)$ and be special, by Lemma 3.2. Therefore, $\gcd(n_t, U_nV_n) = 1$ and n_t divides G_nH_n.

We now wish to conclude that either $n \mid G_n$ or $n \mid H_n$. Note that p is either 1 (mod 4), or -1 (mod 4). If $p \equiv 1 \pmod 4$, then $n \mid G_n$. Indeed, if not, there is a prime factor q of n_t which divides H_n. But by Lemma 5.11, $H_n \mid H_m$. Thus, $q \mid \gcd(G_m, H_m)$ and q is special by Lemma 3.2, which contradicts $q \mid n_t$.

If $p \equiv -1 \pmod 4$, then $n \mid H_n$. Indeed, if $n \nmid H_n$, then there exists a prime q dividing n_t which divides G_n. By Lemma 5.11, $G_n \mid H_m$. So $q \mid \gcd(G_m, H_m)$ and q is special, by Lemma 3.2. But that cannot be since n_t is free of special prime factors. ∎

REMARK. In retrospect, the absence of GH-basic elements > 1, asserted by Theorem 5.17, might well have been expected. Indeed, when $D = -E^2$, P is even, so that, by Proposition 5.2, the only U- and V-basic elements are 1.

COMMENT. Theorem 5.17 guarantees that all integers n in $\mathcal{N}_G$ and in $\mathcal{N}_H$ will be generated *with no exception* if one uses the description of $\mathcal{P}_{G,n}$ and $\mathcal{P}_{H,n}$ of Theorem 5.12 starting at $n = 1$ and incrementing one at a time the number of prime factors of those integers already found to lie in $\mathcal{N}_G \cup \mathcal{N}_H$. Consider, say, the recursion $x^2 - 2x + 5$ with discriminant $D = -16$ and $E = 4$ which has no special primes. Since $G_1 = 3$ and $H_1 = -1$ and the prime 3 is -1 (mod 4), the only integer n in $\mathcal{N}_G \cup \mathcal{N}_H$ with $\Omega(n) = 1$ is $n = 3$ which belongs to $\mathcal{N}_H$. Since $H_3 = -9$, $n = 9 \in \mathcal{N}_G$ is the only integer with $\Omega(n) = 2$ that belongs to $\mathcal{N}_G \cup \mathcal{N}_H$. Now $G_9 = -1917 = -3^3 \times 71$ and both 3 and 71 being -1 (mod 4), 27 and $639 = 9 \times 71$, both in $\mathcal{N}_H$, are the only integers n in $\mathcal{N}_G \cup \mathcal{N}_H$ with $\Omega(n) = 3$. The procedure goes on likewise generating all integers in $\mathcal{N}_G \cup \mathcal{N}_H$. This phenomenon is comparable to what Smyth had observed in [25] for the U and for the V sequences.

5.3. Recursions of discriminant $-3F^2$. Throughout this section, the recursions have characteristic polynomial $x^2 - Px + Q \in \mathbb{Z}[x]$, where as usual $Q \neq 0$ and the discriminant D is non-zero of the form $-3F^2$. We intend to study both pairs of sets, $\mathcal{N}_S$ and $\mathcal{N}_T$, and $\mathcal{N}_Y$ and $\mathcal{N}_Z$, and follow the same template as in the study of the pair of sets $\mathcal{N}_G$

and $\mathcal{N}_H$. Things should begin to seem routine! However, for recursions of discriminant $-3F^2$, two primes, namely 2 and 3, have an idiosyncratic behavior, whereas for recursions of discriminant $-E^2$, only the prime 2 did stand out. For $\mathcal{N}_S$ and $\mathcal{N}_T$, 3 will behave much as 2 did for $\mathcal{N}_G$ and $\mathcal{N}_H$. But for $\mathcal{N}_Y$ and $\mathcal{N}_Z$ both 2 and 3 will have an anomalous behavior.

We first state some trivial, but useful preliminary lemmas.

LEMMA 5.18. *If the discriminant D of $x^2 - Px + Q \in \mathbb{Z}[x]$ is of the form $-3F^2$ and P is odd, then Q is odd.*

Proof. Suppose Q is even. Then $D = P^2 - 4Q \equiv 1 \pmod 8$. But $D = -3F^2 \equiv -3 \pmod 8$ as F and P have the same parity. This contradiction gives the lemma. ∎

LEMMA 5.19. *Let $X = (X_n)$ be an integral linear recurring sequence with a characteristic polynomial $x^2 - Px + Q \in \mathbb{Z}[x]$ of discriminant $D = -3F^2$ such that $3 \nmid X_0$. If 3 is not a special prime, then m does not divide X_m for any m divisible by 3.*

Proof. Because $3 \mid D = -3F^2 = P^2 - 4Q$ and 3 is not special, neither P nor Q is a multiple of 3. But $3 \nmid Q$ implies that $\rho(3) \mid 3 - \epsilon_3$ by Theorem 3.6. But $\epsilon_3 = 0$ so $\rho(3) = 3$. If $3 \mid m$ and $m \mid X_m$, then by Proposition 3.11 we must have $3 \mid X_0$, since $m \equiv 0 \pmod{\rho(3)}$. But $3 \nmid X_0$. Hence, $m \nmid X_m$ for any m divisible by 3. ∎

5.3.1. The sets $\mathcal{N}_S$ and $\mathcal{N}_T$. The lemma that follows generalizes Theorem 3.29 of the present paper and is an analogue of Lemmas 5.5, 5.6 and 5.11.

LEMMA 5.20. *Let n be a positive integer and p be a prime. For $p \equiv 1 \pmod 6$ we have*

(i) $S_n \mid S_{np}$ *and, assuming* $S_n \neq 0$, $S_{np}/S_n \equiv S_n^{p-1} \pmod p$,
(ii) $T_n \mid T_{np}$ *and, assuming* $T_n \neq 0$, $T_{np}/T_n \equiv T_n^{p-1} \pmod p$,

and for $p \equiv -1 \pmod 3$,

(iii) $T_n \mid S_{np}$ *and, if* $T_n \neq 0$, $S_{np}/T_n \equiv T_n^{p-1} \pmod p$,
(iv) $S_n \mid T_{np}$ *and, if* $S_n \neq 0$, $T_{np}/S_n \equiv S_n^{p-1} \pmod p$.

Proof. To prove (i) observe that since p is 1 (mod 6) we have $\omega^p = \omega$ and $\bar\omega^p = \bar\omega$. Therefore,

$$S_{np} = F\frac{(\omega\alpha^n)^p - (\bar\omega\bar\alpha^n)^p}{\alpha - \bar\alpha} = F\frac{\omega\alpha^n - \bar\omega\bar\alpha^n}{\alpha - \bar\alpha} \cdot N = S_n \cdot N,$$

where $N = \sum_{k=0}^{p-1}(\omega\alpha^n)^{p-1-k}(\bar\omega\bar\alpha^n)^k$ is an algebraic integer in $\mathbb{Z}[\omega]$ invariant by conjugation. Hence, N is a rational integer. Therefore, S_n divides S_{np}. If $S_n \neq 0$, then putting $m = p$ and $n = n$ in the multiplication formula (2.75), dividing through by S_n and reducing modulo p yields $S_{pn}/S_n \equiv S_n^{p-1} \pmod p$.

The rest of the lemma is obtained in similar ways. Noting that for primes $p \equiv 1 \pmod 6$, $T_{np} = T_n \cdot N'$, where $N' = \sum_{k=0}^{p-1}(\omega\bar\alpha^n)^{p-1-k}(\bar\omega\alpha^n)^k$ is a rational integer and using the multiplication formula (2.77) with $m = p$ and $n = n$ yields (ii).

For primes $p \equiv -1 \pmod 6$, we have $\omega^p = \bar\omega$ and $\bar\omega^p = \omega$. Thus, $S_{np}/T_n = -\sum_{k=0}^{p-1}(\bar\omega\alpha^n)^{p-1-k}(\omega\bar\alpha^n)^k$ and $T_{np}/S_n = -\sum_{k=0}^{p-1}(\bar\omega\bar\alpha^n)^{p-1-k}(\omega\alpha^n)^k$, being algebraic integers invariant under conjugation, are indeed rational integers. Using the multiplication formulas (2.77) and (2.75) yields respectively (iii) and (iv).

It remains to deal with $p = 2$, which is also a prime $-1 \pmod 3$. By (2.56), we have $S_{2n}/T_n = Z_n$ and $T_{2n}/S_n = Y_n$. Note that $S_1 - Z_1 = 2F$ and $Y_1 - T_1 = 2F$. Since $S_0 = Z_0$ and $T_0 = Y_0$, we have $Z_k \equiv S_k \pmod 2$ and $Y_k \equiv T_k \pmod 2$ for all $k \geq 0$. Therefore, $S_{2n}/T_n \equiv S_n^{2-1} \pmod 2$ and $T_{2n}/S_n \equiv T_n^{2-1} \pmod 2$, when neither S_n nor T_n is zero. ∎

As for the pair (G, H), given a positive integer n in $\mathcal{N}_S \cup \mathcal{N}_T$, we define the two sets of primes $\mathcal{P}_{S,n}$ and $\mathcal{P}_{T,n}$ as

$$\mathcal{P}_{S,n} = \{p;\, np \in \mathcal{N}_S\}, \quad \mathcal{P}_{T,n} = \{p;\, np \in \mathcal{N}_T\}.$$

An integer n in $\mathcal{N}_S$, or in $\mathcal{N}_T$, will be said to be *basic*, or *ST-basic*, if for any prime factor p of n, n/p is neither in $\mathcal{N}_S$, nor in $\mathcal{N}_T$.

The next theorem is a close analogue of Theorem 5.12 with the prime 3 replacing the prime 2 as the 'odd duck'.

THEOREM 5.21. *Let X stand for one of the two sequences S or T, and X^* stand for the other one. Suppose n divides X_n. Necessary and sufficient conditions for a prime p to belong to $\mathcal{P}_{X,n}$, or to $\mathcal{P}_{X^*,n}$, are described below.*

For $p \equiv 1 \pmod 6$, we have

- *$p \in \mathcal{P}_{X,n}$ if and only if $p \mid X_n$, while*
- *$p \in \mathcal{P}_{X^*,n}$ if and only if $p \mid X_n^*$ and n is a product of special primes.*

For $p \equiv -1 \pmod 3$, we have

- *$p \in \mathcal{P}_{X,n}$ if and only if $p \mid X_n^*$ and n is a product of special primes, while*
- *$p \in \mathcal{P}_{X^*,n}$ if and only if $p \mid X_n$.*

The prime 3 belongs to $\mathcal{P}_{X,n}$ if and only if it belongs to $\mathcal{P}_{X^*,n}$, which occurs if and only if $3n$ is a product of special primes.

Proof. Assume $p \equiv 1 \pmod 6$. If $p \mid X_n$ and $X_n \neq 0$, then, by Lemma 5.20(i)–(ii), p divides the integer X_{np}/X_n, i.e., $pX_n \mid X_{np}$. Since $n \mid X_n$, we get $pn \mid X_{np}$, that is, $p \in \mathcal{P}_{X,n}$. If $X_n = 0$, then, as X_n divides X_{np}, $X_{np} = 0$ and trivially $np \mid X_{np}$. If, on the other hand, $p \nmid X_n$, then $p \nmid X_{np}$ since, by Lemma 5.20(i)–(ii), $X_{np} \equiv X_n^p \equiv X_n \pmod p$. All the more, $np \nmid X_{np}$ and $p \notin \mathcal{P}_{X,n}$.

Assume now $np \mid X_{np}^*$, i.e., $p \in \mathcal{P}_{X^*,n}$. Then $n \mid \gcd(S_{np}, T_{np})$, since $n \mid X_n$ and $X_n \mid X_{np}$ imply that $n \mid X_{np}$. But then, by Lemma 3.3, all prime factors of n must be special. By Lemma 5.8, $n \mid V_n$. Since $X_n^* = V_n - X_n$, we conclude that $n \mid X_n^*$. But, given that $n \mid X_n^*$, we have just shown that $p \in \mathcal{P}_{X^*,n}$ iff $p \mid X_n^*$. Hence, $p \mid X_n^*$. Thus, by the latter equivalence, to prove the converse it will suffice to show that $n \mid X_n^*$. But n being a product of special primes, we have $n \mid V_n$. Since, by hypothesis, $n \mid X_n$, we have $n \mid X_n^* = V_n - X_n$.

We now turn to primes $p \equiv -1 \pmod 3$. If $p \mid X_n$ and $X_n \neq 0$, then, by Lemma 5.20(iii)–(iv), $p \mid X_{np}^*/X_n$. Thus, $pX_n \mid X_{np}^*$ and therefore $pn \mid X_{np}^*$. The same conclusion holds in case $X_n = 0$, as, then, $X_{np} = 0$. If $p \nmid X_n$, then $p \nmid X_{np}^*$, since $X_{np}^* \equiv X_n^p \equiv X_n \pmod p$. Thus, $np \nmid X_{np}^*$ and p does not belong to $\mathcal{P}_{X^*,n}$. Hence, $p \mid X_n$ iff $p \in \mathcal{P}_{X^*,n}$.

Suppose that $np \mid X_{np}$. Since $n \mid X_n$ and $X_n \mid X_{np}^*$, it follows that $n \mid X_{np}^*$. Therefore, $n \mid \gcd(S_{np}, T_{np})$. Thus, Lemma 3.3 tells us that all prime factors of n are special. By

Lemma 5.8, $n \,|\, V_n$. But $X_n^* = V_n - X_n$ so $n \,|\, X_n^*$. Thus we conclude that $p \,|\, X_n^*$, as, given that $n \,|\, X_n^*$, we already know that $p \,|\, X_n^*$ iff $p \in \mathcal{P}_{X,n}$. Again to prove the converse it is enough to show that $n \,|\, X_n^*$. Now, n being a product of special primes, n divides V_n. Hence, $n \,|\, V_n - X_n = X_n^*$.

Let us now focus on $p = 3$. To ease notation assume $X = S$, that is, $n \,|\, S_n$; a similar argumentation would hold if X were equal to T. Suppose $3 \in \mathcal{P}_{S,n}$. Then, in particular, $3 \,|\, S_{3n}$, which implies that 3 is special, by Lemma 5.19, since $3 \nmid S_0$. Note that the same reasoning gives that 3 is special if $3 \,|\, T_{3n}$.

Let now q be a prime factor of n. By the identity

$$S_{3n} = V_n T_n Y_n - Q^n S_n,$$

q must divide $V_n T_n Y_n$. Hence, $q \,|\, T_n$, for if $q \,|\, V_n$, then $q \,|\, V_n - S_n = T_n$ and if $q \,|\, Y_n$, then $q \,|\, 2S_n - Y_n = T_n$. Thus, by Lemma 3.3, q is a special prime. If instead of $3 \in \mathcal{P}_{S,n}$ we assume that $3 \in \mathcal{P}_{T,n}$, then, by the identity $T_{3n} = V_n S_n Z_n - Q^n T_n$, q divides QT_n. If $q \,|\, Q$, then since $S_n T_n = Q^n - F^2 U_n^2$, $q \,|\, FU_n = S_n - T_n$. Hence, $q \,|\, T_n$. But $q \,|\, \gcd(S_n, T_n) \Rightarrow q$ is special, by Lemma 3.3.

It remains to see that if $3n$ is a product of special primes then $3n \,|\, \gcd(S_{3n}, T_{3n})$. By Lemma 5.8, $n \,|\, V_n$ and $3n \,|\, V_{3n}$. But by identity (2.60), i.e., $U_{3n} = 3U_n S_n T_n$, $3n \,|\, U_{3n}$. Thus,

$$3n \,|\, V_{3n} = S_{3n} + T_{3n} \quad \text{and} \quad 3n \,|\, FU_{3n} = S_{3n} - T_{3n},$$

which implies that $3n \,|\, 2\gcd(S_{3n}, T_{3n})$. However, $S_{3n} = V_n T_n Y_n - Q^n S_n$ and $T_{3n} = V_n S_n Z_n - Q^n T_n$ yield $n \,|\, \gcd(S_{3n}, T_{3n})$, since $T_n = V_n - S_n$ is divisible by n. Therefore, $3n \,|\, \gcd(S_{3n}, T_{3n})$. ∎

Although not necessary to the development of this chapter, we add a remark adding precision to Theorem 5.21 about when 2 belongs to $\mathcal{P}_{X,n}$, or to $\mathcal{P}_{X^*,n}$.

REMARK 5.22. Suppose, as in Theorem 5.21, that n divides X_n, where $n \geq 1$. Then $2 \in \mathcal{P}_{X^*,n}$ iff, by Theorem 5.21, $2 \,|\, X_n$, which occurs iff either

- 2 is special, or
- P and Q are odd and $n \equiv \pm 1 \pmod 3$ according to whether $2 \,|\, X_1$ or $2 \,|\, X_1^*$, respectively.

Also, $2 \in \mathcal{P}_{X,n}$ iff, by Theorem 5.21, $2 \,|\, X_n^*$ and n is a product of special primes, which occurs iff n is a product of special primes and either

- 2 is special, or
- P and Q are odd and $n \equiv \pm 1 \pmod 6$ according as $2 \,|\, X_1^*$ or $2 \,|\, X_1$, respectively.

Proof of Remark 5.22. If 2 is special, then, by Lemma 5.24, $2 \,|\, X_n$. If P and Q are odd, then, as $U_2 = P$ and $U_3 = P^2 - Q$, $\rho(2) = 3$. Thus, by Proposition 3.11, $2 \,|\, X_n$ iff either $2 \,|\, X_1$ and $n \equiv 1 \pmod 3$, or $2 \,|\, X_2$ and $n \equiv 2 \pmod 3$. But $S_2 = T_1 Y_1$ and $T_2 = S_1 Z_1$ and, as we saw at the end of the proof of Lemma 5.20, T_1 and Y_1 share the same parity and so do S_1 and Z_1. Hence, $2 \,|\, X_2$ iff $2 \,|\, X_1^*$. To complete the case $2 \in \mathcal{P}_{X^*,n}$, it remains to see that if $2 \,|\, X_n$ and 2 is not special, then P and Q must be odd. But, by Lemma 5.18, Q is odd. By Theorem 3.38, the case Q odd and P even implies that all X terms are odd, which contradicts $2 \,|\, X_n$. Thus, indeed, P and Q must both be odd.

We now examine the case $2 \in \mathcal{P}_{X,n}$. Thus, n is a product of special primes and $n \mid X_n$, and we need to show that $2 \mid X_n^*$ iff either 2 is special, or, P and Q are odd and, according as X_1^* or X_1 is even, $n \equiv \pm 1 \pmod 6$. If 2 is special, then, by Lemma 5.24, $2 \mid X_n^*$. If P and Q are odd, then $\rho(2) = 3$, and the same analysis as above, using Proposition 3.11, leads to $2 \mid X_n^*$ iff either $2 \mid X_1^*$ and $n \equiv 1 \pmod 3$, or $2 \mid X_1$ and $n \equiv -1 \pmod 3$. Because n, as a product of special primes, must be odd, the congruences hold modulo 6. For the direct implication ($\Rightarrow$), all that is needed is to see that, when $2 \mid X_n^*$ and 2 is not special, P and Q must be odd. By Lemma 5.18, if Q is even, then P is even. But 2 is not special, so Q is odd. If P were even, then, by Theorem 3.38, no X^* term would be even, contradicting $2 \mid X_n^*$. Hence, the remark holds. ∎

Remark. The descriptions of $\mathcal{P}_{S,n}$ and $\mathcal{P}_{T,n}$ simplify much if we assume that $\gcd(P, Q) = 1$. Suppose $n \mid S_n$. If $n \geq 2$, then the set $\mathcal{P}_{S,n}$ is the set of primes $1 \pmod 6$ that divide S_n, while the set $\mathcal{P}_{T,n}$ is the set of primes $-1 \pmod 6$ that divide S_n. If n is 1, $\mathcal{P}_{S,1}$ contains in addition to primes $1 \pmod 6$ that divide S_1, primes $-1 \pmod 6$ which divide T_1, and, if both P and Q are odd and 2 divides T_1, the prime 2. The set $\mathcal{P}_{T,1}$, besides primes $-1 \pmod 6$ that divide S_1, contains primes $1 \pmod 6$ which divide T_1 and the prime 2 provided P and Q are odd and 2 divides S_1.

Example. For the recursion determined by $(P, Q) = (5, 7)$, where $D = -3$ and $F = 1$, the smallest few integers in $\mathcal{N}_S$ are 1, 2, 8, ... and the first few in $\mathcal{N}_T$ are 1, 4, 16 and $8 \times 47 = 376$ with $\mathcal{P}_{S,1} = \{2\}$, $\mathcal{P}_{T,1} = \emptyset$, $\mathcal{P}_{S,2} = \emptyset$, $\mathcal{P}_{T,2} = \{2\}$, $\mathcal{P}_{S,4} = \{2\}$, $\mathcal{P}_{T,4} = \emptyset$, $\mathcal{P}_{S,8} = \emptyset$ and $\mathcal{P}_{T,8} = \{2, 47\}$, as can be checked by computing the first few positive terms of S and T and using the previous remark.

In the above example, it happens that among the first eight natural numbers, those in $\mathcal{N}_S$ or $\mathcal{N}_T$ are all obtained by starting at 1 and using primes in $\mathcal{P}_{S,1}$, or $\mathcal{P}_{T,1}$, and, given an n in $\mathcal{N}_S \cup \mathcal{N}_T$, by using primes in $\mathcal{P}_{S,n}$ or $\mathcal{P}_{T,n}$, so the natural question is whether this is generally the case, that is, whether there are ST-basic integers other than 1. As in Section 5.2, at the same point, we establish a few lemmas prior to furnishing an answer.

Lemma 5.23. *If m and n are positive integers and $3 \nmid m$, then $S_n T_n \mid S_{mn} T_{mn}$. More precisely, if m has k prime factors that are $-1 \pmod 3$, then*

$$\begin{aligned} &S_n \mid S_{mn} \text{ and } T_n \mid T_{mn} \quad \text{if } k \text{ is even,} \\ &T_n \mid S_{mn} \text{ and } S_n \mid T_{mn} \quad \text{if } k \text{ is odd.} \end{aligned}$$

Proof. Note that it suffices to prove the result for $m = p$ a prime distinct from 3. But for a prime $p \equiv 1 \pmod 6$, Lemma 5.20 says that $S_n \mid S_{np}$ and $T_n \mid T_{np}$. The same lemma gives that $S_n \mid T_{np}$ and $T_n \mid S_{np}$ for primes $p \equiv -1 \pmod 6$ and for $p = 2$. ∎

Lemma 5.24. *Suppose p is a special prime. Then for all integers $n \geq 1$, p divides S_n and T_n, unless $p = 3$, $n = 1$ and $3 \nmid F$.*

Proof. By using inductively the recursion $X_{n+2} = PX_{n+1} - QX_n$ and the fact that p divides both P and Q, we find that $p \mid \gcd(S_n, T_n)$ for all $n \geq 2$. But note that if $p \neq 3$, then, since $-3F^2 = P^2 - 4Q$, $p \mid \gcd(P, Q) \Rightarrow p \mid F$. If $p \equiv \pm 1 \pmod 6$, then clearly $p \mid \gcd(S_1, T_1)$. If $p = 2$, then $2 \mid \gcd(P, F)$ and $Q = (P/2)^2 + 3(F/2)^2$ is even, since 2 is

special. Therefore $P/2$ and $F/2$ have the same parity. Thus, $2 \mid \gcd(S_1, T_1)$. If $p = 3$, then clearly $3 \mid \gcd(S_1, T_1)$ iff $3 \mid F$. ∎

The next lemma is an analogue for the S and T sequences of Lemmas 5.8 and 5.9, which concern arbitrary U and V sequences. It also provides a converse to an immediate consequence of Lemma 3.3, which is that, if n divides S_n and n divides T_n, then n is a product of special primes.

LEMMA 5.25. *If n is a product of special primes, then n divides both S_n and T_n.*

Proof. We proceed by induction on $k = \Omega(n)$ the number of (special) prime factors of n. Since 1 divides S_1 and T_1, assume m is a product of k special primes, where $k \geq 1$, and assume the inductive hypothesis holds for any product of special primes having less than k prime factors.

If 3 is special and $3 \mid m$, then, writing $m = 3n$, we see by the inductive hypothesis that $n \mid S_n$. But then, by Theorem 5.21, $m = 3n$ divides both S_m and T_m.

Otherwise, $3 \nmid m$. Then we write $m = np$, where p is a special prime distinct from 3. Thus, by Lemma 5.24, $p \mid S_n$ and $p \mid T_n$. But then, by Theorem 5.21, we have $p \in \mathcal{P}_{S,n} \cap \mathcal{P}_{T,n}$, since $n \mid S_n$ and n is a product of special primes. That is, $m \mid S_m$ and $m \mid T_m$. ∎

We are now ready for our second theorem concerning $\mathcal{N}_S$ and $\mathcal{N}_T$. Its statement and proof resemble those of Theorem 5.17.

THEOREM 5.26. *Every integer m in $\mathcal{N}_S \cup \mathcal{N}_T$ is either equal to 1, or to a product of primes $p_1 \cdots p_k$ such that $p_1 \cdots p_i$ belongs to $\mathcal{N}_S \cup \mathcal{N}_T$ for each $i = 1, \ldots, k-1$. In particular, 1 is the only ST-basic element.*

Proof. Without loss of generality we assume that $m \mid S_m$, $m > 1$ and m is composite, since trivially $1 \mid S_1$. The case $m \mid T_m$ can be treated in an analogous way. We will use both Lemmas 5.3 and 5.4. So we assume first that m is not of the form 2^ℓ, where $\ell \geq 2$. With p the largest prime factor of m, we write $m = np$. We seek to show that either $n \mid S_n$, or $n \mid T_n$. Note that $p \geq 3$. Since $U_{3m} = 3U_m S_m T_m$, we have $3m \mid U_{3m}$. But $3m$, in case P is odd, is not of the form $2^\ell \cdot 3$, $\ell \geq 3$. Also p is the largest prime factor of $3m$. Thus, by Lemma 5.3, $3n \mid U_{3n}$ and so $n \mid U_n S_n T_n$. Let n_s be the largest factor of n which is a product of special primes and n_t be its cofactor in n, i.e., $n = n_s \cdot n_t$. Note that $\gcd(n_s, n_t) = 1$. By Lemma 5.25, $n_s \mid \gcd(S_{n_s}, T_{n_s})$. If 3 is special, then $3 \nmid n_t$. If 3 is not special, then, by Lemma 5.19, $3 \nmid m$, since $3 \nmid S_0$. In particular, $3 \nmid n_t$. Hence, by Lemma 5.23, $n_s \mid \gcd(S_n, T_n)$. If q is a prime factor of $\gcd(n_t, U_n)$, then $q \mid S_m$, since $n_t \mid m$ and $m \mid S_m$. Also $q \mid U_n$ implies $q \mid U_m$ since $U_n \mid U_m$. Hence, q divides both S_m and U_m, which, by Lemma 3.5, says that q is special. This contradicts $q \mid n_t$. Hence, $\gcd(n_t, U_n) = 1$ and $n_t \mid S_n T_n$. In particular, $n \mid S_n T_n$.

Suppose $p \equiv 1 \pmod 6$. Then by Lemma 5.20, $S_n \mid S_m$ and $T_n \mid T_m$. If $n \nmid S_n$, then since $n_s \mid S_n$, there exists a prime q dividing n_t such that $q \mid T_n$. Therefore $q \mid T_m$. But $q \mid n_t$ and $n_t \mid S_m$ so that $q \mid S_m$. We have reached a contradiction since q dividing both S_m and T_m would be a special prime by Lemma 3.3. Hence $n \mid S_n$.

The case $p \equiv -1 \pmod 6$ can be dealt with similarly. Indeed, in that case, $S_n \mid T_m$ and $T_n \mid S_m$ by Lemma 5.20. If $n \nmid T_n$, then since $n_s \mid T_n$ there is a prime q, $q \mid n_t$, and

$q \mid S_n$. Therefore $q \mid T_m$ and, because q divides n_t and n_t divides m, $q \mid S_m$. Hence q is special. But n_t has no special prime factors, a contradiction. Thus, $n \mid T_n$.

If p is 3, then we saw that $m \mid S_m$ and $3 \mid m$ cannot occur unless 3 is special. Thus, $m = 3n$ being of the form $2^\ell \cdot 3^k$, assuming $n_t > 1$, we have $n_t = 2^\ell$. Since $n_t \mid S_n T_n$ and 2 is not special, 2 does not divide $\gcd(S_n, T_n)$, by Lemma 3.3. Thus, either $n_t \mid S_n$ and $n \mid S_n$, or $n_t \mid T_n$ and $n \mid T_n$.

We now investigate the case $m = 2^\ell$, $\ell \geq 2$. Put $m = 2n$. Suppose P is odd and $m = 2^\ell$, $\ell \geq 3$. Again $m \mid S_m \Rightarrow 3m \mid U_{3m}$. Applying Lemma 5.4 leads to $3 \cdot 2^{\ell-1} \mid U_{3 \cdot 2^{\ell-1}} = 3U_{2^{\ell-1}} S_{2^{\ell-1}} T_{2^{\ell-1}}$. That is, $2^{\ell-1} \mid U_{2^{\ell-1}} S_{2^{\ell-1}} T_{2^{\ell-1}}$. Note that P odd implies that Q is odd by Lemma 5.18. The initial values of the U sequence being 0, 1, P and $P^2 - Q$, $\rho(2) = 3$. By Theorem 3.7, U_n is even iff $3 \mid n$. Hence, $2^{\ell-1} \mid S_{2^{\ell-1}} T_{2^{\ell-1}}$. Since 2 is not special, $2 \nmid \gcd(S_{2^{\ell-1}}, T_{2^{\ell-1}})$ by Lemma 3.3. Thus, either $2^{\ell-1} \mid S_{2^{\ell-1}}$, or $2^{\ell-1} \mid T_{2^{\ell-1}}$.

It remains to look at the cases where $m = 2^\ell$, $\ell \geq 2$, with P even, and $m = 4$ with P odd. Assume first P is even and $m = 2^\ell$, $\ell \geq 2$. Note that Q must be even. Indeed, if Q is odd, then, given that m is even and $m \mid S_m$, Proposition 3.11 implies that 2 must divide $S_0 = 1$, a contradiction. Hence, P and Q are both even. Thus, $n = 2^{\ell-1}$ is a product of special primes and so, by Lemma 5.25, $n \mid \gcd(S_n, T_n)$. Finally, if $m = 4$ and P is odd, then, by Lemma 5.18, Q is odd. Since for P odd, $\rho(2) = 3$, we conclude by Proposition 3.11 that 4 divides S_4 implies $2 \mid S_1$. But $S_1 - T_1 = F \equiv P \equiv 1 \pmod 2 \Rightarrow 2 \nmid T_1$. Hence, $T_2 = PT_1 - QT_0 \equiv 0 \pmod 2$. Thus, $2 \mid T_2$. ∎

Remark. It might have been expected that under the conditions $P \equiv \pm 1 \pmod 6$ and $Q \equiv -1 \pmod 6$ which, by Proposition 5.2, imply that 12 is a U-basic element and $6 = 12/2$ a V-basic element, $4 = 12/3$ might have been an ST-basic element. However, the conditions $P \equiv \pm 1 \pmod 6$ and $Q \equiv -1 \pmod 6$ are incompatible with $D = -3F^2$, since they force D to be congruent to 5 (mod 6).

5.3.2. The sets $\mathcal{N}_Y$ and $\mathcal{N}_Z$. We now seek comparable theorems for the sets $\mathcal{N}_Y$ and $\mathcal{N}_Z$. The Y and Z sequences obey a lemma that is very similar to Lemmas 5.5, 5.6, 5.11 and 5.20. We state this result.

Lemma 5.27. *Suppose X stands for one of the sequences Y or Z and X^* stands for the other. Let n be a positive integer and p be a prime.*

For $p \equiv 1 \pmod 6$ we have

(i) $$X_n \mid X_{np} \quad \text{and, if } X_n \neq 0, \quad X_{np}/X_n \equiv X_n^{p-1} \pmod p.$$

For $p \equiv -1 \pmod 6$ we have

(ii) $$X_n \mid X^*_{np} \quad \text{and, if } X_n \neq 0, \quad X^*_{np}/X_n \equiv X_n^{p-1} \pmod p.$$

Proof. The four divisibility relations are obtained as in Lemma 5.20. For instance for $X = Y$ and $X^* = Z$, we have, assuming $p \equiv -1 \pmod 6$,

$$Z_{np} = \omega\alpha^{np} + \bar{\omega}\bar{\alpha}^{np} = (\bar{\omega}\alpha^n)^p + (\omega\bar{\alpha}^n)^p = Y_n \cdot N,$$

where $N = \sum_{k=0}^{p-1} (-1)^k (\bar{\omega}\alpha^n)^{p-1-k} (\omega\bar{\alpha}^n)^k$ is invariant under conjugation, since $(-1)^k = (-1)^{p-1-k}$ for $k = 0, 1, \ldots, p-1$, and thus is a rational integer.

All four modulo p congruences in the lemma are obtained by putting $m = p$ in the identities (2.76) and (2.78), dividing through by either Y_n, or Z_n, reducing them modulo p and making use of the facts that the binomial coefficients $\binom{p}{k}$ are all divisible by p, for $1 \le k \le p-1$, and $2^{p-1} \equiv 1 \pmod{p}$. ∎

As for the G and H, or for the S and T sequences, we define for a positive integer n in $\mathcal{N}_Y \cup \mathcal{N}_Z$ the two sets of primes $\mathcal{P}_{Y,n}$ and $\mathcal{P}_{Z,n}$ as

$$\mathcal{P}_{Y,n} = \{p;\, np \in \mathcal{N}_Y\}, \quad \mathcal{P}_{Z,n} = \{p;\, np \in \mathcal{N}_Z\}.$$

An integer n in $\mathcal{N}_Y \cup \mathcal{N}_T$ will be said to be *basic*, or *YZ-basic*, if for any prime factor p of n, n/p is neither in $\mathcal{N}_Y$, nor in $\mathcal{N}_Z$.

The next theorem is an analogue for Y and Z of Proposition 5.1, Theorem 5.12 and Theorem 5.21. The analogy with Theorem 5.21 and Remark 5.22 is perfect for all primes, but 2, for which there are subtle differences. The conditions for 2 to belong to $\mathcal{P}_{X,n}$, or $\mathcal{P}_{X^*,n}$, $X = Y$ or Z, are more stringent in the cross-over case, where it is necessary that n be a product of special primes.

THEOREM 5.28. *Suppose n divides Y_n. Then for primes $p \equiv 1 \pmod 6$, we have*

- *$p \in \mathcal{P}_{Y,n}$ if and only if $p \mid Y_n$, while*
- *$p \in \mathcal{P}_{Z,n}$ if and only if $p \mid Z_n$ and n is a product of special primes.*

For $p \equiv -1 \pmod 6$, we have

- *$p \in \mathcal{P}_{Y,n}$ if and only if $p \mid Z_n$ and n is a product of special primes, while*
- *$p \in \mathcal{P}_{Z,n}$ if and only if $p \mid Y_n$.*

The prime 3 belongs to $\mathcal{P}_{Y,n}$ if and only if it belongs to $\mathcal{P}_{Z,n}$, which occurs if and only if $3n$ is a product of special primes.

The prime 2 belongs to either $\mathcal{P}_{Y,n}$ or $\mathcal{P}_{Z,n}$ if and only if n is a product of special primes and

- *either 2 is special, in which case 2 belongs to both $\mathcal{P}_{Y,n}$ and $\mathcal{P}_{Z,n}$,*
- *or P and Q are odd and*
  - *→ either $P \equiv F \pmod 4$, i.e., T_1 and Y_1 are even, in which case*

$$2 \in \mathcal{P}_{Y,n} \quad \text{if and only if} \quad n \equiv -1 \pmod 6,$$
$$2 \in \mathcal{P}_{Z,n} \quad \text{if and only if} \quad n \equiv 1 \pmod 6,$$

  - *→ or $P \equiv -F \pmod 4$, i.e., S_1 and Z_1 are even, in which case*

$$2 \in \mathcal{P}_{Y,n} \quad \text{if and only if} \quad n \equiv 1 \pmod 6,$$
$$2 \in \mathcal{P}_{Z,n} \quad \text{if and only if} \quad n \equiv -1 \pmod 6.$$

Suppose that, instead of n dividing Y_n, n divides Z_n. Then the conditions for a prime p to belong to $\mathcal{P}_{Z,n}$, or to $\mathcal{P}_{Y,n}$, are obtained by interchanging the roles of Y and Z above. In the case p is 2 and P and Q are odd, the conditions remain identical to those stated for the case n divides Y_n.

Proof. We take the assumption that $n \mid Y_n$ first.

For $p \equiv \pm 1 \pmod 6$, the descriptions of the sets $\mathcal{P}_{Y,n}$ and $\mathcal{P}_{Z,n}$ may be obtained by imitating very closely the part of the proof of Theorem 5.21 that gives $\mathcal{P}_{S,n}$ and $\mathcal{P}_{T,n}$, only using Lemma 5.27 instead of Lemma 5.20, using Lemma 3.4 in place of Lemma 3.3 and the identity '$V_n = Y_n + Z_n$' in place of '$V_n = S_n + T_n$'.

If 3 is in $\mathcal{P}_{Y,n}$, then $3n \mid Y_{3n}$. But $3 \nmid Y_0$ so, by Lemma 5.19, 3 is a special prime. Now the relations $n \mid Y_n$ and $V_{3n} = V_n Y_n Z_n$ imply that $n \mid V_{3n}$. But $n \mid \gcd(V_{3n}, Y_{3n})$ implies that n is a product of special primes by Lemma 3.5. Hence $3n$ is a product of special primes. A similar argument shows that if 3 is in $\mathcal{P}_{Z,n}$, then $3n$ is also a product of special primes. Indeed, $3 \mid Z_{3n}$ and $3 \nmid Z_0$ imply, by Lemma 5.19, that 3 is special. Since $n \mid V_{3n}$ and $n \mid Z_{3n}$, n is a product of special primes by Lemma 3.5.

Conversely, if $3n$ is a product of special primes, then $3 \mid Q$, $n \mid V_n$ by Lemma 5.8, and $n \mid \gcd(S_n, T_n)$ by Lemma 5.25. Hence $3n \mid Y_{3n}$, since, by identity (2.71) with $m = 2n$ and $n = n$, $Y_{3n} = 3S_{2n}S_n - Q^n V_n$. Also, as $Z_{3n} = 3T_{2n}T_n - Q^n V_n$, $3n$ divides Z_{3n}.

Given that $n \mid Y_n$, we now prove the necessary and sufficient conditions for 2 to belong to $\mathcal{P}_{Y,n}$.

Suppose $2 \in \mathcal{P}_{Y,n}$. Since $Y_{2n} = Y_n V_n - Q^n$, we have $n \mid Q^n$. So all prime factors of n divide Q. Let q be a prime factor of n. If $q = 2$, then Q is even and, by Lemma 5.18, P is also even. If $q = 3$, then, as both Q and D are multiples of 3, 3 also divides P. Suppose $q > 3$. Since Y satisfies recursion (1.1) and $q \mid Q$, we have $Y_n \equiv P^{n-1} Y_1 \pmod q$. But $q \mid Y_n$ so either $q \mid P$ and q is special, or $q \mid Y_1$. In the latter case, $P \equiv -3F \pmod q$. Thus, $4Q = P^2 + 3F^2 \equiv 12F^2 \pmod q$ so that $q \mid F$. Hence, $q \mid P$. Thus, in all cases, q is special and n is a product of special primes.

If 2 is not special, then, by Lemma 5.18, Q must be odd. If P is even, then, by Theorem 3.38, $2 \nmid S_k T_k$, for any $k \geq 1$. But $S_k T_k \equiv Z_k Y_k \pmod 2$, so Y_k is odd for all $k \geq 1$, contradicting $2 \mid Y_{2n}$. Therefore, P and Q are odd and $\rho(2) = 3$. If $2 \mid Y_1$ (or T_1), then $2 \mid Y_{2n}$ iff $2n \equiv 1 \pmod 3$, by Proposition 3.11, that is, iff $n \equiv -1 \pmod 6$, since n as a product of special primes is odd. If $2 \mid Z_1$ (or S_1), then, by the same reckoning, we find that $n \equiv 1 \pmod 6$. Conversely, if $2n$ is a product of special primes, then $n \mid Q^{n-1}$, by Lemma 5.7. Hence, $2n \mid Q^n$. Also, all V terms are even, so $2n \mid Y_n V_n$. Thus, $2n$ divides Y_{2n}, since $Y_{2n} = Y_n V_n - Q^n$. When 2 is not special, the analysis carried out to prove the necessity of the conditions stated in our theorem for 2 to belong to $\mathcal{P}_{Y,n}$ also proves their sufficiency, as we essentially proceeded by equivalences.

We now assume $n \mid Y_n$ and $2 \in \mathcal{P}_{Z,n}$. This is the cross-over case and it differs from the situation where $n \mid S_n$ and $2 \in \mathcal{P}_{T,n}$, because there is no identity like $T_{2n} = S_n Z_n$ for Z_{2n}. However, we have the identity

$$Z_{2n} = -Y_n^2 + 2Q^n. \tag{5.3}$$

We show that n must be a product of special primes. Let q be a prime factor of n. If q is odd, then $q \mid Y_n$ and $q \mid Z_{2n}$ imply, by (5.3), that $q \mid Q$. But then $Y_n \equiv P^{n-1} Y_1 \pmod q$ and, if $q \mid Y_1$, then $P \equiv -3F \pmod q$. Thus, $4Q = P^2 + 3F^2 \equiv 12F^2 \pmod q$ so that q divides $3F$, and hence P. Therefore, q is special. If q is 2, then $4 \mid 2n$. But Z_{2n} being even, Y_n is even by (5.3) and $4 \mid Y_n^2$. Thus, $2 \mid Q$. But, by Lemma 5.18, P must also be even. Hence, q is special.

It cannot occur that Q be odd and P even, or else $\rho(2) = 2$, $2 \mid Z_{2n}$ and $2 \nmid Z_0$, yet $2n \equiv 0 \pmod{\rho(2)}$, which contradicts Proposition 3.11. By Lemma 5.18, P odd forces Q to be odd. Thus, either 2 is special, or P and Q are both odd. In the latter case, $\rho(2) = 3$. Suppose $P \equiv F \pmod 4$. Then $Z_1 = (P - 3F)/2 \equiv -P \pmod 2$ is odd and Z_2 is even. Therefore, by Proposition 3.11, $2 \mid Z_{2n}$ iff $2n \equiv 2 \pmod 3$, which occurs iff $n \equiv 1 \pmod 6$, since n as a product of special primes is odd. If instead $P \equiv -F \pmod 4$, then Z_1 is even, and thus $2 \mid Z_{2n}$ iff $n \equiv -1 \pmod 6$.

Conversely, assume first that $2n$ is a product of special primes. Then, as shown earlier in this proof, $2 \in \mathcal{P}_{Y,n}$. So, since $Y_{2n} = -Z_n^2 + 2Q^n$, Z_n is even. By Lemma 5.8, $2n$ then divides $Z_n V_n$. Also, by Lemma 5.7, $2n \mid Q^n$. Hence, by the identity $Z_{2n} = Z_n V_n - Q^n$, $2n$ divides Z_{2n} and $2 \in \mathcal{P}_{Z,n}$. So we now assume n to be a product of special primes and P and Q to be odd. By Lemma 5.8, $n \mid V_n$. By Lemma 5.7, $n \mid Q^n$. Thus, $n \mid Z_{2n}$, as $Z_{2n} = Z_n V_n - Q^n$. Note that n is odd so that $2n \mid Z_{2n}$ iff $2 \mid Z_{2n}$. But we already established above, depending on whether $P \equiv \pm F \pmod 4$, the necessary and sufficient conditions on n for 2 to divide Z_{2n}.

Proving the theorem under the assumption that $n \mid Z_n$ can be done in the exact same manner as in the above proof only interchanging Y_n and Z_n, and Y_{2n} and Z_{2n}. ∎

To prove a theorem analogous to Theorem 5.26 for $\mathcal{N}_Y$ and $\mathcal{N}_Z$, we first establish some basic lemmas.

LEMMA 5.29. *If m and n are positive integers and m is prime to 6, then $Y_n Z_n \mid Y_{mn} Z_{mn}$. More precisely, we have, k being the number of prime factors of m that are $-1 \pmod 6$,*

$$\begin{aligned} &Y_n \mid Y_{mn} \text{ and } Z_n \mid Z_{mn} \quad \text{if } k \text{ is even,} \\ &Z_n \mid Y_{mn} \text{ and } Y_n \mid Z_{mn} \quad \text{if } k \text{ is odd.} \end{aligned}$$

Proof. It suffices to prove the lemma for m equal to a prime $p \equiv \pm 1 \pmod 6$. But then it is a consequence of Lemma 5.27. ∎

LEMMA 5.30. *Suppose p is a special prime. Then p divides both Y_n and Z_n for all integers $n \geq 1$.*

Proof. The proof is identical to that of Lemma 5.24 with the additional remarks that for $p = 2$ and $n = 1$, the parity of $F/2$ is the same as that of $3F/2$, and for $p = 3$, $p \mid Y_1$ and $p \mid Z_1$. ∎

LEMMA 5.31. *If n is a product of special primes, then n divides both Y_n and Z_n.*

Proof. As in Lemma 5.25, we proceed by induction on $k = \Omega(n)$. The result holds trivially for $k = 0$. So assume $k \geq 1$ and assume the inductive hypothesis holds for $k - 1$. Let m be a product of k special primes and write m as np with p prime. By the inductive hypothesis $n \mid Y_n$. If $\gcd(m, 6) > 1$, then we may choose p to be either 2, or 3, so that, by Theorem 5.28, $m \mid \gcd(Y_m, Z_m)$. If $\gcd(m, 6) = 1$, then $p \equiv \pm 1 \pmod 6$. By Lemma 5.30, $p \mid \gcd(Y_n, Z_n)$. Also n is a product of special primes. Thus, Theorem 5.28 yields $m \mid \gcd(Y_m, Z_m)$. ∎

LEMMA 5.32. *Suppose 2 is not a special prime. If an even integer m divides Y_m or Z_m, then m is not a multiple of 4.*

Proof. Assume m is even and $m \mid Y_m$. By Lemma 5.18, Q must be odd. Write $m = 2\ell$. By identity (2.58), $Y_{2\ell} = -Z_\ell^2 + 2Q^\ell$. This implies that Z_ℓ is even. Hence, $Y_{2\ell} \equiv 2 \pmod 4$. Thus, $4 \nmid m$. The case $m \mid Z_m$ is dealt with by the same argument but using the identity $Z_{2n} = -Y_n^2 + 2Q^n$. ∎

We now prove our second theorem concerning $\mathcal{N}_Y$ and $\mathcal{N}_Z$.

THEOREM 5.33. *Every integer m in $\mathcal{N}_Y \cup \mathcal{N}_Z$ is either equal to 1, or to a product of primes $p_1 \cdots p_k$ such that $p_1 \cdots p_i$ is in $\mathcal{N}_Y \cup \mathcal{N}_Z$, for each $i = 1, \ldots, k-1$. In particular, 1 is the only YZ-basic element.*

Proof. The general line of proof follows that of Theorems 5.17 and 5.26.

Assume $m \mid Y_m$ and write $m = np$, where p is the largest prime factor of m. Then the theorem will hold if we can show that n divides Y_n, or n divides Z_n. Indeed, the case $m \mid Z_m$ would lead to $n \mid Y_n$, or $n \mid Z_n$, in an entirely analogous way. Since $1 \mid Y_1$, there is only something to prove if we assume that m is composite. Thus, by Lemma 5.32, unless 2 is special and $m = 2^\ell$, $\ell \geq 2$, a case we will treat later in the proof, we may assume that p is ≥ 3. By identity (2.61), if the product $U_m V_m S_m T_m Z_m$ is even, then $6m \mid U_{6m}$. If P is even, then $2 \mid V_m$, since each term of the V sequence is even. If P is odd, then $\rho(2) = 3$. Moreover, Q is odd by Lemma 5.18. Thus, $2 \mid U_m$ iff $3 \mid m$ by Theorem 3.7. Also, either T_1 and S_2 are even, or S_1 and T_2 are even. In both instances, by Proposition 3.11, $2 \mid S_m T_m$ for any m congruent to $\pm 1 \pmod 3$. Hence, the product $U_m V_m S_m T_m Z_m$ is always even. So using Lemma 5.3 we find that $6n \mid U_{6n}$. In particular, $n \mid U_n V_n S_n T_n Y_n Z_n$. Let n_s be the largest factor of n which is a product of special primes and write $n = n_s \cdot n_t$. By Lemma 5.31, $n_s \mid \gcd(Y_{n_s}, Z_{n_s})$. Note that $3 \nmid n_t$. Otherwise, 3 would divide m and, by Lemma 5.19, 3 would be special. However, n_t has no special prime factors. If $2 \nmid n_t$, then n_t is prime to 6 and Lemma 5.29 yields $n_s \mid \gcd(Y_n, Z_n)$. If $2 \mid n_t$, then 2 is not special. By Lemma 5.32, $4 \nmid n_t$. So we may apply Lemma 5.29 (with, in the notation of the lemma, $n = n_s$ and $m = n_t/2$) and find that n_s divides $\gcd(Y_{n/2}, Z_{n/2})$. By Lemma 5.7, $n_s \mid Q^{n_s}$. A fortiori, we have $n_s \mid Q^{n/2}$. But since $Z_n = -Y_{n/2}^2 + 2Q^{n/2}$ and $Y_n = -Z_{n/2}^2 + 2Q^{n/2}$, we get that $n_s \mid \gcd(Y_n, Z_n)$. Therefore, in all cases, $n_s \mid \gcd(Y_n, Z_n)$. We now prove that $n_t \mid Y_n Z_n$. Note that any prime factor q of n_t divides Y_m. So if q divides U_n, then, as $U_n \mid U_m$, we have $q \mid \gcd(Y_m, U_m)$, which, by Lemma 3.5, implies that q is special. However, this contradicts $q \mid n_t$. Note that because $p \neq 2$, $V_n \mid V_m$. Thus q does not divide V_n, or else q, as a divisor of $\gcd(Y_m, V_m)$, would be special, by Lemma 3.5. Hence $n_t \mid S_n T_n Y_n Z_n$. If some prime factor q of n_t is > 2, then $q > 3$, and thus $p > 3$. But then, by Lemma 5.29, $S_n T_n \mid S_m T_m$. If $q \mid S_n T_n$ ($q > 2$), then either q divides $\gcd(Y_m, S_m)$, or q divides $\gcd(Y_m, T_m)$. In either case, q is special, by Lemma 3.5, contradicting $q \mid n_t$. Hence, the largest odd integer factor in n_t divides $Y_n Z_n$. Recall that for all k, $Y_k \equiv T_k \pmod 2$ and $Z_k \equiv S_k \pmod 2$. Thus, if $q = 2$ and $q \mid S_n T_n Y_n Z_n$, then $2 \mid Y_n Z_n$. Since, by Lemma 5.32, $4 \nmid n_t$, we have proved that $n_t \mid Y_n Z_n$. In particular, since $n_s \mid \gcd(Y_n, Z_n)$, $n \mid Y_n Z_n$.

Suppose $p \equiv 1 \pmod 6$. Then by Lemma 5.27, $Y_n \mid Y_m$ and $Z_n \mid Z_m$. If $n \nmid Y_n$, then there has to be a prime q dividing n_t such that $q \mid Z_n$. But then $q \mid \gcd(Y_m, Z_m)$. So q is special by Lemma 3.4, which contradicts $q \mid n_t$. Hence $n \mid Y_n$.

Suppose $p \equiv -1 \pmod 6$. Then $Y_n \mid Z_m$ and $Z_n \mid Y_m$ by Lemma 5.27. If $n \nmid Z_n$, then, since $n_s \mid Z_n$, there is a prime q dividing n_t such that $q \mid Y_n$. Thus, $q \mid \gcd(Y_m, Z_m)$ and q is special, a contradiction. Hence, $n \mid Z_n$.

Suppose now $p = 3$. Then, as we saw earlier from Lemma 5.19, 3 is special, since $3 \mid m$ and $3 \nmid Y_0$. Thus, by Lemma 5.32, either $n_t = 1$, in which case $n = n_s$ divides both Y_n and Z_n, or $n_t = 2$ and then $n_t \mid Y_n Z_n$ implies $2 \mid Y_n$ or $2 \mid Z_n$, and since $\gcd(n_t, n_s) = 1$, we get, respectively, $n \mid Y_n$ or $n \mid Z_n$.

We have not treated the case $m = 2^\ell$, $\ell \geq 2$, when 2 is special. In that case $n = 2^{\ell-1}$ is a product of special primes and, by Lemma 5.31, n divides both Y_n and Z_n. ∎

6. Density of prime factors

Given a set $\mathcal{R}$ of rational primes, we say that $\mathcal{R}$ has a *natural* or a *prime density* if and only if the limit of $\sharp\mathcal{R}(x)/\pi(x)$ as x goes to infinity exists. Here, as is common, $\pi(x)$ denotes the number of primes less than or equal to x. It is known that any set of rational primes defined by an Artin symbol prescription, as specified by the Chebotarev density theorem, has a natural density ([20, Theorem 7.10*]). The prime density $\delta(X)$ of a quadratic integral linear recurring sequence $X = (X_n)$ is defined, if it exists, as the natural density of the set of primes that divide at least one of its terms. That is, $\delta(X)$ is the limit value of the function

$$\#\{p \leq x;\ p \text{ prime and } p \,|\, (X_n)\}/\pi(x),$$

as x goes to ∞.

In [2], the prime density of V sequences was investigated from two main points of view, that we both wish to extend to the G and H sequences, to the S and T sequences, and to the Z and Y sequences. However, since each sequence in each of these three pairs shares the same prime divisors as the other sequence in the same pair, we obviously have, assuming the existence of the densities,

$$\delta(H) = \delta(G), \quad \delta(T) = \delta(S) \quad \text{and} \quad \delta(Y) = \delta(Z).$$

Consequently, throughout the chapter we only consider and mention the G, the S and the Z sequences. We now briefly survey the two points of view developed in [2]. First, it was shown on heuristic grounds that used only elementary arithmetic arguments and the Dirichlet density theorem for primes in arithmetic progressions that we ought to expect most V's to have a prime density of $2/3$. This approach has the advantage of simplicity and of making these densities more readily transparent. But then, we rigorously proved that almost all V sequences have density $2/3$ in a manner we recall here.

A polynomial $x^2 - Px + Q \in \mathbb{Z}[x]$, or the associated pair (P, Q) of rational integers, or the associated U and V Lucas sequences, were said to be *generic* whenever none of the three conditions below was satisfied, where as usual D denoted the discriminant $P^2 - 4Q$.

$$\begin{aligned} &\text{(i)} && Q = \pm z^2 \text{ or } \pm 2z^2, && z \in \mathbb{N}; \\ &\text{(ii)} && D = \pm z^2 \text{ or } \pm 2z^2, && z \in \mathbb{N}; \\ &\text{(iii)} && D = \pm Qy^2 \text{ or } \pm 2Qy^2, && y \in \mathbb{Q}. \end{aligned} \tag{6.1}$$

It was shown that any generic V sequence possesses a prime density equal to $2/3$.

Finally, it was proved (Theorem 1 in [2]) that the set of non-generic pairs (P, Q) is negligible. Equivalently this meant that the integral pairs (P, Q) are almost all generic,

i.e., that the function

$$\#\{(P,Q);\ |P|\le x,\ |Q|\le x,\ (P,Q) \text{ is generic}\}/(4x^2) \tag{6.2}$$

tends to 1 as $x\to\infty$.

In this chapter, we first deal with the rigorous approach. The calculation of the prime densities of the V and the G sequences is done in Section 6.1 when extra conditions are imposed on Q. Similarly, the calculation of the prime densities of the V, S and Z sequences occupies Section 6.2 and is performed under the assumption that Q satisfies yet other particular conditions. In each case, it is shown that the extra conditions imposed on Q are satisfied for 'almost all' recursions of discriminant $-E^2$, or, respectively, $-3F^2$, with a meaning made precise and defined in a way somewhat analogous to (6.2). Then, in Section 6.3, we show that these prime density results could have been anticipated via simple heuristic arguments. This third section splits naturally into two subsections according as $D=-E^2$ or $D=-3F^2$.

Meanwhile, we state and prove here a classic result about the divisor function $d(\cdot)$, which will turn out to be useful in the next two sections. Recall that the divisor function counts the number of natural divisors of an integer. For instance, $d(14)=4$.

LEMMA 6.1. *Given an integer $e\ge 0$ and a real number $\eta>0$, we have*

$$\sum_{n\le x} d(n^e) = o(x^{1+\eta}) \quad \text{as } x\to\infty,$$

where n represents a positive integer and $d(\cdot)$ is the divisor function.

Proof. By Theorem 317 of [9], for any $\epsilon>0$, $d(n)<2^{(1+\epsilon)\log n/\log\log n}$, for n large enough. Thus, given $\epsilon>0$, for n large enough, $d(n^e)<2^{e(1+\epsilon)\log n/\log\log n}$, since $\log\log n^e = (1+o(1))\log\log n$ as $n\to\infty$. Therefore, there exists a $C>0$ such that

$$d(n^e)<2^{C\log n/\log\log n}<n^{C/\log\log n},$$

for any $n\ge 3$. Choosing $n_0\ge 3$ such that $n\ge n_0 \Rightarrow C/\log\log n<1$, we find that $\sum_{n\le x} d(n^e)<\Sigma_0+\Sigma_1+\Sigma_2$, where Σ_0 is the constant $\sum_{n=1}^{n_0-1} d(n^e)$,

$$\Sigma_1=\sum_{n=n_0}^{\sqrt{x}} n^{C/\log\log n}<\sum_{n=n_0}^{\sqrt{x}} n\le x$$

and

$$\Sigma_2=\sum_{\sqrt{x}<n\le x} n^{C/\log\log n}<\sum_{\sqrt{x}<n\le x} x^{C/\log\log\sqrt{x}}\le x\cdot x^{C(1+o(1))/\log\log x}=o(x^{1+\eta}),$$

for any $\eta>0$. Therefore, $\sum_{n\le x} d(n^e)<\Sigma_0+x+o(x^{1+\eta})=o(x^{1+\eta})$, for any $\eta>0$ ([1]). ∎

([1]) We could instead have used the estimate $\sum_{n\le x} d(n)^e = O(x\log^{2^e-1} x)$, since we have $d(n^e)\le d(n)^e$. But this estimate, if obvious for $e=0$ and well known for $e=1$, is not so well known for $e\ge 2$.

We will borrow notation from [2], and write, for each integer $j \geq 1$,

$$\begin{aligned} S_j^+ &= \{p;\, (D\,|\,p) = 1 \text{ and } 2^j \,\|\, p-1\},\\ D_j^+(V) &= \{p \in S_j^+;\, \rho(p) \text{ exists and is odd}\},\\ S_j^- &= \{p;\, (D\,|\,p) = -1 \text{ and } 2^j \,\|\, p+1\},\\ D_j^-(V) &= \{p \in S_j^-;\, \rho(p) \text{ exists and is odd}\}. \end{aligned}$$

Also, for each $j \geq 1$, we consider the two relevant number fields $L_j = \mathbb{Q}\big(\zeta_{2^j}, \sqrt{D}, \sqrt[2^j]{r}\big)$ and $K_j = L_j(\zeta_{2^{j+1}})$. They are normal over $\mathbb{Q}$ ([2, Lemma 4]). The ratio $\alpha/\bar{\alpha}$ is denoted by r. Given $j \geq 1$, we write r_j for a fixed 2^jth root of r. As was shown in Lemma 5 of [2], if p splits in $\mathbb{Q}(\sqrt{D})$ into two ideals $\pi\bar{\pi}$, then ρ, the rank of p and order of $r \pmod{(p)}$, is also the order of $r \pmod{\pi}$.

6.1. Prime density of the V and the G sequences. By the laws of appearance for primes in (V_n) and in (G_n) (Theorems 3.9 and 3.13), any odd prime not dividing Q that divides G has a rank divisible by 4, so has even rank, and thus divides V. In fact, we can see more directly from (2.25) that the prime divisors of G form a subset of the prime divisors of V. However, there is a partial converse to this inclusion for odd primes p not dividing E that have Legendre character $(Q\,|\,p) = -1$. Note first that these primes divide V, since, by Theorem 3.12, $(Q\,|\,p) = -1 \Rightarrow p\,|\,V_{(p-\epsilon_p)/2}$. Since $D = -E^2$, the assumption $p \nmid E$ implies that $\epsilon_p \neq 0$, and thus that 4 divides $p - \epsilon_p$. Therefore, using (2.25) with $n = (p-\epsilon_p)/2$, we have $V_{(p-\epsilon_p)/2} = 2G_{(p-\epsilon_p)/4}H_{(p-\epsilon_p)/4}$. But for primes p not dividing $2Q$, we have

$$p\,|\,G \;\Leftrightarrow\; p\,|\,H \;\Leftrightarrow\; 4\,|\,\rho(p),$$

so we conclude that primes for which Q is a quadratic non-residue divide G. That is, if Q is not a square, then the lower prime density of G is at least $1/2$. If we assume, in addition, that Q is not twice a square, then by an elementary argument using, as Ward [27] did for the Lucas numbers, a Pythagorean identity, here identity (2.19) $G_n^2 + H_n^2 = 2Q^n$, we find that the upper prime density of G is at most equal to $3/4$. Indeed, suppose Q is a quadratic residue and 2 a quadratic non-residue modulo p. If p divides G, then ρ_H exists. Putting $n = \rho_H$ in (2.19) yields $G_{\rho_H}^2 \equiv 2Q^{\rho_H} \pmod{p}$. This contradicts the quadratic character of 2. So no prime p, having both 2 as a quadratic non-residue and Q as a quadratic residue, divides G. This set of primes, under our hypotheses on Q, has prime density $1/4$. Therefore, the prime density of G, assuming it exists, lies between $1/2$ and $3/4$ if Q is neither a square nor twice a square. We will see in Theorem 6.2 below that, under the very same hypotheses on Q, G always has a prime density of $2/3$.

We introduce additional notation that will be specific to this section. For any $j \geq 1$, let

$$\begin{aligned} D_j^+(G) &= \{p \in S_j^+;\, \rho(p) \text{ exists and is not divisible by 4}\},\\ D_j^-(G) &= \{p \in S_j^-;\, \rho(p) \text{ exists and is not divisible by 4}\}. \end{aligned}$$

Also, define the number fields $L_j^* = \mathbb{Q}\big(\zeta_{2^j}, i, \sqrt[2^{j-1}]{r}\big)$ and $K_j^* = L_j(\zeta_{2^{j+1}})$.

THEOREM 6.2. *Let $x^2 - Px + Q \in \mathbb{Z}[x]$ be a polynomial with discriminant $D = -E^2$, where E is a non-zero integer, and Q is neither the square nor twice the square of an integer. Then the prime densities of the associated V, G and H sequences exist. Their values are*

$$\delta(V) = 5/6 \quad \textit{and} \quad \delta(G) = \delta(H) = 2/3.$$

Proof. We begin by establishing the prime density of the V sequence. As usual we actually prove the existence and compute the value of the complementary set of primes, which, up to finitely many primes, is the set of primes p with odd rank $\rho = \rho(p)$. We focus first on primes not dividing E that are congruent to 1 (mod 4), that is, primes such that $(D \,|\, p) = 1$. Fix $j \geq 1$. By Lemma 6 of [2], the density of primes in $D_j^+(V)$ exists and is $\delta_j^+(V) = [L_j : \mathbb{Q}]^{-1} - [K_j : \mathbb{Q}]^{-1}$. Note that since $D = -E^2$, $L_j = \mathbb{Q}\big(\zeta_{2^j}, i, \sqrt[2^j]{r}\big)$. If $j = 1$, then $L_1 = \mathbb{Q}\big(i, \sqrt{r}\big) = K_1$. Thus, $\delta_1^+(V) = 0$. If $j \geq 2$, then $L_j = \mathbb{Q}\big(\zeta_{2^j}, \sqrt[2^j]{r}\big)$. Note that α is in $\mathbb{Q}(i)$ so that $r = \alpha^2/Q \in \mathbb{Q}(\zeta_{2^j})$. Hence, r is a square in $\mathbb{Q}(\zeta_{2^j})$ if and only if Q is a square in $\mathbb{Q}(\zeta_{2^j})$. But since Q is positive and is not the square or twice the square of an integer, $\sqrt{Q}$ does not belong to $\mathbb{Q}(\zeta_{2^j})$, which has at most three quadratic subfields, namely, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. Therefore the degree of L_j over $\mathbb{Q}$ is $2^{j-1} \cdot 2^j = 2^{-1} \cdot 4^j$ and the degree of K_j over $\mathbb{Q}$ is 4^j. It follows that $\delta_j^+(V) = 4^{-j}$, if $j \geq 2$. We now turn our attention to the computation of the densities $\delta_j^-(V) := \delta\big(D_j^-(V)\big)$, $j \geq 1$. Note that we cannot directly apply Lemma 6 of [2], since it assumes that the Galois group Γ_j of $K_j/\mathbb{Q}$ has order $2 \cdot 4^j$. But the proof of Lemma 6 in [2] shows that a prime $p \equiv -1 \pmod 4$, not dividing $2QE$, is in $D_j^-(V)$ iff the Frobenius automorphism of every prime ideal $\mathcal{P}$ of K_j lying over p is the central element τ of Γ_j that satisfies

$$\tau(\zeta_{2^{j+1}}) = -\zeta_{2^{j+1}}^{-1} \quad \text{and} \quad \tau(r_j) = r_j^{-1}, \tag{6.3}$$

provided Γ_j contains such an element. Any element σ of Γ_j must satisfy

$$\sigma(\zeta_{2^{j+1}}) = \zeta_{2^{j+1}}^a \quad \text{and} \quad \sigma(r_j) = \zeta_{2^j}^b r_j^\nu,$$

for some integers a, b and ν with a odd, $1 \leq a \leq 2^{j+1}$, $1 \leq b \leq 2^j$ and $\nu = \pm 1$. But the non-trivial automorphism of $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ being complex conjugation, a and ν are not independent. Indeed, raising $\sigma(r_j) = \zeta_{2^j}^b r_j^\nu$ to the 2^jth power gives $\sigma(r) = r^\nu$. Since r^{-1} is the complex conjugate of r, we must have $\sigma(i) = i^\nu$. Thus, we have

$$i^\nu = \sigma(i) = \sigma(\zeta_{2^{j+1}})^{2^{j-1}} = \zeta_{2^{j+1}}^{a 2^{j-1}} = i^a,$$

so that $a \equiv \nu \pmod 4$. Hence, we have proved that any $\sigma \in \Gamma_j$ must satisfy

$$\sigma(\zeta_{2^{j+1}}) = \zeta_{2^{j+1}}^a \quad \text{and} \quad \sigma(r_j) = \zeta_{2^j}^b r_j^\nu,$$

where $a \equiv \nu \pmod 4$, $1 \leq a \leq 2^{j+1}$, $1 \leq b \leq 2^j$ and $\nu = \pm 1$. There are $2^{j-1} \times 2^j \times 2 = 4^j$ possible such triplets (a, b, ν). Since Γ_j has order 4^j, each element of Γ_j corresponds in a one-to-one way to such an admissible triplet (a, b, ν). Now, the automorphism τ as defined in (6.3) corresponds to the triplet $(a, b, \nu) = (-1 + 2^j, 2^j, -1)$. This latter triplet is admissible if $-1 + 2^j \equiv -1 \pmod 4$, that is, if $j \geq 2$. Therefore, $\delta_1^-(V) = 0$ (in fact, S_1^- is empty, as can be readily checked from its definition), and by the Chebotarev density theorem, $\delta_j^-(V) = 4^{-j}$ if $j \geq 2$. Using the argument in [13, p. 454], one can legitimate

the fact that $\delta(V)$ exists and equals 1 minus the sum

$$\sum_{j\ge 2}\big(\delta_j^+(V)+\delta_j^-(V)\big)=2\sum_{j\ge 2}4^{-j}=\frac{2}{4^2}\frac{1}{1-1/4}=\frac{1}{6}.$$

That is, $\delta(V)=5/6$.

To prove that G has a prime density of $2/3$, we first show that each $D_j^+(G)$ and each $D_j^-(G)$ has a prime density, that is, we work with the set of non-divisors of the G sequence. Note that for primes $p\nmid 2QE$, we have $p\nmid G$ if and only if ρ is either odd or $2\parallel\rho$. Since S_1^+ is empty, we fix a $j\ge 2$ and assume that $p\in S_j^+$. Given a prime ideal π in $\mathbb{Q}(i)$ above p, ρ is the order of $r \pmod\pi$, so we have $p\nmid G$ iff the congruence $r^{(p-1)/2^{j-1}}\equiv 1 \pmod\pi$ holds. By Euler's criterion, this means that the equation $x^{2^{j-1}}-r=0$ is solvable modulo π in $\mathbb{Z}[i]$. But, by the Kummer–Dedekind theorem, this equation is solvable if and only if p splits completely in L_j^*, and not completely in K_j^*, since $p\in S_j^+$ implies that $p\not\equiv 1 \pmod{2^{j+1}}$. Thus, by the Chebotarev density theorem, $D_j^+(G)$ has a prime density equal to $[L_j^*:\mathbb{Q}]^{-1}-[K_j^*:\mathbb{Q}]^{-1}$. As seen in the proof for the V density, the fact that Q is neither a square nor twice the square of an integer, implies that $\sqrt{r}\notin\mathbb{Q}(\zeta_{2^j})$. Therefore, $[L_j^*:\mathbb{Q}]=2^{j-1}\cdot 2^{j-1}=4^{j-1}$ and $[K_j^*:\mathbb{Q}]=2[L_j^*:\mathbb{Q}]$. Hence, $D_j^+(G)$ has a prime density of $2^{-1}\cdot 4^{-j+1}$, for all $j\ge 2$.

We now turn our attention to primes congruent to $-1 \pmod 4$. Since S_1^- is empty, we fix a $j\ge 2$ and a prime $p\in S_j^-$ with $p\nmid Q$. By Theorem 3.6, we find that $\rho(p)$ divides $p+1$. So $4\nmid\rho$ iff the congruence $r^{(p+1)/2^{j-1}}\equiv 1 \pmod{(p)}$ holds, which implies that r is at least a 2^{j-1}th power modulo (p). Reconducting the argument of Lemma 5 in [2], only replacing L_j and K_j respectively by L_j^* and K_j^*, we obtain a criterion for $p\in S_j^-$ to not divide G, namely that p is inert from $\mathbb{Q}$ to $\mathbb{Q}(i)$, that (p) splits completely from $\mathbb{Q}(i)$ to K_j^* and that the congruence $r^{(p+1)/2^{j-1}}\equiv 1 \pmod{(p)}$ holds in $\mathbb{Q}(i)$. Now by the proof of Lemma 6 in [2], one shows that $p\nmid G$ if and only if for any prime ideal $\mathcal{P}$ in K_j^* lying above p, the Frobenius automorphism $\psi=\psi(\mathcal{P}/p)$ satisfies

$$\psi(\zeta_{2^{j+1}})=-\zeta_{2^{j+1}}^{-1}\quad\text{and}\quad\psi(r_{j-1})=r_{j-1}^{-1}. \tag{6.4}$$

If the Galois group Γ_j^* of $K_j^*/\mathbb{Q}$ contains an automorphism acting as ψ, then, since ψ is independent of the choice of $\mathcal{P}$ above p, ψ is a central element of Γ_j^*. Therefore, by the Chebotarev density theorem, $D_j^-(G)$ has a prime density equal to $[K_j^*:\mathbb{Q}]^{-1}=2^{-1}\cdot 4^{-j+1}$. We reiterate the counting argument used in the first part of our proof for non-divisors of V and show that for any $\sigma\in\Gamma_j^*$ there is a triplet (a,b,ν) such that

$$\sigma(\zeta_{2^{j+1}})=\zeta_{2^{j+1}}^a\quad\text{and}\quad\sigma(r_{j-1})=\zeta_{2^{j-1}}^b r_{j-1}^\nu,$$

where $1\le a\le 2^{j+1}$, $a\equiv\nu \pmod 4$, $1\le b\le 2^{j-1}$ and $\nu=\pm 1$. Since there are $\sharp\Gamma_j^*$ such triplets, Γ_j^* must contain an automorphism corresponding to the admissible triplet $(-1+2^j,2^{j-1},-1)$; that is, Γ_j^* contains an element ψ as defined by (6.4). The usual argument [13, p. 454], based on the fact that $S_j^+\backslash D_j^+(G)$ and $S_j^-\backslash D_j^-(G)$ also have prime densities, enables us to assert that the set of prime non-divisors of G has a prime density equal to

$$\sum_{j\ge 2}\big(\delta(D_j^+(G))+\delta(D_j^-(G))\big)=\sum_{j\ge 2}(2^{-1}\cdot 4^{-j+1}+2^{-1}\cdot 4^{-j+1})=\sum_{j\ge 1}4^{-j}=1/3.$$

That is, $\delta(G)=1-1/3=2/3$. ∎

REMARK. Note in passing that a trivial consequence of the hypotheses of Theorem 6.2 is that the G, the V and the U sequences are truly distinct in that they cannot be equal up to a shift of index and/or multiplication by a rational scalar. For instance, if $(P, E) = (2, 2)$, then $Q = 2$, $G_n = V_{n-1}$ and $V_{n+2} = -4U_n$ for all n, but Q is twice a square.

We now wish to show that, in some sense, almost all recursions that have $\mathbb{Q}(i)$ as root field satisfy the conditions of Theorem 6.2, and thus that the associated V and G sequences have prime densities $5/6$ and $2/3$, respectively. We begin with some preliminary definitions and remarks.

DEFINITION. We say that a recursion $x^2 - Px + Q \in \mathbb{Z}[x]$ having root field $\mathbb{Q}(i)$ is a *$\mathbb{Q}(i)$-recursion*. Now, a $\mathbb{Q}(i)$-recursion $x^2 - Px + Q$ is said to be *G-generic* whenever Q is not a square integer or twice a square integer.

We intend to imitate what was done in [2] in the (P, Q)-plane, but instead work in the (P, E)-plane because $\mathbb{Q}(i)$-recursions are in a 1-to-2 correspondence with pairs of even integers (P, E), $E \neq 0$. Indeed, to a $\mathbb{Q}(i)$-recursion $x^2 - Px + Q$ with $D = -E^2$ we associate the two pairs (P, E) and $(P, -E)$. Conversely, given $(P, \pm E)$, where P and E are two even integers and $E \neq 0$, we associate the $\mathbb{Q}(i)$-recursion $x^2 - Px + Q$, where $4Q = P^2 + E^2$. We will write that a $\mathbb{Q}(i)$-recursion is *x-bounded* if the associated P and E parameters satisfy $|P| \leq x$ and $|E| \leq x$. Since the number of pairs of even integers (P, E) with $E \neq 0$ that are x-bounded is asymptotic to x^2, we seek to show that the number of x-bounded $\mathbb{Q}(i)$-recursions that are not G-generic is $o(x^2)$. If so, we will also say that *almost all* $\mathbb{Q}(i)$-recursions are G-generic.

THEOREM 6.3. *Almost all $\mathbb{Q}(i)$-recursions are G-generic. In fact, the number of ordered pairs (P, E) of even integers bounded by x such that $P^2 + E^2$ is the square of an integer or twice the square of an integer, is $o(x^{1+\eta})$ for any given $\eta > 0$, and thus is $o(x^2)$ as x tends to ∞.*

Proof. We may write any positive integer n as $n_1 n_2 n_3$, where $n_j = \prod p^k$, the product being over all primes p such that $p^k \parallel n$ and $p \equiv j \pmod 4$, for $j = 1$, 2 and 3. The number $r(n)$ of representations of an integer n as a sum of two squares of integers, where both sign and order are taken into account, is given by $r(n) = 4d(n_1)$ if n_3 is a square, and by $r(n) = 0$ otherwise, where $d(\cdot)$ is the divisor function ([9, Theorem 278, pp. 241–243]).

Let x be a large positive real number. Put $y = 2x$. Let $\mathcal{N}(x)$ denote the number of x-bounded $\mathbb{Q}(i)$-recursions that are not G-generic. We need to show that $\mathcal{N}(x)$ is $o(x^2)$. For this, it suffices to prove that the number of pairs (P, E) of even integers with absolute values bounded above by x such that Q, or equivalently $4Q$, is of the form n^2 or $2n^2$, is $o(x^2)$. Since $4Q = P^2 + E^2 \leq 2x^2 < y^2$, we have

$$\mathcal{N}(x) \leq \sum_{n=1}^{y} r(n^2) + \sum_{n=1}^{y} r(2n^2) = 2 \sum_{n=1}^{y} r(n^2) \ll \sum_{n=1}^{y} d(n^2).$$

Therefore, by Lemma 6.1 with $e = 2$, $\mathcal{N}(x)$ is $o(y^{1+\eta}) = o(x^{1+\eta})$, for any $\eta > 0$. Thus, the set of $\mathbb{Q}(i)$-recursions that are not G-generic is indeed negligible within the set of $\mathbb{Q}(i)$-recursions. ∎

REMARK. By Lemma 2.1, the sets of prime divisors of all four sequences $(G_n(\pm P, \pm E))$ are identical. Thus, in counting $\mathbb{Q}(i)$-recursions that are not G-generic, we could have restricted ourselves to positive even values of P and E.

6.2. Prime densities of the V, S and Z sequences. Here, our intention is to follow the same steps as in the previous section. That is, we find conditions on a $-3F^2$ recursion that guarantee certain values for the prime densities of the V, the S and the Z sequences, and show that, in some reasonable sense, these conditions are met for 'amost all' $-3F^2$ recursions. In order to perform this last step we will need a classical proposition about the number of representations $r^*(n)$ of a positive integer n as $A^2 + 3B^2$, where A and B are integers. This proposition and its proof turn out to be useful in establishing two lemmas that will be crucial in proving our core density theorems. For this reason, we begin by proving this classical result.

The content and the elementary proof of this proposition mimic the proof about the number $r(n)$ of representations of n as a sum of two squares that appears in [9, pp. 241–43], and was also re-expressed in [8, pp. 18–19].

For n a positive integer, we write $n = n_0 n_1 n_2$, where $n_j = \prod p^r$, $p^r \parallel n$ and $p \equiv j \pmod 3$, $j = 0$, 1 or 2. The ring $\mathbb{Z}[\omega]$, $\omega = e^{2i\pi/6}$, is well-known to be, as the Gaussian ring $\mathbb{Z}[i]$, a euclidean ring with, in particular, unique factorization into primes. The units in $\mathbb{Z}[\omega]$ are the six roots of unity ω^k, $k = 0, 1, \ldots, 5$. The primes of $\mathbb{Z}[\omega]$ are, up to associates, $\sqrt{-3}$, all rational primes p congruent to 2 (mod 3), and all pairs of non-associate primes $a \pm b\sqrt{-3}$ whose product is a rational prime congruent to 1 (mod 3). Recall that all primes congruent to 1 (mod 3) are indeed representable as $a^2 + 3b^2$, where a and b are integers, and that 3 is $-(\sqrt{-3})^2$.

PROPOSITION 6.4. *For any positive integer n with 4 dividing n, we have*

$$r^*(n) = \begin{cases} 6d(n_1) & \text{if } n_2 \text{ is a square,} \\ 0 & \text{otherwise,} \end{cases}$$

where $d(\cdot)$ is the divisor function.

Proof. Suppose $n = n_0 \cdot n_1 \cdot n_2 = 3^s \cdot \prod p^t \cdot \prod q^u$, where the p's and q's are rational primes with $p \equiv 1 \pmod 3$, $q \equiv 2 \pmod 3$, and t and u depend on p and q respectively. The factorization of n into primes of $\mathbb{Z}[\omega]$ has the form

$$(\sqrt{-3})^s (-\sqrt{-3})^s \prod (a + b\sqrt{-3})^t (a - b\sqrt{-3})^t \prod q^u.$$

Assuming n to be representable as $A^2 + 3B^2$, unique factorization in $\mathbb{Z}[\omega]$ implies that

$$A + B\sqrt{-3} = \omega^k (\sqrt{-3})^s \prod (a + b\sqrt{-3})^{t_1} (a - b\sqrt{-3})^{t_2} \prod q^{u_1},$$
$$A - B\sqrt{-3} = \omega^{5k} (-\sqrt{-3})^s \prod (a + b\sqrt{-3})^{t_2} (a - b\sqrt{-3})^{t_1} \prod q^{u_1},$$

with $t_1 + t_2 = t$ and $2u_1 = u$. The condition $2u_1 = u$ entails that n_2 is a square. That is, should n_2 not be a square, then $r^*(n) = 0$. The six choices for k may affect the values of A and B. There are $t + 1$ choices for t_1 and no choice for u_1. Thus, there are up to $6 \prod (t + 1) = 6d(n_1)$ choices of parameters which could yield distinct pairs of integers (A, B) in the representation of n as $A^2 + 3B^2$. But two distinct values of t_1 between 0 and

t must yield distinct pairs (A, B), or else $A + B\sqrt{-3}$ would have two essentially distinct prime decompositions in $\mathbb{Z}[\omega]$. A simple verification shows that multiplying $A + B\sqrt{-3}$ by successive powers of ω yields six pairwise distinct pairs of integers (A, B), namely

$$(A, B) \mapsto \left(\frac{A - 3B}{2}, \frac{A + B}{2}\right) \mapsto \left(\frac{-A - 3B}{2}, \frac{A - B}{2}\right) \mapsto (-A, -B),$$

the next two pairs being the two middle pairs above, but with opposite signs. All six pairs are indeed pairs of integers rather than possibly half-integers. Indeed, as 4 divides n, A and B must be two integers of the same parity. Therefore the six successive pairs are all integral. Thus, $r^*(n)$ is indeed $6\, d(n_1)$. ∎

We now establish two lemmas. The first lemma shows that, given a recursion $x^2 - Px + Q$ with discriminant $-3F^2$, simple conditions imposed on Q, simpler than conditions (6.1), suffice to guarantee that the recursion is generic.

LEMMA 6.5. *Suppose the recursion $x^2 - Px + Q$ has discriminant $D = -3F^2$, where F is an integer ≥ 1. Then Q is not twice or six times a square.*

If Q is not a square or three times a square, then $x^2 - Px + Q$ is a generic recursion.

Proof. If Q were an integer of the form $2n^2$ or $6n^2$, then so would $4Q$. By Proposition 6.4, numbers of either of these two forms are not representable by the form $x^2 + 3y^2$. But this contradicts the fact that $4Q = P^2 + 3F^2$.

Now assume that Q is neither of the form n^2 nor $3n^2$. We must check that none of the conditions (i)–(iii) of (6.1) is satisfied. Because $D = P^2 - 4Q < 0$, we have $Q > 0$. But we just saw that Q is not twice a square, and, by hypothesis, Q is not a square. This ensures that condition (i) is not satisfied. The hypothesis $D = -3F^2$ is not compatible with condition (ii) of (6.1). It remains to check that D cannot equal $-Qy^2$ or $-2Qy^2$ for any rational number y. Writing y as A/B where A and B are coprime natural numbers, $D = -Qy^2$ implies that $3F^2B^2 = QA^2$. But this latter equation implies that $Q = 3n^2$ for some $n \in \mathbb{N}$, contradicting the hypothesis. Secondly, $D = -2Qy^2$ implies that $2Q = 3n^2$, i.e., $4Q = 6n^2$ for some natural number n. But, as we saw, this contradicts Proposition 6.4. ∎

NOTATION. For an integer $j \geq 1$, we define the sets of primes

$$\begin{aligned} T_j^+ &= \{p;\ (D \,|\, p) = 1 \text{ and } 3^j \parallel p - 1\}, \\ D_j^+(S) &= \{p \in T_j^+;\ \rho(p) \text{ exists and is not a multiple of } 3\}, \\ T_j^- &= \{p;\ (D \,|\, p) = -1 \text{ and } 3^j \parallel p + 1\}, \\ D_j^-(S) &= \{p \in T_j^-;\ \rho(p) \text{ exists and is not a multiple of } 3\}. \end{aligned}$$

Also for all $j \geq 1$, we will consider the two normal number fields

$$N_j = \mathbb{Q}(\zeta_{3^j}, \sqrt[3^j]{r}), \qquad M_j = \mathbb{Q}(\zeta_{3^{j+1}}, \sqrt[3^j]{r}).$$

Our second lemma is most important. In order to facilitate its proof we state and use a proposition, which is a direct corollary of a theorem of Schinzel [22] on separable radical field extensions. A proof of Schinzel's theorem can also be found in [26, p. 343].

PROPOSITION 6.6. *Let m be an integer ≥ 1, not divisible by 8. Assume F is a number field and $x^m - a_1$, $x^m - a_2$ are irreducible polynomials in $F[x]$. Let α_1, α_2 be complex numbers that are roots of, respectively, $x^m - a_1$ and $x^m - a_2$. If $F(\alpha_1) = F(\alpha_2)$, then $a_1 = a^m a_2^i$ for some integer i prime to m and some a in F.*

LEMMA 6.7. *Suppose $D = P^2 - 4Q = -3F^2$, $F \geq 1$ and Q is not of the form $\lambda n_1^3 n^2$, where λ is either 1 or 3, n_1 is a positive integer whose prime factors are all congruent to 1 (mod 3) and n is a positive integer. Let $j \geq 1$. Then $r = \alpha/\bar{\alpha}$ is not the cube of an element in $\mathbb{Q}(\zeta_{3^j})$. Consequently, $[N_j : \mathbb{Q}] = 2 \cdot 3^{2j-1}$.*

Proof. Suppose the contrary holds, that is, $\sqrt[3]{r} \in \mathbb{Q}(\zeta_{3^j})$. Since $(\sqrt[3]{r})^3 = r \in \mathbb{Q}(\zeta_3)$, $\sqrt[3]{r}$ is algebraic of degree at most 6. The cyclotomic extension $\mathbb{Q}(\zeta_{3^j})/\mathbb{Q}$ being cyclic, $\sqrt[3]{r}$ must lie in the degree six number field $\mathbb{Q}(\zeta_9)$. That is, there is an x_1 in $\mathbb{Q}(\zeta_9)$ such that $x_1^3 = r = \alpha/\bar{\alpha} = \alpha^2/Q = (\alpha Q)^2/Q^3$. Therefore, $(\alpha Q)^2$ and αQ are cubes in $\mathbb{Q}(\zeta_9)$, a field of class number one. So there is an x in $\mathbb{Q}(\zeta_9)$ such that $x^3 = \alpha Q$. The polynomial $x^3 - \alpha Q$ is either irreducible over $\mathbb{Q}(\zeta_3)$, or reduces completely. In case it is irreducible over $\mathbb{Q}(\zeta_3)$ then $\mathbb{Q}(\sqrt[3]{\alpha Q}) = \mathbb{Q}(\zeta_9)$. Applying Proposition 6.6 to the polynomials $x^3 - \alpha Q$ and $x^3 - \zeta_3$ and the field $F = \mathbb{Q}(\zeta_3)$ yields

$$\alpha Q = a^3 \zeta_3^i, \qquad \text{for some } a \in \mathbb{Q}(\zeta_3) \text{ and } i = 1 \text{ or } 2.$$

If $x^3 - \alpha Q$ reduces over $\mathbb{Q}(\zeta_3)$, then $\alpha Q = a^3$, for some $a \in \mathbb{Q}(\zeta_3)$. Thus, in any case, we may conclude that there exist an $a \in \mathbb{Q}(\zeta_3)$ and an $i = 0, 1$ or 2 such that

$$\alpha Q = a^3 \zeta_3^i = \omega^{2i} a^3.$$

Note that αQ and a are algebraic integers in the ring $\mathbb{Z}[\omega]$. Also, α may be factored as

$$\omega^k (\sqrt{-3})^s \cdot \prod (b + c\sqrt{-3})^t \cdot \prod q^u,$$

where in the first product the $b + c\sqrt{-3}$'s are pairwise non-conjugate and non-associate primes in $\mathbb{Z}[\omega]$ and, in the second product, the q's are rational primes all distinct from 3. Since $\alpha Q = \alpha \bar{\alpha} \alpha$, we have

$$\alpha Q = \omega^{2i} a^3 = \omega^k (\sqrt{-3})^s 3^s \cdot \prod (b + c\sqrt{-3})^{2t} (b - c\sqrt{-3})^t \cdot \prod q^{3u}.$$

Unique factorization into primes in the ring $\mathbb{Z}[\omega]$ implies that each t equals $3t'$, for some integer $t' \geq 1$. Hence, Q has the form $3^s (\prod p)^{3t'} \prod q^{2u}$, where all prime factors p are 1 (mod 3). Thus, Q may be written as $\lambda n_1^3 n^2$, where $\lambda = 1$ or 3, all prime factors of n_1 are 1 (mod 3) and n is a natural number. That is, we have reached a contradiction.

By Kummer theory, the degree of the Kummer extension N_j/K is equal to the order of r in $K^\times/(K^\times)^{3^j}$, where $K = \mathbb{Q}(\zeta_{3^j})$. Thus, $[N_j : \mathbb{Q}] = [K : \mathbb{Q}] \times [N_j : K] = 2 \cdot 3^{j-1} \cdot 3^j$ as claimed. ∎

THEOREM 6.8. *Let $x^2 - Px + Q \in \mathbb{Z}[x]$ be a polynomial with discriminant $D = -3F^2$, where F is a positive integer, and Q is not of the form $\lambda n_1^3 n^2$, where $\lambda = 1$ or 3, n_1 is 1 or a product of primes congruent to 1 (mod 3) and n is an integer. Then the associated S sequence has a prime density $\delta(S)$ with*

$$\delta(S) = 3/4.$$

Moreover, prime divisors of S split equally into the two arithmetic progressions $\pm 1 \pmod 3$, the two subsets of primes each having density $3/8$.

Proof. We essentially follow the classical method of Hasse–Lagarias as adapted in [2]. Thus, we first consider primes p that split in $\mathbb{Q}(\sqrt{-3})$, that is, primes that are congruent to 1 (mod 3). This set of primes is the disjoint union of the T_j^+'s for $j \geq 1$. Note that each T_j^+ being the set of primes of the form $1 + \eta 3^j \pmod{3^{j+1}}$, where η is either 1 or -1, has a prime density equal to $2/\varphi(3^{j+1}) = 3^{-j}$, by the Dirichlet density theorem for primes in arithmetic progressions. Fix a $j \geq 1$. Given p in T_j^+, $p \nmid Q$, we have, by Theorem 3.19, that $p \nmid S$ iff p is in $D_j^+(S)$, which holds iff $r^{(p-1)/3^j} \equiv 1 \pmod{\pi}$, where π is a prime ideal in $\mathbb{Z}[\omega]$ above p. This in turn holds iff the equation $x^{3^j} - r = 0$ is solvable modulo π, in $\mathbb{Q}(\sqrt{-3})$. Using the Kummer–Dedekind theorem, we find that primes in $D_j^+(S)$ are the primes that split completely in N_j, but not completely in M_j. Thus, by the Chebotarev density theorem, $D_j^+(S)$ has a prime density

$$\delta(D_j^+(S)) = [N_j : \mathbb{Q}]^{-1} - [M_j : \mathbb{Q}]^{-1},$$

which, by Lemma 6.7, is $\delta(D_j^+(S)) = (1 - 1/3)(2 \cdot 3^{2j-1})^{-1} = 9^{-j}$.

We now turn to inert primes, i.e., to primes congruent to -1 (mod 3). Let $j \geq 1$. We wish to characterize, up to finitely many exceptions, primes in T_j^- which do not divide S, that is, primes in $D_j^-(S)$. Given p in T_j^-, $p \nmid Q$, let $\mathcal{P}$ be a prime ideal in M_j above p and let ψ denote the Frobenius automorphism of $\mathcal{P}$ over p. Since p is inert in $\mathbb{Q}(\sqrt{-3})$, we have $r^{-1} = \bar{r} = \psi(r) \equiv r^p \pmod{(p)}$ so that the order of $r \pmod{(p)}$, that is, the rank ρ of p, is a divisor of $p + 1$. Thus, $p \in D_j^-(S)$ iff $\rho \mid (p+1)/3^j$. Assuming that p belongs to $D_j^-(S)$, we necessarily have

$$\psi(\sqrt[3^j]{r}) \equiv (\sqrt[3^j]{r})^p = (\sqrt[3^j]{r})^{-1} r^{(p+1)/3^j} \equiv (\sqrt[3^j]{r})^{-1} \pmod{\mathcal{P}},$$

and if $p = -1 + \eta \cdot 3^j \pmod{3^{j+1}}$, with $\eta = \pm 1$, then

$$\psi(\zeta_{3^{j+1}}) \equiv \zeta_{3^{j+1}}^p = \zeta_{3^{j+1}}^{-1+\eta 3^j} \pmod{\mathcal{P}}.$$

Except, possibly, for finitely many primes p in $D_j^-(S)$, these two congruences imply that

$$\psi(\sqrt[3^j]{r}) = (\sqrt[3^j]{r})^{-1} \quad \text{and} \quad \psi(\zeta_{3^{j+1}}) = \zeta_{3^{j+1}}^{-1+\eta 3^j}. \tag{6.5}$$

But this means that the Frobenius automorphism ψ of $\mathcal{P}$ over p is independent of the choice of $\mathcal{P}$ above p, and therefore that it must be a central element of the Galois group of $M_j/\mathbb{Q}$. (It is of order 6 as can easily be checked by verifying that p is of order six $\pmod{3^{j+1}}$). Thus, if the Galois group of $M_j/\mathbb{Q}$ contains two automorphisms satisfying (6.5), one for each value of η, then, by the Chebotarev density theorem, $D_j^-(S)$ has a density equal to $2 \times [M_j : \mathbb{Q}]^{-1}$. By Lemma 6.7, it would mean that $\delta(D_j^-(S)) = 9^{-j}$. To check that the Galois group of $M_j/\mathbb{Q}$ contains two automorphisms, as defined by (6.5), it is sufficient to observe that any automorphism σ in this group must send $\zeta_{3^{j+1}}$ to $\zeta_{3^{j+1}}^k$, for some k, $1 \leq k \leq 3^{j+1}$, $3 \nmid k$, and send $\sqrt[3^j]{r}$ to $\zeta_{3^j}^{\ell}(\sqrt[3^j]{r})^{\nu}$, for some integer ℓ, $1 \leq \ell \leq 3^j$ and $\nu = \pm 1$. The number of such triplets (k, ℓ, ν) is $3^j \times 3^j \times 2$, which is the order of the Galois group of $M_j/\mathbb{Q}$, by Lemma 6.7. Thus, each such triplet, and in particular $(k_\eta, 3^j, -1)$, for $k_\eta = -1 + \eta 3^j \pmod{3^{j+1}}$, $\eta = \pm 1$, which correspond to the automorphisms ψ in (6.5),

represents an element of the Galois group of M_j over $\mathbb{Q}$. Hence, the set of primes which do not divide S has a density which can be argued to be

$$\sum_{j\geq 1} \delta(D_j^+(S)) + \delta(D_j^-(S)) = 2\sum_{j\geq 1} 9^{-j} = 1/4.$$

Therefore, we get the existence and the value of $3/4$ for the prime density of S. Since $\delta(D_j^+(S)) = \delta(D_j^-(S))$ for all $j \geq 1$, density-wise, prime divisors of S are equally split among the two arithmetic progressions $p \equiv \pm 1 \pmod 3$, each subset having density $3/8$. ∎

THEOREM 6.9. *Let $x^2 - Px + Q \in \mathbb{Z}[x]$ have discriminant $-3F^2$, where F is a non-zero integer. Assume Q is not of the form $\lambda n_1^3 n^2$, where n is integral, λ is 1 or 3, and n_1 is 1 or a product of primes all congruent to 1 (mod 3). Then each of the five sequences V, S, T, Y and Z has a prime density. Their values are*

$$\delta(V) = 2/3, \quad \delta(S) = \delta(T) = 3/4, \quad \text{and} \quad \delta(Y) = \delta(Z) = 1/2.$$

In addition, the prime divisors of each of these five sequences divide equally into two subsets of equal densities according to whether their residue class modulo 3 is ± 1.

Proof. By Lemma 6.5, the conditions on Q imply that $x^2 - Px + Q$ is a generic recursion. Hence, by Theorem 1 of [2], $\delta(V)$ exists and equals $2/3$. Theorem 7 of [2] states that the prime divisors of V are equally distributed among split and inert primes in $\mathbb{Q}(\sqrt{D})$, two classes which, when $D = -3F^2$, correspond to the two arithmetic progressions $\pm 1 \pmod 3$. Also, since Q is not a square, Theorem 6.8 says that S and T have a prime density equal to $3/4$ and prime divisors of S are equally divided into the two progressions $\pm 1 \pmod 3$.

It remains to prove that $\delta(Z)$ exists and is $1/2$. By Theorem 3.22, a prime p divides Z iff $6 \mid \rho(p)$. Because $6 \mid \rho$ iff $2 \mid \rho$ and $3 \mid \rho$ and since $1/2 = 2/3 \times 3/4 = \delta(V) \times \delta(S)$, it amounts to showing, that, in some sense, the two events '$p \mid V$' and '$p \mid S$' are statistically independent. Algebraically, this will translate into showing that the various extensions L_j and N_k, for j and $k \geq 1$, intersect as 'simply' as possible. We will proceed, as usual, by studying the set of primes that do not divide Z. So let $C = \{p;\, 6 \nmid \rho(p)\}$. Then $C = A \cup B$, where $A = \{p;\, 2 \nmid \rho(p)\}$ and $B = \{p;\, 3 \nmid \rho(p)\}$. Suppose we show that $A \cap B$ has a natural density, then it will follow that C has a natural density equal to

$$\delta(A) + \delta(B) - \delta(A \cap B). \tag{6.6}$$

Let us introduce notation. Given j and $k \geq 1$, let $I_{j,k}^+$ (resp. $I_{j,k}^-$) be the sets of primes p satisfying $\nu_2(p-1) = j$ and $\nu_3(p-1) = k$ (resp. $\nu_2(p+1) = j$ and $\nu_3(p+1) = k$) that belong to $A \cap B$. Thus, primes p congruent to 1 (mod 3) that divide neither V nor S form the disjoint union $\bigcup_{j,k} I_{j,k}^+$, while primes $p \equiv -1 \pmod 3$ dividing neither V nor S make up the disjoint union $\bigcup_{j,k} I_{j,k}^-$. If each $I_{j,k}^+$ (resp. each $I_{j,k}^-$) possesses a natural density, then, because primes satisfying $\nu_2(p-1) = j$ and $\nu_3(p-1) = k$ (resp. $\nu_2(p+1) = j$ and $\nu_3(p+1) = k$) have a prime density by the Dirichlet density theorem, it follows that the sets complementary to the $I_{j,k}^+$'s (resp. to the $I_{j,k}^-$'s) within the sets of primes satisfying $\nu_2(p-1) = j$ and $\nu_3(p-1) = k$ (resp. $\nu_2(p+1) = j$ and $\nu_3(p+1) = k$) also have a density, and the usual argument (see [13, p. 454]) will carry over and prove that $\delta(A \cap B)$ exists

and is the sum of the series $\sum_{j,k}(\delta(I^+_{j,k}) + \delta(I^-_{j,k}))$. Given two integers j and $k \geq 1$, we denote the composite field of L_j and N_k by $F_{j,k}$. Thus, $F_{j,k} = \mathbb{Q}(\zeta_{2^j \cdot 3^k}, \sqrt[2^j]{r}, \sqrt[3^k]{r})$.

Let us first consider primes congruent to 1 (mod 3). We fix a $j \geq 1$ and a $k \geq 1$. Then, from the proofs of Lemma 5 in [2] and Theorem 6.8, we find that $p \in I^+_{j,k}$ iff p splits completely in $F_{j,k}$, but not completely in $F_{j,k}(\zeta_{2^{j+1}})$, or in $F_{j,k}(\zeta_{3^{k+1}})$. Hence, by the Chebotarev density theorem, and the Inclusion-Exclusion principle, $I^+_{j,k}$ has a prime density equal to

$$[F_{j,k} : \mathbb{Q}]^{-1} - [F_{j,k}(\zeta_{2^{j+1}}) : \mathbb{Q}]^{-1} - [F_{j,k}(\zeta_{3^{k+1}}) : \mathbb{Q}]^{-1} + [F_{j,k}(\zeta_{2^{j+1} \cdot 3^{k+1}}) : \mathbb{Q}]^{-1}. \quad (6.7)$$

Now, by Lemma 6.7, since Q is not a square, the normal extension $N_k/\mathbb{Q}(\sqrt{-3})$ has degree 3^{2k-1}. Therefore, the extension $F_{j,k}/L_j$ is normal of degree 3^{2k-1} (see [18, Theorem 7, p. 263] and note that $N_k/\mathbb{Q}(\sqrt{-3})$ is normal, L_j is an extension of $\mathbb{Q}(\sqrt{-3})$ and $N_k \cap L_j = \mathbb{Q}(\sqrt{-3})$; the latter fact can be derived from $\gcd([N_k : \mathbb{Q}], [L_j : \mathbb{Q}]) = \gcd(2 \cdot 3^{2k-1}, 4^j) = 2$ and $\sqrt{-3} \in N_k \cap L_j$).

By Lemma 6.5 and the hypothesis on Q, we deduce that Q is neither a square or twice a square, nor thrice a square or six times a square. So, from the proof of Theorem 1 in [2] with $D = -3F^2$, we get $[L_j : \mathbb{Q}] = 4^j$. Hence, $[F_{j,k} : \mathbb{Q}] = [L_j : \mathbb{Q}] \times [F_{j,k} : L_j] = 4^j \cdot 3^{2k-1}$. Applying this result to (6.7) yields

$$\delta(I^+_{j,k}) = [F_{j,k} : \mathbb{Q}]^{-1}[1 - 1/2 - 1/3 + 1/6] = 4^{-j} \cdot 9^{-k}.$$

We now turn to primes congruent to -1 (mod 3). Again, we fix j and k each ≥ 1. For better legibility and till the end of our proof, $\zeta_{2^{j+1} \cdot 3^{k+1}}$ will be denoted by ζ. Also $K_{j,k}$ denotes the field extension $F_{j,k}(\zeta)$. Consider a prime p satisfying $\nu_2(p+1) = j$ and $\nu_3(p+1) = k$. Recall that $p \in I^-_{j,k}$ iff $p \nmid V$ and $p \nmid S$. Let $\mathcal{P}$ be a prime ideal in $K_{j,k}$ lying above p and let ψ designate the Frobenius automorphism of $\mathcal{P}$ over p. Since $p \in I^-_{j,k}$ iff $2 \nmid \rho(p)$ and $3 \nmid \rho(p)$, we may reconduct the arguments developed in the second parts of Lemmas 5 and 6 of [2], and of Theorem 6.8 of this paper, to find that, up to possibly finitely many exceptional primes in $I^-_{j,k}$,

$$\begin{aligned} \psi(\zeta) &= -\zeta_3^{\eta} \cdot \zeta^{-1}, \quad \eta = \pm 1, \\ \psi(\sqrt[2^j]{r}) &= (\sqrt[2^j]{r})^{-1}, \\ \psi(\sqrt[3^k]{r}) &= (\sqrt[3^k]{r})^{-1}, \end{aligned} \quad (6.8)$$

To obtain the first identity in (6.8), combine the facts that $\psi(\zeta_{3^{k+1}}) = \zeta_{3^{k+1}}^{-1 \pm 3^k} = \zeta_3^{\pm 1}\zeta_{3^{k+1}}^{-1}$ and $\psi(\zeta_{2^{j+1}}) = -\zeta_{2^{j+1}}^{-1}$, together with the existence of an integer ℓ, prime to 6, such that $\zeta = (\zeta_{2^{j+1}} \cdot \zeta_{3^{k+1}})^{\ell}$.

We now prove that the Galois group of $K_{j,k}/\mathbb{Q}$ contains two elements ψ as defined by (6.8), one for each value of η.

A priori, any σ in $\mathrm{Gal}(K_{j,k}/\mathbb{Q})$ must send

$$\begin{aligned} \zeta &\mapsto \zeta^a, && 0 \leq a < 2^{j+1} \cdot 3^{k+1},\ \gcd(a, 6) = 1, \\ \sqrt[2^j]{r} &\mapsto \zeta_{2^j}^b (\sqrt[2^j]{r})^{\mu}, && 0 \leq b < 2^j,\ \mu = \pm 1, \\ \sqrt[3^k]{r} &\mapsto \zeta_{3^k}^c (\sqrt[3^k]{r})^{\nu}, && 0 \leq c < 3^k,\ \nu = \pm 1. \end{aligned}$$

But any such σ either reduces to the identity automorphism of $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ or to the non-trivial automorphism that sends $\sqrt{-3}$ to $-\sqrt{-3}$. In the former case, σ fixes α and $\bar{\alpha}$, hence r, and we necessarily have $\mu = \nu = 1$, while, in the latter case, α and $\bar{\alpha}$, and thus r and r^{-1}, are interchanged, and so $\mu = \nu = -1$. Hence, we always have $\mu = \nu$. Moreover, since $\zeta_3 = (-1 + \sqrt{-3})/2$ and $\zeta_3^{-1} = (-1 - \sqrt{-3})/2$, we have

$$\zeta_3^{\nu} = \sigma(\zeta_3) = \sigma(\zeta^{2^{j+1}\cdot 3^k}) = \zeta^{a\cdot 2^{j+1}\cdot 3^k} = \zeta_3^a,$$

implying that $a \equiv \nu \pmod 3$. Therefore, a being both odd and congruent to $\nu \pmod 3$, there are $2^{j+1}\cdot 3^{k+1}/2\cdot 3 = 2^j \cdot 3^k$ values that a may take. Thus, the number of 'admissible' quadruplets (a, b, c, ν) corresponding to automorphisms of $\mathrm{Gal}(K_{j,k}/\mathbb{Q})$ is at most equal to $2^j \cdot 3^k \times 2^j \times 3^k \times 2 = 2 \cdot 4^j \cdot 9^k$. But the number $2 \cdot 4^j \cdot 9^k$ is also the degree of $K_{j,k}/\mathbb{Q}$, since, in the first part of our proof, we showed that $[F_{j,k} : \mathbb{Q}]$ is $4^j \cdot 3^{2k-1}$, and, by the same token, that $[K_{j,k} : \mathbb{Q}] = 6 \times [F_{j,k} : \mathbb{Q}] = 2 \cdot 4^j \cdot 9^k$. That is, each so-called 'admissible' quadruplet described above does correspond to an element of $\mathrm{Gal}(K_{j,k}/\mathbb{Q})$.

Noting that $-\zeta_3^{\eta} \cdot \zeta^{-1} = \zeta^{2^j\cdot 3^{k+1}}\zeta^{\eta\cdot 2^{j+1}\cdot 3^k}\zeta^{-1} = \zeta^{2^j\cdot 3^k(2\eta+3)-1}$, the automorphisms ψ in (6.8) correspond to the quadruplets

$$\big(2^j \cdot 3^k(2\eta + 3) - 1, 0, 0, -1\big), \qquad \eta = \pm 1.$$

Since $2^j \cdot 3^k(2\eta+3)-1$ is prime to 6 and congruent to $\nu = -1 \pmod 3$, these quadruplets are admissible and the Galois group of $K_{j,k}/\mathbb{Q}$ contains such elements.

Applying the Chebotarev density theorem yields the existence and the value of the density of $I_{j,k}^-$, which is

$$\delta(I_{j,k}^-) = 2 \times [K_{j,k} : \mathbb{Q}]^{-1} = 4^{-j} \cdot 9^{-k} = \delta(I_{j,k}^+).$$

Hence, $\delta(A \cap B) = 2 \cdot \sum_{j\geq 1} 4^{-j} \cdot \sum_{k\geq 1} 9^{-k} = 2 \cdot 1/3 \cdot 1/8 = 1/12$. Thus $\delta(C) = \delta(A) + \delta(B) - \delta(A \cap B) = 1/3 + 1/4 - 1/12 = 1/2$. Hence, $\delta(Z) = 1 - \delta(C) = 1/2$.

Because for each choice of j and k, $\delta(I_{j,k}^-) = \delta(I_{j,k}^+)$, primes congruent to 1 (mod 3) in $A \cap B$, and primes congruent to -1 (mod 3) in $A \cap B$ account each for half of the 1/12th density of $A \cap B$. As referenced earlier, the densities $\delta(A)$ and $\delta(B)$ split each into two equal subdensities in the two arithmetic progressions $\pm 1 \pmod 3$, so that primes 1 (mod 3) and primes -1 (mod 3) account each for a half of the 1/2 density of prime divisors of Z. ∎

As we did in Section 6.1, our intention is to prove that the hypotheses of Theorem 6.9 are typical of almost all recursions with root field $\mathbb{Q}(\sqrt{-3})$. We first indicate what we mean by 'almost all'.

We begin with some formal definition.

Definition. We say that $x^2 - Px + Q \in \mathbb{Z}[x]$ is a $\mathbb{Q}(\omega)$-*recursion* whenever the root field of $x^2 - Px + Q$ is $\mathbb{Q}(\omega)$. Such a recursion is said to be *S-generic* whenever Q cannot be written as either a square times the cube of an integer having all its prime factors 1 (mod 3), or three times a square times such a cube.

Since there is a 1-to-2 correspondence between $\mathbb{Q}(\omega)$-recursions and pairs (P, F) of integers with $P \equiv F \pmod 2$ and $F \neq 0$, where a $\mathbb{Q}(\omega)$-recursion $x^2 - Px + Q$ of

discriminant $-3F^2$ corresponds to the two pairs $(P, \pm F)$, and since the number of *x-bounded* such pairs (P, F), i.e., for which $|P| \le x$ and $|F| \le x$, is asymptotic to $2x^2$ as $x \to \infty$, we define formally what the expression 'almost all' means within the set of $\mathbb{Q}(\omega)$-recursions.

DEFINITION. A property will be said to hold for *almost all* $\mathbb{Q}(\omega)$-recursions $x^2 - Px + Q$, where $Q = (P^2 + 3F^2)/4$, if the number of pairs $(P, F) \in \mathbb{Z}^2$, $|P| \le x$ and $|F| \le x$, for which the property is not satisfied, is $o(x^2)$ as x goes to infinity.

We are now ready to prove a theorem that shows that Theorem 6.9 is true for almost all $\mathbb{Q}(\omega)$-recursions.

THEOREM 6.10. *Almost all $\mathbb{Q}(\omega)$-recursions are S-generic. In fact, the number of x-bounded $\mathbb{Q}(\omega)$-recursions such that $P^2 + 3F^2$ is of the form $\lambda n_1^3 n^2$, where n_1 and n are integers and λ equal to 1 or 3, is $o(x^{5/3+\eta})$, for any $\eta > 0$.*

Proof. Given $\eta > 0$, we wish to prove that $\mathcal{N}^*(x)$, the number of pairs (P, F), $P \equiv F \pmod 2$, $|P| \le x$, $1 \le |F| \le x$ such that $P^2 + 3F^2$ is of the form $n_1^3 n^2$ or $3n_1^3 n^2$, is $o(x^{5/3+\eta})$ as $x \to \infty$. Put $y = 2x$. Note that $P^2 + 3F^2$ is $\le 4x^2 = y^2$. By Proposition 6.4, $r^*(n_1^3 n^2) = r^*(3n_1^3 n^2)$. The estimation we are about to establish is obtained regardless of the restriction on the prime factors of n_1 that characterize $\mathbb{Q}(\omega)$-recursions that are not S-generic. Now, using Proposition 6.4, we have

$$\mathcal{N}^*(x) \le 2 \sum_{n_1^3 n^2 \le y^2} r^*(n_1^3 n^2) \le 12 \sum_{n_1^3 n^2 \le y^2} d(n_1^3 n^2) \le 12 \sum_{n_1^3 n^2 \le y^2} d((n_1 n)^3)$$

$$= 12 \sum_{n=1}^{y} \sum_{n_1=1}^{(y/n)^{2/3}} d((n_1 n)^3) \le 12 \sum_{n=1}^{y} \sum_{t=1}^{y^{2/3}} d(t^3) \le 12y \sum_{t=1}^{y^{2/3}} d(t^3),$$

which, by Lemma 6.1, is $12y \times o(y^{2/3+\eta}) = o(x^{5/3+\eta})$. Taking $\eta = 1/3$ shows that almost all $\mathbb{Q}(\omega)$-recursions are S-generic. ∎

6.3. Prime densities heuristically. Simple heuristic arguments could have helped us guess at the densities of generic V and G sequences for $-E^2$ discriminants, as well as at densities of the generic V, S and Z sequences of $-3F^2$ discriminants. We briefly present these heuristic calculations here.

6.3.1. Density heuristics for $-E^2$ discriminants. Given an $\epsilon = \pm 1$ and a $j \ge 2$, we consider the primes p in S_j^σ, where σ is the sign of ϵ. Recall that the Dirichlet density theorem for primes in arithmetic progressions allowed us to conclude that each S_j^σ possesses a prime density $d_j^\sigma = 2^{-j}$. Given a prime p in S_j^σ, the probability that $2 \nmid \rho(p)$, that is, the probability that r be of odd order modulo (p) is proportional to the number of non-zero residue classes of odd order modulo p, which is $(p - \epsilon)/2^j$. Note that when $\epsilon = -1$, we used the fact that ρ must divide $p + 1$, so we calculated the proportion of such residues within the subgroup of order $p + 1$ of the multiplicative cyclic group of the finite field $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_{p^2}$. Thus, we have $\mathrm{Prob}_{j,\epsilon}\{2 \nmid \rho\} = 2^{-j}$, which is independent

of ϵ ([2]). Similarly, the probability that $4 \nmid \rho$, i.e., that $p \nmid G$, is $(p-\epsilon)/2^{j-1}$ divided by $p-\epsilon$, since there are $(p-\epsilon)/2^{j-1}$ residue classes modulo (p) whose order is either odd, or divisible by 2, but not by 4.

Thus, the expected density of primes not dividing V is

$$\sum_{\substack{j\geq 2\\ \epsilon=\pm 1}} d_j^\sigma \cdot \ \mathrm{Prob}_{j,\epsilon}\{2 \nmid \rho\} = 2\sum_{j\geq 2} 2^{-j}\cdot 2^{-j} = 1/6,$$

so that we expect $\delta(V)$ to be $1-1/6 = 5/6$, which corresponds to the density of a G-generic V sequence.

Similarly, the expected density of primes not dividing G is

$$\sum_{\substack{j\geq 2\\ \epsilon=\pm 1}} d_j^\sigma \cdot \ \mathrm{Prob}_{j,\epsilon}\{4 \nmid \rho\} = 2\sum_{j\geq 2} 2^{-j}\cdot 2^{-j+1} = 1/3,$$

yielding accurately, according to Theorem 6.2, $\delta(G) = 2/3$.

6.3.2. Density heuristics for the $-3F^2$ discriminants. Fix an $\epsilon = \pm 1$, a j and a k both ≥ 1. Using the notation of the proof of Theorem 6.9, we wish to evaluate heuristically the proportion of primes in $C = \{p;\, 6 \nmid \rho(p)\}$, i.e., of primes not dividing Z, among primes in $I_{j,k}^\sigma$, where σ is the sign of ϵ, and $I_{j,k}^\sigma$ is the set of primes p with $\epsilon_p = \epsilon$, $2^j \,\|\, p-\epsilon$ and $3^k \,\|\, p-\epsilon$. The density $d_{j,k}^\sigma$ of $I_{j,k}^\sigma$ exists and equals $2/\varphi(2^{j+1}\cdot 3^{k+1})$ by the Dirichlet density theorem for primes in arithmetic progressions. Indeed, primes p satisfying both $2^j \,\|\, p-\epsilon$ and $3^k \,\|\, p-\epsilon$ form two disjoint arithmetic progressions with common difference $2^{j+1}\cdot 3^{k+1}$. Thus, $d_{j,k}^\sigma = 2^{-j}\cdot 3^{-k}$, for each value of ϵ. For primes in $I_{j,k}^\sigma$, the probability that $6 \nmid \rho$ is equal to the probability that $2 \nmid \rho$ plus the probability that $3 \nmid \rho$ minus the probability that neither 2 nor 3 divides ρ. We may estimate the probabilities that $2 \nmid \rho$ and $3 \nmid \rho$ for primes in $I_{j,k}^\sigma$ as

$$\mathrm{Prob}_{j,k,\epsilon}\{2 \nmid \rho\} = \frac{1}{p-\epsilon}\cdot\frac{p-\epsilon}{2^j} = 2^{-j},$$
$$\mathrm{Prob}_{j,k,\epsilon}\{3 \nmid \rho\} = \frac{1}{p-\epsilon}\cdot\frac{p-\epsilon}{3^k} = 3^{-k}.$$

Indeed, either $\epsilon = 1$ and, except for the finitely many primes dividing Q, r belongs to the multiplicative cyclic group of integers modulo p, or $\epsilon = -1$ and, since ρ divides $p+1$, r belongs to the subgroup of order $p+1$ of the multiplicative group of algebraic integers of the finite field $\mathbb{Z}[\omega]/(p) \simeq \mathbb{F}_{p^2}$. Thus, $(p-\epsilon)/2^j$, or $(p-\epsilon)/3^k$, represent the number of potential residues of orders prime to 2, or, respectively, to 3, that r may take modulo p. Therefore, assuming independence of the two events $2 \nmid \rho$ and $3 \nmid \rho$, we find that

$$\mathrm{Prob}_{j,k,\epsilon}\{6 \nmid \rho\} = 2^{-j} + 3^{-k} - 2^{-j}\cdot 3^{-k}.$$

Note that it does not depend on ϵ. The weight associated with the probability $\mathrm{Prob}_{j,k,\epsilon}\{6\nmid\rho\}$, for fixed j, k and ϵ, should be equal to the density of primes in $I_{j,k}^\sigma$.

([2]) These heuristics are not assumption-free. They are valid for a generic r. For instance here we assume Q is not a square, or else $r = \alpha^2/Q$ is a square in $\mathbb{Z}/p$, or in $\mathbb{Z}[i]/(p)$ and the probability that its order be odd would be at least 2^{1-j}.

Thus, the density of primes p not dividing Z should be

$$\sum_{\substack{j,k\geq 1\\ \epsilon=\pm 1}} d^{\sigma}_{j,k}\cdot\ \mathrm{Prob}_{j,k,\epsilon}\{6\nmid\rho\} = 2\sum_{j,k\geq 1} 2^{-j}\cdot 3^{-k}\cdot(2^{-j}+3^{-k}-2^{-j}\cdot 3^{-k})$$
$$= 2\sum_{k\geq 1} 9^{-k} + 2\sum_{j\geq 1} 4^{-j}\cdot\sum_{k\geq 1} 3^{-k} - 2\sum_{j\geq 1} 4^{-j}\cdot\sum_{k\geq 1} 9^{-k}$$
$$= 2\times\left[\frac{1}{8}+\frac{1}{3}\cdot\frac{1}{2}-\frac{1}{3}\cdot\frac{1}{8}\right] = \frac{1}{2}.$$

Therefore, the expected density of the Z sequence is $1-1/2=1/2$.

The heuristic density for V sequences corresponding to discriminants $-3F^2$ would be identical to that given in [2], i.e., $2/3$, and does not need to be re-calculated. The expected heuristic density of S sequences, with notation that should now speak up for itself, is

$$\delta(S) = 1-\sum_{\substack{k\geq 1\\ \epsilon=\pm 1}} d^{\sigma}_{k}\cdot\ \mathrm{Prob}_{k,\epsilon}\{3\nmid\rho\}$$
$$= 1-2\sum_{k\geq 1} 3^{-k}\cdot 3^{-k} = 1-2\sum_{k\geq 1} 9^{-k} = 1-1/4 = 3/4.$$

These densities are those of Theorem 6.9.

References

[1] C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. 551 (1995), 102 pp.

[2] C. Ballot, *On the* 1/3 *density of odd ranked primes in Lucas sequences*, Unif. Distrib. Theory 3 (2008), 129–145.

[3] C. Ballot, *Strong arithmetic properties of the integral solutions of* $X^3 + DY^3 + D^2Z^3 - 3DXYZ = 1$*, where* $D = M^3 \pm 1$*,* $M \in \mathbb{Z}^*$, Acta Arith. 89 (1999), 259–277.

[4] C. Ballot, *A further generalization of a congruence of Wolstenholme*, J. Integer Seq. 15 (2012), no. 8, art. 12.8.7, 16 pp.

[5] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) 15 (1913–14), 30–48, 49–70.

[6] D. A. Cox, *Primes of the Form* $x^2 + ny^2$*: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, 1989.

[7] H. Davenport, *The Higher Arithmetic. An Introduction to the Theory of Numbers*, Dover Publ., New York, 1983.

[8] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer, New York, 1985.

[9] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Clarendon Press, Oxford, 1960.

[10] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 225 (1967), 209–220.

[11] G. J. Janusz, *Algebraic Number Fields*, Pure Appl. Math. 55, Academic Press, New York, 1973.

[12] W. Kimball and W. Webb, *Some generalizations of Wolstenholme's theorem*, in: Applications of Fibonacci Numbers, Vol. 8 (Rochester, NY, 1998), Kluwer, Dordrecht, 1999, 213–18.

[13] J. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. 118 (1985), 449–461; Errata, ibid. 162 (1994), 393–397.

[14] R. Laxton, *On groups of linear recurrences I*, Duke Math. J. 26 (1969), 721–736.

[15] R. Laxton, *On groups of linear recurrences II. Elements of finite order*, Pacific J. Math. 32 (1970), 173–179.

[16] É. Lucas, *Théorie des fonctions simplement périodiques*, Amer. J. Math. 1 (1878), 184–240, 289–321.

[17] É. Lucas, *Théorie des Nombres*, Tome I, Albert Blanchard, 1961.

[18] D. A. Marcus, *Number Fields*, Springer, New York, 1977.

[19] S. Müller, E. Roettger and H. Williams, *A cubic extension of the Lucas functions*, Ann. Sci. Math. Québec 33 (2009), 185–224.

[20] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN–Polish Sci. Publ., Warszawa, 1974.

[21] P. Ribenboim, *The Fibonacci numbers and the Arctic Ocean*, in: Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics (Munich, 1993), Sympos. Gaussiana, de Gruyter, Berlin, 1995, 41–83.

[22] A. Schinzel, *On the linear dependence of roots*, Acta Arith. 28 (1975), 161–175.
[23] L. Somer, *Divisibility of terms in Lucas sequences by their subscripts*, in: Applications of Fibonacci Numbers, Vol. 5 (St. Andrews, 1992), Kluwer, Dordrecht, 1993, 515–525.
[24] L. Somer, *Divisibility of terms in Lucas sequences of the second kind by their subscripts*, in: Applications of Fibonacci Numbers, Vol. 6 (Pullman, WA, 1994), Kluwer, Dordrecht, 1996, 473–86.
[25] C. Smyth, *The terms in Lucas sequences divisible by their indices*, J. Integer Seq. 13 (2010), art. 10.2.4, 18 pp.
[26] W. Vélez, *Several results on radical extensions*, Arch. Math. (Basel) 45 (1985), 342–349.
[27] M. Ward, *The prime divisors of Fibonacci numbers*, Pacific J. Math. 11 (1961), 379–386.
[28] H. C. Williams, *A generalization of the Lucas functions*, unpublished Ph.D. thesis, Univ. of Waterloo, Ont., 1969.
[29] H. C. Williams, *Some properties of a special set of recurring sequences*, Pacific J. Math. 77 (1978), 273–285.
[30] H. C. Williams, *Édouard Lucas and Primality Testing*, Canad. Math. Soc. Ser. Monogr. Adv. Texts, Wiley, 1998.
[31] J. Wolstenholme, *On certain properties of prime numbers*, Quart. J. Pure Appl. Math. 5 (1862), 35–39.

List of symbols and vocabulary

ζ_n denotes the complex number $e^{2i\pi/n}$
ω is equal to ζ_6
α, $\bar{\alpha}$ 15, 18
r is equal to $\alpha/\bar{\alpha}$
U_n, V_n 5
G_n, H_n 15
S_n, T_n, Y_n, Z_n 18, 19
D discriminant $P^2 - 4Q$ of $x^2 - Px + Q$
ϵ_p 6, 25
ρ_X, $\rho_X(p)$: rank of p in the sequence X 25
ρ, $\rho(m)$: rank of m 25
$m \mid n$ means that m divides n
$d \mid x$, with d an integer and x a rational 10, 43
$p^a \parallel n$: p^a divides n and p^{a+1} does not divide n
$\nu_p(n) = a$ means that $p^a \parallel n$
$\sim_p$ 37
$:=$ 'is by definition equal to'
$\pi(x)$ prime counting function 74
$d(\cdot)$ number of divisors function
$\ll$ usual Vinogradov symbol
$o(f)$ Landau symbol, little o of f
$\delta(X)$ 74
$r(\cdot)$ 79
$r^*(\cdot)$ 80
$\#A$ cardinality of A
S_j^+, $D_j^+(V)$, S_j^-, $D_j^-(V)$ 76
$D_j^+(G)$, $D_j^-(G)$, L_j^*, K_j^* 76
T_j^+, $D_j^+(S)$, T_j^-, $D_j^-(S)$ 81
N_j, M_j 81
special prime 23, 55
X-basic 55
cross-over 56
GH-basic 59
ST-basic 64
YZ-basic 69
generic recursion 74
G-generic recursion 79
S-generic recursion 86
$\mathbb{Q}(i)$-recursion 79
$\mathbb{Q}(\omega)$-recursion 86