p-adic quotient sets

by

Stephan Ramon Garcia (Claremont, CA),
Yu Xuan Hong (Claremont, CA),
Florian Luca (Johannesburg, Bonn and Ostrava),
Elena Pinsker (Claremont, CA), Carlo Sanna (Torino),
Evan Schechter (Claremont, CA) and Adam Starr (Claremont, CA)

1. Introduction. For $A \subseteq \mathbb{N} = \{1, 2, \ldots\}$ let $R(A) = \{a/a' : a, a' \in A\}$ denote the corresponding *ratio set* (or *quotient set*). The question of when $R(A)$ is dense in the positive real numbers $\mathbb{R}_+$ has been examined by many authors over the years [3, 4, 5, 6, 7, 13, 18, 19, 22, 23, 24, 26, 30, 31, 35, 36, 37]. Analogues in the Gaussian integers [11] and, more generally, in imaginary quadratic number fields [34] have also been considered.

Since $R(A)$ is a subset of the rational numbers $\mathbb{Q}$, there are other important metrics that can be considered. Fix a prime number p and observe that each nonzero rational number has a unique representation of the form $r = \pm p^k a/b$, in which $k \in \mathbb{Z}$, $a, b \in \mathbb{N}$ and $(a, p) = (b, p) = (a, b) = 1$. The *p-adic valuation* of such an r is $\nu_p(r) = k$ and its *p-adic absolute value* is $\|r\|_p = p^{-k}$. By convention, $\nu_p(0) = \infty$ and $\|0\|_p = 0$. The *p-adic metric* on $\mathbb{Q}$ is $d(x, y) = \|x - y\|_p$. The field $\mathbb{Q}_p$ of *p-adic numbers* is the completion of $\mathbb{Q}$ with respect to the p-adic metric. Further information can be found in [14, 20].

Garcia and Luca [12] recently proved that the set of quotients of Fibonacci numbers is dense in $\mathbb{Q}_p$ for all p. Their result has been extended by Sanna [33], who proved that the quotient set of the k-generalized Fibonacci numbers is dense in $\mathbb{Q}_p$, for all integers $k \geq 2$ and primes p. Other than these isolated results, the study of quotient sets in the p-adic setting appears largely neglected. We seek here to initiate the general study of p-adic quotient sets. Techniques from elementary, algebraic, and analytic number

theory are employed in this endeavor. We also pose many open questions that should be of general interest.

Section 2 introduces several simple, but effective, lemmas. In Section 3, we compare and contrast the p-adic setting with the "real setting." The potential p-adic analogues (or lack thereof) of known results from the real setting are discussed.

Sums of powers are studied in Section 4. Theorem 4.1 completely describes for which m and primes p the ratio set of $\{x_1^2 + \cdots + x_m^2 : x_i \geq 0\}$ is dense in $\mathbb{Q}_p$. Cubes are considerably trickier; Theorem 4.2 gives the somewhat surprising answer.

In Section 5, we consider sets whose elements are generated by a second-order recurrence. Theorem 5.2 provides an essentially complete answer for recurrences of the form $a_{n+2} = r a_{n+1} + s a_n$ with $a_0 = 0$ and $a_1 = 1$. Examples are given that demonstrate the sharpness of our result.

Fibonacci and Lucas numbers are considered in Corollary 5.3, which recovers the main result of [12]: the set of quotients of Fibonacci numbers is dense in each $\mathbb{Q}_p$. The situation for Lucas numbers is strikingly different: the set of quotients of Lucas numbers is dense in $\mathbb{Q}_p$ if and only if $p \neq 2$ and p divides a Lucas number.

In Section 6, we examine certain unions of arithmetic progressions. For instance, the ratio set of $A = \{5^j : j \geq 0\} \cup \{7^j : j \geq 0\}$ is dense in $\mathbb{Q}_7$ but not in $\mathbb{Q}_5$. This sort of asymmetry is not unusual. Section 7 is devoted to the proof of Theorem 6.3, which asserts that there are infinitely many pairs of primes (p, q) such that p is not a primitive root modulo q while q is a primitive root modulo p^2. The proof is somewhat technical and involves a sieve lemma due to Heath-Brown, along with a little heavy machinery in the form of the Brun–Titchmarsh and Bombieri–Vinogradov theorems. The upshot of Theorem 6.3 is that there are infinitely many pairs of primes (p, q) so that the ratio set of $\{p^j : j \geq 0\} \cup \{q^k : k \geq 0\}$ is dense in $\mathbb{Q}_p$ but not in $\mathbb{Q}_q$. A number of related questions are posed at the end of Section 6.

2. Preliminaries. We collect here a few preliminary observations and lemmas that will be fruitful in what follows. Although these observations are all elementary, we state them explicitly as lemmas since we will refer to them frequently.

LEMMA 2.1. *If S is dense in $\mathbb{Q}_p$, then for each finite value of the p-adic valuation, there is an element of S with that valuation.*

Proof. If $q \in \mathbb{Q}_p^\times$ can be arbitrarily well approximated with elements of S, then there is a sequence $s_n \in S$ such that $|p^{-\nu_p(s_n)} - p^{-\nu_p(q)}| = \big| \|s_n\|_p - \|q\|_p \big| \leq \|s_n - q\|_p \to 0$. On $\mathbb{Q}^\times$, the p-adic valuation assumes only integral values, so $\nu_p(s_n)$ eventually equals $\nu_p(q)$. ∎

The converse of the preceding lemma is false as $S = \{p^k : k \in \mathbb{Z}\}$ demonstrates. More generally, we have the following lemma.

LEMMA 2.2. *If A is a geometric progression in $\mathbb{Z}$, then $R(A)$ is not dense in any $\mathbb{Q}_p$.*

Proof. If $A = \{cr^n : n \geq 0\}$, in which c and r are nonzero integers, then $R(A) = \{r^n : n \in \mathbb{Z}\}$. Let p be a prime. If $p \nmid r$, then $R(A)$ is not dense in $\mathbb{Q}_p$ by Lemma 2.1. If $p \mid r$, then $r^k \equiv -1 \pmod{p^2}$ is impossible since -1 is a unit modulo p. Thus, $R(A)$ is bounded away from -1 in $\mathbb{Q}_p$. ∎

To simplify our arguments, we frequently appeal to the "transitivity of density." That is, if X is dense in Y and Y is dense in Z, then X is dense in Z. This observation is used in conjunction with the following lemma.

LEMMA 2.3. *Let $A \subseteq \mathbb{N}$.*

(a) *If A is p-adically dense in $\mathbb{N}$, then $R(A)$ is dense in $\mathbb{Q}_p$.*
(b) *If $R(A)$ is p-adically dense in $\mathbb{N}$, then $R(A)$ is dense in $\mathbb{Q}_p$.*

Proof. (a) If A is p-adically dense in $\mathbb{N}$, it is p-adically dense in $\mathbb{Z}$. Inversion is continuous on $\mathbb{Q}_p^\times$, so $R(A)$ is p-adically dense in $\mathbb{Q}$, which is dense in $\mathbb{Q}_p$.

(b) Suppose that $R(A)$ is p-adically dense in $\mathbb{N}$. Since inversion is continuous on $\mathbb{Q}_p^\times$, the result follows from the fact that $\mathbb{N}$ is p-adically dense in $\{x \in \mathbb{Q} : \nu_p(x) \geq 0\}$. ∎

Although the hypothesis of (a) implies the hypothesis of (b), we have stated them separately. We prefer to use (a) whenever possible. We turn to (b) when confronted with problems that do not succumb easily to (a). This can occur since the hypothesis of (a) is not necessary for $R(A)$ to be dense in $\mathbb{Q}_p$. If A is the set of even numbers, then $R(A) = \mathbb{Q}$ is dense in $\mathbb{Q}_p$ for all p, but A is not 2-adically dense in $\mathbb{N}$. The following lemma concerns more general arithmetic progressions.

LEMMA 2.4. *Let $A = \{an + b : n \geq 0\}$.*

(a) *If $p \nmid a$, then $R(A)$ is dense in $\mathbb{Q}_p$.*
(b) *If $p \mid a$ and $p \nmid b$, then $R(A)$ is not dense in $\mathbb{Q}_p$.*

Proof. (a) Let $p \nmid a$ and let $n \in \mathbb{N}$ be arbitrary. If $r \geq 1$, let $i \equiv a^{-1}(n-b) \pmod{p^r}$ so that $ai + b \equiv n \pmod{p^r}$. Then A is p-adically dense in $\mathbb{N}$, so $R(A)$ is dense in $\mathbb{Q}_p$ by Lemma 2.3.

(b) If $p \mid a$ and $p \nmid b$, then $\nu_p(an+b) = 0$ for all n. Thus, $R(A)$ is not dense in $\mathbb{Q}_p$ by Lemma 2.1. ∎

3. Real versus p-adic setting. A large amount of work has been dedicated to studying the behavior of quotient sets in the "real setting." By this, we refer to work focused on determining conditions upon A which

ensure that $R(A)$ is dense in $\mathbb{R}_+$. Accordingly, we begin our investigations by examining the extent to which known results in the real setting remain valid in the p-adic setting.

3.1. Independence from the real case. The behavior of a quotient set in the p-adic setting is essentially independent from its behavior in the real setting. To be more specific, a concrete example exists for each of the four statements of the form "$R(A)$ is (dense/not dense) in every $\mathbb{Q}_p$ and (dense/not dense) in $\mathbb{R}_+$."

(a) Let $A = \mathbb{N}$. Then $R(A)$ is dense in every $\mathbb{Q}_p$ and dense in $\mathbb{R}_+$.
(b) Let $F = \{1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots\}$ denote the set of Fibonacci numbers. Then $R(F)$ is dense in each $\mathbb{Q}_p$ (cf. [12]); see Theorem 5.2 for a more general result. On the other hand, Binet's formula ensures that $R(F)$ accumulates only at integral powers of the golden ratio, so $R(F)$ is not dense in $\mathbb{R}_+$.
(c) Let $A = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$ denote the set of prime numbers. The p-adic valuation of a quotient of primes belongs to $\{-1, 0, 1\}$, so Lemma 2.1 ensures that $R(A)$ is not dense in any $\mathbb{Q}_p$. The density of $R(A)$ in $\mathbb{R}_+$ is a well known consequence of the prime number theorem: see [9, Problem 218], [10, Ex. 4.19], [13, Cor. 4], [19, Thm. 4], [27, Ex. 7, p. 107], [29, Thm. 4], [35, Cor. 2] (this last result dates back at least to Sierpiński, who attributed it to Schinzel [26]).
(d) Let $A = \{2, 6, 30, 210, \ldots\}$ denote the set of *primorials*; the nth primorial is the product of the first n prime numbers. The p-adic valuation of a quotient of primorials belongs to $\{-1, 0, 1\}$, so Lemma 2.1 ensures that $R(A)$ is not dense in any $\mathbb{Q}_p$. Moreover, $R(A) \cap [1, \infty) \subseteq \mathbb{N}$, so $R(A)$ is not dense in $\mathbb{R}_+$.

3.2. Independence across primes. Not only is the behavior of a quotient set in the p-adic setting unrelated to its behavior in the real setting, the density of a quotient set in one p-adic number system is completely independent, in a very strong sense, from its density in another.

THEOREM 3.1. *For each set P of prime numbers, there is an $A \subseteq \mathbb{N}$ such that $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p \in P$.*

Proof. Let P be a set of prime numbers, let Q be the set of prime numbers not in P, and let $A = \{a \in \mathbb{N} : \nu_q(a) \leq 1 \ \forall q \in Q\}$. Lemma 2.1 ensures that $R(A)$ is not dense in $\mathbb{Q}_q$ for any $q \in Q$. Fix $p \in P$, let $\ell \geq 0$, and let $n = p^k m \in \mathbb{N}$ with $p \nmid m$. Dirichlet's theorem on primes in arithmetic progressions provides a prime of the form $r = p^\ell j + m$. Then $p^k r \in A$ and $p^k r \equiv p^k(p^\ell j + m) \equiv p^k m \equiv n \pmod{p^\ell}$. Since n was arbitrary, Lemma 2.3 ensures that $R(A)$ is dense in $\mathbb{Q}_p$. ∎

3.3. Arithmetic progressions. There exists a set $A \subseteq \mathbb{N}$ which contains arbitrarily long arithmetic progressions and such that $R(A)$ is not dense in $\mathbb{R}_+$ [3, Prop. 1]. On the other hand, there exists a set A that contains no arithmetic progressions of length three and such that $R(A)$ is dense in $\mathbb{R}_+$ [3, Prop. 6]. The same results hold, with different examples, in the p-adic setting.

EXAMPLE 3.2 (Arbitrarily long arithmetic progressions). The celebrated Green–Tao theorem asserts that the set of primes contains arbitrarily long arithmetic progressions [15]. However, its ratio set is dense in no $\mathbb{Q}_p$ (see (c) in Section 3.1).

A set without long arithmetic progressions can have a quotient set that is dense in some $\mathbb{Q}_p$. Consider the set $A = \{2^n : n \geq 2\} \cup \{3^n : n \geq 2\}$, which contains no arithmetic progressions of length three [3]. The upcoming Theorem 6.1 implies that $R(A)$ is dense in $\mathbb{Q}_3$. One can confirm that $R(A)$ is bounded away from 5 in $\mathbb{Q}_2$, so $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p = 3$. However, we can do much better.

THEOREM 3.3. *There is a set $A \subseteq \mathbb{N}$ that contains no arithmetic progression of length three and which is dense in each $\mathbb{Q}_p$.*

Proof. Fix an enumeration (q_n, r_n) of the set of all pairs (q, r) in which q is a prime power and $0 \leq r < q$; observe that each of the pairs $(q, 0), (q, 1),$ $\ldots, (q, q - 1)$ appears exactly once in this enumeration. Construct A, initially empty, according to the following procedure. Include the first natural number a_1 for which $a_1 \equiv r_1 \pmod{q_1}$, then include the first a_2 such that $a_2 > a_1$ and $a_2 \equiv r_2 \pmod{q_2}$. Next, select $a_3 > a_2$ such that $a_3 \equiv r_3 \pmod{q_3}$ and such that a_1, a_2, a_3 is not an arithmetic progression of length three. Continue in this manner, so that a natural number $a_n > a_{n-1}$ is produced in the nth stage such that $a_n \equiv r_n \pmod{q_n}$ and $a_1, \ldots, a_n$ contains no arithmetic progression of length three. Since $A = \{a_n : n \geq 1\}$ contains a complete set of residues modulo each prime power, it is p-adically dense in $\mathbb{N}$ for each prime p. Thus, $R(A)$ is dense in each $\mathbb{Q}_p$ by Lemma 2.3. By construction, A contains no arithmetic progression of length three. ∎

3.4. Asymptotic density. For $A \subseteq \mathbb{N}$, define $A(x) = A \cap [1, x]$. Then $|A(x)|$ denotes the number of elements in A that are at most x. The *lower asymptotic density* of A is

$$\underline{d}(A) = \liminf_{n \to \infty} \frac{|A(n)|}{n}$$

and the *upper asymptotic density* of A is

$$\overline{d}(A) = \limsup_{n \to \infty} \frac{|A(n)|}{n}.$$

If $\underline{d}(A) = \overline{d}(A)$, then their common value is denoted $d(A)$ and called the *asymptotic density* (or *natural density*) of A. In this case, $d(A) = \lim_{n\to\infty} |A(n)|/n$. Clearly $0 \leq \underline{d}(A) \leq \overline{d}(A) \leq 1$.

A striking result of Strauch and Tóth is that if $\underline{d}(A) \geq 1/2$, then $R(A)$ is dense in $\mathbb{R}_+$ [36] (see also [3] for a detailed exposition). That is, $1/2$ is a critical threshold in the sense that any subset of $\mathbb{N}$ that contains at least half of the natural numbers has a quotient set that is dense in $\mathbb{R}_+$. On the other hand, the critical threshold in the p-adic setting is 1.

THEOREM 3.4.

(a) *If* $\overline{d}(A) = 1$, *then* $R(A)$ *is dense in each* $\mathbb{Q}_p$.
(b) *For each* $\alpha \in [0,1)$, *there is an* $A \subseteq \mathbb{N}$ *such that* $R(A)$ *is dense in no* $\mathbb{Q}_p$ *and* $\underline{d}(A) \geq \alpha$.

Proof. (a) Suppose that $\overline{d}(A) = 1$. If A contained no representative from some congruence class modulo a prime power p^r, then $\overline{d}(A) \leq 1 - 1/p^r < 1$, a contradiction. Thus, A contains a representative from every congruence class modulo each prime power p^r. Let $n, r \in \mathbb{N}$ and select $a, b \in A$ so that $a \equiv n \pmod{p^r}$ and $b \equiv 1 \pmod{p^r}$. Then $a \equiv bn \pmod{p^r}$, and hence $\nu_p(a/b - n) = \nu_p(a - bn) \geq r$. Thus, $R(A)$ is dense in $\mathbb{Q}_p$ by Lemma 2.3.

(b) Let $\alpha \in (0,1)$, let p_n denote the nth prime number, and let r_n be so large that $2^n \leq (1 - \alpha)p_n^{r_n}$ for $n \geq 1$. If
$$A = \{a \in \mathbb{N} : \nu_{p_n}(a) \leq r_n \ \forall n\},$$
then $R(A)$ is dense in no $\mathbb{Q}_p$ by Lemma 2.1. Since A omits every multiple of $p_n^{r_n}$,
$$\underline{d}(A) \geq 1 - \sum_{n=1}^{\infty} \frac{1}{p_n^{r_n}} \geq 1 - \sum_{n=1}^{\infty} \frac{(1-\alpha)}{2^n} = \alpha. \ \blacksquare$$

It is also known that if $\underline{d}(A) + \overline{d}(A) \geq 1$, then $R(A)$ is dense in $\mathbb{R}_+$ [36, p. 71]. The p-adic analogue is false: for $\alpha \geq 1/2$, the set A from Theorem 3.4(b) satisfies $\underline{d}(A) + \overline{d}(A) \geq 1$ and is dense in no $\mathbb{Q}_p$. On the other extreme, we have the following theorem.

THEOREM 3.5. *There is an* $A \subseteq \mathbb{N}$ *with* $d(A) = 0$ *for which* $R(A)$ *dense in every* $\mathbb{Q}_p$.

Proof. Let q_n denote the increasing sequence $2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, \ldots$ of prime powers. Construct A according to the following procedure. Add the first q_1 numbers to A (that is, $1, 2 \in A$) and skip the next $q_1!$ numbers (that is, $3, 4 \notin A$). Then add the next q_2 numbers to A (that is, $5, 6, 7 \in A$) and skip the next $q_2!$ numbers (that is, $8, 9, 10, 11, 12, 13 \notin A$). The rapidly increasing sizes of the gaps between successive blocks of elements of A ensure that $d(A) = 0$. Since A contains arbitrarily long blocks of consecutive integers, it contains a complete set of residues modulo each q_n.

Thus, A is p-adically dense in $\mathbb{N}$ for each prime p, and hence $R(A)$ is dense in each $\mathbb{Q}_p$ by Lemma 2.3. ∎

3.5. Partitions of $\mathbb{N}$**.** If $\mathbb{N} = A \sqcup B$, then at least one of $R(A)$ or $R(B)$ is dense in $\mathbb{R}_+$ [6]; this is sharp in the sense that there exists a partition $\mathbb{N} = A \sqcup B \sqcup C$ such that none of $R(A)$, $R(B)$, and $R(C)$ is dense in $\mathbb{R}_+$. See [3] for a detailed exposition of these results. Things are different in the p-adic setting.

EXAMPLE 3.6. Fix a prime p and let

$$A = \{p^j n \in \mathbb{N} : j \text{ even}, (n, p) = 1\}, \qquad B = \{p^j n \in \mathbb{N} : j \text{ odd}, (n, p) = 1\}.$$

Then $A \cap B = \emptyset$, but neither $R(A)$ nor $R(B)$ is dense in $\mathbb{Q}_p$ by Lemma 2.1.

PROBLEM 3.7. *Is there a partition* $\mathbb{N} = A \sqcup B$ *such that* A *and* B *are dense in no* $\mathbb{Q}_p$*?*

4. Sums of powers. The representation of integers as the sum of squares dates back to antiquity, although this study only truly flowered with the work of Fermat, Lagrange, and Legendre. Later authors studied more general quadratic forms and also representations of integers as sums of higher powers. From this perspective, it is natural to consider the following family of problems. Let

$$A = \{a \in \mathbb{N} : a = x_1^n + x_2^n + \cdots + x_m^n, \ x_i \geq 0\}.$$

For what m, n, and p is $R(A)$ dense in $\mathbb{Q}_p$? For squares and cubes, Theorems 4.1 and 4.2 provide complete answers.

THEOREM 4.1. *Let* $S_n = \{a \in \mathbb{N} : a \text{ is the sum of } n \text{ squares, with } 0 \text{ permitted}\}$.

(a) $R(S_1)$ *is not dense in any* $\mathbb{Q}_p$.
(b) $R(S_2)$ *is dense in* $\mathbb{Q}_p$ *if and only if* $p \equiv 1 \pmod 4$.
(c) $R(S_n)$ *is dense in* $\mathbb{Q}_p$ *for all* p *whenever* $n \geq 3$.

Proof. (a) Let p be a prime. Then $2 \mid \nu_p(s)$ for all $s \in S_1$, and hence $R(S_1)$ is dense in no $\mathbb{Q}_p$ by Lemma 2.1.

(b) There are three cases to consider: (b1) $p = 2$; (b2) $p \equiv 1 \pmod 4$; (b3) $p \equiv 3 \pmod 4$.

(b1) Since $\nu_2(3) = 0$, any element $a/b \in R(S_2)$ that is sufficiently close in $\mathbb{Q}_2$ to 3 must have $\nu_2(a) = \nu_2(b)$. Without loss of generality, we may assume that a and b are odd. Then $a \equiv b \equiv 1 \pmod 4$ since $a, b \in S_2$, so $a \equiv 3b \pmod 4$ is impossible. Thus, $R(S_2)$ is bounded away from 3 in $\mathbb{Q}_2$.

(b2) Let $p \equiv 1 \pmod 4$. By Lemma 2.3, it suffices to show that for each $n \geq 0$ and $r \geq 1$, the congruence $x^2 + y^2 \equiv n \pmod{p^r}$ has a solution with $p \nmid x$. We proceed by induction on r. Since there are precisely $(p + 1)/2$ quadratic residues modulo p, the sets $\{x^2 : x \in \mathbb{Z}/p\mathbb{Z}\}$ and

$\{n - y^2 : y \in \mathbb{Z}/p\mathbb{Z}\}$ have a nonempty intersection. Thus, $x^2 + y^2 \equiv n \pmod{p}$ has a solution. If $p \nmid n$, then p cannot divide both x and y; in this case we may assume that $p \nmid x$. If $p \mid n$, let $x = 1$ and $y^2 \equiv -1 \pmod{p}$; such a y exists since $p \equiv 1 \pmod 4$. This establishes the base case $r = 1$.

Suppose that $x^2 + y^2 \equiv n \pmod{p^r}$ and $p \nmid x$. Then $x^2 + y^2 = n + mp^r$ for some $m \in \mathbb{Z}$. Let $i \equiv -2^{-1}x^{-1}m \pmod{p}$ so that $p \mid (2ix + m)$. Then

$$(x + ip^r)^2 + y^2 = x^2 + 2ixp^r + i^2 p^{2r} + y^2$$
$$\equiv n + (2ix + m)p^r \pmod{p^{r+1}} \equiv n \pmod{p^{r+1}}.$$

This completes the induction.

(b3) Let $p \equiv 3 \pmod 4$. If $a, b \in S_2$, then a theorem of Fermat ensures that $\nu_p(a)$ and $\nu_p(b)$ are both even. Then $\nu_p(a) - \nu_p(b) = \nu_p(a/b) \neq 1 = \nu_p(p)$ for all $a, b \in S_2$. Thus, S_2 is bounded away from p in $\mathbb{Q}_p$.

(c) Lagrange's four-square theorem asserts that $S_n = \mathbb{N}$ for $n \geq 4$, so $R(S_n) = \mathbb{Q}$ is dense in $\mathbb{Q}_p$ for $n \geq 4$. Thus, we consider only $n = 3$. Again there are three cases: (c1) $p = 2$; (c2) $p \equiv 1 \pmod 4$; (c3) $p \equiv 3 \pmod 4$.

(c1) Recall that Legendre's three-square theorem asserts that a natural number is in S_3 if and only if it is not of the form $4^i(8j + 7)$ for any $i, j \geq 0$. Consequently, if the 2-adic order of a natural number is odd, then it is the sum of three squares. Let $n \in \mathbb{N}$ be odd and let $k \in \mathbb{N}$. If k is odd, let $a = 2^k n$ and $b = 1$; if k is even, let $a = 2^{k+1}n$ and $b = 2$. Then $a = 2^k nb$ and $a, b \in S_3$ since $\nu_2(a)$ is odd. Consequently, $a \equiv 2^k nb \pmod{2^r}$ for all $r \in \mathbb{N}$, so $R(S_3)$ is 2-adically dense in $\mathbb{N}$. Lemma 2.3 ensures that $R(S_3)$ is dense in $\mathbb{Q}_2$.

(c2) If $p \equiv 1 \pmod 4$, then $R(S_3)$ contains $R(S_2)$, which is dense in $\mathbb{Q}_p$ by (b2).

(c3) Let $p \equiv 3 \pmod 4$. Since $4^j(8k + 7)$ is congruent to either 0, 4, or 7 modulo 8, it follows that S_3 contains the infinite arithmetic progression $A = \{8k + 1 : k \geq 0\}$. Lemma 2.4 ensures that $R(A)$ is dense in $\mathbb{Q}_p$, so $R(S_3)$ is dense in $\mathbb{Q}_p$ too. ∎

THEOREM 4.2. *Let $C_n = \{a \in \mathbb{N} : a$ is the sum of n cubes, with 0 permitted$\}$.*

(a) *$R(C_1)$ is not dense in any $\mathbb{Q}_p$.*
(b) *$R(C_2)$ is dense in $\mathbb{Q}_p$ if and only if $p \neq 3$.*
(c) *$R(C_n)$ is dense in all $\mathbb{Q}_p$ for all p whenever $n \geq 3$.*

Proof. (a) Let p be a prime. Then $3 \mid \nu_p(c)$ for all $c \in C_1$, so Lemma 2.1 ensures that $R(C_1)$ is dense in no $\mathbb{Q}_p$.

(b) There are three cases: (b1) $p \neq 3, 7$; (b2) $p = 3$; and (b3) $p = 7$.

(b1) The congruence $x^3 + y^3 \equiv n \pmod{m}$ has a solution for each n if and only if $7 \nmid m$ or $9 \nmid m$ [2, Thm. 3.3]. Consequently, C_2 is p-adically dense in $\mathbb{N}$ if $p \neq 3, 7$, so $R(C_2)$ is dense in $\mathbb{Q}_p$ for $p \neq 3, 7$ by Lemma 2.3.

(b2) If $x/y \in R(C_2)$ is sufficiently close to 3 in $\mathbb{Q}_3$, then $\nu_3(x) = \nu_3(y)+1$. Without loss of generality, we may suppose that $\nu_3(x) = 1$ and $\nu_3(y) = 0$. A sum of two cubes modulo 9 must be among $0, 1, 2, 7, 8$, so $\nu_3(x) = 1$ is impossible for $x \in C_2$. Thus, $R(C_2)$ is not dense in $\mathbb{Q}_3$.

(b3) Let $p = 7$. For each integer m congruent to 0, 1, 2, 5 or 6 modulo 7 and each $r \geq 1$, we use induction on r to show that $x^3 + y^3 \equiv m \pmod{7^r}$ has a solution with $7 \nmid x$. The cubes modulo 7 are $0, 1, 6$, and hence each of the residue classes $0, 1, 2, 5, 6$ is a sum of two cubes modulo 7, at least one of which is nonzero. This is the base of the induction. Suppose that n is congruent to 0, 1, 2, 5 or 6 modulo 7 and that $x^3 + y^3 \equiv m \pmod{7^r}$ with $7 \nmid x$. Then $x^3 + y^3 = m + 7^r \ell$ for some $\ell \in \mathbb{Z}$. Let $i \equiv -5\ell x^{-2} \pmod{7}$, so that $7 \mid (3ix^2 + \ell)$. Then

$$(x + 7^r i)^3 + y^3 \equiv x^3 + y^3 + 3x^2 \cdot 7^r i \pmod{7^{r+1}}$$

$$\equiv m + 7^r (3ix^2 + \ell) \pmod{7^{r+1}} \equiv m \pmod{7^{r+1}}.$$

Since $7 \nmid x$, we have $7 \nmid (x + 7^r i)$. This completes the induction.

The inverses of $1, 2, 5, 6$ modulo 7 are $1, 4, 3, 6$, respectively. Consequently, for each m congruent to 1, 3, 4 or 6 modulo 7, the congruence $(x^3+y^3)^{-1} \equiv m \pmod{7^r}$ has a solution with $7 \nmid x$.

Each residue class modulo 7 is a product of an element in $\{0, 1, 2, 5, 6\}$ with an element in $\{1, 3, 4, 6\}$. Given a natural number n and $r \geq 0$, write $n \equiv m_1 m_2 \pmod{7^r}$, in which m_1 modulo 7 is in $\{0, 1, 2, 5, 6\}$ and m_2 modulo 7 is in $\{1, 3, 4, 6\}$. Then there are $c_1, c_2 \in C_2$ such that $c_1 c_2^{-1} \equiv m_1 m_2 \equiv n \pmod{7^r}$. Lemma 2.3 ensures that $R(C_2)$ is dense in $\mathbb{Q}_7$.

(c) There are two cases to consider: (c1) $n \geq 4$; (c2) $n = 3$ and $p = 3$.

(c1) Almost every natural number, in the sense of natural density, is the sum of four cubes [8]. For each prime power p^r and each $n \in \mathbb{N}$, the congruence $x \equiv n \pmod{p^r}$ must have a solution with $x \in C_4$ since otherwise the natural density of C_4 would be at most $1 - 1/p^r$. Lemma 2.3 ensures that $R(C_4)$ is dense in $\mathbb{Q}_p$.

(c2) Modulo 9, the set of cubes is $\{0, 1, 8\}$; modulo 9, the set of sums of three cubes is $\{0, 1, 2, 3, 6, 7, 8\}$. Since $4 \cdot 7 \equiv 5 \cdot 2 \equiv 1 \pmod{9}$, each element of $\{1, 4, 5, 8\}$ is the inverse, modulo 9, of a residue class that is the sum of three cubes.

A lifting argument similar to that used in the proof of (b3) confirms that whenever $m \equiv 0, 1, 2, 3, 6, 7, 8 \pmod{9}$, the congruence $x^3 + y^3 + z^3 \equiv m \pmod{3^r}$ has a solution with $3 \nmid x$ for all $r \geq 2$. Thus, whenever $m \equiv 1, 4, 5, 8 \pmod{9}$, the congruence $(x^3 + y^3 + z^3)^{-1} \equiv m \pmod{3^r}$ has a solution with $3 \nmid x$ for all $r \geq 2$.

Each residue class modulo 9 is the product of an element in $\{0, 1, 2, 3, 6, 7, 8\}$ and an element of $\{1, 4, 5, 8\}$. Given a natural number n and $r \geq 2$, write $n \equiv m_1 m_2 \pmod{3^r}$ where m_1 modulo 9 is in $\{0, 1, 2, 3, 6, 7, 8\}$ and

m_2 modulo 9 is in $\{1, 4, 5, 8\}$. Then there are $c_1, c_2 \in C_3$ such that $c_1 c_2^{-1} \equiv m_1 m_2 \equiv n \pmod{3^r}$. Lemma 2.3 ensures that $R(C_2)$ is dense in $\mathbb{Q}_3$. ∎

We close this section with a couple open problems. In light of Theorems 4.1 and 4.2, the following question is the next logical step.

PROBLEM 4.3. *What about sums of fourth powers? Fifth powers?*

Turning in a different direction, instead of sums of squares one might consider quadratic forms. Cubic and biquadratic forms might also eventually be considered.

PROBLEM 4.4. *Let Q be a quadratic form and let $A = \{a \in \mathbb{N} : Q$ represents $a\}$. For which primes p is $R(A)$ dense in $\mathbb{Q}_p$?*

5. Second-order recurrences. Garcia and Luca [12] showed that the set of quotients of Fibonacci numbers is dense in $\mathbb{Q}_p$ for all p. The proof employed a small amount of algebraic number theory and some relatively obscure results about Fibonacci numbers. The primes $p = 2$ and $p = 5$ required separate treatment. This result has been extended by Sanna [33], who proved that the quotient set of the k-generalized Fibonacci numbers is dense in $\mathbb{Q}_p$ for all integers $k \geq 2$ and all primes p. The proof made use of p-adic analysis. In this section, we establish a result for certain second-order recurrences that include the Fibonacci numbers as a special case.

Given two fixed integers r and s, let $(a_n)_{n \geq 0}$ be defined by

$$a_0 = 0, \quad a_1 = 1, \quad a_{n+2} = r a_{n+1} + s a_n,$$

and let $(b_n)_{n \geq 0}$ be defined by

$$b_0 = 2, \quad b_1 = r, \quad b_{n+2} = r b_{n+1} + s b_n.$$

Sequences like $(a_n)_{n \geq 0}$ and $(b_n)_{n \geq 0}$ are usually known as *Lucas sequences of the first kind* and *second kind*, respectively. We assume that the *characteristic polynomial* $x^2 - rx - s$ has two nonzero roots $\alpha, \beta \in \mathbb{C}$ such that α/β is not a root of unity. In particular, α and β are distinct. Under this hypothesis, it is well known that

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad b_n = \alpha^n + \beta^n$$

for all integers $n \geq 0$, and that $a_n, b_n \neq 0$ for all $n \geq 1$. For each prime number p such that $p \nmid s$, let $\tau(p)$ be the *rank of appearance* of p in $(a_n)_{n \geq 0}$, that is, the smallest positive integer k such that $p \mid a_k$ (such a k exists, see [28]). Regarding the p-adic valuation of $(a_n)_{n \geq 0}$, we have the following result [32, Theorem 1.5].

THEOREM 5.1. *If $p \nmid s$, then*

$$\nu_p(a_n) = \begin{cases} \nu_p(n) + \nu_p(a_p) - 1 & \text{if } p \mid \Delta, \ p \mid n, \\ 0 & \text{if } p \mid \Delta, \ p \nmid n, \\ \nu_p(n) + \nu_p(a_{p\tau(p)}) - 1 & \text{if } p \nmid \Delta, \ \tau(p) \mid n, \ p \mid n, \\ \nu_p(a_{\tau(p)}) & \text{if } p \nmid \Delta, \ \tau(p) \mid n, \ p \nmid n, \\ 0 & \text{if } p \nmid \Delta, \ \tau(p) \nmid n, \end{cases}$$

for all positive integers n, where $\Delta = r^2 + 4s$.

Actually, in [32] the above theorem is proved under the hypothesis that s and r are relatively prime, but it can be readily checked that the proof works exactly in the same way also if s and r are not coprime.

Our result is the following:

THEOREM 5.2. *Let $A_n = \{a_n : n \geq 1\}$ and $B_n = \{b_n : n \geq 1\}$.*

(a) *If $p \mid s$ and $p \nmid r$, then $R(A)$ is not dense in $\mathbb{Q}_p$ ([1]).*
(b) *If $p \nmid s$, then $R(A)$ is dense in $\mathbb{Q}_p$.*
(c) *For all odd primes p, $R(B)$ is dense in $\mathbb{Q}_p$ if and only if there exists a positive integer n such that $p \mid b_n$.*

Proof. (a) If $p \mid s$ and $p \nmid r$, then induction confirms that $a_n \equiv r^{n-1}$ (mod p) so that $\nu_p(a_n) = 0$ for $n \geq 0$. Thus, $R(A)$ is not dense in $\mathbb{Q}_p$ by Lemma 2.1.

(b) Suppose that $p \nmid s$. From Theorem 5.1 it follows quickly that for any integer $j \geq 1$ there exists an integer $m \geq 1$ such that $\nu_p(a_m) \geq j$. Therefore,

$$a_m = \frac{\alpha^m - \beta^m}{\alpha - \beta} \equiv 0 \ (\text{mod } p^j),$$

so that

$$(5.1) \qquad \qquad \alpha^m \equiv \beta^m \ (\text{mod } p^j).$$

Setting $k = 2mp^{j-1}(p-1)$, by (5.1) we get

$$\alpha^k \equiv \beta^k \equiv (\alpha^m \beta^m)^{p^{j-1}(p-1)} \equiv (-s)^{mp^{j-1}(p-1)} \equiv 1 \ (\text{mod } p^j),$$

since $\alpha\beta = -s$, $p \nmid s$, and thanks to Euler's theorem. Hence,

$$\frac{a_{kn}}{a_k} = \frac{(\alpha^k)^n - (\beta^k)^n}{\alpha^k - \beta^k} = (\alpha^k)^{n-1} + (\alpha^k)^{n-2}(\beta^k) + \cdots + (\beta^k)^{n-1} \equiv n \ (\text{mod } p^j)$$

for all positive integers n. Since n and j are arbitrary, Lemma 2.3 ensures that $R(A)$ is dense in $\mathbb{Q}_p$.

(c)($\Rightarrow$) We prove the contrapositive. If $p \nmid b_n$ for all $n \geq 1$, then $\nu_p(b_n) = 0$ for all $n \geq 1$. Then $R(B)$ is not dense in $\mathbb{Q}_p$ by Lemma 2.1.

([1]) If $p \mid s$ and $p \mid r$, then anything can happen. See the remarks after Corollary 5.3.

(c)($\Leftarrow$) Suppose that p is an odd prime that divides b_n for some $n \geq 1$. Since $b_n = a_{2n}/a_n$, we have

$$\nu_p(b_n) = \nu_p(a_{2n}) - \nu_p(a_n).$$

Hence, $\nu_p(a_{2n}) > \nu_p(a_n)$. Keeping in mind that p is odd, from Theorem 5.1 we deduce that

(5.2) $$p \nmid \Delta, \quad \tau(p) \nmid n, \quad \tau(p) \mid 2n,$$

which in turn implies that

(5.3) $$\nu_2(\tau(p)) = \nu_2(n) + 1.$$

For an integer $j \geq 1$, set

$$k = p^{j+1} \cdot \frac{p-1}{2^{\nu_2(p-1)}} \cdot n.$$

On the one hand, by (5.3) we have $\tau(p) \nmid k$, so that Theorem 5.1 yields $\nu_p(a_k) = 0$. On the other hand, $\tau(p) \mid 2k$ and $p \mid 2k$. Hence, by Theorem 5.1,

$$\nu_p(a_{2k}) = \nu_p(2k) + \nu_p(a_{p\tau(p)}) - 1 \geq j.$$

Therefore,

$$\nu_p(b_k) = \nu_p(a_{2k}) - \nu_p(a_k) \geq j,$$

so that

$$\alpha^k \equiv -\beta^k \pmod{p^j}.$$

Setting $h = 2^{\nu_2(p-1)}$, we have

$$(\alpha^k)^{2h} \equiv (\alpha^k)^h(\alpha^k)^h \equiv (\alpha^k)^h(-\beta^k)^h$$
$$\equiv (\alpha^k)^h(\beta^k)^h \equiv (-s)^{p^{j+1}(p-1)n} \equiv 1 \pmod{p^j},$$

since $\alpha\beta = -s$, $p \nmid s$, and thanks to Euler's theorem. Noting that $2h$ and p^j are relatively prime, by the Chinese remainder theorem, for any positive integer m, we can pick a positive integer ℓ such that

$$\ell \equiv m \pmod{p^j} \quad \text{and} \quad \ell \equiv 1 \pmod{2h}.$$

Therefore, since ℓ is odd,

$$\frac{b_{k\ell}}{b_k} = \frac{(\alpha^k)^\ell + (\beta^k)^\ell}{\alpha^k + \beta^k} = (\alpha^k)^{\ell-1} + (\alpha^k)^{\ell-2}(-\beta^k) + \cdots + (-\beta^k)^{\ell-1}$$
$$\equiv \ell(\alpha^k)^{\ell-1} \equiv m \pmod{p^j}.$$

Since j, n are arbitrary, Lemma 2.3 tells us that $R(B)$ is dense in $\mathbb{Q}_p$. ∎

Theorem 5.2 has the following corollary, whose first part is the main result of [12].

COROLLARY 5.3. *Let* $(F_n)_{n \geq 0}$ *be the sequence of Fibonacci numbers and let* $(L_n)_{n \geq 0}$ *be the sequence of Lucas numbers. Set* $F = \{F_n : n \geq 1\}$ *and* $L = \{L_n : n \geq 1\}$.

(a) $R(F)$ *is dense in* $\mathbb{Q}_p$ *for all* p.

(b) $R(L)$ *is dense in* $\mathbb{Q}_p$ *if and only if* $p \neq 2$ *and* $p \mid L_n$ *for some* $n \geq 1$.

Proof. Pick $r = s = 1$.

(a) This follows immediately from Theorem 5.2(b).

(b) For odd p, the claim is a consequence of Theorem 5.2(c). For $p = 2$, it is enough to note that $(L_n)_{n \geq 0}$ is periodic modulo 8 and $8 \nmid L_n$ for all $n \geq 1$. Hence, the claim follows from Lemma 2.1. ∎

The set of primes that divide some Lucas number L_n has relative density $2/3$ as a subset of the primes [21] (see [1] for more such results). In particular, $R(L)$ is dense in $\mathbb{Q}_p$ more often than not.

Theorem 5.2(a–b) is sharp in the following sense: if $p \mid s$ and $p \mid r$, then $R(A)$ may or may not be dense in $\mathbb{Q}_p$. Consider the following examples.

EXAMPLE 5.4. Let $p = 3$, $r = 15$, and $s = -54$; note that $p \mid s$ and $p \mid r$. Then $\alpha = 9$ and $\beta = 6$, so

$$a_n = \frac{9^n - 6^n}{9 - 6} = 3^{n-1}(3^n - 2^n).$$

We claim that $R(A)$ is not dense in $\mathbb{Q}_3$. Since $\nu_3(3) = 1$ and $\nu_3(a_m/a_n) = (m-1) - (n-1) = m - n$ for $m, n \geq 0$, any element of $R(A)$ that is sufficiently close to 3 in $\mathbb{Q}_3$ must be of the form a_{n+1}/a_n for some $n \geq 1$. However,

$$\nu_3\left(\frac{a_{n+1}}{a_n} - 3\right) = \nu_3\left(\frac{3^n(3^{n+1} - 2^{n+1})}{3^{n-1}(3^n - 2^n)} - 3\right) = 1 + \nu_3\left(\frac{3^{n+1} - 2^{n+1}}{3^n - 2^n} - 1\right)$$
$$= 1 + \nu_3(3^{n+1} - 2^{n+1} - 3^n + 2^n)$$
$$= 1 + \nu_3\left(3^n(3 - 1) - 2^n(2 - 1)\right)$$
$$= 1 + \nu_3(2 \cdot 3^n - 2^n) = 1 + \nu_3(3^n - 2^{n-1}) = 1,$$

so $R(A)$ is bounded away from 3 in $\mathbb{Q}_3$.

EXAMPLE 5.5. Let $p = 5$, $r = 20$, and $s = -75$; note that $p \mid s$ and $p \mid r$. Then $\alpha = 15$ and $\beta = 5$, so

$$a_n = \frac{15^n - 5^n}{15 - 5} = 5^{n-1}\frac{3^n - 1}{2}.$$

We claim that $R(A)$ is dense in $\mathbb{Q}_5$. Let $N \in \mathbb{N}$ be given and write $N = 5^t N_0$, in which $5 \nmid N_0$. Let $r \geq t$ be large and such that $r \not\equiv t - 1 \pmod 4$. Since $\phi(5^{r+1}) = 4 \cdot 5^r$, Euler's theorem permits us to write

$$(5.4) \qquad 3^{4 \cdot 5^r} - 1 = 5^{r+1}\ell, \qquad 5 \nmid \ell.$$

Let $m \geq 1$ satisfy

$$(5.5) \qquad m \equiv \ell^{-1} N_0(3^{r-t+1} - 1) \pmod{5^{r+1}};$$

Euler's theorem ensures that $5 \nmid m$ since $4 \nmid (r - t + 1)$. If $n = 4 \cdot 5^r m$, then

$$(3^{n+r-t+1} - 1)\frac{a_n}{a_{n+r-t+1}} = 5^{n-1}\left(\frac{3^n - 1}{2}\right)\left(\frac{2}{5^{n+r-t}}\right) = 5^{-r+t-1}(3^{4\cdot 5^r m} - 1)$$

$$= 5^t\left(\frac{3^{4\cdot 5^r m} - 1}{3^{4\cdot 5^r} - 1}\right)\left(\frac{3^{4\cdot 5^r} - 1}{5^{r+1}}\right)$$

$$= 5^t\left(\frac{(3^{4\cdot 5^r})^m - 1}{3^{4\cdot 5^r} - 1}\right)\ell \qquad\qquad \text{(by (5.4))}$$

$$= 5^t\left((3^{4\cdot 5^r})^{m-1} + (3^{4\cdot 5^r})^{m-2} + \cdots + 1\right)\ell$$

$$\equiv 5^t m\ell \pmod{5^{r+1}} \qquad\qquad (\text{since } \phi(5^{r+1}) = 4\cdot 5^r)$$

$$\equiv 5^t N_0(3^{r-t+1} - 1) \pmod{5^{r+1}} \qquad (\text{by (5.5)})$$

$$\equiv N(3^{r-t+1} - 1) \pmod{5^{r+1}} \qquad (\text{since } N = 5^t N_0)$$

$$\equiv N(3^{n+r-t+1} - 1) \pmod{5^{r+1}} \qquad (\text{since } \phi(5^{r+1}) \mid n).$$

Since $4 \mid n$ and $4 \nmid (r - t + 1)$, it follows that $5 \nmid (3^{n+r-t+1} - 1)$, and hence

$$\nu_5\left(\frac{a_n}{a_{n+r-t+1}} - N\right) \geq r + 1.$$

Thus, $R(A)$ is 5-adically dense in $\mathbb{N}$, so it is dense in $\mathbb{Q}_5$ by Lemma 2.3.

Where do the preceding two examples leave us? Suppose that $p \mid s$ and $p \mid r$. Then $d = (r, s)$ is divisible by p. Induction confirms that $d^{\lfloor n/2 \rfloor}$ divides a_n for $n \geq 0$. To be more specific,

$$a_n = \sum_{k=0}^{n-1} \binom{n-1-k}{k} r^{\max\{n-1-2k,0\}} s^{\max\{\lfloor(2k+1)/2\rfloor,0\}},$$

and hence it is difficult to precisely evaluate $\nu_p(a_n)$. Consequently, we are unable at this time to completely characterize when $R(A)$ is dense in $\mathbb{Q}_p$ if $p \mid s$ and $p \mid r$. However, in most instances, ad hoc arguments can handle these situations. Consider the following examples.

EXAMPLE 5.6. The integer sequence

$$0, 1, 2, -1, -12, -19, 22, 139, 168, -359, -1558, -1321, 5148, \ldots$$

is generated by the recurrence

$$a_0 = 0, \quad a_1 = 1, \quad a_{n+2} = 2a_{n+1} - 5a_n, \quad n \geq 0.$$

In this case, $\alpha = 1 + 2i$ and $\beta = 1 - 2i$ are nonreal. Let $A = \{a_n : n \geq 1\}$ and confirm by induction that $5 \nmid a_n$ for all $n \geq 1$. Apply Lemma 2.1 and Theorem 5.2 to see that $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p \neq 5$.

EXAMPLE 5.7. Let b be an integer not equal to ± 1 and consider the sequence $a_n = b^n - 1$, which is generated by

$$a_0 = 0, \quad a_1 = b - 1, \quad a_{n+2} = (b+1)a_{n+1} - ba_n.$$

Apply Theorem 5.2 with $r = b + 1$ and $s = -b$ to the set $A = \{a_n : n \geq 1\}$ and conclude that $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p \nmid b$. For instance, the set $\{1, 3, 7, 15, 31, \ldots\}$ is dense in $\mathbb{Q}_p$ if and only if $p \neq 2$.

6. Unions of geometric progressions. The ratio set of $A = \{2^n : n \in \mathbb{N}\} \cup \{3^n : n \in \mathbb{N}\}$ is dense in $\mathbb{R}_+$ [3, Prop. 6]. The argument relies upon the irrationality of $\log_2 3$ and the inhomogeneous form of Kronecker's approximation theorem [16, Thm. 440]. We consider such sets in the p-adic setting, restricting our attention to prime bases. The reader should have no difficulty stating the appropriate generalizations if they are desired.

An integer g is called a *primitive root modulo m* if g is a generator of the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$. Gauss proved that primitive roots exist only for the moduli 2, 4, p^k, and $2p^k$, in which p is an odd prime [25, Thm. 2.41]. Consequently, our arguments here tend to focus on odd primes.

THEOREM 6.1. *Let p be an odd prime, let b be a nonzero integer, and let*

$$A = \{p^j : j \geq 0\} \cup \{b^j : j \geq 0\}.$$

Then $R(A)$ is dense in $\mathbb{Q}_p$ if and only if b is a primitive root modulo p^2.

Proof. ($\Rightarrow$) Suppose that $R(A)$ is dense in $\mathbb{Q}_p$. We first claim that b is a primitive root modulo p. If not, then there is an $m \in \{2, 3, \ldots, p-1\}$ such that $b^j \not\equiv m \pmod{p}$ for all $j \in \mathbb{Z}$. Then $R(A)$ is bounded away from m in $\mathbb{Q}_p$, a contradiction. Thus, b must be a primitive root modulo p.

Suppose toward a contradiction that b is not a primitive root modulo p^2. Since b is a primitive root modulo p, the order of b modulo p^2 is at least $p - 1$. On the other hand, the order must divide $\Phi(p^2) = p(p-1)$. Since p is prime, it follows that the order of b modulo p^2 must be exactly $p - 1$. Thus, $b^{p-1} \equiv 1 \pmod{p^2}$.

If $b^n \equiv p + 1 \pmod{p^2}$, then $b^n \equiv 1 \pmod{p}$, and hence n is a multiple of $p - 1$. Then $b^n \equiv 1 \pmod{p^2}$, a contradiction. Thus, $R(A)$ is bounded away from $p + 1$ in $\mathbb{Q}_p$. This contradiction shows that b must be a primitive root modulo p^2.

($\Leftarrow$) Let $r \geq 1$ and let $n = p^k m \in \mathbb{N}$ with $p \nmid m$. Since b is a primitive root modulo p^2, it is a primitive root modulo $p^3, p^4, \ldots$ [25, Thm. 2.40], so there is a j such that $b^j m \equiv 1 \pmod{p^r}$. Thus,

$$\nu_p\left(n - \frac{p^k}{b^j}\right) = k + \nu_p\left(m - \frac{1}{b^j}\right) \geq \nu_p(b^j m - 1) \geq r,$$

so $R(A)$ is dense in $\mathbb{Q}_p$ by Lemma 2.3. ∎

A primitive root modulo p is not necessarily a primitive root modulo p^2. For instance, 1 is a primitive root modulo 2, but not modulo 4. A less trivial example is furnished by $p = 29$, for which 14 is a primitive root modulo p, but not modulo p^2. Similarly, if $p = 37$, then 18 is a primitive root modulo p, but not modulo p^2.

EXAMPLE 6.2. Consider $p = 5$ and $q = 7$; note that 5 is a primitive root modulo 7 and vice versa. However, 5 is a primitive root modulo 7^2, but 7 is not a primitive root modulo 5^2. Let

$$A = \{5, 7, 25, 49, 125, 343, 625, 2401, 3125, \ldots\} = \{5^j : j \geq 0\} \cup \{7^j : j \geq 0\}.$$

Then Theorem 6.1 ensures that $R(A)$ is dense in $\mathbb{Q}_7$ but not in $\mathbb{Q}_5$.

This sort of asymmetry is not unusual. The following theorem tells us that infinitely many such pairs of primes exist. The proof is considerably more difficult than the preceding material and it requires a different collection of tools (e.g., a sieve lemma of Heath-Brown, the Brun–Titchmarsh theorem, and the Bombieri–Vinogradov theorem). Consequently, the proof of Theorem 6.3 is deferred until Section 7.

THEOREM 6.3. *There exist infinitely many pairs of primes (p, q) such that p is not a primitive root modulo q, but q is a primitive root modulo p^2.*

COROLLARY 6.4. *There are infinitely many pairs of primes (p, q) such that the ratio set of $\{p^j : j \geq 0\} \cup \{q^k : k \geq 0\}$ is dense in $\mathbb{Q}_p$ but not in $\mathbb{Q}_q$.*

Let $a \prec b$ denote "a is a primitive root modulo b." The following table shows some of the various logical possibilities (bear in mind that a primitive root modulo p^2 is automatically a primitive root modulo p).

p	q	$p \prec q$	$q \prec p$	$p \prec q^2$	$q \prec p^2$
3	5	T	T	T	T
5	7	T	T	T	F
3	7	T	F	T	F
5	11	F	F	F	F
7	19	F	T	F	F

Despite an extensive computer search, we have been unable to find a pair (p, q) of primes for which $p \prec q$ and $q \prec p$, but $p \nprec q^2$ and $q \nprec p^2$. We hope to revisit this question in later work. For now we are content to pose the following question.

PROBLEM 6.5. *Is there a pair (p, q) of primes for which $p \prec q$ and $q \prec p$, but $p \nprec q^2$ and $q \nprec p^2$*

On the other hand, numerical evidence and heuristic arguments suggest that there are infinitely many pairs (p, q) of primes for which $p \prec q^2$

and $q \prec p^2$. Although we have given the proof of the closely related Theorem 6.3, we feel that attempting to address more questions of this nature would draw us too far afield. Consequently, we postpone this venture until another day.

PROBLEM 6.6. *Prove that there are infinitely many pairs of primes (p, q) for which $p \prec q^2$ and $q \prec p^2$.*

7. Proof of Theorem 6.3

STEP 1. We start with a sieve lemma due to Heath-Brown. It is a weaker version of [17, Lem. 3]. In what follows, p always denotes an odd prime. We write $\left(\frac{a}{p}\right)$ for the Legendre symbol of a with respect to p and write $x \prec y$ to indicate that x is a primitive root modulo y.

LEMMA 7.1 (Heath-Brown). *Let q, r, s be primes, let $k \in \{1, 2, 3\}$, and let u, v be positive integers such that*

(a) $16 \,|\, v$,
(b) $2^k \,|\, (u - 1)$,
(c) $((u - 1)/2^k, v) = 1$,
(d) *if $p \equiv u \pmod{v}$, then $\left(\frac{-3}{p}\right) = \left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) = -1$.*

Then for large x, the set of primes

$$\mathcal{P}(x; u, v) = \big\{ p \leq x : p \equiv u \pmod{v}, \ (p-1)/2^k \text{ is prime or a product of }$$
$$\text{two primes, and one of } q, r, s \text{ is a primitive root modulo } p \big\}$$

has cardinality satisfying

$$|\mathcal{P}(x; u, v)| \gg \frac{x}{(\log x)^2}.$$

Consider the primes $q = 7$, $r = 11$, and $s = 19$. Let

$$v = 70{,}224 = 16 \times 3 \times 7 \times 11 \times 19$$

and observe that $16 \,|\, v$, so (a) is satisfied. Let $u = 2{,}951$ so that

$$u - 1 = 2{,}950 = 2 \times 5^2 \times 59,$$

so that (b) is satisfied with $k = 1$. Then (c) is satisfied since $u - 1$ and v have no common factors. If $p \equiv u \pmod{v}$, then

(7.1) $\qquad p \equiv 3 \pmod 4, \quad p \equiv 2 \pmod 3, \quad \text{and} \quad p \equiv 25 \pmod{qrs}.$

Since $q \equiv r \equiv s \equiv 3 \pmod 4$, quadratic reciprocity ensures that q, r, s are quadratic nonresidues modulo p. For instance,

(7.2) $$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{25}{q}\right) = -1$$

and similarity if q is replaced with r or s. In addition,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$$

by (7.1) and quadratic reciprocity. Thus, (d) is satisfied.

STEP 2. With $u = 2{,}951$, $v = 70{,}224$, $q = 7$, $r = 11$, and $s = 19$ as above, let

$$\mathcal{P} = \{p \equiv u \ (\text{mod } v) : \text{one of } q, r, s \text{ is a primitive root modulo } p\}$$

and let $\mathcal{P}(x) = \mathcal{P} \cap [1, x]$. Since $\mathcal{P}(x; u, v) \subseteq \mathcal{P}(x)$, Lemma 7.1 ensures that

$$|\mathcal{P}(x)| \geq \frac{x}{(\log x)^2}.$$

If $p \in \mathcal{P}$, then $\left(\frac{p}{q}\right) = 1$ by (7.2), so p is a quadratic residue modulo q and hence it fails to be a primitive root modulo q. Since (7.2) holds with q replaced with r or s, we conclude that p is not a primitive root modulo q, r, or s.

STEP 3. The definition of $\mathcal{P}(x)$ ensures that one of the primes q, r, s is a primitive root for at least $\frac{1}{3}|\mathcal{P}(x)|$ primes $p \leq x$. Without loss of generality, we may assume that this prime is q since the specific numerical values of q, r, s are irrelevant in what follows (save that they are all congruent to 3 modulo 4). Let

$$\mathcal{P}_1(x) = \left\{\frac{x}{(\log x)^2} < p \leq x : p \equiv u \ (\text{mod } v) \text{ and } q \prec p\right\}$$

and let $\pi(x)$ denote the number of primes at most x. Then the prime number theorem implies that

$$|\mathcal{P}_1(x)| \geq \tfrac{1}{3}|\mathcal{P}(x)| - \pi\left(\frac{x}{(\log x)^2}\right) \gg \frac{x}{(\log x)^2} - O\left(\frac{x}{(\log x)^3}\right) \gg \frac{x}{(\log x)^2}.$$

STEP 4. Let $\mathcal{P}_2(x)$ be the set of $p \in \mathcal{P}_1(x)$ for which $q \prec p^2$; let $\mathcal{P}_3(x) = \mathcal{P}_1(x) \setminus \mathcal{P}_2(x)$ be the subset for which $q \not\prec p^2$. One of these two possibilities must occur at least half the time. This leads to two cases.

STEP 4.a. If

(7.3) $$|\mathcal{P}_2(x)| \geq \tfrac{1}{2}|\mathcal{P}_1(x)|,$$

then there are $\gg x/(\log x)^2$ pairs of primes (p, q) with $p \leq x$ for which $q \prec p^2$ and $p \not\prec q$.

STEP 4.b. Suppose that

(7.4) $$|\mathcal{P}_3(x)| \geq \tfrac{1}{2}|\mathcal{P}_1(x)|.$$

For $p \in \mathcal{P}_3(x)$ consider primes of the form

(7.5) $$\ell = q + 4hp, \quad h \in [1, x^{3/2} - 1] \cap \mathbb{Z},$$

first observing that $\ell \ll x^{5/2}$. The prime number theorem for arithmetic progressions asserts that the number of such primes is $\pi(4x^{3/2}p; 4p, q) + O(1)$, where $\pi(x; m, a)$ denotes the number of primes at most x that are congruent to $a \pmod{m}$. For such a prime ℓ, quadratic reciprocity and (7.2) ensure that

$$\left(\frac{p}{\ell}\right) = -\left(\frac{\ell}{p}\right) = -\left(\frac{q + 4hp}{p}\right) = -\left(\frac{q}{p}\right) = 1$$

since $p, q \equiv 3 \pmod 4$. Consequently, $p \nmid \ell$. Since

$$\ell^{p-1} = (q + 4hp)^{p-1} \equiv q^{p-1} + 4h(p-1)q^{p-2}p \pmod{p^2}$$
$$\equiv 1 + 4h(p-1)q^{p-2}p \pmod{p^2},$$

we see that ℓ is a primitive root modulo p^2 whenever $p \nmid h$. The Brun–Titchmarsh theorem ensures that the number of primes ℓ of the form (7.5) for which $p \mid h$ is

$$\pi(4x^{3/2}p; 4p^2, q) + O(1) \ll \frac{x^{3/2}p}{p^2 \log(x^{3/2}p)} \ll \frac{x^{3/2}}{p \log x}.$$

Thus, for each $p \in \mathcal{P}_3(x)$, there are

$$\pi(4x^{3/2}p; 4p, q) - \pi(4x^{3/2}p; 4p^2, q) + O(1)$$

primes $\ell \leq x^{5/2}$ for which $p \nmid \ell$ and $\ell \prec p^2$.

STEP 5. Let $\mathcal{P}_4(x)$ be the subset of $p \in \mathcal{P}_3(x)$ such that

$$(7.6) \qquad \pi(4x^{3/2}p; 4p, q) - \pi(4x^{3/2}p; 4p^2, q) \geq \frac{x^{3/2}}{(\log x)^2},$$

and let $\mathcal{P}_5(x) = \mathcal{P}_3(x) \setminus \mathcal{P}_4(x)$. We intend to show that $|\mathcal{P}_5(x)|$ is small, and hence that (7.6) holds for most $p \in \mathcal{P}_3(x)$. Suppose that $p \in \mathcal{P}_5(x)$, that is,

$$\pi(4x^{3/2}p; 4p, q) - \pi(4x^{3/2}p; 4p^2, q) < \frac{x^{3/2}}{(\log x)^2}.$$

Then

$$\left|\pi(4x^{3/2}p; 4p; q) - \frac{\pi(4x^{3/2}p)}{\phi(4p)}\right|$$

$$\geq \frac{\pi(4x^{3/2}p)}{\phi(4p)} - |\pi(4x^{3/2}p; 4p, q) - \pi(4x^{3/2}p; 4p^2, q)| - \pi(4x^{3/2}p; 4p^2, q)$$

$$\gg \frac{x^{3/2}}{\log x} + O\left(\frac{x^{3/2}}{(\log x)^2} + \frac{x^{3/2}}{p \log x}\right) \gg \frac{x^{3/2}}{\log x}$$

because $p \geq x/(\log x)^2$ by the definition of $\mathcal{P}_1(x)$. Thus,

$$\max_{\substack{1 \leq a \leq 4p \\ (a,4p)=1 \\ 1 \leq y \leq 4x^{5/2}}} \left| \pi(y; 4p, a) - \frac{\pi(y)}{\phi(4p)} \right| \geq \left| \pi(4x^{3/2}p; 4p, q) - \frac{\pi(4x^{3/2}p)}{\phi(4p)} \right| \gg \frac{x^{3/2}}{\log x}.$$

Summing up the above inequality over all $p \in \mathcal{P}_5(x)$ and appealing to the Bombieri–Vinogradov theorem, for large x we obtain

$$\left(\frac{x^{3/2}}{\log x} \right) |\mathcal{P}_5(x)| \ll \sum_{p \in \mathcal{P}_5(x)} \max_{\substack{1 \leq a \leq 4p \\ (a,4p)=1 \\ 1 \leq y \leq 4x^{5/2}}} \left| \pi(y; 4p, a) - \frac{\pi(y)}{\phi(4p)} \right|$$

$$\ll \sum_{\substack{m \leq 4x}} \max_{\substack{1 \leq a \leq m \\ (a,m)=1 \\ y \leq x^{5/2}}} \left| \pi(y; m, a) - \frac{\pi(y)}{\phi(m)} \right| \ll \frac{x^{5/2}}{(\log x)^4}.$$

Thus,

$$|\mathcal{P}_5(x)| \ll \frac{x}{(\log x)^3},$$

and hence

$$|\mathcal{P}_4(x)| = |\mathcal{P}_3(x)| - |\mathcal{P}_5(x)| \geq \tfrac{1}{2}|\mathcal{P}_3(x)| \gg \frac{x}{(\log x)^2}$$

when (7.4) holds and x is sufficiently large. Comparing this with (7.6), we conclude that the number of pairs (p, ℓ) with $p \nmid \ell$ and $\ell \prec p^2$ and $p < \ell \leq 4x^{5/2}$ is

$$(7.7) \qquad\qquad \gg \left(\frac{x^{3/2}}{(\log x)^2} \right) \left(\frac{x}{(\log x)^2} \right) \gg \frac{x^{5/2}}{(\log x)^4}.$$

STEP 6. If (7.3) holds, then the number of pairs (p, q) for which $p \in \mathcal{P}_1(x)$, $q \prec p^2$, and $p \nmid q$ is $\gg x/(\log x)^2$, which is dominated by (7.7) for large x. For such p we have $\max\{p, q\} \leq x < 4x^{5/2}$. If $y = 4x^{5/2}$ is sufficiently large, then the number of pairs of primes (p, q) with $\max\{p, q\} \leq y$ and for which $p \nmid q$ and $q \prec p^2$ is

$$\gg \frac{x}{(\log x)^2} \gg \frac{y^{2/5}}{(\log y)^2}.$$

This completes the proof of Theorem 6.3. ∎

REMARK 7.2. A more careful application of the Bombieri–Vinogradov theorem shows that this count can be improved to $y^{1/2-\varepsilon}$ for any $\varepsilon > 0$ fixed (just replace $x^{3/2}$ in (7.5) by $x^{1+\varepsilon}$), or even to $y^{1/2}/(\log y)^A$ for some constant $A > 0$, but we do not get into such details.

References

[1] C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. 115 (1995), no. 551, viii+102 pp.

[2] K. A. Broughan, *Characterizing the sum of two cubes*, J. Integer Seq. 6 (2003), no. 4, art. 03.4.6, 7 pp.

[3] B. Brown, M. Dairyko, S. R. Garcia, B. Lutz, and M. Someck, *Four quotient set gems*, Amer. Math. Monthly 121 (2014), 590–599.

[4] J. Bukor and P. Csiba, *On estimations of dispersion of ratio block sequences*, Math. Slovaca 59 (2009), 283–290.

[5] J. Bukor, P. Erdős, T. Šalát, and J. T. Tóth, *Remarks on the (R)-density of sets of numbers, II*, Math. Slovaca 47 (1997), 517–526.

[6] J. Bukor, T. Šalát, and J. T. Tóth, *Remarks on R-density of sets of numbers*, Tatra Mount. Math. Publ. 11 (1997), 159–165.

[7] J. Bukor and J. T. Tóth, *On accumulation points of ratio sets of positive integers*, Amer. Math. Monthly 103 (1996), 502–504.

[8] H. Davenport, *On Waring's problem for cubes*, Acta Math. 71 (1939), 123–143.

[9] J.-M. De Koninck and A. Mercier, *1001 Problems in Classical Number Theory*, Amer. Math. Soc., Providence, RI, 2007.

[10] B. Fine and G. Rosenberger, *Number Theory: An Introduction via the Distribution of Primes*, Birkhäuser, Boston, 2007.

[11] S. R. Garcia, *Quotients of Gaussian primes*, Amer. Math. Monthly 120 (2013), 851–853.

[12] S. R. Garcia and F. Luca, *Quotients of Fibonacci numbers*, Amer. Math. Monthly 123 (2016), 1039–1044.

[13] S. R. Garcia, V. Selhorst-Jones, D. E. Poore, and N. Simon, *Quotient sets and Diophantine equations*, Amer. Math. Monthly 118 (2011), 704–711.

[14] F. Q. Gouvêa, *p-Adic Numbers. An Introduction*, 2nd ed., Universitext, Springer, Berlin, 1997.

[15] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) 167 (2008), 481–547.

[16] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford Univ. Press, Oxford, 2008.

[17] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) 37 (1986), 27–38.

[18] S. Hedman and D. Rose, *Light subsets of ℕ with dense quotient sets*, Amer. Math. Monthly 116 (2009), 635–641.

[19] D. Hobby and D. M. Silberger, *Quotients of primes*, Amer. Math. Monthly 100 (1993), 50–52.

[20] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, 2nd ed., Grad. Texts in Math. 58, Springer, New York, 1984.

[21] J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific
      J. Math. 118 (1985), 449–461.
[22] F. Luca, C. Pomerance, and Š. Porubský, *Sets with prescribed arithmetic densities*,
      Unif. Distrib. Theory 3 (2008), no. 2, 67–80.
[23] A. Micholson, *Quotients of primes in arithmetic progressions*, Notes Number Theory
      Discrete Math. 18 (2012), no. 2, 56–57.
[24] L. Mišik, *Sets of positive integers with prescribed values of densities*, Math. Slovaca
      52 (2002), 289–296.
[25] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory
      of Numbers*, 5th ed., Wiley, New York, 1991.
[26] A. Nowicki, in: Editor's endnotes, Amer. Math. Monthly 117 (2010), 755–756.
[27] P. Pollack, *Not Always Buried Deep: A Second Course in Elementary Number The-
      ory*, Amer. Math. Soc., Providence, RI, 2009.
[28] M. Renault, *The period, rank, and order of the* (a,b)-*Fibonacci sequence mod* m,
      Math. Mag. 86 (2013), 372–380.
[29] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Universitext, Springer, New
      York, 2001.
[30] T. Šalát, *On ratio sets of sets of natural numbers*, Acta Arith. 15 (1969), 273–278.
[31] T. Šalát, Corrigendum to [30], Acta Arith. 16 (1969), 103.
[32] C. Sanna, *The p-adic valuation of Lucas sequences*, Fibonacci Quart. 54 (2016),
      118–124.
[33] C. Sanna, *The quotient set of k-generalised Fibonacci numbers is dense in* $\mathbb{Q}_p$, Bull.
      Austral. Math. Soc. (2017, online).
[34] B. D. Sittinger, *Quotients of primes in a quadratic number ring*, arXiv:1607.08319
      (2016).
[35] P. Starni, *Answers to two questions concerning quotients of primes*, Amer. Math.
      Monthly 102 (1995), 347–349.
[36] O. Strauch and J. T. Tóth, *Asymptotic density of* $A \subset \mathbb{N}$ *and density of the ratio
      set* $R(A)$, Acta Arith. 87 (1998), 67–78.
[37] O. Strauch and J. T. Tóth, Corrigendum to Theorem 5 of [36], Acta Arith. 103
      (2002), 191–200.

Stephan Ramon Garcia, Yu Xuan Hong,
Elena Pinsker, Evan Schechter, Adam Starr
Department of Mathematics
Pomona College
610 N. College Ave.
Claremont, CA 91711, U.S.A.
E-mail: stephan.garcia@pomona.edu
http://pages.pomona.edu/˜sg064747

Carlo Sanna
Department of Mathematics
Università degli Studi di Torino
Via Carlo Alberto, 10
10123 Torino, Italy
E-mail: carlo.sanna.dev@gmail.com

Florian Luca
School of Mathematics
University of the Witwatersrand
Private Bag 3
Wits 2050, Johannesburg, South Africa
and
Max Planck Institute for Mathematics
Vivatsgasse 7
53111 Bonn, Germany
and
Department of Mathematics
Faculty of Science
University of Ostrava
30. dubna 22
701 03 Ostrava 1, Czech Republic
E-mail: Florian.Luca@wits.ac.za