ACTA ARITHMETICA
175.2 (2016)

Further irreducibility criteria for polynomials with non-negative coefficients

by

MORGAN COLE (Santa Clarita, CA), SCOTT DUNN (Columbia, SC) and
MICHAEL FILASETA (Columbia, SC)

1. Introduction. If $d_n d_{n-1} \dots d_1 d_0$ is the decimal representation of a prime, then a result of A. Cohn [11] asserts that

$$f(x) = d_n x^n + d_{n-1} x^{n-1} + \dots + d_1 x + d_0$$

is irreducible over the integers. This paper is inspired by the following two natural questions. If one views $f(x)$ as being a general polynomial with non-negative integer coefficients with $f(10)$ prime, does the irreducibility of $f(x)$ in $\mathbb{Z}[x]$ really depend on its coefficients being less than 10? Is there a particular reason that base 10 is special or do analogous results hold when 10 is replaced by some other integer?

Some answers to these questions have already been given in the literature. The result of Cohn has been extended to all bases $b \geq 2$ by J. Brillhart, A. Odlyzko and the third author [3], to base b representations of kp where k is a positive integer $< b$ and p is a prime by the third author [5] (see also [8]), and to an analog in function fields over finite fields by M. R. Murty [9]. Furthermore, [3] allows the coefficients d_j in Cohn's theorem to satisfy $0 \leq d_j \leq 167$ rather than $0 \leq d_j \leq 9$; and later the third author [6] showed that the d_j need only satisfy $0 \leq d_j \leq 10^{30} d_n$, and further that simply $d_j \geq 0$ suffices if $n \leq 31$. Some further work on upper bounds for d_j can be found in [1] and [2].

Recent work by S. Gross and the third author [7] extended this last line of investigation even further. They showed that if $f(x)$ is a polynomial with

2010 *Mathematics Subject Classification*: Primary 11R09; Secondary 11C08, 12E05, 26C10.
Key words and phrases: irreducibility, polynomial, root, prime value.
Received 7 December 2015; revised 29 April 2016.
Published online 15 September 2016.

DOI: 10.4064/aa8376-5-2016

non-negative coefficients bounded above by

$$49598666989151226098104244512918$$

and $f(10)$ is prime, then $f(x)$ is irreducible over $\mathbb{Z}$. They also showed that if instead the coefficients were bounded above by

$$8592444743529135815769545955936773,$$

then $f(x)$ is either irreducible over $\mathbb{Z}$ or divisible by $x^2-20x+101$. Furthermore, and perhaps most surprising, they established that these two upper bounds are sharp.

The main goal of this paper is to extend the results in [7] to different bases. We focus on bases $b \in [2,20]$. As we will see, the smaller the base, the more difficult the analysis becomes. We use $\Phi_n(x)$ to denote the nth cyclotomic polynomial, and irreducibility throughout will refer to irreducibility in $\mathbb{Z}[x]$. Our main goal is to establish the following.

THEOREM 1.1. *Fix an integer $b \in [2,20]$, and let $M_1(b)$ and $M_2(b)$ be as given in Tables* 1 *and* 2*, respectively. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_j \geq 0$ for each j and $f(b)$ prime. If each $a_j \leq M_1(b)$, then $f(x)$ is irreducible. Also, for $3 \leq b \leq 5$, if each $a_j \leq M_2(b)$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_3(x-b)$. Similarly, for $6 \leq b \leq 20$, if each $a_j \leq M_2(b)$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$.*

We will show that, for $3 \leq b \leq 20$, the bound $M_1(b)$ is sharp. For $4 \leq b \leq 20$, we will likewise show that the bound $M_2(b)$ is sharp.

We suspect the bound $M_1(2) = 7$ as given in Table 1 is not sharp. Of some related interest is the example

$$f(x) = x^{15}+9x^{10}+9x^9+9x^8+9x^7+9x^6+8x^5+10x^4+7x^3+10x^2+9x+3.$$

Here $f(2) = 51157$ is prime, the largest coefficient of $f(x)$ is 10, and $f(x)$ is divisible by x^2-3x+3. This example shows that the largest permissible value of $M_1(2)$ is ≤ 9. Therefore, this largest permissible value is 7, 8 or 9.

Computations in this paper were done using MAPLE 2015. The "isprime" routine was used to detect likely primes in our computations, and these were verified by using primality tests in SAGE v. 4.6.

2. Preliminary results. We begin with an instructive lemma adapted from [3].

LEMMA 2.1. *Fix an integer $b \geq 2$. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ be such that each $a_j \geq 0$ and $f(b)$ is prime. If $f(x)$ is reducible, then $f(x)$ has a non-real root in the disc $\mathcal{D}_b = \{z \in \mathbb{C} : |b-z| \leq 1\}$.*

Proof. Assume that $f(x)$ is reducible. Then we may write $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ have integer coefficients, $g(x) \not\equiv \pm 1$, and $h(x) \not\equiv \pm 1$. Since $f(b)$ is prime, one of $g(b)$ or $h(b)$ is ± 1. Without loss of

Table 1. $M_1(b)$ for $2 \le b \le 20$

b	$M_1(b)$
2	7
3	3795
4	8925840
5	56446139763
6	568059199631352
7	4114789794835622912
8	75005556404194608192050
9	1744054672674891153663590400
10	49598666989151226098104244512918
11	1754638089240473418053140582402752512
12	77040233750234318697380885880167588145722
13	4163976197614743889240641877839816882986680320
14	274327682731486702351640132483696971555362645663790
15	53237820409607236753887375170676537338756637987992240128
16	826743902509790173824819141451861039372680293578372832 7213632
17	126851405272079175658294461380208517509620085899496335987327 5789312
18	2100753785440048721903258296068360516321923712022160816682846 09637499040
19	3862536865580805292769435930162027257682225220024725436969612 8549408630374400
20	7965097815841643900684276577174036821605756035173863133380627 98297971858847052888 0

Table 2. $M_2(b)$ for $3 \leq b \leq 20$

b	$M_2(b)$
3	38480
4	48391200
5	125096244608
6	618804424079121
7	20721057406576714163
8	945987466487208056191224
9	55940538191331708311472104400
10	8592444743529135815769545955936773
11	1105373397761828143241737786386991708671
12	265147852448848502098555773338261457838146021
13	113377707741342790682562542077632396490643820979692
14	24009263205154407934683568810167126075855812416879485120
15	22547247502066821801492753280147763291252392992548016988539633
16	19350424243438912354196828588241701700337532166126769432980017078701
17	9771327410580082069204544811203201727273697038452545098276035319668495967
18	18439243120912559342277005462816793883105685612493543792760301014308216264410886
19	22643757580438427563497442159186765674826769157538919581661674785897250981739624957239
20	29644302367525205637719953585031678840057791870868847598894287680701297351967464608428822343

generality, we may assume that $g(b) = \pm 1$. Since $g(x) \not\equiv \pm 1$, we know that $g(x)$ has positive degree.

Let c be the leading coefficient of $g(x)$, and let $\beta_1, \ldots, \beta_r$ be the roots of $g(x)$ including multiplicities. Thus, the degree of $g(x)$ is r, and we have

$$1 = |g(b)| = |c| \prod_{j=1}^{r} |b - \beta_j| \geq \prod_{j=1}^{r} |b - \beta_j|.$$

Therefore, at least one root of $g(x)$, and hence of $f(x)$, is in $\mathcal{D}_b$.

We complete the lemma by noting that since $f(x)$ has non-negative coefficients, $f(x)$ has no positive real roots. ∎

As a quick example of the usefulness of such a lemma and to help motivate the ideas that follow, we establish the following result based on ideas from [6].

THEOREM 2.2. *Fix an integer b such that $b \geq 2$, and let $D = D(b)$ be as given in Table 3. Let $f(x) = \sum_{j=0}^{n} a_j x^j$ be a non-constant polynomial in $\mathbb{Z}[x]$ with each $a_j \geq 0$ and with $f(b)$ prime. If the degree of $f(x)$ is $\leq D$, then $f(x)$ is irreducible.*

Table 3. Maximum degree $D = D(b)$

b	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
D	5	9	12	15	18	21	25	28	31	34	37	40	43	47	50	53	56	59	62

Proof. Assume $f(x)$ is reducible. Then it has a non-real root $\alpha \in \mathcal{D}_b = \{z \in \mathbb{C} : |b - z| \leq 1\}$ by Lemma 2.1. Since the complex conjugate of α is also a root of $f(x)$, we may assume that α has a positive imaginary part.

Note that the line passing through the origin and tangent to $\mathcal{D}_b$ from above has slope $\sin^{-1}(1/b)$. We write $\alpha = re^{i\theta}$, where $r \geq b - 1$ and $0 < \theta \leq \sin^{-1}(1/b)$. A direct computation shows that for each $k \in \{1, \ldots, D\}$ we have $0 < k\theta \leq D \sin^{-1}(1/b) < \pi$. This gives

$$\operatorname{Im}(\alpha^k) = r^k \sin(k\theta) > 0 \quad \text{for } 1 \leq k \leq D.$$

As $f(x)$ has non-negative coefficients and $\deg f = n$ with $1 \leq n \leq D$, we have

$$\operatorname{Im}(f(\alpha)) \geq \operatorname{Im}(\alpha^n) > 0,$$

contradicting the fact that α is a root of $f(x)$. ∎

The bounds $D(b)$ given in Table 3 are not all sharp, but are so for many b. Take for example $b = 4$. We see that

$$f(x) = x^{13} + x^3 + 235835x + 16576651$$

is of degree 13, $f(4) = 84628919$ is prime, each coefficient is ≤ 16576651, and $f(x)$ is divisible by $\Phi_3(x-4) = x^2 - 7x + 13$. Thus, $D(4)$ in Table 3 is sharp.

In Section 4, we will give sharp bounds $D(b)$ for all $b \in [2, 20]$. Additionally, although this is not the focus of this paper, we will give sharp bounds on the size of the coefficients when $f(x)$ is reducible and of degree $D(b) + 1$.

A motivating idea for the next two sections is to replace the disk $\mathcal{D}_b$ in Lemma 2.1 with a set of points such that if $\alpha = re^{i\theta}$ is in the new set of points, then $|\theta|$ is bounded above by a number smaller than $\sin^{-1}(1/b)$. This will then allow us to determine sharp bounds for $D(b)$ in place of those given in Table 3 for Theorem 2.2.

3. A root bounding function. For a given $b \in \{2, \ldots, 20\}$, our main goal is to establish the upper bounds $M_1(b)$ and $M_2(b)$ given in Theorem 1.1, and further to show that they are sharp as described after the statement of the theorem. We will utilize three main methods as in [7]. First, we will introduce certain rational functions that will give us information on the location of possible roots of $f(x)$. These rational functions will vary depending on b. Even in the case $b = 10$, we will be able to obtain slightly better information than in [7] by using a modification of the rational function given there. Second, we obtain an initial value for $M_1(b)$ and $M_2(b)$ using a result first introduced in [1] and [2] but based on the main ideas in the earlier work [6]. Third, we use information gained from recursive relations on the possible factors of $f(x)$, as outlined in [7], to establish sharp values of $M_1(b)$ for $b \geq 3$ and sharp values of $M_2(b)$ for $b \geq 4$. In this section, we focus on the first of these ideas.

We recall that $\Phi_n(x)$ denotes the nth cyclotomic polynomial, and we use $\zeta_n = e^{2\pi i/n}$. Fix an integer b with $2 \leq b \leq 20$. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ be such that $a_j \geq 0$ and $f(b)$ is prime.

As in the proof of Lemma 2.1, we consider the case that $f(x)$ is reducible, so that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials with integer coefficients and are not identically ± 1. We may and do suppose that they have positive leading coefficients. Given that $f(p)$ is prime, we take, without loss of generality, $g(b) = \pm 1$. Lemma 2.1 implies that $g(x)$ has a non-real root in $\mathcal{D}_b$. Using the ideas of [7], we wish to show that either $g(x)$ has a root in common with one of

$$\begin{aligned}
\Phi_3(x-b) &= x^2 - (2b-1)x + b^2 - b + 1,\\
\Phi_4(x-b) &= x^2 - 2bx + b^2 + 1,\\
\Phi_6(x-b) &= x^2 - (2b+1)x + b^2 + b + 1,
\end{aligned}$$

or $g(x)$ has roots in a certain region $\mathcal{R}_b$ to be defined shortly.

We define

$$F_b(z) = \frac{N_b(z)}{D_b(z)}, \tag{3.1}$$

where

$$N_b(z) = |b-1-z|^{2e_2}(|b+\zeta_3-z|\,|b+\overline{\zeta_3}-z|)^{2e_3} \cdot (|b+i-z|\,|b-i-z|)^{2e_4}(|b+\zeta_6-z|\,|b+\overline{\zeta_6}-z|)^{2e_6},$$

$$D_b(z) = |b-z|^{4(e_3+e_4+e_6)+2(e_2+d+1)},$$

and $e_2 = e_2(b)$, $e_3 = e_3(b)$, $e_4 = e_4(b)$, $e_6 = e_6(b)$ and $d = d(b)$ are all non-negative integers. For Theorem 1.1, the numbers e_2, e_3, e_4, e_6 and d for a given b are given in Table 4.

Table 4. Numbers used in $F_b(z)$ for b

b	2	3	4	5	$6 \le b \le 20$
$e_2(b)$	20	0	0	0	0
$e_3(b)$	4	15	9	6	4
$e_4(b)$	0	2	2	2	2
$e_6(b)$	0	0	3	3	3
$d(b)$	0	3	3	3	3

We note that these are not the only choices for $e_2(b), e_3(b), e_4(b), e_6(b)$, and $d(b)$ that can serve our purposes. For example, $e_2(10) = 0$, $e_3(10) = 3$, $e_4(10) = 2$, $e_6(10) = 3$, and $d(10) = 3$ are the numbers for $b = 10$ that were used in [7]. Our choices for the numbers in Table 4 are based on trial and error to see what would give us the best results. In the case of $b = 10$, there is a slight advantage that will arise from the use of the e_j's given in Table 4.

Setting $z = x + iy$, it is not difficult to see or to use direct computations to verify that each of the expressions

$$|b-1-z|^2, \quad (|b+\zeta_3-z|\,|b+\overline{\zeta_3}-z|)^2, \quad (|b+i-z|\,|b-i-z|)^2$$
$$(|b+\zeta_6-z|\,|b+\overline{\zeta_6}-z|)^2 \quad \text{and} \quad |b-z|^2$$

is a polynomial in $\mathbb{Z}[b,x,y]$. Therefore, $N_b(z)$ and $D_b(z)$ are polynomials in $\mathbb{Z}[b,x,y]$, so $F_b(z)$ is a rational function in b, x and y.

We write $g(x)$ in the form

$$g(x) = c\prod_{j=1}^{r}(x-\beta_j),$$

where c is the leading coefficient of $g(x)$ and $\beta_1, \dots, \beta_r$ are the roots of $g(x)$, and therefore also roots of $f(x)$. For ease of notation, we define

$$\widetilde{g_b}(n) = g(b+\zeta_n)g(b+\overline{\zeta_n}).$$

One then checks that the two expressions

$$\frac{|g(b-1)|^{2e_2}|\widetilde{g_b}(3)|^{2e_3}|\widetilde{g_b}(4)|^{2e_4}|\widetilde{g_b}(6)|^{2e_6}}{|g(b)|^{4(e_3+e_4+e_6)+2(e_2+d+1)}} \quad \text{and} \quad \frac{1}{c^{2(d+1)}}\prod_{j=1}^{r}F_b(\beta_j)$$

are equal. We denote this common value by $V = V_b(g)$.

Now, each of $\widetilde{g_b}(3)$, $\widetilde{g_b}(4)$, $\widetilde{g_b}(6)$ is a symmetric polynomial, with integer coefficients, in the roots of an irreducible monic quadratic in $\mathbb{Z}[x]$. Hence, each of these expressions is an integer. Also, $g(b-1)$ is an integer. Thus, the numerator of the first expression for V above is an integer. Since $g(b) = \pm 1$ and $V \geq 0$, we know that either $V = 0$ or $V \in \mathbb{Z}^+$.

We recall that $f(x)$ is a polynomial with non-negative integer coefficients. Thus, $f(x)$ cannot have a positive real root, and neither can $g(x)$ which is a factor of $f(x)$. Therefore, $g(b-1) \neq 0$. Either definition of V now implies that $V = 0$ if and only if at least one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, $\Phi_6(x-b)$ is a factor of $g(x)$. If none of these quadratics is a factor of $g(x)$, we necessarily have $V \in \mathbb{Z}^+$. In this case, the product in the second expression for V above must be a positive integer. Since $F_b(z)$ is a non-negative real number for all $z \in \mathbb{C}$, we deduce that $F_b(\beta_j) \geq 1$ for at least one value of $j \in \{1, \ldots, r\}$. In other words, there is a root β of $g(x)$, and consequently of $f(x)$, satisfying $F_b(\beta) \geq 1$.

Summarizing the above ideas, given only that $g(x) \in \mathbb{Z}[x]$, $g(b-1) \neq 0$, $g(x) \not\equiv \pm 1$ and $g(b) = \pm 1$, we have shown that either $g(x)$ has at least one of the factors $\Phi_3(x-b)$, $\Phi_4(x-b)$, $\Phi_6(x-b)$, or $g(x)$ has a root β in the region

$$\mathcal{R}_b = \{z \in \mathbb{C} : F_b(z) \geq 1\}. \tag{3.2}$$

In the latter case, we will use an analysis of the region $\mathcal{R}_b$ in the complex plane to obtain important information about the location of β.

It is of some interest to note that the conditions above that $g(x) \in \mathbb{Z}[x]$, $g(x) \not\equiv \pm 1$ and $g(b) = \pm 1$ are sufficient to show that $g(x)$ has a root in $\mathcal{D}_b$. Figures 1, 2 and 3 depict regions $\mathcal{R}_b$ for $b \in \{2, 3, 4\}$ where $e_2(b)$, $e_3(b)$, $e_4(b)$, $e_6(b)$ and $d(b)$ are as given in Table 4. The circle is the unit circle centered at b, the boundary of $\mathcal{D}_b$. These graphs are, of course, obtained from plotting only a finite set of points and are not used in our proofs but are intended to help visualize $\mathcal{R}_b$.

Figure 4 shows $\mathcal{R}_{10}$ for our choice of $e_2(10) = 0$, $e_3(10) = 4$, $e_4(10) = 2$, $e_6(10) = 3$ and $d(10) = 3$ while Figure 5 shows $\mathcal{R}_{10}$ for the choice of $e_2(10) = 0$, $e_3(10) = 3$, $e_4(10) = 2$, $e_6(10) = 3$ and $d(10) = 3$ used in [7]. Although the difference is subtle, Figure 5 is symmetric about the vertical line $x = 10$, while Figure 4 is slightly narrower at the front of the region.

In what follows, we will sometimes refer to points (x, y) in $\mathcal{R}_b$, and this is to be interpreted as the point $z = x + iy$ in the complex plane in $\mathcal{R}_b$. For example, taking $b = 6$, we will see later that all the points $(x, y) \in \mathcal{R}_6$ lie below the line $y = \tan(\pi/21)x$. This then means that any point $z = x + iy \in \mathcal{R}_6$ satisfies $y \leq \tan(\pi/21)x$.

To further help us analyze the region $\mathcal{R}_b$, we define

$$P_b(x, y) = D_b(x + iy) - N_b(x + iy). \tag{3.3}$$

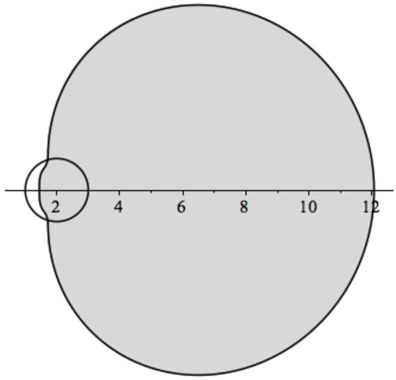

Fig. 1. Image of $\mathcal{R}_2$

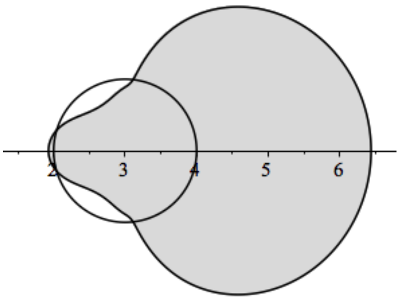

Fig. 2. Image of $\mathcal{R}_3$

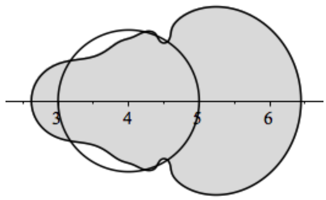

Fig. 3. Image of $\mathcal{R}_4$

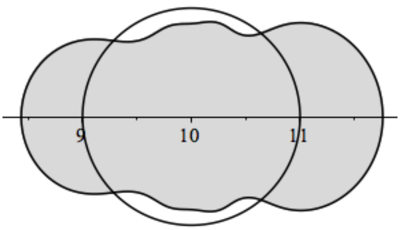

Fig. 4. Our choice for $\mathcal{R}_{10}$

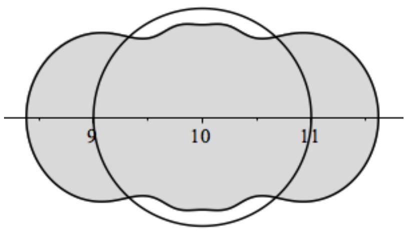

Fig. 5. $\mathcal{R}_{10}$ used in [7]

Direct computations for each $b \in \{2, \ldots, 20\}$ show that we can write

$$P_b(x, y) = \sum_{j=0}^{r} a_j(b, x) y^{2j}, \tag{3.4}$$

where $r = 2(e_3+e_4+e_6)+e_2+d+1$ and each $a_j(b, x)$ is an integer polynomial in b and x. Furthermore, the definition of $D_b(z)$ implies that $D_b(z) > 0$ for all $z \in \mathbb{C}$ with $z \neq b$. Thus,

$$F_b(x + iy) \geq 1 \quad \text{and} \quad P_b(x, y) \leq 0$$

are equivalent for $z \neq b$. Also, the equations $F_b(x+iy) = 1$ and $P_b(x, y) = 0$ are equivalent for $z \neq b$. Note that $P_b(b, 0) = D_b(b) - N_b(b) = 0 - 1 = -1$. Therefore, the $z = x + iy \in \mathbb{C}$ such that $F_b(z) = 1$ correspond exactly to the points (x, y) where $P_b(x, y) = 0$.

We introduce the following technical lemma that corresponds to [7, Lemma 2].

LEMMA 3.1. *Fix an integer $2 \leq b \leq 20$. Then there exist real numbers $a_0 = a_0(b)$, $a_1 = a_1(b)$, and a non-negative real-valued function $\rho_b(x)$ defined on the interval $I_b = [b - a_0, b + a_1]$ such that:*

(i) *$P_b(x, y) \neq 0$ for all $x \notin I_b$ and $y \in \mathbb{R}$.*
(ii) *$P_b(x, \rho_b(x)) = 0$ for all $x \in I_b$.*
(iii) *$\rho_b(b - a_0) = 0$ and $\rho_b(b + a_1) = 0$.*
(iv) *The function $\rho_b(x)$ is continuously differentiable on the interior of I_b and is continuous on I_b.*
(v) *If x and y are real numbers for which $P_b(x, y) \leq 0$, then $x \in I_b$ and $|y| \leq \rho_b(x)$.*

In view of the above lemma, complex numbers of the form $x + i\rho_b(x)$ are boundary points of $\mathcal{R}_b$ which are on or above the real axis. Since $P_b(x, y)$ is a polynomial in y^2 with coefficients in $\mathbb{Z}[b, x]$, our region $\mathcal{R}_b$ is symmetric about the real axis. Thus, the points $x - i\rho_b(x)$ are boundary points of $\mathcal{R}_b$ which are on or below the real axis. The points $b - a_0$ and $b + a_1$ are boundary points on the real axis.

To prove Lemma 3.1, we use the Implicit Function Theorem (cf. [12]), which we state next.

LEMMA 3.2. *Let $\mathfrak{D}$ be an open set in $\mathbb{R}^2$ and let $W : \mathfrak{D} \to \mathbb{R}$. Suppose W has continuous partial derivatives W_x and W_y on $\mathfrak{D}$. Let $(x_0, y_0) \in \mathfrak{D}$ be such that*

$$W(x_0, y_0) = 0 \quad \text{and} \quad W_y(x_0, y_0) \neq 0.$$

Then there is an open interval $\mathfrak{I} \in \mathbb{R}$ and a real-valued, continuously differentiable function ϕ defined on $\mathfrak{I}$ such that $x_0 \in \mathfrak{I}$, $\phi(x_0) = y_0$, $(x, \phi(x)) \in \mathfrak{D}$ for all $x \in \mathfrak{I}$, and $W(x, \phi(x)) = 0$ for all $x \in \mathfrak{I}$.

Our proof of Lemma 3.1 is a variation of [7, proof of Lemma 2]. A number of changes and some simplifications are introduced. In particular, the proof in [7] used more than once the fact that a certain discriminant is non-zero, which no longer applies in our case, so some changes in the arguments here become necessary.

We give a proof based on the values of (e_2, e_3, e_4, e_6, d) given in Table 4 for each b. Before delving into the proof, we note that we will want analogous results for other choices of (e_2, e_3, e_4, e_6, d) in the next section and that the same lemma holds following the same line of argument. Specifically, we will additionally use Lemma 3.1 for $(e_2, e_3, e_4, e_6, d) = (0, 2, 1, 0, 1)$ and $b = 2$, for $(e_2, e_3, e_4, e_6, d) = (0, 2, 3, 0, 8)$ and $b = 3$, for $(e_2, e_3, e_4, e_6, d) = (0, 2, 4, 0, 8)$ and $b = 4$ or 5, for $(e_2, e_3, e_4, e_6, d) = (0, 2, 5, 0, 12)$ and $b = 6$ or 7, for $(e_2, e_3, e_4, e_6, d) = (0, 1, 8, 0, 14)$ and $8 \le b \le 14$, and for $(e_2, e_3, e_4, e_6, d) = (0, 1, 10, 0, 24)$ and $15 \le b \le 20$.

Proof of Lemma 3.1. We fix an integer $b \in [2, 20]$, and let $e_2 = e_2(b)$, $e_3 = e_3(b)$, $e_4 = e_4(b)$, $e_6 = e_6(b)$ and $d = d(b)$ be as in Table 4. We set $r = 2(e_3 + e_4 + e_6) + e_2 + d + 1$, and let $P_b(x, y)$ be as in (3.4). For $0 \le j \le r$, define $p_j(b, x) = a_j(b, x + b)$, and set

$$\overleftarrow{P_b}(x, y) = \sum_{j=0}^{r} p_j(b, x) y^j = \sum_{j=0}^{r} a_j(b, x + b) y^j.$$

Thus,

$$\overleftarrow{P_b}(x, y^2) = P_b(x + b, y). \tag{3.5}$$

Observe that the points (x, y) corresponding to $\overleftarrow{P_b}(x, y^2) \le 0$ are the points $(x-b, y)$ where $(x, y) \in \mathcal{R}_b$; in other words, the (x, y) satisfying $\overleftarrow{P_b}(x, y^2) \le 0$ correspond to the $(x, y) \in \mathcal{R}_b$ translated to the left by b.

For fixed $b \in [2, 20]$, the expression p_j is a polynomial with integer coefficients in the variable x. The dependence on b only arises in our choice of $e_2(b)$, $e_3(b)$, $e_4(b)$, $e_6(b)$ and $d(b)$. Since the same choice is used for each $b \in [6, 20]$, we have only five sets of $p_j(b, x)$ to consider. We computed these explicitly to help with the analysis that follows.

To simplify our notation and avoid confusion, we use $\overleftarrow{P_b}(y)$ for $\overleftarrow{P_b}(x, y)$ when we are viewing $\overleftarrow{P_b}(x, y)$ as a polynomial in y whose coefficients are polynomials in x. Table 5 lists r, the degree of $\overleftarrow{P_b}(y)$, for each b.

Table 5. Degree r of $\overleftarrow{P_b}(y)$ for $b \in [2, 20]$

b	r
2	29
3	38
4	32
5	26
$6 \le b \le 20$	22

Using a Sturm sequence, we verify that $p_0(b, x)$ has exactly two distinct real roots. One checks that $p_0(b, x) = 0$ has a negative root, which we denote by $-a_0$, and a positive root, which we call a_1. Computations give us the values of a_0 and a_1 for $b \in [2, 20]$, accurate to the digits shown in Table 6. We show that a_0 and a_1 have the properties stated in Lemma 3.1.

Table 6. Values of a_0 and a_1 for $b \in [2, 20]$

b	a_0	a_1	$\hat{a}_0$	$\hat{a}_1$
2	$0.5523770847\ldots$	$10.0651310946\ldots$	0.5523	10.06
3	$1.0721963435\ldots$	$3.4397713145\ldots$	1.07	3.43
4	$1.3782037799\ldots$	$2.4446162254\ldots$	1.37	2.44
5	$1.4754544841\ldots$	$2.0416766993\ldots$	1.47	2.04
$6 \leq b \leq 20$	$1.5638035689\ldots$	$1.7605007116\ldots$	1.56	1.76

Let J_b denote the interval $[-a_0, a_1]$. Using a Sturm sequence, one can verify that for each $j \in \{1, \ldots, r\}$, the polynomial $p_j(b, x)$ has all of its real roots in the interval $[-\hat{a}_0, \hat{a}_1] \subset J_b$, where $\hat{a}_0$ and $\hat{a}_1$ are given in Table 6.

Recalling (3.5), we see that to prove part (i), we need only show that for each $x_0 \notin J_b$ the real roots of $\overleftarrow{P}_b(x_0, y)$ are all negative. A simple calculation shows that $p_j(b, \pm 11) > 0$ for all $j \in \{0, 1, \ldots, r\}$ (and each b). Since each $p_j(b, x)$ has its real roots inside J_b, we deduce that $p_j(b, x_0) > 0$ for each j. From Descartes' rule of signs, we find that $\overleftarrow{P}_b(x_0, y)$ has no positive real roots. Part (i) now follows. We note for further use that also

$$P_b(x, y) > 0 \quad \text{for all } x \notin I_b \text{ and all } y \in \mathbb{R}. \tag{3.6}$$

We turn to the remaining parts of Lemma 3.1. For a given $x \in I_b$, we want to define $\rho_b(x)$ as the largest non-negative real root of $P_b(x, y)$. First, however, we need to show that such a non-negative real root exists. From (3.5), we see that for $x \in J_b$ we want $(\rho_b(x + b))^2$ to be a root of $\overleftarrow{P}_b(y)$. Further, showing $P_b(x, y)$ has a non-negative real root for each $x \in I_b$ is equivalent to showing $\overleftarrow{P}_b(y)$ has a non-negative real root for each $x \in J_b$.

A direct computation gives $p_0(b, 0) = -1$ and $p_r(b, x) \equiv 1$. Since $p_0(b, x)$ has only the two real roots $-a_0$ and a_1, it follows that $p_0(b, x_0) < 0$ for all $x_0 \in (-a_0, a_1)$. Since $\overleftarrow{P}_b(y)$ is monic and of degree $r > 0$, we deduce that $\overleftarrow{P}_b(x_0, y) = 0$ has a positive real root in y for all $x_0 \in (-a_0, a_1)$.

We now consider the case that $x_0 = -a_0$ or $x_0 = a_1$. As noted earlier, for each $j \in \{1, \ldots, r\}$, the polynomial $p_j(b, x)$ has its roots in the interval $[-\hat{a}_0, \hat{a}_1]$ and $p_j(b, \pm 11) > 0$. Since each of $-a_0$, a_1 and ± 11 is not in $[-\hat{a}_0, \hat{a}_1]$ while $x_0 = -a_0$ or $x_0 = a_1$, it follows that $p_j(b, x_0) > 0$ for each such j. From Descartes' rule of signs, we deduce that $\overleftarrow{P}_b(x_0, y)$ has no positive real roots. Thus, $\overleftarrow{P}_b(x_0, y)$ has 0 as its largest real root.

For a given $x \in I_b$, we now define $\rho_b(x)$ as the largest non-negative real root of $P_b(x, y)$. The above arguments show that $\rho_b(x)$ is well-defined.

For each $x \in J_b$, define

$$\psi_b(x) = \max\{y \in \mathbb{R} : \overleftarrow{P}_b(y) = 0\}.$$

Since $\overleftarrow{P_b}(y)$ has real roots for any given $x \in J_b$, we see that $\psi_b(x)$ is well-defined. Moreover, we have seen that $\psi_b(x) > 0$ for all $x \in (-a_0, a_1)$, and $\psi_b(-a_0) = \psi_b(a_1) = 0$. Parts (ii) and (iii) now follow by observing that $\rho_b(x) = \sqrt{\psi_b(x-b)}$ for each $x \in I_b$.

Next, we turn to (iv) and (v). The arguments for these parts are similar to those for [7, Lemma 2(d), (e)]. To prove $\rho_b(x)$ is a continuously differentiable function on $(b-a_0, b+a_1)$, it is sufficient to show that, given any $x_0 \in (-a_0, a_1)$, there exists an open interval $J' \subseteq (-a_0, a_1)$ containing x_0 such that $\psi_b(x)$ is a continuously differentiable function on J'. To prove that $\rho_b(x)$ is a continuous function on $[b-a_0, b+a_1]$, we will also want to show that

$$\lim_{x\to -a_0^+} \psi_b(x) = 0 \quad \text{and} \quad \lim_{x\to a_1^-} \psi_b(x) = 0.$$

Fix $x_0 \in (-a_0, a_1)$, and let $y_0 = \psi_b(x_0)$. We make use of Lemma 3.2 with $W(x,y) = \overleftarrow{P_b}(x,y)$. Since $W(x,y)$ is then a polynomial, both W_x and W_y are continuous on all of $\mathbb{R}^2$. The definition of y_0 implies $W(x_0, y_0) = 0$.

For Lemma 3.2, we also want to show that $W_y(x_0, y_0) \neq 0$. In the case $b \neq 2$, we calculate the discriminant $\Delta_b(x)$ of $\overleftarrow{P_b}(y)$. A Sturm sequence computation shows that $\Delta_b(x) \neq 0$ for all $x \in \mathbb{R}$. To clarify, the computation of the Sturm sequence was shortened by first factoring the discriminant and then showing $\Delta_b(x) \neq 0$ for all $x \in \mathbb{R}$ by establishing that each factor of $\Delta_b(x)$ is non-zero for all $x \in \mathbb{R}$ using a separate Sturm sequence for each factor. Therefore, in the case $b \neq 2$, we see that $\overleftarrow{P_b}(x_0, y)$ has no repeated roots, so $W_y(x_0, y_0) \neq 0$.

In the case $b = 2$, a Sturm sequence computation shows that $\Delta_2(x)$ is non-zero on J_2 when $x \neq -1/2$. Thus, $\overleftarrow{P_2}(x,y)$ has a repeated root for $x \in J_2$ only when $x = -1/2$. By factoring $\overleftarrow{P_2}(-1/2, y)$, one sees that the only repeated root of $\overleftarrow{P_2}(-1/2, y)$ is $y = -1/4$. Therefore, in our case where $y_0 \geq 0$, $W_y(x_0, y_0) \neq 0$.

Now define $\mathfrak{D} = \{(x,y) \in \mathbb{R}^2 : -a_0 < x < a_1 \text{ and } y > 0\}$. By Lemma 3.2, there exist an open interval $J'' \subseteq (-a_0, a_1)$ containing x_0 and a continuously differentiable function $\phi(x)$ defined on J'' such that both $\phi(x_0) = y_0$ and $\overleftarrow{P_b}(x, \phi(x)) = 0$ for all $x \in J''$. By the definition of $\psi_b(x)$, we know that $\phi(x) \leq \psi_b(x)$ for all $x \in J''$. We will show that there exists an open interval $J' \subseteq J''$ containing x_0 such that $\psi_b(x) = \phi(x)$ for all $x \in J'$.

By way of contradiction, assume that no such interval J' exists. Then there exists a sequence $\{x_n\}_{n=1}^{\infty}$ satisfying $\lim_{n\to\infty} x_n = x_0$ and having the property that, for all $n \geq 1$, $\psi_b(x_n) > \phi(x_n)$. Since $x_0 \in J''$, we suppose further as we may that each x_n is in J''. Define $y_n = \psi_b(x_n)$. In particular, $\overleftarrow{P_b}(x_n, y_n) = 0$.

We justify that $\{y_n\}_{n=1}^{\infty}$ is a bounded sequence. In fact, we show that there is an absolute constant M such that for $x' \in J_b$ and $z \in \mathbb{C}$ satisfying $\overleftarrow{P_b}(x', z) = 0$, we have $|z| \leq M$. Since each $p_j(b, x)$ is continuous on J_b and J_b is compact, there exists an absolute constant $A \geq 0$ such that $|p_j(b, x)| \leq A$ for all $j \in \{0, \ldots, r\}$ and $x \in J_b$. Recall $p_r(b, x) \equiv 1$. Since $x' \in J_b$ and $\overleftarrow{P_b}(x', z) = 0$, we deduce

$$0 = \Big|\sum_{j=0}^{r} p_j(b, x') z^j\Big| \geq |z|^r - \sum_{j=0}^{r-1} |p_j(b, x')|\,|z|^j \geq |z|^r - A\sum_{j=0}^{r-1} |z|^j.$$

Thus, $|z|$ is less than or equal to the positive real root M of the polynomial

$$x^r - Ax^{r-1} - Ax^{r-2} - \cdots - Ax - A.$$

We deduce that $\{y_n\}_{n=1}^{\infty}$ is a sequence with $|y_n| \leq M$ for all n.

It follows now that $\{y_n\}_{n=1}^{\infty}$ has a convergent subsequence $\{y_{n_j}\}_{j=1}^{\infty}$. Let $L = \lim_{j\to\infty} y_{n_j}$. The continuity of $\overleftarrow{P_b}(x, y)$ implies

$$\overleftarrow{P_b}(x_0, L) = \lim_{j\to\infty} \overleftarrow{P_b}(x_{n_j}, y_{n_j}) = 0.$$

Since

$$y_0 = \psi_b(x_0) = \max\{y \in \mathbb{R} : \overleftarrow{P_b}(x_0, y) = 0\},$$

we deduce that $L \leq y_0$. Since $\phi(x)$ is continuous on J'' and $\phi(x_{n_j}) \leq \psi_b(x_{n_j}) = y_{n_j}$ for all $j \geq 1$, we also have

$$L = \lim_{j\to\infty} y_{n_j} = \lim_{j\to\infty} \psi_b(x_{n_j}) \geq \lim_{j\to\infty} \phi(x_{n_j}) = \phi\Big(\lim_{j\to\infty} x_{n_j}\Big) = \phi(x_0) = y_0.$$

Thus, $L = y_0$. In particular,

$$\lim_{j\to\infty} \psi_b(x_{n_j}) = y_0 = \lim_{j\to\infty} \phi(x_{n_j}). \tag{3.7}$$

We show that this implies a contradiction.

Consider

$$\big|W(x_{n_j}, \psi_b(x_{n_j})) - W(x_{n_j}, \phi(x_{n_j}))\big| = 0.$$

By the Mean Value Theorem, we have

$$|\psi_b(x_{n_j}) - \phi(x_{n_j})|\,|W_y(x_{n_j}, \xi_j)| = 0 \tag{3.8}$$

for some $\xi_j \in [\phi(x_{n_j}), \psi_b(x_{n_j})]$. Since $\psi_b(x_{n_j}) > \phi(x_{n_j})$, we deduce from (3.8) that

$$W_y(x_{n_j}, \xi_j) = 0.$$

Taking the limit as $j \to \infty$, we find by (3.7) that $\lim_{j\to\infty} \xi_j = y_0$ so that $W_y(x_0, y_0) = 0$. But this contradicts the fact that $W_y(x_0, y_0) \neq 0$. Therefore, there exists an open interval $J' \subseteq J''$ containing x_0 such that $\psi_b(x) = \phi(x)$ for all $x \in J'$.

To finish the proof of (iv), we need only show that $\psi_b(x)$ is continuous at the endpoints of J_b. Let $\{x_n\}_{n=1}^{\infty} \subset J_b$ be a sequence that converges to one of the endpoints of J_b, say a'. Take $y_n = \psi_b(x_n)$. With M as before, we have $|y_n| \le M$. To show that

$$\lim_{n\to\infty} \psi_b(x_n) = 0 = \psi_b(a'),$$

it suffices to prove that every convergent subsequence of y_n converges to 0.

Suppose that $\{y_{n_j}\}$ is such that $\lim_{j\to\infty} y_{n_j} = L$ for some $L \in \mathbb{R}$. Since we know that $y_{n_j} = \psi_b(x_{n_j}) \ge 0$, we deduce $0 \le L \le M$. Now,

$$\overleftarrow{P_b}(a', L) = \lim_{j\to\infty} \overleftarrow{P_b}(x_{n_j}, y_{n_j}) = \lim_{j\to\infty} \overleftarrow{P_b}(x_{n_j}, \psi_b(x_{n_j})) = 0.$$

Therefore, $L \le \psi_b(a') = 0$. Hence, $L = 0$, completing the proof of (iv).

To establish (v), we first observe that the definition of $\rho_b(x)$ implies if $x \in I_b$ and $y \in \mathbb{R}$ are such that $P_b(x,y) = 0$, then $|y| \le \rho_b(x)$. Part (i) also implies that if $P_b(x,y) = 0$ for some real numbers x and y, then $x \in I_b$. Now, consider real numbers x_0 and y_0 for which $P_b(x_0,y_0) < 0$. Note that (3.6) implies $x_0 \in I_b$ and $P_b(0,0) > 0$. Since $P_b(x,y)$ is a continuous function from $\mathbb{R}^2$ to $\mathbb{R}$, we deduce that along any path from $(0,0)$ to (x_0,y_0) in $\mathbb{R}^2$, there must be a point (x,y) satisfying $P_b(x,y) = 0$. We use again the fact that for any $x \in J_b$, the number M is a bound on the absolute value of the roots of $\overleftarrow{P_b}(y)$. We deduce from (3.5) that $\rho_b(x) \le \sqrt{M}$ for all $x \in I_b$. If $x_0 \in I_b$ and $y_0 > \rho_b(x_0)$, then one can consider the path consisting of line segments from $(0,0)$ to $(0, 1+\sqrt{M})$, from $(0, 1+\sqrt{M})$ to $(x_0, 1+\sqrt{M})$ and from $(x_0, 1+\sqrt{M})$ to (x_0,y_0) to obtain a contradiction. If $x_0 \in I_b$ and $y_0 < -\rho_b(x_0)$, one can consider a similar path but from $(0,0)$ to $(0, -1-\sqrt{M})$ to $(x_0, -1-\sqrt{M})$ to (x_0,y_0) to obtain a contradiction. Therefore, $x_0 \in I_b$ and $|y_0| \le \rho_b(x_0)$. This establishes part (v), completing the proof of Lemma 3.1. ∎

In the following sections we will use Lemma 3.1 to prove irreducibility criteria based on the degree of $f(x)$ and on the size of the coefficients of $f(x)$.

4. Irreducibility criteria based on degree. Fix an integer $b \in [2,20]$. Let $f(x) \in \mathbb{Z}[x]$ have non-negative coefficients, with $f(b)$ prime. Theorem 2.2 led us to deduce the irreducibility of $f(x)$ given bounds $D(b)$ on the degree of $f(x)$. As noted there, those bounds were not necessarily sharp. In this section, we use the region $\mathcal{R}_b$ to establish sharp bounds corresponding to Theorem 2.2.

Take for example $b = 6$. Theorem 2.2 and Table 3 tell us that if $f(6)$ is prime and the degree of $f(x)$ is ≤ 18, then $f(x)$ is irreducible. We now prove that if $f(6)$ is prime and the degree of $f(x)$ is ≤ 19, then $f(x)$ is irreducible. Furthermore, we give an example to show that this bound is sharp.

Our next lemma follows from the proof of Theorem 2.2 given in Section 2.

LEMMA 4.1. *Let n be a positive integer. A complex number $\alpha = re^{i\theta}$ with $0 < \theta < \pi/n$ cannot be a root of a non-zero polynomial with non-negative integer coefficients and degree $\leq n$.*

Now, we can establish the following improvement on Theorem 2.2.

THEOREM 4.2. *Fix an integer $b \in [2, 20]$, and let $D = D(b)$, $D_1 = D_1(b)$, and $D_2 = D_2(b)$ be as in Table 7. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_j \geq 0$ for each j and with $f(b)$ prime. If the degree of $f(x)$ is $\leq D$, then $f(x)$ is irreducible. Additionally, if $\deg f(x) \leq D_1$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$ and not divisible by $\Phi_3(x-b)$. Furthermore, if $\deg f(x) \leq D_2$ and $f(x)$ is reducible, then $f(x)$ is divisible by either $\Phi_4(x-b)$ or $\Phi_3(x-b)$.*

Table 7. $D(b)$, $D_1(b)$, $D_2(b)$, $\vartheta(b)$, and $m(b)$ for $b \in [2, 20]$

b	$D(b)$	$D_1(b)$	$D_2(b)$	$\vartheta(b)$	$m(b)$
2	6	–	7	$\pi/7$	13/27
3	9	–	11	$\pi/11$	32/109
4	12	–	15	$\pi/15$	17/80
5	15	16	18	$\pi/18$	70/397
6	19	20	22	$\pi/22$	67/466
7	22	23	25	$\pi/25$	1/8
8	25	27	29	$\pi/29$	5/46
9	28	30	33	$\pi/33$	2/21
10	31	34	37	$\pi/37$	4/47
11	34	38	40	$\pi/40$	7/89
12	37	41	44	$\pi/44$	1/14
13	40	45	47	$\pi/47$	1/15
14	44	49	51	$\pi/51$	4/65
15	47	52	55	$\pi/55$	125/2186
16	50	56	58	$\pi/58$	2/37
17	53	59	62	$\pi/62$	4/79
18	56	63	65	$\pi/65$	43/889
19	59	67	69	$\pi/69$	1/22
20	62	70	72	$\pi/72$	1/23

We note that for $b \in \{2, 3, 4\}$, there is no value for D_1 due to the equality
$$\left\lfloor \frac{\pi}{\arg(b+\zeta_4)} \right\rfloor = \left\lfloor \frac{\pi}{\arg(b+\zeta_3)} \right\rfloor \quad \text{for } b \in \{2, 3, 4\}.$$
By way of examples, we will demonstrate later that the values of $D(b)$ and $D_1(b)$ given in Table 7 are sharp. We do not know whether this is the case for the values of $D_2(b)$. It is also worth noting that $D_2(10)$ above is an improvement over the value 36 established in [7].

Proof of Theorem 4.2. Following the remarks before the proof of Lemma 3.1, we set
$$(e_2, e_3, e_4, e_6, d) = \begin{cases} (0, 2, 1, 0, 1) & \text{for } b = 2, \\ (0, 2, 3, 0, 8) & \text{for } b = 3, \\ (0, 2, 4, 0, 8) & \text{for } b = 4 \text{ or } 5, \\ (0, 2, 5, 0, 12) & \text{for } b = 6 \text{ or } 7, \\ (0, 1, 8, 0, 14) & \text{for } 8 \leq b \leq 14, \\ (0, 1, 10, 0, 24) & \text{for } 15 \leq b \leq 20. \end{cases}$$

We define $F_b(z)$ as in (3.1), $P_b(x,y)$ as in (3.3), and $\mathcal{R}_b$ as in (3.2). In addition to $D = D(b)$, $D_1 = D_1(b)$ and $D_2 = D_2(b)$, we set $\vartheta = \vartheta(b)$ and $m = m(b)$ as in Table 7. We note that m is a rational number.

We consider the line $y = \tan(\vartheta)x$ or equivalently the points $x + i\tan(\vartheta)x$ in the complex plane. A simple computation gives $\tan(\vartheta) > m$. So the line $y = mx$ lies strictly below $y = \tan(\vartheta)x$ for $x > 0$. Applying Lemma 3.1, we find that $\rho_b(b - a_0) = 0$ and $\rho_b(x)$ is continuous. We use a Sturm sequence to verify that $P_b(x, mx)$ has no real roots. Since the coefficients of $P_b(x, mx)$ are rational, this computation involves only exact arithmetic. Using Lemma 3.1(ii), we can deduce that $\mathcal{R}_b$ does not intersect the line $y = mx$. Therefore, the entire region $\mathcal{R}_b$ lies below that line.

We recall the set-up from Section 3. We suppose $f(x)$ is reducible and write $f(x) = g(x)h(x)$, where both $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, $g(x) \not\equiv \pm 1$, $h(x) \not\equiv \pm 1$, and both $g(x)$ and $h(x)$ have positive leading coefficients. Furthermore, without loss of generality, we suppose that $g(b) = \pm 1$. In Section 3, we showed that either $g(x)$ has a root in common with at least one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, $\Phi_6(x-b)$, or $g(x)$ has a root $\beta \in \mathcal{R}_b$. Since $f(x)$ has non-negative coefficients and the real numbers in $\mathcal{R}_b$ are positive, we see that $\beta \notin \mathbb{R}$.

With our choices above, $b + \zeta_6$ lies below the line $y = mx$ for each $b \in [2, 20]$. This is illustrated in Figure 6 for $b = 5$, where the straight line passes through the origin and its slope is 70/397.

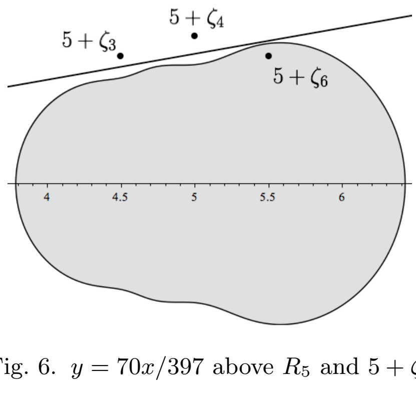

Fig. 6. $y = 70x/397$ above R_5 and $5 + \zeta_6$

We conclude that either $g(x)$ has a root in common with $\Phi_3(x-b)$ or with $\Phi_4(x-b)$, or $g(x)$ has a root $\beta = \sigma + it$ such that $0 < t < m\sigma < \tan(\vartheta)\sigma$. Note that the latter implies that if $\beta = re^{i\vartheta'}$, then $\vartheta' < \vartheta$. With an eye toward applying Lemma 4.1, we deduce from Table 7 that $\vartheta' < \vartheta = \pi/D_2 < \pi/D$ for $b \in \{2, 3, 4\}$ and $\vartheta' < \vartheta = \pi/D_2 < \pi/D_1 < \pi/D$ for $b \in [5, 20]$.

For $b \geq 3$, a computation gives $\arg(b+\zeta_3) < \pi/D$ and $\arg(b+\zeta_4) < \pi/D$. Thus, by Lemma 4.1, we find that $f(x)$ is irreducible if $\deg f \leq D$.

In the case of $b = 2$, we have $\arg(2 + \zeta_4) < \pi/D$ but $\arg(2 + \zeta_3) = \pi/D$. We show that in this case, if $\deg f(x) = D = 6$ and $f(x)$ is divisible by $\Phi_3(x - 2)$, then $f(2)$ is necessarily composite, contradicting our original assumption.

Since we want $\Phi_3(x - 2) = x^2 - 3x + 3$ to be a factor of $f(x)$, and $\deg f(x) = 6$, the other factor of $f(x)$ is $u_1x^4 + u_2x^3 + u_3x^2 + u_4x + u_5$, where $u_1, u_2, u_3, u_4, u_5 \in \mathbb{Z}$ and $u_1 \geq 1$. This yields

$$\begin{aligned} f(x) &= (x^2 - 3x + 3)(u_1x^4 + u_2x^3 + u_3x^2 + u_4x + u_5) \\ &= u_1x^6 + (u_2 - 3u_1)x^5 + (3u_1 - 3u_2 + u_3)x^4 + (3u_2 - 3u_3 + u_4)x^3 \\ &\quad + (3u_3 - 3u_4 + u_5)x^2 + (3u_4 - 3u_5)x + 3u_5. \end{aligned}$$

Observe that $2 + \zeta_3$ is a root of $f(x)$ and each coefficient of $f(x)$ is non-negative. Also, the imaginary part of $(2+\zeta_3)^j$ is > 0 for $j \in \{1, \ldots, 5\}$, and $(2 + \zeta_3)^6 = -27$. If one of the coefficients of x, x^2, x^3, x^4 or x^5 in $f(x)$ is > 0, then $\mathrm{Im}(f(2 + \zeta_3)) > 0$, contradicting the fact that $2 + \zeta_3$ is a root of $f(x)$. Thus, $u_2 - 3u_1 = 0$, $3u_1 - 3u_2 + u_3 = 0$, $3u_2 - 3u_3 + u_4 = 0$, $3u_3 - 3u_4 + u_5 = 0$ and $3u_4 - 3u_5 = 0$. Solving for u_2, u_3, u_4 and u_5, we obtain $u_2 = 3u_1$, $u_3 = 6u_1$, $u_4 = 9u_1$ and $u_5 = 9u_1$. This gives $f(x) = u_1x^6 + 27u_1$. Hence, $f(2) = 91u_1 = 7 \cdot 13 \cdot u_1$, so $f(2)$ is composite. Thus, the case $b = 2$ also leads to the statement involving the bound D in Theorem 4.2.

We now turn to establishing the statements concerning D_1 and D_2.

For $b \geq 5$, we have $\arg(b+\zeta_3) < \pi/D_1$, $\arg(b+\zeta_4) > \pi/D_1$, and $D_1 > D$. Thus, by Lemma 4.1, if $f(x)$ is reducible and $\deg f(x) \leq D_1$, then $f(x)$ is divisible by $\Phi_4(x - b)$. For $2 \leq b \leq 20$, we have $\arg(b + \zeta_3) > \pi/D_2$, $\arg(b + \zeta_4) > \pi/D_2$, and $D_2 > D$. Thus, by Lemma 4.1, if $f(x)$ is reducible and $\deg f(x) \leq D_2$, then $f(x)$ is divisible by $\Phi_3(x - b)$ or $\Phi_4(x - b)$. Note that what is significant, in this part of the argument, is that $\tan(\pi/D_2) \geq m$ and $y = mx$ lies above the region $\mathcal{R}_b$.

This completes the proof of Theorem 4.2. ∎

Examples given later in Tables 19 and 20 will show that the bounds $D(b)$ and $D_1(b)$ are sharp. For example, take $b = 6$, where we see that $D(6)$ has increased from 18 in Theorem 2.2 to 19 in Theorem 4.2. The polynomial

$$\begin{aligned} f(x) = x^{20} &+ 2x^3 + 13519269991320x^2 + 610418402115746x \\ &+ 610418402115527 \end{aligned}$$

is of degree 20, $f(6) = 8415780974560931$ is prime, each coefficient of $f(x)$ is at most 610418402115746, and $f(x)$ is divisible by $\Phi_4(x - 6) = x^2 - 12x + 37$. Although not our ultimate goal, we will prove later in Section 8 that this polynomial is also optimal in terms of the size of its coefficients. We will show that if $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree 20 with non-negative integer coefficients which are ≤ 610418402115745 and $f(6)$ is prime, then $f(x)$ is irreducible. More generally, we will establish the following result.

THEOREM 4.3. *Fix an integer $b \in [2, 20]$, let $D = D(b)$ and $D_1 = D_1(b)$ (for $b \geq 5$) be as in Table 7, let $N_1 = N_1(b)$ be as in Table 8, and let $N_2 = N_2(b)$ (for $b \geq 5$) be as in Table 9. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ be such that $a_j \geq 0$ for each j and $f(b)$ is prime. If $\deg f(x) = D + 1$ and each $a_j \leq N_1$, then $f(x)$ is irreducible. In the case $5 \leq b \leq 20$, if $\deg f(x) = D_1 + 1$ and each $a_j \leq N_2$, then $f(x)$ is either irreducible, or divisible by $\Phi_3(x - b)$ if $b = 5$, or divisible by $\Phi_4(x - b)$ if $b \in [6, 20]$.*

As indicated before, the bounds $N_1(b)$ and $N_2(b)$ given in Tables 8 and 9 will all be shown to be sharp and will involve coming up with explicit examples. These details appear in Section 8.

5. A first bound on the coefficients. Throughout this section, $\mathcal{R}_b$ is as defined in (3.2), with $F_b(z)$ given by (3.1) and $P_b(x, y)$ given by (3.3). The numbers $e_2(b)$, $e_3(b)$, $e_4(b)$, $e_6(b)$ and $d(b)$ are as given in Table 4.

We summarize the previous sections and set the goal for this section. We have fixed an integer $b \in [2, 20]$, and taken a polynomial $f(x)$ with each coefficient non-negative and $f(b)$ prime. We considered $f(x) = g(x)h(x)$, with $g(x) \not\equiv \pm 1$, $h(x) \not\equiv \pm 1$, and both $g(x)$ and $h(x)$ having positive leading coefficients. Using the fact that $f(b)$ is prime, we reduced our considerations to $g(b) = \pm 1$. We then showed that either $g(x)$, and thus $f(x)$, is divisible by at least one of $\Phi_3(x - b)$, $\Phi_4(x - b)$, $\Phi_6(x - b)$, or $g(x)$ has a root $\beta \in \mathcal{R}_b$.

Now we consider the latter case, that $g(x)$, and thus $f(x)$, has a root $\beta \in \mathcal{R}_b$, and obtain a lower bound on the coefficients of $f(x)$ in this case. We will rely heavily on the following lemma.

LEMMA 5.1. *Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$, where $a_j \geq 0$ for $j \in \{0, 1, \ldots, n\}$. Suppose $\alpha = re^{i\theta}$ is a root of $f(x)$ with $0 < \theta < \pi/2$ and $r > 1$. Let*

$$B = \max_{\pi/(2\theta) < k < \pi/\theta} \left\{ \frac{r^k (r - 1)}{1 + \cot(\pi - k\theta)} \right\},$$

where the maximum is over $k \in \mathbb{Z}$. Then there is some $j \in \{0, 1, \ldots, n - 1\}$ such that $a_j > Ba_n$.

The proof of Lemma 5.1 is similar to that of [6, Theorem 5] and is established in the above form in [7] (cf. [1] and [2]).

We use Lemma 5.1 to prove the following corollary.

Table 8. $N_1(b)$ for $2 \leq b \leq 20$

b	$N_1(b)$
2	20
3	7237
4	16576650
5	91182226358
6	610418402115745
7	4847692211281203599
8	97507223325452990654864
9	2200192048605247301544844663
10	61091041047613095559860106055488
11	2119463830567700564381021297555803479
12	91564212244130952550165806988723772810934
13	4881903128237975594282131856777716345570591059
14	278336811480425292328491552981955444943583501062423
15	61074859962290535565373333952146687505375635458305881677
16	9401468271903366135972500856333110049503488294231938850008746
17	1431397180112955678634451120632703115867308362290036476121595252119
18	235429303540695115385709981455936954415388002209380091524801717697233924
19	43022718318161585107154947899035503608645093219967711021015380107341305221367
20	8823216088819058575067389247090576700176541906366627393606717738052119209880430672

Table 9. $N_2(b)$ for $5 \leq b \leq 20$

b	$N_2(b)$
5	191323668587
6	674230217165580
7	28742111886541897923
8	1253983385808624632627228
9	71643145402933591346271299994
10	10711129748782895331986694273844450
11	1348312606061131031866295541636879998621
12	317699679060331989000972232918817782815082246
13	133836842972863294264378339144272828940083307482001
14	24387207020849741198805521258225261909442987625989599492
15	25997099578885789071666507880388951117236365690861374779176372
16	22101669396534492309769837392257109525030072284533419115394237532818
17	11068765075055445663455770678250929757451117392105995069831359511491726050
18	20735705634139764535088061088222548432649983454342556572811034473965649791911450
19	25299051628958894639347305083391076959171276290019053473973793001833084973083685273178
20	32928510793081933959100006751886500402513174060644405058830097977688613093584851358050701812

Corollary 5.2. *Fix an integer b with $b \geq 2$. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ be such that $a_j \geq 0$ for each j and $f(b)$ is prime. If*

$$0 \leq a_j \leq B_b a_n \quad \text{for } 0 \leq j \leq n-1 \qquad \text{with } B_b \text{ as in Table 10},$$

then either $f(x)$ is irreducible, or $f(x)$ is divisible by at least one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, $\Phi_6(x-b)$.

Table 10. Values of B_b

b	2	3	4	5	6
B_b	7	4712	5.8802×10^{7}	4.149×10^{11}	6.616×10^{14}
b	7	8	9	10	11
B_b	8.762×10^{19}	1.401×10^{25}	1.412×10^{30}	2.749×10^{35}	5.203×10^{40}
b	12	13	14	15	16
B_b	1.159×10^{46}	6.969×10^{51}	2.689×10^{57}	1.598×10^{63}	1.869×10^{69}
b	17	18	19	20	
B_b	1.269×10^{75}	2.075×10^{81}	1.245×10^{87}	3.942×10^{93}	

Before proceeding to the argument for Corollary 5.2, we note that the value for B_{10} given in Table 10 is an improvement over the analogous result given in [7]. This is due to our choice of $e_2(10)$, $e_3(10)$, $e_4(10)$, $e_6(10)$ and $d(10)$ in Table 4, which differs from that used in [7]. On the other hand, the methods used in both cases are similar.

Proof of Corollary 5.2. For a fixed integer $b \in [2, 20]$, let θ and θ' be real numbers such that $0 \leq \theta < \theta' \leq \tan^{-1}(R_b)$, where R_b is given in Table 11. We are interested in the set of points $\mathcal{R}_b(\theta, \theta')$ that are in $\mathcal{R}_b$ between the line passing through the origin making an angle θ with the positive x-axis and the line passing through the origin making an angle θ' with the positive x-axis. Explicitly, we define

$$\mathcal{R}_b(\theta, \theta') = \{(x, y) \in \mathcal{R}_b : \tan(\theta) \leq y/x < \tan(\theta')\}.$$

We are still considering the case that $g(x)$ has a root $\beta \in \mathcal{R}_b$. We write $\beta = x_0 + iy_0$ for some $(x_0, y_0) \in \mathcal{R}_b$, where we may take $y_0 > 0$.

Along the lines of the proof of Theorem 4.2, we use a Sturm sequence to show that the line $y = R_b x$ does not intersect the region $\mathcal{R}_b$, where the value of R_b is given in Table 11. In other words, we take the rational equivalent of the decimal expression in Table 11 and show that the region $\mathcal{R}_b$ lies completely under the line $y = R_b x$ by verifying with a Sturm sequence that the polynomial $P_b(x, R_b x) \in \mathbb{Q}[x]$ has no real roots.

To utilize Lemma 5.1, we specify a set $\Theta_b = \{\theta_0, \theta_1, \ldots, \theta_{m-1}, \theta_m\}$ where

$$0 = \theta_0 < \theta_1 < \cdots < \theta_{m-1} < \theta_m < \pi/2,$$

Table 11. Values of R_b

b	2	3	4	5	6	7	8
R_b	1.6	0.5	0.26	0.18	0.15	0.124	0.108115
b	9	10	11	12	13	14	
R_b	0.096	0.08622	0.0783	0.072	0.0664	0.0617	
b	15	16	17	18	19	20	
R_b	0.0577	0.054053	0.05091	0.0481	0.0456	0.043327	

and where $\tan(\theta_l) = r_l \in \mathbb{Q}$ for $0 \le l \le m$, $\tan(\theta_1) = 1/1000$ and $\tan(\theta_m) = R_b$. Thus,

$$(x_0, y_0) \in \bigcup_{l=0}^{m-1} \mathcal{R}_b(\theta_l, \theta_{l+1}).$$

Next, for each $l \in \{0, 1, \dots, m-1\}$, we use Lemma 5.1 to find a bound $B'_b(\theta_l, \theta_{l+1})$ so that for all $(x_0, y_0) \in \mathcal{R}_b(\theta_l, \theta_{l+1})$, there is a $j \in \{0, 1, \dots, n-1\}$ for which $a_j > B'_b(\theta_l, \theta_{l+1}) a_n$. We can then deduce that some coefficient of $f(x)$ must exceed

$$\min_{0 \le l \le m-1} \{B'_b(\theta_l, \theta_{l+1})\} \cdot a_n. \tag{5.1}$$

We judiciously choose each $\theta_l \in \Theta_b$ so that always $B'_b(\theta_l, \theta_{l+1}) > B_b$, where B_b is listed in Table 10. Corollary 5.2 will then follow.

We begin by considering the first sector $\mathcal{R}_b(\theta_0, \theta_1)$, where we have already stated that $\theta_0 = 0$ and $\theta_1 = \tan^{-1}(1/1000)$, independent of the value of $b \in [2, 20]$. Take

$$k = k(\theta) = \left\lfloor \frac{25\pi}{26\theta} \right\rfloor \quad \text{where } 0 < \theta \le \tan^{-1}\left(\frac{1}{1000}\right).$$

We note that

$$k \in \left(\frac{\pi}{2\theta}, \frac{\pi}{\theta}\right)$$

since

$$k\theta \le \frac{25\pi}{26} < \pi$$

and

$$k\theta > \left(\frac{25\pi}{26\theta} - 1\right)\theta = \frac{25\pi}{26} - \theta \ge \frac{25\pi}{26} - \tan^{-1}\left(\frac{1}{1000}\right) > \frac{\pi}{2}.$$

Later we will use the fact that

$$\frac{\pi}{2} > \pi - k\theta \ge \pi - \frac{25\pi}{26} = \frac{\pi}{26},$$

which gives $\cot(\pi - k\theta) \le \cot(\pi/26)$.

From our definition of k and the range of θ above, we have

$$k = \left\lfloor \frac{25\pi}{26\theta} \right\rfloor \geq \left\lfloor \frac{25\pi/26}{\tan^{-1}(1/1000)} \right\rfloor = 3020.$$

We recall that for each $z \in \mathcal{R}_b$, regardless of the b we are using, we have $\mathrm{Re}(z) \geq 1.447$, as implied by Table 6. Thus, for each $z = re^{i\theta} \in \mathcal{R}_b$, we have $r = |z| \geq 1.447$. For each such z, we see that

$$\frac{r^k(r-1)}{1+\cot(\pi - k\theta)} \geq \frac{1.447^{3020}(1.447-1)}{1+\cot(\pi/26)} > 1.99 \times 10^{483}.$$

From Lemma 5.1, with $\theta_0 = 0$ and $\theta_1 = \tan^{-1}(1/1000)$, we see that we may take

$$B_b'(\theta_0,\theta_1) = B_b'\left(0, \tan^{-1}\left(\frac{1}{1000}\right)\right) = 1.99 \times 10^{483}. \tag{5.2}$$

Observe that $1.99 \times 10^{483} > B_b$ for each $b \in [2, 20]$.

There is quite a bit of freedom in choosing the remaining values of θ_l for each b. We want some idea of where the line $y = \tan(\theta_l)x$ intersects $\mathcal{R}_b$. Since the boundary of $\mathcal{R}_b$ consists of the points (x, y) such that $P_b(x, y) = 0$, we want an estimate of the real numbers x for which $P(x, \tan(\theta_l)x) = 0$. However, we want to avoid computations that approximate the real roots of a polynomial based on coefficients that are themselves just approximations of the actual real coefficients. To this end, we recall $r_l = \tan(\theta_l)$, where r_l is a rational number. We then find a close rational lower bound approximation x_l' to the minimum real root of $P_b(x, r_l x) = 0$. Since $P_b(x, r_l x) \in \mathbb{Q}[x]$ and $x_l' \in \mathbb{Q}$, we can use a Sturm sequence to verify, with exact arithmetic, that $P_b(x, r_l x)$ has no roots in the interval $[0, x_l']$. Thus, x_l' provides us with a lower bound on the x-coordinate of the intersection of $y = \tan(\theta_l)x$ with $\mathcal{R}_b$. Observe that by construction $r_1 = 1/1000$.

The values of $r_l = \tan(\theta_l)$ we used for each $b \in [2, 20]$ can be found in [4]. As the exact values are not so significant, we do not duplicate them all here but rely instead on tabulating the choices we used for $b = 2$ and $b = 10$ as examples. For $b = 2$, the r_l are given in Table 12; for $b = 10$, the r_l are given in Table 13.

We explain the notation in Table 13 for the values of $\theta_0, \theta_1, \ldots, \theta_m$. The value r_a corresponds to the first value of $\tan(\theta_l)$ being considered in that row, and the value r_b corresponds to the last value of $\tan(\theta_{l+1})$. We used the rational equivalents of the decimals given for r_a and r_b in our computations to ensure exact arithmetic when computing x_l' as described earlier. If d is the number of divisions indicated in the third column of the same row, then the corresponding intervals (θ_l, θ_{l+1}) for that row are given by

$$\theta_l = \tan^{-1}\left(r_a + \frac{(r_b - r_a)j}{d}\right), \qquad \theta_{l+1} = \tan^{-1}\left(r_a + \frac{(r_b - r_a)(j+1)}{d}\right),$$

Table 12. Values of $B_2'(\theta_l, \theta_{l+1})$

l	$r_l = \tan(\theta_l)$	$B_2'(\theta_l, \theta_{l+1})$	l	$r_l = \tan(\theta_l)$	$B_2'(\theta_l, \theta_{l+1})$
0	$0 = 0$	1.99×10^{483}	25	$\frac{3}{10} = 0.3$	8.48120
1	$\frac{1}{1000} = 0.001$	1.67316×10^{333}	26	$\frac{31}{100} = 0.31$	7.68540
2	$\frac{3}{2000} = 0.0015$	1.88152×10^{249}	27	$\frac{8}{25} = 0.32$	7.86165
3	$\frac{1}{500} = 0.002$	1.78851×10^{165}	28	$\frac{33}{100} = 0.33$	7.61940
4	$\frac{3}{1000} = 0.003$	2.25395×10^{123}	29	$\frac{17}{50} = 0.34$	7.31188
5	$\frac{1}{250} = 0.004$	1.59285×10^{98}	30	$\frac{7}{20} = 0.35$	7.41486
6	$\frac{1}{200} = 0.005$	3.13071×10^{81}	31	$\frac{71}{200} = 0.355$	7.20197
7	$\frac{3}{500} = 0.006$	3.66576×10^{69}	32	$\frac{9}{25} = 0.36$	7.22629
8	$\frac{7}{1000} = 0.007$	3.99316×10^{60}	33	$\frac{37}{100} = 0.37$	7.28552
9	$\frac{1}{125} = 0.008$	3.51475×10^{53}	34	$\frac{19}{50} = 0.38$	7.34184
10	$\frac{9}{1000} = 0.009$	1.01194×10^{48}	35	$\frac{39}{100} = 0.39$	7.38453
11	$\frac{1}{100} = 0.01$	2.52294×10^{31}	36	$\frac{2}{5} = 0.4$	7.39514
12	$\frac{3}{200} = 0.015$	1.13455×10^{23}	37	$\frac{41}{100} = 0.41$	7.74498
13	$\frac{1}{50} = 0.02$	8.071030×10^{14}	38	$\frac{21}{50} = 0.42$	7.72610
14	$\frac{3}{100} = 0.03$	6.506270×10^{10}	39	$\frac{11}{25} = 0.44$	7.95266
15	$\frac{1}{25} = 0.04$	2.576910×10^{8}	40	$\frac{47}{100} = 0.47$	8.65642
16	$\frac{1}{20} = 0.05$	5.92576×10^{6}	41	$\frac{1}{2} = 0.5$	8.64546
17	$\frac{3}{50} = 0.06$	479437	42	$\frac{11}{20} = 0.55$	8.47305
18	$\frac{7}{100} = 0.07$	62346.5	43	$\frac{3}{5} = 0.6$	7.34988
19	$\frac{2}{25} = 0.08$	12234.5	44	$\frac{7}{10} = 0.7$	8.44235
20	$\frac{9}{100} = 0.09$	4547.64	45	$\frac{3}{4} = 0.75$	8.10185
21	$\frac{1}{10} = 0.1$	118.104	46	$\frac{4}{5} = 0.8$	7.69225
22	$\frac{3}{20} = 0.15$	28.2727	47	$\frac{9}{10} = 0.9$	7.46715
23	$\frac{1}{5} = 0.2$	11.9817	48	$\frac{11}{10} = 1.1$	7.72974
24	$\frac{1}{4} = 0.25$	7.41419	49	$\frac{16}{10} = 1.6$	–

for $0 \leq j \leq d-1$, where l as indicated depends on j. The fourth column indicates the minimum value of $B_{10}'(\theta_l, \theta_{l+1})$ for (θ_l, θ_{l+1}) considered in that row, and therefore serves as a value of $B_{10}'(\theta_a, \theta_b)$. We explain momentarily how the bounds $B_b'(\theta_l, \theta_{l+1})$ were obtained. The number m of intervals (θ_l, θ_{l+1}) for $b = 10$ is 1134, given by the total number of divisions from the third column of Table 13. This is slightly misleading as the last division of $(r_a, r_b) = (0.0861, 0.08622)$ into 1000 intervals of equal length leads

Table 13. Values of $B'_{10}(\theta_l, \theta_{l+1})$

$r_a = \tan(\theta_a)$	$r_b = \tan(\theta_b)$	# of Divisions	$B'_{10}(\theta_a, \theta_b)$
0	0.001	1	1.88×10^{483}
0.001	0.002	2	1.35945×10^{1452}
0.002	0.01	8	9.47832×10^{288}
0.01	0.02	2	5.96751×10^{143}
0.02	0.08	6	1.33634×10^{36}
0.08	0.085	5	3.38637×10^{35}
0.085	0.086	100	2.83670×10^{35}
0.086	0.0861	10	2.75920×10^{35}
0.0861	0.08622	1000	2.74964×10^{35}

to a number of cases where $\mathcal{R}_{10}(\theta_l, \theta_{l+1})$ is the empty set. In other words, $y = \tan(\theta_l)x$ will lie above $\mathcal{R}_{10}$ for $\theta_l \approx 0.08622$. These values of l are to be ignored. What is significant here in fact is that for the last θ_{l+1} considered, $y = \tan(\theta_{l+1})x$ is above $\mathcal{R}_{10}$. This is the case due to the value of R_{10} in Table 11.

As suggested by Table 13, for $b \geq 3$, we want the gaps between consecutive r_l considered to become smaller when $B'_b(\theta_l, \theta_{l+1})$ is near the minimum value obtained (in the last column). A priori, we did not know where the minimum occurs, so we revised the number of divisions (ending with the indicated values in the third column) to be larger until the minimum value of $B'_b(\theta_l, \theta_{l+1})$ was accurate to the first few digits shown.

For a fixed $l \in \{1, \ldots, m-1\}$, we now show how to obtain a value for $B'_b(\theta_l, \theta_{l+1})$. We have already shown how to find a verifiable lower bound x'_l for the leftmost point (x, y) on the intersection of the line $y = \tan(\theta_l)x$ and $\mathcal{R}_b$. This was done using a Sturm sequence for a polynomial in $\mathbb{Q}[x]$.

Let

$$\alpha = x_0 + iy_0 = re^{i\theta} \quad \text{where } (x_0, y_0) \in \mathcal{R}_b(\theta_l, \theta_{l+1}). \tag{5.3}$$

We will show that both $x_0 \geq x'_l$ and $y_0 \geq \tan(\theta_l)x'_l$. We begin with the former. By way of contradiction, assume that $x_0 < x'_l$. Let (x_1, y_1) be the point where $y = \tan(\theta)x$ intersects $\mathcal{R}_b$ with x_1 being minimal. Therefore, (x_1, y_1) lies on the boundary of $\mathcal{R}_b$, and, by Lemma 3.1, we have $y_1 = \rho_b(x_1)$. Also, $x_1 \leq x_0 < x'_l$ and, by Lemma 3.1(i), $b - a_0 \leq x_1 \leq b + a_1$ where a_0 and a_1 are given in Table 6. By Lemma 3.1(iii)–(iv), the function $\rho_0(x) = \rho_b(x) - r_l x$ is continuous on $I_b = [b - a_0, b + a_1]$ and such that $\rho_0(b - a_0) < 0$. However, since $(x_1, y_1) \in \mathcal{R}_b(\theta_l, \theta_{l+1})$, it lies above the line $y = \tan(\theta_l)x$. This gives

$$\rho_b(x_1) = y_1 = \tan(\theta)x_1 \geq \tan(\theta_l)x_1 = r_l x_1,$$

so $\rho_0(x_1) \geq 0$. By the Intermediate Value Theorem, there exists a $u \in [b - a_0, x_1]$

such that $\rho_0(u) = 0$. Thus, $\rho_b(u) = r_l u$, which yields $P_b(u, r_l u) = 0$. Since

$$u \le x_1 \le x_0 < x'_l,$$

we obtain a contradiction to the definition of x'_l. Therefore, $x_0 \ge x'_l$. To show that $y_0 \ge \tan(\theta_l)x'_l$, we now simply observe that

$$y_0 = \tan(\theta)x_0 \ge \tan(\theta_l)x_0 \ge \tan(\theta_l)x'_l.$$

To get a value for $B'_b(\theta_l, \theta_{l+1})$, we used 100-digit approximations in Maple 17 to perform the calculations indicated below. Further details can be found in [4]. We let L_l be a lower bound approximation of $\sec(\theta_l)x'_l$ so that, for any $\alpha = re^{i\theta}$ as in (5.3), we have

$$r = \sqrt{x_0^2 + y_0^2} \ge \sqrt{1 + \tan^2(\theta_l)}x'_l \ge L_l.$$

Now, for every $l \in \{1, \dots, m-1\}$, we let $k_1 = k_1(l)$ be the largest integer $\le \pi/\theta_{l+1}$. We define

$$k_2 = k_2(l) = \begin{cases} k_1 - 1 & \text{if } k_1 - 1 \ge \pi/(2\theta_l) + 10^{-10}, \\ k_1 & \text{otherwise.} \end{cases}$$

Notably, these values depend on the values for r_l and θ_l chosen earlier. In every case, for our choices of r_l and θ_l, the inequalities

$$\frac{\pi}{2\theta_l} + 10^{-10} \le k_2 \le k_1 \le \frac{\pi}{\theta_{l+1}} - 10^{-10}$$

held. The specific choice of 10^{-10} is not significant here or later below, but it provides us with some measure of how much accuracy was needed for our computations. For each $\theta \in [\theta_l, \theta_{l+1}]$, we are able to conclude that

$$\frac{\pi}{2\theta} \le \frac{\pi}{2\theta_l} < k_2 \le k_1 < \frac{\pi}{\theta_{l+1}} \le \frac{\pi}{\theta}.$$

Hence, in each case, k_1 and k_2 are in the interval $(\pi/(2\theta), \pi/\theta)$.

For each b and l, we compute $c(k_1)$ and $c(k_2)$ such that

$$\cot(\pi - k_j\theta) \le \cot(\pi - k_j\theta_{l+1}) \le c(k_j) - 10^{-10} \quad \text{for } j \in \{1, 2\}. \tag{5.4}$$

From the above, Lemma 5.1 now allows us to take

$$B'_b(\theta_l, \theta_{l+1}) = \max\left\{ \frac{L_l^{k_1}(L_l - 1)}{1 + c(k_1)}, \frac{L_l^{k_2}(L_l - 1)}{1 + c(k_2)} \right\}.$$

These bounds, combined with (5.1) and (5.2), give the lower bound of $B_b a_n$ for at least one of the coefficients of $f(x)$, where B_b is as listed in Table 10. Corollary 5.2 now follows. ∎

Before leaving this section, we note that a certain precaution had to be made in (5.4) that is connected to an irrationality result. What happens if our choices for θ_{l+1} and k_j cause the expression $\cot(\pi - k_1\theta_{l+1})$ to be undefined? This in fact can happen. Observe that $k_1 = \lfloor \pi/\theta_{l+1} \rfloor$. The expression $\cot(\pi - k_1\theta_{l+1})$ is undefined precisely when $\pi/\theta_{l+1} \in \mathbb{Z}$. If this happens, then θ_{l+1} is a rational multiple of π. Recall that $r_{l+1} = \tan(\theta_{l+1})$ is also rational. The only rational values of the form $\tan(u\pi)$ with $u \in \mathbb{Q}$ are 0 and ± 1 (cf. [10, Corollary 3.12]). Thus, for our set-up where $0 < \theta_{l+1} < \pi/2$, we need only avoid $r_{l+1} = 1$. Since R_b is an upper bound on $r_{l+1} = \tan(\theta_{l+1})$, we deduce from Table 11 that the possibility of $r_{l+1} = 1$ only occurs for $b = 2$. This explains the choice of r_{47} and r_{48} in Table 12, where we avoided using the rational number 1 for a value of r_l.

6. Bounds based on recursive relations. We will now examine another method to bound the coefficients of $f(x)$ that is motivated by Corollary 5.2. In the case that $f(x)$ is divisible by one of the quadratics $\Phi_3(x-b)$, $\Phi_4(x-b)$ and $\Phi_6(x-b)$, we find sharp lower bounds for the maximum coefficient of $f(x)$. The bound that we find will depend on our choice of b and the quadratic.

As much of this section is based on the work in [7] for $b = 10$, we give enough background from there to describe our work for $b \in [2, 20]$ but refer to [7] for the details of the arguments.

Fix positive integers A and B. Let b_j be integers such that

$$(b_0x^s + b_1x^{s-1} + \cdots + b_{s-1}x + b_s)(x^2 - Ax + B) \tag{6.1}$$

is a polynomial of degree $s + 2$ with non-negative coefficients. We will want A and B to be chosen so that the quadratic on the right is one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, $\Phi_6(x-b)$. With $f(x) = g(x)h(x)$ as before and $g(x)$ being the quadratic, we view $h(x)$ as the polynomial factor on the left in (6.1) and further $n = \deg f(x) = s + 2$. The choice of b_j as the coefficient of x^{s-j} will help us view the b_j as forming a sequence and be more appropriate for the arguments that follow. If (6.1) is expanded, we obtain $f(x)$ so that the resulting coefficients are all non-negative.

We define $b_j = 0$ for all $j < 0$ and all $j > s$. Since the coefficients of $f(x)$ are all non-negative, we deduce that

$$b_0 \geq 1 \quad \text{and} \quad b_j \geq Ab_{j-1} - Bb_{j-2} \quad \text{for all } j \in \mathbb{Z}. \tag{6.2}$$

Define

$$\beta_j = \begin{cases} 0 & \text{if } j < 0, \\ 1 & \text{if } j = 0, \\ A\beta_{j-1} - B\beta_{j-2} & \text{if } j \geq 1, \end{cases} \tag{6.3}$$

so the β_j satisfy a recursive relation for $j \geq 0$. In particular, $\beta_1 = A$ and $\beta_2 = A^2 - B$. For each A and B corresponding to a quadratic $x^2 - Ax + B$

equal to one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, $\Phi_6(x-b)$ for some $b \in [2, 20]$, the values of β_j vary in sign as j increases. Let J be a positive integer for which

$$\beta_j > 0 \quad \text{for } 0 \le j \le J. \tag{6.4}$$

As shown in [7], we have

$$b_j \ge \beta_j b_0 \quad \text{for all integers } j \le J+1. \tag{6.5}$$

Although it is natural to consider J maximal satisfying (6.4) as in [7], what we want for our purposes is the least J for which $\beta_{J+1} < \beta_J$. In [7], these notions are equivalent; but in general, they are not. Tables 14 and 15 show the A, B, J and β_J for $b \in [2, 20]$. Note that

$$\beta_J = \max_{0 \le j \le J} \{\beta_j\}.$$

Let

$$U = \max_{j \ge 0}\{b_j\} \quad \text{and} \quad L = \min_{j \ge 0}\{b_j\}.$$

Since $b_j = 0$ for $j > s$, we have the trivial bound $L \le 0$. From (6.5), we obtain $U \ge \beta_J b_0$.

We are interested in A and B such that $f(x)$ is divisible by $x^2 - Ax + B$. We view A and B as fixed. We want $f(x)$ to have non-negative integer coefficients but with the largest coefficient as small as possible. Let $M = M(A, B)$ be the maximum coefficient for such an $f(x)$. For this definition, we do not require that $f(b)$ is prime. Thus, if $f_0(x) \in \mathbb{Z}[x]$ has non-negative integer coefficients and is divisible by $x^2 - Ax + B$, then $f_0(x)$ has a coefficient that is $\ge M$.

We now describe important inequalities obtained in [7]. Let $\ell \in \mathbb{Z}^+$. Define $\mu_0, \mu_1, \dots, \mu_{\ell-1}$ to be the solution to the matrix equation

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ -A & B & 0 & \cdots & 0 & 0 & 0 \\ 1 & -A & B & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & B & 0 & 0 \\ 0 & 0 & 0 & \cdots & -A & B & 0 \\ 0 & 0 & 0 & \cdots & 1 & -A & B \end{pmatrix} \begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \\ \vdots \\ \mu_{\ell-3} \\ \mu_{\ell-2} \\ \mu_{\ell-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The above corresponds to a system of ℓ equations in the ℓ unknowns μ_j where $0 \le j \le \ell - 1$. The system depends only on A, B and ℓ. Ideally, we want to know that a unique solution to this system exists and each μ_j is in $[0, 1]$. For each choice of A, B and ℓ we use, this can be verified with a direct computation. We therefore suppose this is the case.

We set

$$u = \mu_0 B, \quad v = \mu_{\ell-2} - \mu_{\ell-1} A \quad \text{and} \quad w = \mu_{\ell-1}. \tag{6.6}$$

Table 14. Values of β_J for bases $2 \leq b \leq 12$

b	A	B	J	β_J
2	3	3	4	9
2	4	5	5	44
2	5	7	7	1265
3	5	7	7	1265
3	6	10	8	7696
3	7	13	11	1275120
4	7	13	11	1275120
4	8	17	11	4839120
4	9	21	15	4342010751
5	9	21	15	4342010751
5	10	26	14	7358602624
5	11	31	18	29466877337101
6	11	31	18	29466877337101
6	12	37	17	21848430755052
6	13	43	22	668421206663764973
7	13	43	22	668421206663764973
7	14	50	20	111210534995557376
7	15	57	26	21999708522958326888168
8	15	57	26	21999708522958326888168
8	16	65	24	15001111280838892163841
8	17	73	29	981412950725117689674949200
9	17	73	29	981412950725117689674949200
9	18	82	27	268316103488444479287132160
9	19	91	33	117704722514097750900952684327901
10	19	91	33	117704722514097750900952684327901
10	20	101	30	604861792550624708513466396499
10	21	111	37	12146960414965144431227887762494414381
11	21	111	37	12146960414965144431227887762494414381
11	22	122	33	17372654348915578396565748340621312
11	23	133	40	2388719391431067586473475435479832953496811
12	23	133	40	2388719391431067586473475435479832953496811
12	24	145	36	631477325821592776208040048198094984801
12	25	157	44	852463967980020982575658211110018018726645270524
13	25	157	44	852463967980020982575658211110018018726645270524
13	26	170	39	28717077224929268201659599157515978503356416
13	27	183	47	$15292524334493253461581890961 \times 10^{25}$
				$+\,8898892202903263801780160$

Table 15. Values of β_J for bases $13 \le b \le 20$

b	A	B	J	β_J
14	27	183	47	152925243344932534615818909618898892202903263801780160
14	28	197	42	1613692251361686484421412544021746891502133209787
14	29	211	51	123209002743534545363348378580042422356570453511191349664151
15	29	211	51	123209002743534545363348378580042422356570453511191349664151
15	30	226	46	270242743195975821085722716602418971262724050700468224
15	31	241	55	91708171769852665185766960133846927489751337280221656080474014591
16	31	241	55	91708171769852665185766960133846927489751337280221656080474014591
16	32	257	49	36581588606627883797558369090790311476667269627361629766432
16	33	273	58	40544927014855112320350808345241500943044386051670311611103880994475087
17	33	273	58	40544927014855112320350808345241500943044386051670311611103880994475087
17	34	290	52	4935852345217088547015348691836907296094166766517367159039983616
17	35	307	62	67543015094917799788560459570757486751302877701441552354433337048748044924582
18	35	307	62	67543015094917799788560459570757486751302877701441552354433337048748044924582
18	36	325	55	724397857048292662725261481402882936662732314490400281614774515991376
18	37	343	66	73758168014457418773607303450119757898458531457781497008669950442662055315112784877
19	37	343	66	73758168014457418773607303450119757898458531457781497008669950442662055315112784877
19	38	362	58	118847288171717085931367259389600838697914622154606936522141933998180401152
19	39	381	69	86426537514650745299475083338284777959352162888830459471995007815455677410983861832154001
20	39	381	69	86426537514650745299475083338284777959352162888830459471995007815455677410983861832154001
20	40	401	61	22003032640446530112387504356834355860789381312634981031438198848010272343841240
20	41	421	73	$250714312379800306559196007794041584507088620364 \times 10^{48}$
				$+ 503305220058795561622034471001070474059605249481$

Then [7] establishes that

$$M \geq \left\lceil \frac{u^2-(v+w)^2}{u} \cdot U \right\rceil \geq \frac{u^2-(v+w)^2}{u} \cdot U \geq \frac{u^2-(v+w)^2}{u} \cdot \beta_J b_0 \geq \frac{(u^2-(v+w)^2)\beta_J}{u} \tag{6.7}$$

and

$$0 \leq -L \leq \frac{v+w}{u^2-(v+w)^2} \cdot M. \tag{6.8}$$

The inequalities (6.7) and (6.8) can be used to estimate L and U, respectively. We also use (6.7) to find a lower bound for $M(A,B)$ that is exactly, or is close to, best possible. With some additional work, as we shall see, we can determine the exact value of $M(A,B)$. Note that the variables in (6.7) and (6.8) all depend on b, A and B, and in addition u, v and w (as given in (6.6)) depend on ℓ. For ℓ, we will choose $\ell = J+1$ where J is given in Tables 14 and 15.

As an example of the use of (6.7), we can obtain an immediate improvement on Corollary 5.2. Take $b = 4$, $A = 9$ and $B = 21$. Computing $\mu_0, \mu_1, \ldots, \mu_\ell$ with $\ell = 16$, we check that the μ_j are in $[0,1]$, and compute u, v and w using (6.6). Denoting by a_n the leading coefficient of $f(x)$ as in Corollary 5.2, we have $b_0 = a_n$. Table 14 gives a lower bound $b_0\beta_{15} = a_n\beta_{15}$ for $U = U(9,21)$. From (6.7), we see that

$$M = M(9,21) \geq \frac{u^2-(v+w)^2}{u} \cdot U \geq 5.6446 \times 10^{10} a_n.$$

This implies that any polynomial $f(x)$ with non-negative coefficients and leading coefficient a_n that is divisible by $x^2 - 9x + 21$ must have a coefficient as large as $5.6446 \cdot 10^{10} a_n$. From Corollary 5.2, we see that if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}$ is such that $f(4)$ is prime and

$$0 \leq a_j \leq 5.8802 \cdot 10^7 a_n \quad \text{for } 0 \leq j \leq n,$$

then either $f(x)$ is irreducible or $f(x)$ is divisible by $\Phi_3(x-4) = x^2 - 7x + 13$ or $\Phi_4(x-4) = x^2 - 8x + 17$. Repeating the analogous calculations for bases $2 \leq b \leq 20$, with the aid of Corollary 5.2, we can deduce the following.

Corollary 6.1 (Improvement of Corollary 5.2). *Fix an integer b with $b \geq 2$. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ be such that $a_j \geq 0$ for each j and $f(b)$ is prime. If*

$$0 \leq a_j \leq B_b a_n \quad \text{for } 0 \leq j \leq n-1 \quad \text{with } B_b \text{ as in Table } 10,$$

then either $f(x)$ is irreducible, or $f(x)$ is divisible by $\Phi_3(x-b)$ or $\Phi_4(x-b)$.

Similarly, for each $b \in [2,20]$, we can apply (6.7) to find a lower bound for $M(A,B)$ in case $g(x) = x^2 - Ax + B$ is $\Phi_3(x-b)$ or $\Phi_4(x-b)$. Tables 16 and 17

Table 16. Lower bound on $M(A,B)$ for $3 \le b \le 9$

b	A	B	Lower bound on $M(A,B)$ from (6.7)
2	3	3	9
2	4	5	88
3	5	7	3795
3	6	10	38480
4	7	13	8925840
4	8	17	48391200
5	9	21	56446139763
5	10	26	125096244608
6	11	31	618804424079121
6	12	37	568059199631352
7	13	43	20721057406576714162
7	14	50	4114789794835622912
8	15	57	945987466487208056191223
8	16	65	75005556404194608192049
9	17	73	55940538191331708311472104399
9	18	82	1744054672674891153663590399

list b, A, B, and a lower bound for $M(A,B)$ obtained from our computations. To clarify, these lower bounds are simply $(u^2 - (v+w)^2)\beta_J/u$ as given in (6.7), where again we take $\ell = J+1$ and we use (6.6) to compute u, v and w.

Before proceeding, we note that we have finished establishing the case $b = 2$ of Theorem 1.1. In other words, we can now deduce that if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $0 \le a_j \le 7$ for each j and $f(2)$ prime, then $f(x)$ is irreducible. For $b \in \{3,4,5,6,7,14\}$, the bounds $M(A,B)$ come particularly close to what we want. These bounds establish that $M_1(b)$ can be taken to be 1 less than what appears in Table 1. In other words, for these b, we can now deduce that if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $0 \le a_j \le M_1(b) - 1$ for each j and $f(b)$ prime, then $f(x)$ is irreducible. As we shall see, it is possible for $f(x)$ to have all its coefficients in $[0, M_1(b)]$ with $f(x)$ divisible by $x^2 - Ax + B$. Even though this quadratic has the value 1 at $x = b$, we will see that for such an $f(x)$, $f(b)$ cannot be prime.

7. A sharp bound for $M(A,B)$. We are now ready to complete the proof of Theorem 1.1. At the end of the previous section, we noted that the case $b = 2$ is complete. For a fixed $b \in [3,20]$, we are interested in the case that $f(x) = g(x)h(x)$, where $g(x) = x^2 - Ax + B$ is $\Phi_3(x-b)$ or $\Phi_4(x-b)$, $h(x)$ has a positive leading coefficient that we have denoted by b_0, and $f(x)$ has maximal coefficient $M(A,B)$.

Table 17. Lower bound on $M(A, B)$ for $10 \leq b \leq 20$

b	A	B	Lower bound on $M(A, B)$ from (6.7)
10	19	91	859244474352913581576954595593677 1
10	20	101	49598666989151226098104244512916
11	21	111	1105373397761828143241737786386991708670
11	22	122	17546380892404734180531405824027525 10
12	23	133	26514785244884850209855577333826145783814601 9
12	24	145	770402337502343186973808858801675881457 20
13	25	157	1133777077413427906825625420776323964906438209796 90
13	26	170	41639761976147438892406418778398168829866803 19
14	27	183	240092632051544079346835688101671260758558124168794851 20
14	28	197	2743276827314867023516401324836969715553626456637 90
15	29	211	225472475020668218014927532801477632912523929925480169885396 30
15	30	226	532378204096072367538873751706765373387566379879922401 26
16	31	241	1935042424343891235419682858824170170033753216612676943298001707869 9
16	32	257	82674390250979017382481914145186103937268029357837283272136 29
17	33	273	97713274105800820692045448112032017272736970384525450982760353196684959 66
17	34	290	1268514052720791756582944613802085175096200858994963359873275789 309
18	35	307	184392431209125593422770054628167938831056856124935437927603010143082162644108 82
18	36	325	2100753785440048721903258296068360516321923712022160816682846096374990 36
19	37	343	22643757580438427563497442159186765674826769157538919581661674785897250981739624957 237
19	38	362	3862536865580805292769435930162027257682225220024725436969612854940863037 4397
20	39	381	296443023675252056377199535850316788400577918708688475988942876807012973519674646084288223 40
20	40	401	7965097815841643900684276577174036821605756035173863133380627982979718588470528 878

We view A and B as fixed. It is worth recalling that $M = M(A, B)$ is as small as possible. Recall also that we did not require that $f(b)$ is prime in the definition of M.

To finish the proof of Theorem 1.1, one checks that it suffices to show both of the following:

(A) The value of $M(A, B)$ is $(1 - A + B) \cdot \beta_J$ for each appropriate choice of (A, B) as shown in Tables 14 and 15.

(B) If the maximal coefficient of $f(x)$ equals M, then $f(b)$ is composite.

Note that in (B), we are supposing as indicated above that $f(x)$ is divisible by $x^2 - Ax + B$. For example, take $b = 8$. Then (A) implies

$$M(16, 65) = 75005556404194608192050,$$
$$M(15, 57) = 94598746648720805619l224.$$

These are respectively the values of $M_1(8)$ and $M_2(8)$ given in Tables 1 and 2. Corollary 5.2 implies that if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $0 \le a_j \le M(15, 57)$ for each j and $f(x)$ is reducible, then $f(x)$ is divisible by either $\Phi_3(x - 8)$ or $\Phi_4(x - 8)$. It follows that if $0 \le a_j \le M(16, 65) = M_1(8)$, then $f(x)$ is either irreducible or divisible by $\Phi_4(x - 8)$. From (B), if also $f(8)$ is prime, then $f(x)$ cannot be divisible by $\Phi_4(x - 8) = x^2 - 16x + 65$. Therefore, the conditions of $f(8)$ being prime and $0 \le a_j \le M_1(8)$ in Theorem 1.1 imply $f(x)$ is irreducible. Similarly, $f(8)$ being prime and $0 \le a_j \le M_2(8)$ in Theorem 1.1 imply that either $f(x)$ is irreducible, or $f(x)$ is divisible by $\Phi_4(x - 8)$. A similar argument holds for each $b \in [3, 20]$.

We begin by establishing (A). We suppose first that

$$M(A, B) \le (1 - A + B) \cdot \beta_J. \tag{7.1}$$

Observe that we will want eventually to obtain a contradiction if strict inequality holds in (7.1), but there will be a significance to seeing what the inequality as written in (7.1) gives us. We are interested in the case that $x^2 - Ax + B$ is $\Phi_3(x - b)$ or $\Phi_4(x - b)$.

From (6.7) and (7.1), we have

$$b_0 \beta_J \le U(A, B) \le \frac{uM(A, B)}{u^2 - (v + w)^2} \le \frac{u(1 - A + B) \cdot \beta_J}{u^2 - (v + w)^2}. \tag{7.2}$$

We compute the leftmost and right-most sides of (7.2), based on u, v and w from (6.6) with $\ell = J + 1$ as before, on $b \in [3, 20]$ and on $x^2 - Ax + B$ being $\Phi_3(x - b)$ or $\Phi_4(x - b)$. In all cases, (7.2) gives a contradiction if $b_0 \ge 2$, so that we only consider now the possibility that $h(x)$ is monic. Setting $b_0 = 1$ in (7.2), by the same computations above we obtain $U = \beta_J$. In other words,

$$\beta_J = \left\lfloor \frac{u(1 - A + B) \cdot \beta_J}{u^2 - (v + w)^2} \right\rfloor$$

for all $b \in [3, 20]$ and $x^2 - Ax + B$ equal to $\Phi_3(x - b)$ or $\Phi_4(x - b)$.

Using (7.1) with u, v and w as before leads to

$$\frac{v+w}{u^2-(v+w)^2}\cdot M\in(0,1)$$

for each $b\in[3,20]$ and pair (A,B). Hence, (6.8) implies that $L=0$.

Thus, we have established that (7.1) implies $h(x)$ is monic, the largest coefficient of $h(x)$ corresponds to the value of β_J as indicated in Tables 14 and 15, and all of the coefficients of $h(x)$ are non-negative.

The approach given in [7] for $b=10$ follows through for general b directly at this point to give us more information about the structure of $h(x)$, based on the information just obtained about $h(x)$. Following the arguments there, still under the assumption of (7.1), we deduce that $h(x)$ can be written as a sum over some non-negative integers k of polynomials which are x^k times

$$(7.3)\qquad \begin{aligned}&(\beta_0x^J+\beta_1x^{J-1}+\cdots+\beta_J)x^{J+t'}+(x^{J+t'-1}+x^{J+t'-2}+\cdots+x^J)\beta_J\\&\quad+(\beta_J-\beta_0)x^{J-1}+(\beta_J-\beta_1)x^{J-2}+\cdots+(\beta_J-\beta_{J-1}),\end{aligned}$$

where $t'=t'(k)$ is a non-negative integer. The k cannot be arbitrary. There should be no overlapping terms for different k, and the coefficient of x^{k-1} in $h(x)$ should be 0 for each k.

We are ready to prove (A). Assume that strict inequality holds in (7.1). For $b\in[3,20]$, we see that $J\geq 7$ in Tables 14 and 15. Observe that, since $f(x)=(x^2-Ax+B)h(x)$ with $h(x)$ as above, $f(x)$ has a coefficient equal to

$$\begin{aligned}(\beta_J-\beta_1)-A(\beta_J-\beta_0)+B\beta_J&=(1-A+B)\beta_J-\beta_1+A\beta_0\\&=(1-A+B)\beta_J,\end{aligned}$$

corresponding to the coefficient of x^J when the expression in (7.3) is multiplied by x^2-Ax+B. This contradicts our assumption.

Thus far, we have shown that $M(A,B)\geq(1-A+B)\beta_J$. On the other hand, we know the form $h(x)$ must have if $M(A,B)=(1-A+B)\beta_J$. Motivated by (7.3) with $t'=0$, we consider

$$\begin{aligned}h_0(x)&=\beta_0x^{2J}+\beta_1x^{2J-1}+\cdots+\beta_Jx^J\\&\quad+(\beta_J-\beta_0)x^{J-1}+(\beta_J-\beta_1)x^{J-2}+\cdots+(\beta_J-\beta_{J-1}).\end{aligned}$$

The recursive definition of β_j now implies that

$$\begin{aligned}(x^2-Ax+B)h_0(x)&=x^{2J+2}+\big((1-A)\beta_J+B\beta_{J-1}-1\big)x^{J+1}\\&\quad+(1-A+B)\beta_Jx^J+\cdots+(1-A+B)\beta_Jx^2\\&\quad+\big((B-A)\beta_J+A\beta_{J-1}-B\beta_{J-2}\big)x+B(\beta_J-\beta_{J-1}).\end{aligned}$$

Note that the coefficient of x here can be rewritten as $(1-A+B)\beta_J$.

Furthermore, the constant term of $(x^2 - Ax + B)h_0(x)$ can be rewritten as

$$(1 - A + B)\beta_J - \beta_J + \beta_{J+1}.$$

Recalling that the definition of J gives $\beta_{J-1} \le \beta_J$ and $\beta_{J+1} < \beta_J$, we see that the maximal coefficient of $(x^2 - Ax + B)h_0(x)$ is $(1 - A + B)\beta_J$. The definition of $M(A, B)$ now implies the equality given in (A).

Now, we prove (B). The approach here differs from that given in [7] and necessarily has to be different for some values of $b \in [3, 20]$. By (A), we know $M(A, B) = (1 - A + B)\beta_J$, so that $f(x) = (x^2 - Ax + B)h(x)$ where $h(x)$ is a sum over some non-negative integers k of polynomials which are x^k times polynomials of the form (7.3). We refer to the polynomial in (7.3) as *part* of $h(x)$. We begin by showing that with A, B and J fixed, but t' arbitrary, each part of $h(x)$ is divisible by

$$h_1(x) = \sum_{j=0}^{J} (\beta_{J-j} - \beta_{J-j-1})x^j,$$

where we recall that $\beta_{-1} = 0$. From this definition of $h_1(x)$, we have

$$\sum_{j=0}^{J} \beta_{J-j}x^j \equiv \sum_{j=0}^{J} \beta_{J-j-1}x^j \equiv \sum_{j=1}^{J} \beta_{J-j}x^{j-1} \pmod{h_1(x)}.$$

We deduce that the polynomial given in (7.3) is

$$\begin{aligned}
&\Big(\sum_{j=0}^{J} \beta_{J-j}x^j\Big)x^{J+t'} + \Big(\sum_{j=0}^{J+t'-1} x^j\Big)\beta_J - \sum_{j=1}^{J} \beta_{J-j}x^{j-1} \\
&\qquad \equiv \Big(\sum_{j=1}^{J} \beta_{J-j}x^{j-1}\Big)x^{J+t'} + \Big(\sum_{j=0}^{J+t'-1} x^j\Big)\beta_J - \sum_{j=1}^{J} \beta_{J-j}x^{j-1} \\
&\qquad \equiv \Big(\sum_{j=0}^{J} \beta_{J-j}x^j\Big)x^{J+t'-1} + \Big(\sum_{j=0}^{J+t'-2} x^j\Big)\beta_J - \sum_{j=1}^{J} \beta_{J-j}x^{j-1} \\
&\qquad \equiv \Big(\sum_{j=0}^{J} \beta_{J-j}x^j\Big)x^{J+t'-2} + \Big(\sum_{j=0}^{J+t'-3} x^j\Big)\beta_J - \sum_{j=1}^{J} \beta_{J-j}x^{j-1} \\
&\qquad \ \vdots \\
&\qquad \equiv \sum_{j=0}^{J} \beta_{J-j}x^j - \sum_{j=1}^{J} \beta_{J-j}x^{j-1} \equiv 0 \pmod{h_1(x)}.
\end{aligned}$$

Thus, each part of $h(x)$, and therefore $h(x)$ itself, is divisible by $h_1(x)$. Since $h(x)$ consists of at least one part as in (7.3) with $t' \ge 0$ and $J \ge 1$, we obtain

$$h(b) \ge (\beta_0 b^J + \beta_1 b^{J-1} + \cdots + \beta_J)b^J > \beta_0 b^J + \beta_1 b^{J-1} + \cdots + \beta_J > h_1(b) > 1.$$

Hence, $h(b)$ is the integer $h_1(b)$ times an integer that is > 1. We deduce that $f(b) = g(b)h(b) = h(b)$ is composite. This finishes the proof of (B).

Recall that this completes our proof of Theorem 1.1, but we are still interested in showing that most of the bounds in that theorem are sharp, as indicated after its statement.

To establish the sharpness, we find explicit examples of reducible $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients, with maximal coefficient equal to $(1 - A + B)\beta_J + 1$ and with $f(b)$ prime. To this end, we fix an integer $b \in [3, 20]$, choose the appropriate A, B and J using Tables 14 and 15, and then we take $h_1(x)$ to be as given in (7.3). In each case, we set $t' = 0$ except for the case $(b, A, B) = (15, 30, 226)$ where we set $t' = 1$. With some trial and error, we found a quadratic $h_2(x) \in \mathbb{Z}[x]$ such that $h(x) = h_1(x) + h_2(x)$ satisfies the following conditions:

- $f(x) = (x^2 - Ax + B)h(x)$ has non-negative coefficients,
- $f(b)$ is prime,
- the largest coefficient of $f(x)$ is $(1 - A + B)\beta_J + 1$,

where β_J is given in Tables 14 or 15. So as to save space in the representations of the polynomial examples we found, we indicate $f(x)$ by only tabulating $h_2(x)$. Observe that the value of $h_2(x)$ uniquely determines an $f(x)$ as described. Table 18 below gives our explicit choices of $h_2(x)$ to construct $f(x)$ showing us that the bounds $M_1(b)$ for $b \in [3, 20]$ and the bounds $M_2(b)$ for $b \in [4, 20]$ given in Theorem 1.1 are sharp.

Table 18. Examples of $h_2(x)$ for $M_1(b)$ and $M_2(b)$

b	$h_2(x)$ for $M_1(b)$	$h_2(x)$ for $M_2(b)$	b	$h_2(x)$ for $M_1(b)$	$h_2(x)$ for $M_2(b)$
3	$x^2 + 5x + 9$	–	12	$x^2 + 19x + 126$	$x^2 + 23x + 135$
4	$x^2 + 5x + 10$	$x^2 + 8x + 40$	13	$x^2 + 16x + 122$	$x^2 + 13x + 83$
5	$x^2 + 7x + 23$	$x^2 + 10x + 44$	14	$x^2 + 14x + 114$	$x^2 + 23x + 164$
6	$x^2 + 8x + 32$	$x^2 + 11x + 48$	15	$x^2 + 24x + 198$	$x^2 + 15x + 123$
7	$x^2 + 9x + 39$	$x^2 + 13x + 46$	16	$x^2 + 12x + 114$	$x^2 + 31x + 565$
8	$x^2 + 15x + 72$	$x^2 + 15x + 106$	17	$x^2 + 18x + 178$	$x^2 + 19x + 176$
9	$x^2 + 16x + 76$	$x^2 + 17x + 115$	18	$x^2 + 19x + 198$	$x^2 + 35x + 742$
10	$x^2 + 8x + 54$	$x^2 + 11x + 66$	19	$x^2 + 29x + 279$	$x^2 + 27x + 272$
11	$x^2 + 14x + 84$	$x^2 + 21x + 133$	20	$x^2 + 21x + 232$	$x^2 + 39x + 522$

8. Final arguments. We finish by supplying a proof of Theorem 4.3 and, in particular, examples justifying that the degree bounds in Theorem 4.2 and the coefficient bounds in Theorem 4.3 are sharp. The bounds from Corollary 6.1 imply that we need only consider the case that $f(x) = g(x)h(x)$ where $g(x) = x^2 - Ax + B$ is $\Phi_3(x - b)$ or $\Phi_4(x - b)$ and where

$h(x)$ can be taken in the form of the first factor in (6.1). In particular, (6.1) equals $f(x)$.

Fix $b \in [2, 20]$. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ be such that $a_j \geq 0$ for each j and $f(b)$ is prime. From (6.5), we have

$$b_j \geq \beta_j b_0 \quad \text{if } \beta_i > 0 \text{ for } 0 \leq i \leq j-1.$$

Set

$$J_0 = J_0(b, A, B) = \begin{cases} J & \text{if } \beta_{J+1} < 0, \\ J+1 & \text{if } \beta_{J+1} \geq 0. \end{cases}$$

For $(b, A, B) = (2, 3, 3)$, one checks that $\beta_{J_0} = \beta_{J+1} = 0$. For all other (b, A, B) under consideration, $\beta_{J_0} > 0$. Thus,

$$\beta_j > 0 \quad \text{for } 0 \leq j \leq J_0, \quad \text{if } (b, A, B) \neq (2, 3, 3) \text{ or } j \neq J_0.$$

For $(b, A, B) \neq (2, 3, 3)$, we deduce that $b_j > 0$ for all $j \leq J_0$; in particular, $s = \deg h \geq J_0$ and $\deg f \geq J_0 + 2$. In the proof of Theorem 4.2, we established $\deg f \geq J_0 + 2$ in the case $(b, A, B) = (2, 3, 3)$. In fact, for $b \in [2, 20]$, we note that $J_0 + 1$ agrees with the values of $D(b)$ and $D_1(b)$ in Table 7. In particular, to justify $D(b)$ is sharp and to justify the value of $N_1(b)$ in Table 8, we will take $s = J_0$ and $\deg f = J_0 + 2$ with the maximal coefficient of $f(x)$ as small as possible.

Recall b_j has been defined for all integers j. We now set

$$\kappa_j = b_j - Ab_{j-1} + Bb_{j-2} \quad \text{for } j \in \mathbb{Z}. \tag{8.1}$$

Observe that $\kappa_j \geq 0$ for all $j \in \mathbb{Z}$. For integers u and t, we also let

$$\kappa'(u, t) = \sum_{j=0}^{u} \beta_j \kappa_{t-j}.$$

Thus, $\kappa'(u, t) = \kappa'(u-1, t) + \beta_u \kappa_{t-u}$. Recall $\beta_0 = 1$, $\beta_1 = A$ and $\beta_{j+1} = A\beta_j - B\beta_{j-1}$ for $j \geq 1$. Using the definition of κ_j, we deduce

$$\begin{aligned} b_t &= \beta_1 b_{t-1} - B\beta_0 b_{t-2} + \kappa'(0, t) \\ &= \beta_1(Ab_{t-2} - B\beta_0 b_{t-3} + \kappa_{t-1}) - B\beta_0 b_{t-2} + \kappa'(0, t) \\ &= \beta_2 b_{t-2} - B\beta_1 b_{t-3} + \kappa'(1, t) = \cdots = \beta_{t-2} b_2 - B\beta_{t-3} b_1 + \kappa'(t-3, t) \\ &= \beta_{t-1} b_1 - B\beta_{t-2} b_0 + \kappa'(t-2, t) = \beta_t b_0 + \kappa'(t-1, t). \end{aligned}$$

For reference purposes, we summarize the above as

$$b_t = \beta_t b_0 + \kappa'(t-1, t). \tag{8.2}$$

There are two strategies we consider at this point. The first one is derived from [7] and applies in most cases. In each strategy, the basic idea is that $h(x)$ should not differ much from

$$h_3(x) = \beta_0 x^{J_0} + \beta_1 x^{J_0 - 1} + \cdots + \beta_{J_0 - 1} x + \beta_{J_0},$$

where the subscript 3 on the left is used only to avoid conflicts with previous notation. We will tabulate examples of $f(x)$ more efficiently by tabulating instead

$$h_4(x) = h(x) - h_3(x) = \sum_{j=0}^{J_0} (b_j - \beta_j) x^{J_0 - j}.$$

Thus, $f(x) = (x^2 - Ax + B)\big(h_3(x) + h_4(x)\big)$, where A and B come from the coefficients of either $\Phi_3(x - b)$ or $\Phi_4(x - b)$ and where $h_3(x)$ is derived directly from the recurrence for β_j made explicit in (6.3).

Given the above, the expression $(x^2 - Ax + B)h_3(x)$ can be viewed as an approximation of $f(x)$. The coefficient of x in $(x^2 - Ax + B)h_3(x)$ and the constant term of $(x^2 - Ax + B)h_3(x)$ are

$$B\beta_{J_0-1} - A\beta_{J_0} \quad \text{and} \quad B\beta_{J_0},$$

respectively. Strategy I will provide us with the $h_4(x)$ we want in the case that the constant term is at least as large as the coefficient of x. Thus, we use Strategy I when

$$B\beta_{J_0} \geq B\beta_{J_0-1} - A\beta_{J_0}.$$

Note that, in particular, this inequality holds if $\beta_{J_0} \geq \beta_{J_0-1}$, which is typically the case. Strategy II applies when the above inequality does not hold. This leads to applying Strategy II only in the cases $b \in \{6, 14\}$ (with $g(x)$ either $\Phi_3(x - b)$ or $\Phi_4(x - b)$) and $(b, A, B) = (2, 3, 3)$. The case $(b, A, B) = (7, 14, 50)$ is the unique case in our computations where Strategy I applies but $\beta_{J_0} < \beta_{J_0-1}$.

The results of applying Strategies I and II appear in Tables 19 and 20, respectively. In Table 20, the second column distinguishes whether $\Phi_3(x-b)$ or $\Phi_4(x-b)$ is being used, the value 3 referring to the former and the value 4 to the latter.

Table 19. $h_4(x)$ from Strategy I

b	$h_4(x)$ for $\Phi_3(x-b)$	$h_4(x)$ for $\Phi_4(x-b)$
2	–	3
3	$x + 8$	0
4	$x + 7$	$x + 13$
5	$2x + 28$	14
7	$6x + 95$	8
8	$x + 29$	$5x + 80$
9	$6x + 115$	$4x + 92$
10	$3x + 60$	$4x + 90$
11	21	28
12	$x + 48$	$4x + 102$
13	$x + 62$	2
15	$6x + 192$	$9x + 279$
16	$x + 68$	$4x + 139$
17	$3x + 100$	12
18	$5x + 211$	$2x + 113$
19	$4x + 176$	12
20	$x + 72$	$5x + 233$

Table 20. $h_4(x)$ from Strategy II

b	Φ	$h_4(x)$
2	3	$x+7$
6	3	4662361342700
6	4	$2x + 13519269991344$
14	3	$2x + 542371818196896628226455583595687935400617086393962 90$
14	4	$9x + 19042701543625053682051012101468329328645426 0001$

STRATEGY I. The basic idea here is to focus on the constant term of $f(x)$ as being its largest coefficient. We take $t = J_0$ in (8.2). The constant term of $h(x)$ is b_{J_0}, and we view (8.2) as indicating how far this constant term is from $\beta_{J_0} b_0$. Note that the constant term of $f(x)$ is Bb_{J_0}. If the maximal coefficient of $f(x)$ is M, then necessarily $Bb_{J_0} \le M$ and we deduce

$$\beta_{J_0} b_0 + \sum_{j=0}^{J_0-1} \beta_j \kappa_{J_0-j} = b_{J_0} \le \frac{M}{B}. \tag{8.3}$$

The idea is to choose an upper bound search value M' for M that is close to $B\beta_{J_0}$. We take $M' = B\beta_{J_0} + M_0'$ where $M_0' > 0$ is relatively small (a value ≤ 95000 sufficed for each polynomial we tested but often much smaller values as well). We then seek to determine the polynomials $f(x)$ with maximal coefficient $M \in [B\beta_{J_0}, M']$ that are of the form (6.1). If none exists, we increase the value of M_0'. As long as we find such an $f(x)$ with $M_0' \le \beta_{J_0}$, we know from (8.3) that $b_0 = 1$ when M is minimal. The definition of κ_0 then implies in this case that $\kappa_0 = 1$.

From (8.3), we obtain

$$\beta_{J_0} + \sum_{j=0}^{J_0-1} \beta_j \kappa_{J_0-j} \le \frac{B\beta_{J_0} + M_0'}{B} = \beta_{J_0} + \frac{M_0'}{B}.$$

Hence,

$$\sum_{j=0}^{J_0-1} \beta_j \kappa_{J_0-j} \le \frac{M_0'}{B}. \tag{8.4}$$

Since the values of β_j grow quickly as j increases, if M_0' is relatively small, then (8.4) forces κ_{J_0-j} to be 0 unless j is small. This then allows us to determine a small number of choices for the κ_j and, therefore, a small number of choices of b_j from (8.1). Thus, we are left with a small number of $h(x)$, and hence $f(x)$, to examine.

As an example, consider $b = 7$ and $g(x) = \Phi_3(x-7) = x^2 - 13x + 43$. Thus, $A = 13$ and $B = 43$, and one checks that $J_0 = J = 22$. Take $M_0' = 5000$. Then (8.4) implies

$$\sum_{j=0}^{21} \beta_j \kappa_{22-j} \le \frac{5000}{43} \le 116.28.$$

Given $\beta_0 < \beta_1 < \cdots < \beta_{22} \approx 6.68 \cdot 10^{17}$ and

$$\beta_0 = 1, \quad \beta_1 = 13, \quad \beta_2 = 126, \quad \ldots,$$

we deduce $\kappa_0 = \kappa_1 = \cdots = \kappa_{20} = 0$, $\kappa_{21} \le 8$, and $\kappa_{22} \le 116$. Thus, there are 9 possibilities for $\kappa_{21} \in [0, 8]$ and 117 choices for $\kappa_{22} \in [0, 116]$, giving a total of $9 \times 117 = 1053$ choices for the κ_j. Each of these leads to a polynomial $h(x) = \sum_{j=0}^{22} b_j x^j$ by using (8.1). These 1053 polynomials $h(x)$ include all possibilities for $h(x) \in \mathbb{Z}[x]$ for which $f(x) = (x^2 - 13x + 43)h(x)$ is of degree 24 and has non-negative coefficients all bounded above by $B\beta_{J_0} + 5000$. We are interested in those $f(x)$ for which $f(7) = h(7)$ is prime, and we want the maximal coefficient of such an $f(x)$ to be as small as possible. A direct check gives that $\kappa_{21} = 6$ and $\kappa_{22} = 17$ produces such an $f(x)$.

Strategy II. For this approach, we focus on both the coefficient of x and the constant term of $f(x)$. Recall that these coefficients are

$$Bb_{J_0-1} - Ab_{J_0} \quad \text{and} \quad Bb_{J_0},$$

respectively. If the maximal coefficient of $f(x)$ is M, then a weighted average of these coefficients must also be $\le M$. In particular, we deduce that

$$\frac{B^2}{A+B} b_{J_0-1} = \frac{B}{A+B}\big(Bb_{J_0-1} - Ab_{J_0}\big) + \frac{A}{A+B}\big(Bb_{J_0}\big) \le M.$$

We apply (8.2) with $t = J_0 - 1$ to deduce that

$$\beta_{J_0-1} b_0 + \sum_{j=0}^{J_0-2} \beta_j \kappa_{J_0-1-j} = \beta_{J_0-1} b_0 + \kappa'(J_0-2, J_0-1) = b_{J_0-1} \le \frac{A+B}{B^2} \cdot M.$$

We deduce that $M \ge B^2 \beta_{J_0-1}/(A+B)$. We choose an upper bound search value M' for M that is close to $B^2 \beta_{J_0-1}/(A+B)$. We take

$$M' = \frac{B^2}{A+B} \cdot \beta_{J_0-1} + M'_0, \quad \text{with} \quad M'_0 < \frac{B^2}{A+B} \cdot \beta_{J_0-1}.$$

The upper bound on M'_0 is considerably larger than we want in general, and this upper bound ensures that $b_0 = 1$ and hence, by definition, $\kappa_0 = 1$. We deduce now that

$$\sum_{j=0}^{J_0-2} \beta_j \kappa_{J_0-1-j} \le \frac{A+B}{B^2} \cdot M'_0. \tag{8.5}$$

With M'_0 small, we are able to deduce reasonable upper bounds from (8.5) for every κ_j except κ_{J_0}.

The value κ_{J_0} can be very large, and the idea is to find a very close approximation $\kappa^* \in \mathbb{Z}$ to κ_{J_0} and to use this to narrow down the possibilities for κ_{J_0}. The value of κ^* will depend on the values of $\kappa_0, \kappa_1, \ldots, \kappa_{J_0-1}$. We fix κ_j for $j \in \{0,1,\dots,J_0-1\}$ from the finite collection of possibilities determined by (8.5). By the definition of the κ_j, the values of b_j are determined for $j \in \{0,1,\dots,J_0-1\}$. The idea now is to choose κ^* so that the selection $\kappa_{J_0} = \kappa^*$ forces the coefficient of x in $f(x)$ to be close to the constant term of $f(x)$. One can check that this leads to

$$\kappa^* = \left\lfloor Bb_{J_0-2} - Ab_{J_0-1} + \frac{Bb_{J_0-1}}{A+B} + \frac{1}{2} \right\rfloor, \tag{8.6}$$

though the justification of this choice for κ^* is not needed to see that it provides us with an estimate that will allow us to determine κ_{J_0}. We explain this next.

Fixing κ^* as above, we show that κ_{J_0} must be close to κ^*. Set $\kappa_{J_0} = \kappa^* + t$. Thus, we are interested in showing that $|t|$ is not very large. Since the coefficients of $f(x)$ must be $\le M$, by looking at the coefficient of x in $f(x)$, we deduce that

$$Bb_{J_0-1} - A\big(Ab_{J_0-1} - Bb_{J_0-2} + \kappa^* + t\big) = Bb_{J_0-1} - Ab_{J_0} \le M.$$

From the definition of κ^*, the expression between parentheses above is bounded above by

$$\frac{Bb_{J_0-1}}{A+B} + \frac{1}{2} + t.$$

From the definition of M', we deduce that

$$Bb_{J_0-1} - \frac{ABb_{J_0-1}}{A+B} - \frac{A}{2} - At \le M \le M' = \frac{B^2}{A+B} \cdot \beta_{J_0-1} + M_0',$$

which simplifies to

$$t \ge \frac{B^2}{A(A+B)} \cdot (b_{J_0-1} - \beta_{J_0-1}) - \frac{M_0'}{A} - \frac{1}{2}. \tag{8.7}$$

By looking at the constant term in $f(x)$, we deduce that

$$B\big(Ab_{J_0-1} - Bb_{J_0-2} + \kappa^* + t\big) = Bb_{J_0} \le M \le M' = \frac{B^2}{A+B} \cdot \beta_{J_0-1} + M_0'.$$

Since

$$\kappa^* > Bb_{J_0-2} - Ab_{J_0-1} + \frac{Bb_{J_0-1}}{A+B} - \frac{1}{2},$$

we are led to

$$t < -\frac{B}{A+B} \cdot (b_{J_0-1} - \beta_{J_0-1}) + \frac{M_0'}{B} + \frac{1}{2}. \tag{8.8}$$

Observe that (8.2) implies $b_{J_0-1} - \beta_{J_0-1} \ge 0$. Although not needed, (8.5) also implies $b_{J_0-1} - \beta_{J_0-1}$ is not very large. In particular, we deduce that

$$-\frac{M_0'}{A} - \frac{1}{2} \le t < \frac{M_0'}{B} + \frac{1}{2}.$$

Given $\kappa_{J_0} = \kappa^* + t$, we are left with only a small number of choices for κ_{J_0}, and can test for $f(x)$ as in Strategy I.

As an example, we consider $(b, A, B) = (6, 12, 37)$. We take $M_0' = 200$. One checks that $J_0 = J + 1 = 18$. As is easily checked, then, $0 < \beta_0 < \beta_1 < \cdots < \beta_{J_0-1}$ and $0 < \beta_{J_0} < \beta_{J_0-1}$. Also,

$$\frac{(A+B)M_0'}{B^2} = \frac{49 \cdot 200}{37^2} = 7.1585\ldots.$$

From (8.5), we deduce $\kappa_0 = \kappa_1 = \cdots = \kappa_{16} = 0$ and $0 \le \kappa_{17} \le 7$. We set $b_0 = 1$. For each value of $\kappa_{17} \in [0, 7]$, we use (8.2) to compute the values of $b_1, b_2, \ldots, b_{17}$, (8.6) to compute κ^*, and (8.7) and (8.8) to find the bounds for t. The choice of κ_{17} that leads to the maximal coefficient of an $f(x)$ as small as possible and with $f(6)$ prime is $\kappa_{17} = 2$. This choice of κ_{17} gives

$$\kappa^* = 13519269991324 \quad \text{and} \quad -12 \le t \le 4.$$

The desired $f(x)$ comes from the choice $t = -4$, where

$$\begin{aligned} b_{18} &= 12b_{17} - 37b_{16} + \kappa^* + t = 12b_{17} - 37b_{16} + 13519269991320 \\ &= 16497794651771. \end{aligned}$$

Thus,

$$f(x) = (x^2 - 12x + 37)h(x) \quad \text{with} \quad h(x) = b_0x^{18} + b_1x^{17} + \cdots + b_{17}x + b_{18}$$

and with $f(6) = h(6)$ prime. The maximal coefficient of $f(x)$ is

$$6104184021157746,$$

corresponding to the coefficient of x in $f(x)$.

A similar use of Strategy II for $(b, A, B) = (6, 11, 31)$ establishes that the smallest maximal coefficient of an $f(x)$ having non-negative coefficients with $f(x)$ divisible by $\Phi_3(x - 6)$ and $f(6)$ prime is 674230217165581. In terms of Theorem 4.3, these examples justify the values of $N_1(6) = 610418402115745$ and $N_2(6) = 674230217165580$ given in Tables 8 and 9 are sharp.

9. Concluding remarks. Having dealt with the cases $b \in [2, 20]$, it is natural to ask what can be said for $b \ge 21$ or b large. In a subsequent paper, we plan to discuss results for general $b \ge 2$, where what we have established in this paper can be combined with analysis for larger b to obtain explicit results for all $b \ge 2$. For example, Theorem 4.2 in combination with an analysis for larger b leads to the following.

THEOREM 9.1. *Let b be an integer ≥ 2, and let $D = D(b) = \lfloor \pi/\tan^{-1}(1/b) \rfloor$. Then there are no reducible $f(x) \in \mathbb{Z}[x]$ of degree $\le D$ having non-negative integer coefficients for which $f(b)$ is prime. Furthermore, for every integer $n > D$, there are infinitely many reducible $f(x) \in \mathbb{Z}[x]$ of degree n having non-negative integer coefficients with $f(b)$ prime.*

As indicated early on in this paper, the analysis for smaller b tends to be more difficult. In particular, recall that we have not been able to establish a sharp bound for $M_1(2)$ or $M_2(3)$. We view finding a sharp bound for $M_1(2)$ as a particularly interesting challenge for further investigation.

Acknowledgements. The third author expresses his gratitude to the NSA for support during this research.

References

[1] J. Alexander, *Irreducibility criteria for polynomials with non-negative coefficients*, Master's Thesis, Univ. of South Carolina, 1987.

[2] B. Angle, *Irreducibility criteria for polynomials with non-negative integer coefficients*, Senior Honors Thesis, University of South Carolina, 1993.

[3] J. Brillhart, M. Filaseta, and A. Odlyzko, *On an irreducibility theorem of A. Cohn*, Canad. J. Math. 33 (1981), 1055–1059.

[4] S. M. Dunn, *Explorations in elementary and analytic number theory*, Doctoral Dissertation, Univ. of South Carolina, 2014, 150 pp.

[5] M. Filaseta, *A further generalization of an irreducibility theorem of A. Cohn*, Canad. J. Math. 34 (1982), 1390–1395.

[6] M. Filaseta, *Irreducibility criteria for polynomials with non-negative coefficients*, Canad. J. Math. 40 (1988), 339–351.

[7] M. Filaseta and S. Gross, *49598666989151226098104244512918*, J. Number Theory 137 (2014), 16–49.

[8] M. Mignotte, review MR0678678 of [5].

[9] M. R. Murty, *Prime numbers and irreducible polynomials*, Amer. Math. Monthly 109 (2002), 452–458.

[10] I. Niven, *Irrational Numbers*, Carus Math. Monogr. 11, Math. Assoc. Amer., Wiley, New York, 1956.

[11] G. Pólya und G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, Springer, Berlin, 1964.

[12] W. Rudin, *Principles of Mathematical Analysis*, 3rd ed., Internat. Ser. Pure Appl. Math., McGraw-Hill, New York, 1976.

Morgan Cole
Department of Mathematics
College of the Canyons
26455 Rockwell Canyon Rd
Santa Clarita, CA 91355, U.S.A.
E-mail: morgan.cole@canyons.edu

Scott Dunn, Michael Filaseta
Department of Mathematics
University of South Carolina
Columbia, SC 29208, U.S.A.
E-mail: dunnsm@math.sc.edu
filaseta@math.sc.edu