49598666989151226098104244512918

Michael Filaseta
Department of Mathematics
University of South Carolina
Columbia, SC 29208

Samuel Gross
Department of Mathematics
University of South Carolina
Columbia, SC 29208

Abstract: Let $f(x)$ be a polynomial with non-negative integer coefficients for which $f(10)$ is prime. A result of A. Cohn implies that if the coefficients of $f(x)$ are ≤ 9, then $f(x)$ is irreducible. In 1988, the first author showed that the bound 9 could be replaced by 10^{30}. We show here that the bound 9 can be replaced by the number in the title and that this is the largest integer with this property. Other related results are established.

1. Introduction

Let $d_n d_{n-1} \dots d_1 d_0$ be the decimal representation of a prime, and let

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

A result attributed to A. Cohn in [8] asserts that such an $f(x)$ is irreducible. Here and throughout this paper, irreducibility is in the ring $\mathbb{Z}[x]$ unless stated otherwise. In particular, for $f(x)$ as above and for most polynomials considered in this paper, $f(10)$ is a prime so that if $f(x)$ is a constant, then it is also irreducible.

Cohn's result has been extended to all bases $b \geq 2$ in [3], to base b representations of kp where k is a positive integer $< b$ and p is a prime in [4], and an analog to function fields over finite fields in [7]. This paper focuses more in the direction of [5] where the coefficients of $f(x)$ are allowed to be larger. More specifically, we begin with an $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_j \geq 0$ for each j and for which $f(10)$ is a prime. If $a_j \leq 9$ for all j, then Cohn's theorem implies $f(x)$ is irreducible. But what happens in the case that the a_j are not bounded by 9?

Before delving into the subject further, we give a simple argument with a perhaps surprising conclusion that will be instructive for later purposes. Fix $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ satisfying $a_j \geq 0$ for each j and $f(10)$ is a prime as above. For now, we require no upper bound on the size of the coefficients a_j. Suppose $f(x)$ is reducible over $\mathbb{Q}$. Then $f(x) = g(x)h(x)$ for some $g(x)$ and $h(x)$ having integer coefficients, positive degrees and positive leading coefficients. The condition $f(10)$ is prime implies that one of $g(10)$ or $h(10)$ is ± 1. We may suppose $g(10) = \pm 1$ and do so. Since $f(x)$ has non-negative coefficients, $f(x)$ and, therefore, $g(x)$ cannot have positive real roots. Since the leading coefficient of $g(x)$ is positive, we deduce from the classical Intermediate Value Theorem that $g(10) > 0$. Thus, $g(10) = 1$. Let b denote the leading coefficient of $g(x)$ and $\beta_1, \dots, \beta_r$ the roots of $g(x)$ included to their multiplicities. Thus, $\deg g = r$, and we have

$$1 = |g(10)| = b \prod_{j=1}^{r} |10 - \beta_j| \ge \prod_{j=1}^{r} |10 - \beta_j|.$$

We deduce that at least one root of $g(x)$ is in the disc

$$\mathcal{D} = \{z \in \mathbb{C} : |10 - z| \le 1\}.$$

Recalling $f(x)$ has no positive real roots, we have the following.

Lemma 1.1. *Let $f(x)$ be a reducible polynomial with non-negative integer coefficients such that $f(10)$ is a prime. Then $f(x)$ has a non-real root in $\mathcal{D}$.*

Next, since the complex conjugate of a root of $f(x)$ will be a root of $f(x)$, there is a root $\alpha \in \mathcal{D}$ of $f(x)$ with positive imaginary part. One can easily argue then that

$$\alpha = re^{i\theta}, \quad \text{where } r \ge 9 \text{ and } 0 < \theta \le \sin^{-1}(1/10).$$

One checks that for each $k \in \{1, 2, \dots, 31\}$, we have

$$0 < k\theta \le 31 \sin^{-1}(1/10) < \pi.$$

As a consequence, we see that

$$\mathrm{Im}(\alpha^k) = r^k \sin(k\theta) > 0, \quad \text{for } 1 \le k \le 31.$$

Recall again that the coefficients of $f(x)$ are non-negative. Assuming $1 \le n \le 31$ where $n = \deg f$, then $\mathrm{Im}(f(\alpha)) \ge \mathrm{Im}(\alpha^n) > 0$, contradicting that α is a root of $f(x)$. In other words, we have the following.

Theorem 1.2. *Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ satisfying $a_j \ge 0$ for each j and $f(10)$ is a prime. If $\deg f \le 31$, then $f(x)$ is irreducible.*

Therefore, as long as the polynomial $f(x)$ has degree ≤ 31, no upper bound on the coefficients of $f(x)$ are needed to deduce that $f(x)$ is irreducible. The coefficients need not be digits at all, just non-negative integers with $f(10)$ prime.

The above result was observed in [5]. With a little work, one can come up with an example of a *reducible* $f(x)$ with non-negative integer coefficients satisfying $f(10)$

is prime. An example similar to the following was given in [5]:

$$x^{32} + 4\,x^3 + 10\,x^2 + 56032867540101415671615726389 24\,x \\ + 6109104104761309555986010605548 9.$$

One checks that this polynomial $f(x)$ is divisible by $x^2 - 20x + 101$ and satisfies $f(10)$ is prime. Thus, the bound 31 is best possible in Theorem 1.2.

One goal of this paper is to show that the above example is best possible in another sense.

Theorem 1.3. *Let $f(x)$ be a polynomial with non-negative integer coefficients satisfying $f(10)$ is prime. If $\deg f = 32$ and the coefficients of $f(x)$ are*

$$\le 61091041047613095559860106055488,$$

then $f(x)$ is irreducible.

The above, however, is not the focus of our paper. We are interested in the more general question of what happens for polynomials $f(x)$ of arbitrary degree. If $\deg f > 32$, the conclusion of Theorem 1.3 is no longer true. One example is given by the polynomial

$$\begin{aligned} x^{129} &+ 62081485465607662756750390368 19\,x^{98} \\ &+ 49598666989151226098104244512918\,x^{97} \\ &+ \cdots + 49598666989151226098104244512918\,x^{32} \\ &+ 49598666989151226098104244512917\,x^{31} \\ &+ 49598666989151226098104244512918\,x^{30} \\ &+ \cdots + 49598666989151226098104244512918\,x^{5} \\ &+ 49598666989151226098104244512919\,x^{4} \\ &+ 49598666989151226098104244512918\,x^{3} \\ &+ 49598666989151226098104244512721\,x^{2} \\ &+ 49598666989151226098104244512898\,x \\ &+ 43390518442590459822429205486401. \end{aligned}$$

To clarify, if $f(x)$ is the above polynomial, then it has terms of every degree ≤ 98 with each coefficient skipped in the "$\cdots$" notation above equal to

$$N = 49598666989151226098104244512918.$$

One checks that $f(x)$ is divisible by $x^2 - 20x + 101$ and that $f(10)$ is prime.

It is not a coincidence that N is the number given in the title of our paper. Observe that $f(x)$ has one coefficient, the one for x^4, that is equal to $N+1$. This is the only coefficient of $f(x)$ that exceeds N. The main goal of this paper is to show that if all the coefficients $f(x) \in \mathbb{Z}[x]$ are non-negative and $\le N$ and if $f(10)$ is prime, then $f(x)$ is irreducible. The above example shows that this result is sharp.

In fact, we prove more, explaining the important role of $x^2-20x+101$ in our above examples.

Theorem 1.4. *Let $f(x)$ be a polynomial with non-negative integer coefficients and with $f(10)$ prime. If the coefficients are each $\leq N$, then $f(x)$ is irreducible. Furthermore, if the coefficients are*

$$\leq 8592444743529135815769545955936773$$

and $f(x)$ is reducible, then $f(x)$ is divisible by $x^2-20x+101$.

We will postpone giving further examples in this paper until later, but as we will see, the second bound in Theorem 1.4 is also sharp. Suppose still that $f(x)$ is a polynomial with non-negative integer coefficients and with $f(10)$ prime. We will also see that if the coefficients of $f(x)$ are $\leq 1.169 \times 10^{34}$ and $f(x)$ is reducible, then $f(x)$ is divisible by one of $x^2-20x+101$ and $x^2-19x+91$. To put this in perspective, $N = 4.9598\ldots \times 10^{31}$ and the second bound on the coefficients in Theorem 1.4 is $8.5924\ldots \times 10^{33}$.

A multitude of related problems are suggested by these results. As noted earlier, analogous results should hold with $f(10)$ replaced by $f(b)$ where b is an integer ≥ 2 and with the bounds in the results modified. The authors are obtaining such results, but they are not complete and involve changes to a function $F(z)$ that plays an important role in this paper and is described in the next section. As might be expected, smaller values of b are somewhat more difficult to handle and this is particularly the case for $b=2$.

Related to Theorem 1.2, we will establish that if $f(x)$ is a reducible polynomial with non-negative integer coefficients satisfying $f(10)$ prime and $\deg f \leq 34$, then $f(x)$ is divisible by $x^2-20x+101$. An example will show that 34 is sharp for this bound. We will also see later that if instead $\deg f \leq 36$, then $f(x)$ is divisible by one of $x^2-20x+101$ and $x^2-19x+91$. One can extend results of this nature as follows. Fix a positive integer D. Then there is a finite set of polynomials $\mathcal{S}_1(D)$ such that

- If $g(x) \in \mathcal{S}_1(D)$, then $\deg g \geq 1$ and $g(10)=1$.
- If $f(x) \in \mathbb{Z}[x]$ is reducible, has degree $\leq D$, has non-negative coefficients and satisfies $f(10)$ is prime, then $f(x)$ is divisible by some $g(x) \in \mathcal{S}_1(D)$.

On the other hand, the two bounds given in Theorem 1.4 suggest that given a fixed upper bound B, there is a finite set of polynomials $\mathcal{S}_2(B)$ satisfying both the following:

- If $g(x) \in \mathcal{S}_2(B)$, then $\deg g \geq 1$ and $g(10)=1$.
- If $f(x) \in \mathbb{Z}[x]$ is reducible, has non-negative coefficients each $\leq B$ and satisfies $f(10)$ is prime, then $f(x)$ is divisible by some $g(x) \in \mathcal{S}_2(B)$.

Although we can establish that $\mathcal{S}_1(D)$ exists, we do not know whether $\mathcal{S}_2(B)$ exists.

To what extent can the approaches here be extended to obtain results in the case that $f(10)$ or, more generally, $f(b)$ is not prime but instead a small multiple of a prime? As suggested earlier, if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $0 \le a_j \le 9$ and $f(10) = kp$ where p is a prime and k a positive integer ≤ 9, then $f(x)$ is irreducible over $\mathbb{Q}$. If $k = 10$, then $a_0 = 0$ and $f(x)$ will have the factor x. Nevertheless, as noted in [4] and [6], still more can be said. For example, if instead $f(10) = kp$ where p is a prime and k a positive integer ≤ 81, then either $f(x)$ is irreducible or there is a linear factor $g(x)$ of $f(x)$ with $g(10)$ a divisor of k. Results from [5] imply that some of this work can be generalized to allow for the coefficients a_j of $f(x)$ to be larger than 9. It would be interesting to know to what extent the approach here can lead to best possible results on the size of a_j in these cases.

Reminiscent of the results in [5], suppose we ask instead for the limit infimum of the numbers $N_0 \in \mathbb{R}$ having the property that if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $0 \le a_j \le N_0 a_n$ for each j and with $f(10)$ prime, then $f(x)$ is irreducible. What can be said about the precise value of N_0? Although Theorem 1.4 implies $N_0 \le N + 1$, maybe $N_0 > N$.

Let $\mathcal{T}$ be the set of positive integers m with the property that if $d_n d_{n-1} \dots d_1 d_0$ is the decimal (or base b for a fixed b) representation of m, then $\sum_{j=0}^{n} d_j x^j$ is irreducible. Probably $\mathcal{T}$ has asymptotic density 1 in the set of positive integers, but this is not known. There are other nice classes of integers besides small multiples of primes which belong to $\mathcal{T}$, notably the integers of the form 5^k and 16^k for an arbitrary positive integer k, but we do not even know if $\mathcal{T}$ includes a set of positive density in the set of positive integers.

The results of the next section will imply that if $g(x)$ is a non-constant polynomial in $\mathbb{Z}[x]$ and $g(0) = 1$, then either $g(x)$ has at least one of i, $(1 + i\sqrt{3})/2$ and $(-1 + i\sqrt{3})/2$ as a root or $g(x)$ has a root α with $|\operatorname{Re}(\alpha)| < 1.617$ and $|\operatorname{Im}(\alpha)| < 0.856$. What kind of extensions of this result exist? E. Dobrowolski (private communication) has given an argument to show that there is a similar region with $g(x)$ having the property that either it has one of a finite list of factors or it has a root with $|\operatorname{Im}(\alpha)| < 0.76$. He has also shown that this no longer holds if one replaces the upper bound 0.76 by a number $< 1/2$.

Before continuing, we note that the computations in this paper were done with Maple 15 and the primality of relevant numbers encountered checked using Sage. It is also worth noting that some preliminary bounds making use of prior techniques were obtained in [1] and [2]. As we will see, some preliminary results based on [1] and [5] play a role in the approach given here.

2. A root bounding function

Let $f(x)$ be a non-constant polynomial with non-negative integer coefficients such that $f(10)$ is a prime. Assume $f(x)$ is reducible so that $f(x) = g(x)h(x)$ where each of $g(x)$ and $h(x)$ is in $\mathbb{Z}[x]$, has positive degree and has positive leading coefficient. As before, $f(10)$ being prime allows us to deduce one of $g(10)$ and $h(10)$ equals 1.

We suppose, as we may, that $g(10) = 1$.

There will be three main ideas used to obtain the results in this paper. One of the main ideas involves the use of a certain rational function that will enable us to obtain important information about the location of a root of the factor $g(x)$. The second idea is to use an approach in [5] in combination with the first idea to bound the coefficients of $f(x)$ in the case that $f(x)$ is reducible but not divisible by one of $\Phi_3(x-10)$, $\Phi_4(x-10)$ and $\Phi_6(x-10)$, where $\Phi_n(x)$ is the nth cyclotomic polynomial. The third idea is tied to bounding the coefficients of the second factor $h(x)$ by elements formed from a certain recursion relation and using this information to obtain bounds on the coefficients of $f(x)$ in the case that $f(x)$ is divisible by one of $\Phi_3(x-10)$, $\Phi_4(x-10)$ and $\Phi_6(x-10)$. In this section, we give the details of the first idea.

The proof of Lemma 1.1 implies that $g(x)$ has a non-real root in $\mathcal{D}$. We now obtain some different information about a root of $g(x)$. The basic idea is to say that either $g(x)$ has a root in common with one of

$$\Phi_3(x-10) = (x-10)^2 + (x-10) + 1 = x^2 - 19x + 91,$$

$$\Phi_4(x-10) = (x-10)^2 + 1 = x^2 - 20x + 101$$

and

$$\Phi_6(x-10) = (x-10)^2 - (x-10) + 1 = x^2 - 21x + 111,$$

or $g(x)$ has roots near 10 and closer to the real axis than the roots of these three quadratics. In addition to the notation $\Phi_n(x)$ already indicated above, we make use of ζ_n to denote $e^{2\pi i/n}$.

Let $z = x + iy$, and consider the function

$$F(z) = \frac{N(x,y)}{D(x,y)}$$

where

$$N(x,y) = |10 + \zeta_6 - z|^6 |10 + \overline{\zeta_6} - z|^6 |10 + \zeta_3 - z|^6 \cdot |10 + \overline{\zeta_3} - z|^6 |10 + i - z|^4 |10 - i - z|^4$$

and

$$D(x,y) = |10 - z|^{40}.$$

As can be verified by a direct computation, the expressions

$$|10 + \zeta_6 - z|^2 \, |10 + \overline{\zeta_6} - z|^2, \quad |10 + \zeta_3 - z|^2 \, |10 + \overline{\zeta_3} - z|^2, \quad |10 + i - z|^2 \, |10 - i - z|^2, \quad \text{and} \quad |10 - z|^2$$

are all polynomials in $\mathbb{Z}[x,y]$. Thus, $N(x,y)$ and $D(x,y)$ are in $\mathbb{Z}[x,y]$ and $F(z)$ is a rational function in x and y.

To motivate the role of $F(z)$, we express $g(x)$ in the form

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

Thus, b is the leading coefficient of $g(x)$, and $\beta_1, \ldots, \beta_r$ are the roots of $g(x)$ and, hence, also roots of $f(x)$. Observe that the expressions

$$\frac{|g(10+\zeta_6)|^6 \left|g\left(10+\overline{\zeta_6}\right)\right|^6 |g(10+\zeta_3)|^6 \left|g\left(10+\overline{\zeta_3}\right)\right|^6 |g(10+i)|^4 |g(10-i)|^4}{|g(10)|^{40}}$$

and

$$\frac{1}{b^8} \prod_{j=1}^{r} F(\beta_j)$$

are equal. We denote these common values by V. Now, each of

$$g(10+\zeta_6)\, g\left(10+\overline{\zeta_6}\right), \quad g(10+\zeta_3)\, g\left(10+\overline{\zeta_3}\right), \quad \text{and} \quad g(10+i)\, g(10-i)$$

is a symmetric polynomial, with coefficients in $\mathbb{Z}$, in the roots of an irreducible monic quadratic in $\mathbb{Z}[x]$. Hence, each of these expressions is a rational integer. Thus, the numerator of the first expression for V above is in $\mathbb{Z}$. Since also $g(10) = 1$ and $V \geq 0$, we deduce that either $V = 0$ or $V \in \mathbb{Z}^+$. The definition of V also implies that $V = 0$ precisely when at least one of $\Phi_3(x-10)$, $\Phi_4(x-10)$ and $\Phi_6(x-10)$ is a factor of $g(x)$. If none of these quadratics is a factor of $g(x)$, we necessarily have that $V \in \mathbb{Z}^+$. In this case, the product in the second expression for V above must be a positive integer. Since $F(z)$ is a non-negative real number for all $z \in \mathbb{C}$, we deduce that $F(\beta_j) \geq 1$ for at least one value of $j \in \{1, 2, \ldots, r\}$. In other words, there is a root β of $g(x)$, and consequently of $f(x)$, satisfying $F(\beta) \geq 1$. Note that $g(10) = 1$ implies $\beta \neq 10$.

Before delving further into the arguments in this section, we summarize the important role of $F(z)$. Only using that $g(x) \in \mathbb{Z}[x]$ and $g(10) = 1$, we have shown that either $g(x)$ has at least one of the factors $\Phi_3(x-10)$, $\Phi_4(x-10)$ and $\Phi_6(x-10)$, or $g(x)$ has a root

$$\beta \in \mathcal{R} = \{z \in \mathbb{C} : F(z) \geq 1\}.$$

In the latter case, an analysis of the region $\mathcal{R}$ in the complex plane will enable us to obtain important information about β. The graph in Figure 1 depicts the region $\mathcal{R}$. In the graph, $8.383 < \mathrm{Re}(z) < 11.617$ and $|\mathrm{Im}(z)| < 0.856$. Although the graph is only based on numerical approximations, it helps motivate the subsequent arguments that give us precise information about β. For simplicity, we will sometimes refer to points (x, y) being in $\mathcal{R}$, and this is to be interpreted as the point $x + iy$ in the complex plane being in $\mathcal{R}$. For example, we will see later that all the points $(x, y) \in \mathcal{R}$ lie below the line $y = \tan(\pi/36)x$. This then means that the $x + iy \in \mathcal{R}$ satisfy $y \leq \tan(\pi/36)x$.

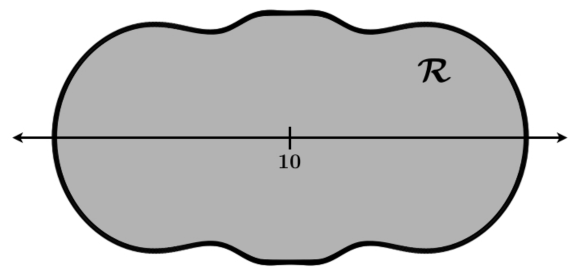

Figure 1

To analyze the complex $z = x + iy$ for which $F(z) \geq 1$, we return to our representation of $F(z)$ as $N(x, y)/D(x, y)$ where $N(x, y)$ and $D(x, y)$ are explicit polynomials in $\mathbb{Z}[x, y]$. We define

$$P\,(x, y) = D\,(x, y) - N\,(x, y)\,.$$

By direct computation (or a little thought) one sees that

$$P(x, y) = \sum_{j=0}^{20} a_j(x) y^{2j}$$

where each $a_j(x)$ is in $\mathbb{Z}[x]$. The definition of $D(x, y)$ implies that $D(x, y) > 0$ for all $(x, y) \in \mathbb{R}^2$ with $(x, y) \neq (10, 0)$. We deduce that

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

are equivalent for $(x, y) \neq (10, 0)$. The equations $F(z) = 1$ and $P(x, y) = 0$ are similarly equivalent for $(x, y) \neq (10, 0)$. In other words, pairs $(x, y) \in \mathbb{R}^2$ satisfying $P(x, y) = 0$ correspond precisely to those complex numbers $z = x + iy$, with x and y in $\mathbb{R}$, satisfying $F(z) = 1$.

Lemma 2.1. *There exists an $a > 0$ and a function $\rho\,(x)$ defined on an interval I of the form $[10 - a, 10 + a]$ satisfying the following:*

(a) For any given $x \notin I$, $P\,(x, y) = 0$ has no real roots in y.
(b) $\rho\,(10 \pm a) = 0$.
(c) $P\,(x, \rho\,(x)) = 0$ for all $x \in I$.
(d) $\rho\,(x)$ is a continuously differentiable function on the interior of I and continuous on I.
(e) If x and y are real numbers for which $P\,(x, y) \leq 0$, then $x \in I$ and $|y| \leq \rho(x)$.

To help explain Lemma 2.1, we note that the complex numbers $x + i\rho(x)$ are the points along the boundary of the region $\mathcal{R}$ which are on or above the real axis. Thus, $10 \pm a$ correspond to the points where this boundary intersects the real axis. Given that $P(x, y)$ is a polynomial in y^2 with coefficients in $\mathbb{Z}[x]$, we see that $\mathcal{R}$ is symmetric about the real axis so that the points $x - i\rho(x)$ are the points along the boundary of $\mathcal{R}$ that are on or below the real axis.

Our proof of Lemma 2.1, in particular part (d), will make use of the well-known Implicit Function Theorem (see, for example, [9]), which we state next.

Lemma 2.2. *Let $\mathcal{O}$ be an open set in $\mathbb{R}^2$ and let $W : \mathcal{O} \longrightarrow \mathbb{R}$. Suppose W has continuous partial derivatives W_x and W_y on $\mathcal{O}$. Let $(x_0, y_0) \in \mathcal{O}$ be such that*

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

Then there is an open interval $I_0 \in \mathbb{R}$ and a real valued, continuously differentiable function ϕ defined on I_0 such that $x_0 \in I_0$, $\phi\left(x_0\right) = y_0$, $\left(x, \phi\left(x\right)\right) \in \mathcal{O}$ for all $x \in I_0$, and $W\left(x, \phi\left(x\right)\right) = 0$ for all $x \in I_0$.

Proof of Lemma 2.1. For $0 \leq j \leq 20$, define $p_j(x) = a_j(x + 10)$, and set

$$P_0(x, y) = \sum_{j=0}^{20} p_j(x) y^j = \sum_{j=0}^{20} a_j(x + 10) y^j.$$

Thus,

$$P_0\left(x, y^2\right) = P\left(x + 10, y\right). \tag{2.1}$$

To follow the arguments below the reader will want to use the explicit formulation of $P(x, y) \in \mathbb{Z}[x]$ prior to Lemma 2.1 to compute the exact values of $p_j(x)$. To simplify our notation and avoid confusion, we use $P_0\left(y\right)$ for $P_0\left(x, y\right)$ when we are viewing $P_0(x, y)$ as a polynomial in y. We calculate the discriminant $\Delta(x)$ of $P_0\left(y\right)$. After obtaining $\Delta(x)$, a polynomial in $\mathbb{Z}[x]$ of degree 304, we use a Sturm sequence to check that $\Delta(x)$ has no real roots. Also, $\Delta(0) < 0$, so it follows that $\Delta(x) < 0$ for all real x.

For each real x, the inequality $\Delta\left(x\right) \neq 0$ implies that $P_0\left(y\right)$ has no repeated roots. The polynomial $P_0(y)$ is monic, that is $p_{20}(x) = 1$. In particular, this means that for each real x, the degree of $P_0(y)$ is 20, and $P_0(y)$ must have an even number of real roots. We show next that $P_0(y)$ has at least one real root.

For a fixed x, if the roots of $P_0\left(y\right)$ are $\alpha_1, \ldots, \alpha_{20}$, then

$$\Delta\left(x\right) = \prod_{1 \leq i < j \leq 20} \left(\alpha_i - \alpha_j\right)^2, \tag{2.2}$$

where we have used that $P_0(y)$ is monic. For convenience, relabel the roots of $P_0\left(y\right)$ so that $\alpha_1, \ldots, \alpha_{r_1}$ are the real roots and $\beta_1, \overline{\beta_1}, \ldots, \beta_{r_2}, \overline{\beta_{r_2}}$ are the non-real roots.

Then

$$\begin{aligned}
\Delta(x) = &\left(\prod_{1\le j<k\le r_1} (\alpha_j - \alpha_k)^2 \right) \times \left(\prod_{j=1}^{r_1} \prod_{k=1}^{r_2} (\alpha_j - \beta_k)^2 \left(\alpha_j - \overline{\beta_k}\right)^2 \right) \\
&\times \left(\prod_{1\le j<k\le r_2} (\beta_j - \beta_k)^2 \left(\overline{\beta_j} - \overline{\beta_k}\right)^2 \left(\beta_j - \overline{\beta_k}\right)^2 \left(\overline{\beta_j} - \beta_k\right)^2 \right) \\
&\times \left(\prod_{j=1}^{r_2} \left(\beta_j - \overline{\beta_j}\right)^2 \right) \\
= &\left(\prod_{1\le j<k\le r_1} (\alpha_j - \alpha_k)^2 \right) \times \left(\prod_{j=1}^{r_1} \prod_{k=1}^{r_2} |\alpha_j - \beta_k|^4 \right) \\
&\times \left(\prod_{1\le j<k\le r_2} |\beta_j - \beta_k|^4 \left|\beta_j - \overline{\beta_k}\right|^4 \right) \times \left(\prod_{j=1}^{r_2} \left(\beta_j - \overline{\beta_j}\right)^2 \right) \\
= &\; C_1 \times C_2 \times C_3 \times (-1)^{r_2} 4^{r_2} \prod_{j=1}^{r_2} \left(\mathrm{Im}(\beta_j)\right)^2,
\end{aligned}$$

where C_1, C_2 and C_3 are positive. Since $\Delta(x) < 0$, we deduce that r_2 is odd. Also, $\deg P_0(y) = 20$ implies $r_1 + 2r_2 = 20$. Therefore, $r_1 > 0$, and $P_0(y)$ has a positive even number of real roots.

Using a Sturm sequence, we verify that $p_0(x)$ has exactly two distinct real roots. One checks that $p_0(x)$ is a polynomial in x^2 so that $p_0(x)$ has a positive root, which we call a and a negative root which will be $-a$. A computation gives $a = 1.6167\ldots$, accurate to the digits shown. We show that a has the properties stated in the lemma. Let J denote the interval $[-a, a]$. Using Sturm sequences, one can verify that for each $j \in \{1, 2, \ldots, 20\}$, the polynomial $p_j(x)$ has all of its real roots in the interval $[-1.5, 1.5] \subset J$.

Recalling (2.1), we see that to prove (a), we need only show that for any given $x_0 \notin J$, the real roots of $P_0(x_0, y)$ are all negative. A simple calculation shows that $p_j(\pm 2) > 0$ for all $j \in \{0, 1, \ldots, 20\}$. Since none of the $p_j(x)$ have real roots outside of J, we deduce that $p_j(x_0) > 0$ for each j. From Descartes' rule of signs, we obtain that $P_0(x_0, y)$ has no positive real roots. Since $P_0(x_0, 0) = p_0(x_0) \neq 0$, part (a) now follows.

We turn to the remaining parts of Lemma 2.1. For a given $x \in I$, we define $\rho(x)$ to be the largest real root of $P(x, y)$. We will need to show that such a root exists and is ≥ 0. From (2.1), we see that for $x \in J$, we want $(\rho(x + 10))^2$ to be a root of $P_0(y)$. Further, showing $P(x, y)$ has a root ≥ 0 for each $x \in I$ is equivalent to showing $P_0(y)$ has a root ≥ 0 for each $x \in J$.

Now, fix x_0 in the interior of J, so $x_0 \in (-a, a)$. We have already observed that $p_0(x)$ has no real roots other than $\pm a$. Since $p_0(0) = -1$, it follows that $p_0(x) < 0$ for all x in the interior of J. Hence, $p_0(x_0) < 0$. On the other hand, $p_0(x_0)$ is the product of all the roots of $P_0(x_0, y)$. Since the product of non-zero conjugate pairs is always positive, we deduce that $P_0(x_0, y)$ has an odd number of negative real roots. As shown earlier, $P_0(x_0, y)$ has a positive, even number of real roots, so we obtain that $P_0(x_0, y)$ must have an odd number of positive real roots, and hence at least one such root.

We now consider the case that $x_0 = \pm a$. As noted earlier, for each $j \in \{1, 2, \ldots, 20\}$, the polynomial $p_j(x)$ has its roots in the interval $[-1.5, 1.5]$ and $p_j(\pm 2) > 0$. Since $a \notin [-1.5, 1.5]$ and $x_0 = \pm a$, it follows that $p_j(x_0) > 0$ for each such j. From Descartes' rule of signs, we deduce that $P_0(x_0, y)/y$ has no positive real roots. Thus, $P_0(x_0, y)$ has 0 as its largest real root.

For each $x \in \mathbb{R}$, define

$$\psi(x) = \max\{y \in \mathbb{R} : P_0(y) = 0\}.$$

Since $P_0(y)$ has real roots for any given x, then $\psi(x)$ is well defined. Moreover, we have now seen that $\psi(x) > 0$ for all $x \in (-a, a)$, $\psi(\pm a) = 0$, and $\psi(x) < 0$ for all $x \notin J$. Parts (b) and (c) now follow by defining $\rho(x) = \sqrt{\psi(x - 10)}$ for each $x \in I$.

Next, we establish (d). To prove $\rho(x)$ is a continuously differentiable function on $(10-a, 10+a)$ and continuous on $[10-a, 10+a]$, it is sufficient to show that, given any $x_0 \in J$, including its endpoints, there exists an open interval I_0 containing x_0 such that $\psi(x)$ is a continuously differentiable function on I_0. Fix $x_0 \in J$, and let $y_0 = \psi(x_0)$. We make use of Lemma 2.2 with $W(x, y) = P_0(x, y)$. Since then $W(x, y)$ is a polynomial, both W_x and W_y are continuous on all of $\mathbb{R}^2$. The definition of y_0 implies $W(x_0, y_0) = 0$. Recall that we have shown that the polynomial $W(x_0, y) = P_0(x_0, y)$ in y has no repeated roots. It follows that $W_y(x_0, y_0) \neq 0$. From Lemma 2.2, there exists an open interval J_0 containing x_0 and a continuously differentiable function $\phi(x)$ defined on J_0 such that $\phi(x_0) = y_0$ and $P_0(x, \phi(x)) = 0$ for all $x \in J_0$. By the definition of $\psi(x)$, we know that $\phi(x) \leq \psi(x)$ for all $x \in J_0$. We need only show now that there exists an open interval $I_0 \subseteq J_0$ containing x_0 such that $\psi(x) = \phi(x)$ for all $x \in I_0$.

Assume that no such interval I_0 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 $\psi(x_n) > \phi(x_n)$ for all $n \geq 1$. Since $x_0 \in J = [-a, a] \subset [-2, 2]$ and $x_0 \in J_0$, we suppose further as we may that each $x_n \in [-2, 2] \cap J_0$. Define $y_n = \psi(x_n)$. In particular, $P_0(x_n, y_n) = 0$. 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 $x' \in [-2, 2]$ and $z \in \mathbb{C}$ satisfying $P_0(x', z) = 0$, we have $|z| \leq M$. Since each $p_j(x)$ is continuous on $[-2, 2]$ and $[-2, 2]$ is compact, there exists an absolute constant $A \geq 0$ such that $|p_j(x)| \leq A$ for all $j \in \{0, \ldots, 20\}$ and $x \in [-2, 2]$. Recall $p_{20}(x) = 1$. Since $x' \in [-2, 2]$ and $P_0(x', z) = 0$, we deduce

$$0 = \left| \sum_{j=0}^{20} p_j(x') z^j \right| \geq |z|^{20} - \sum_{j=0}^{19} |p_j(x')| \, |z|^j \geq |z|^{20} - A \sum_{j=0}^{19} |z|^j.$$

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

$$x^{20} - Ax^{19} - Ax^{18} - \cdots - Ax - A.$$

We deduce that $\{y_n\}_{n=1}^{\infty}$ is a sequence with $|y_n| \leq M$ for all n. Hence, the sequence $\{y_n\}_{n=1}^{\infty}$ has a convergent subsequence $\left\{y_{n_j}\right\}_{j=1}^{\infty}$. Let $L = \lim_{j\to\infty} y_{n_j}$. The continuity of $P_0\,(x, y)$ implies

$$P_0(x_0, L) = \lim_{j\to\infty} P_0\left(x_{n_j}, y_{n_j}\right) = 0.$$

Since

$$y_0 = \psi(x_0) = \max\{y \in \mathbb{R} : P_0(x_0, y) = 0\},$$

we deduce that $L \leq y_0$. Since $\phi(x)$ is continuous on J_0 and $\phi(x_{n_j}) \leq \psi(x_{n_j}) = y_{n_j}$ for all $j \geq 1$, we also have that

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

Thus, $L = y_0$. In particular,

$$\lim_{j\to\infty} \psi(x_{n_j}) = y_0 = \lim_{j\to\infty} \phi(x_{n_j}). \tag{2.3}$$

We show that this implies a contradiction.

Since $\Delta(x)$ is continuous on $[-2, 2]$ and $\Delta(x) < 0$ for all $x \in [-2, 2]$, $|\Delta(x)|$ obtains a minimum value δ on $[-2, 2]$ with $\delta > 0$. Recall that for each $x \in [-2, 2]$, the roots of $P_0(x, y)$ in $\mathbb{C}$ are all bounded in absolute value by M. From the definition of $\Delta(x)$, we obtain for every positive integer j that

$$\delta \leq \left|\Delta\left(x_{n_j}\right)\right| \leq (2M)^{2\left(\binom{20}{2}-1\right)} \left|\psi\left(x_{n_j}\right) - \phi\left(x_{n_j}\right)\right|^2.$$

For j sufficiently large, (2.3) implies that the right side above is less than the left side, giving the desired contradiction. This proves (d).

To establish (e), we first observe that the definition of $\psi(x)$ and (2.1) imply that if $x \in I$ and $y \in \mathbb{R}$ are such that $P(x, y) = 0$, then $|y| \leq \rho(x)$. Part (a) also implies if $P(x, y) = 0$ for some real numbers x and y, then $x \in I$. Now, consider real numbers x_0 and y_0 for which $P(x_0, y_0) < 0$. One checks that $P(0, 0) > 0$. Since $P(x, y)$ 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 $P(x, y) = 0$. We use again that for any $x \in I$, the number M is a bound on the absolute value of the roots of $P_0(x, y)$. We deduce from (2.1) that $\rho(x) \leq \sqrt{M}$ for all $x \in I$. If $x_0 \notin I = [10 - a, 10 + a]$ or if $x_0 \in I$ and $y_0 > \rho(x_0)$, 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 $x_0 \in I$ and $y_0 < -\rho(x_0)$, 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, we must have $x_0 \in I$ and $|y_0| \leq \rho(x_0)$. This establishes (e), completing the proof. □

As noted in the proof of Lemma 2.1, $a = 1.6167\ldots$. Thus, we have at least a good approximation for the left and right endpoints of $I = [10 - a, 10 + a]$. The proof did not give us much information as to the shape of the region $\mathcal{R}$, but as we show now, what we know is sufficient to give us something new.

Consider the line $y = \tan(\pi/36)\,x$ or equivalently the points $x + i\tan(\pi/36)x$ in the complex plane. A computation gives $\tan(\pi/36) > 2/23$. Thus, the line $y = (2/23)x$ lies below the line $y = \tan(\pi/36)x$ for $x > 0$. From $\rho(10 - a) = 0$ and $\rho(x)$ being continuous, we deduce that if $y = (2/23)x$ does not intersect the graph of $y = \rho(x)$, then $y = (2/23)x$ and, hence, $y = \tan(\pi/36)x$ lie above the region $\mathcal{R}$. By part (c) of Lemma 2.1, a point $(x, \rho(x))$ on the graph of $y = \rho(x)$ satisfies $P(x, \rho(x)) = 0$. Thus, if $y = (2/23)x$ intersects $y = \rho(x)$, then the polynomial $P(x, 2x/23)$ has a real root. Since the coefficients of $P(x, 2x/23)$ are rational, the Sturm sequence for this polynomial is easily computed and can be used to verify that $P(x, 2x/23)$ has no real roots. Thus, $y = \tan(\pi/36)x$ lies above the region $\mathcal{R}$.

Recall that we began this section with $f(x) \in \mathbb{Z}[x]$ having non-negative coefficients and satisfying $f(10)$ is prime. Under the assumption that $f(x)$ is reducible, we wrote $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, have positive degrees and have positive leading coefficients. We took $g(10) = 1$ and showed that either $g(x)$ has a root in common with one of $\Phi_3(x-10)$, $\Phi_4(x-10)$ and $\Phi_6(x-10)$ or $g(x)$ has a root $\beta \in \mathcal{R}$. In the latter case, since the coefficients of $f(x)$ are non-negative and the real numbers in $\mathcal{R}$ are positive, $\beta \notin \mathbb{R}$. Note that the point $(10.5, \sqrt{3}/2)$, corresponding to $10+\zeta_6$ in the complex plane, is also below the line $y = \tan(\pi/36)x$. Thus, we can deduce that either $g(x)$ has a root in common with one of $\Phi_3(x-10)$ and $\Phi_4(x-10)$ or $g(x)$ has a root $\beta = u + iv$ satisfying $0 < v < \tan(\pi/36)u$.

Based on the simple argument we had for Theorem 1.2 in Section 1, we have the following.

Lemma 2.3. *Let n be a positive integer. A complex number $\alpha = re^{i\theta}$ satisfying $r > 0$ and $0 < \theta < \pi/n$ cannot be a root of a non-zero polynomial which has degree $\leq n$ and has non-negative real coefficients.*

In the case above that $\beta = u + iv$ with $0 < v < \tan(\pi/36)u$, we see that $\beta = re^{i\theta}$ where $r > 0$ and $0 < \theta < \pi/36$. Recalling that β is necessarily a root of $f(x)$ which has non-negative coefficients, we obtain from Lemma 2.3 that $\deg f > 36$. Observing that $10 + \zeta_3 = 9.5 + (\sqrt{3}/2)i$ where

$$\frac{\sqrt{3}/2}{9.5} < \tan(\pi/34),$$

we can deduce further the following consequence of Lemma 2.1 and Lemma 2.3.

Corollary 2.4. *Let $f(x) \in \mathbb{Z}[x]$ have non-negative coefficients. Suppose that $f(10)$ is a prime and $f(x)$ is reducible. If the degree of $f(x)$ is ≤ 34, then $f(x)$ is divisible by $x^2 - 20x + 101$. Furthermore, if the degree of $f(x)$ is ≤ 36, then $f(x)$ is divisible by at least one of $x^2 - 20x + 101$ and $x^2 - 19x + 91$.*

The example

$$x^{35} + 3x^3 + 3x^2 + 8915724223128729685478774429437 84\,x$$
$$+ 1071112974878289533198669427384445 1$$

shows that the bound 34 in the first assertion of the corollary is best possible. This polynomial is prime at $x = 10$ and has the factor $x^2 - 19x + 91$. Later we will see that this example is optimal in another way: if $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree 35 with non-negative coefficients bounded above by

$$10711129748782895331986694273844450$$

and with $f(10)$ prime, then $f(x)$ cannot be divisible by $x^2 - 19x + 91$. Therefore, in this case, either $f(x)$ is irreducible or $f(x)$ is divisible by $x^2 - 20x + 101$.

We do not know if the bound 36 in Corollary 2.4 is best possible, and we suspect that it is not. The example

$$x^{39} + 52x^2 + 5987151062128356497901627122342281344 18\,x \\ + 1348312606061131031866295541636880002063$$

shows that 36 cannot be replaced by 39. This polynomial is prime at $x = 10$ and has the factor $x^2 - 21x + 111$.

Before leaving this section, we note that the idea above of using Sturm sequences to determine whether lines intersect $\mathcal{R}$ can be used to justify the earlier numerical estimate that $|\operatorname{Im}(z)| < 0.856$ for all $z \in \mathcal{R}$. Recall that the region $\mathcal{R}$ is symmetric about the real line since $P(x, y)$ is a polynomial in x and y^2. A Sturm sequence verifies that $P(x, 184/215)$ has no real roots. From Lemma 2.1, we deduce that the line $y = 184/215 = 0.8558\ldots$ lies above $\mathcal{R}$. Hence, in fact, we have the more precise bound $|\operatorname{Im}(z)| < 184/215$ for all $z \in \mathcal{R}$.

3. A first bound on the coefficients

In the notation of the previous section, we have seen that either $g(x)$ has at least one of the factors $\Phi_3(x-10)$, $\Phi_4(x-10)$ and $\Phi_6(x-10)$, or $g(x)$ has a root $\beta \in \mathcal{R}$. In this section, we show that in the latter case we can obtain a lower bound of $1.169 \cdot 10^{34}$ on the coefficients of $f(x)$. To do this, we make use of an idea introduced in [5] and formulated as below in [1] and [2]. As the latter two are not easily accessible, we give a detailed proof of our next lemma, noting its similarity to the proof in [5, Theorem 5].

Lemma 3.1. *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 $a_j > B a_n$.

Proof. Observe that $\pi/\theta > 2$ implies there is an integer in $\big(\pi/(2\theta), \pi/\theta\big)$. Fix an arbitrary integer $k \in \big(\pi/(2\theta), \pi/\theta\big)$. It suffices to show that there is a $j \in$

$\{0, 1, \ldots, n-1\}$ such that

$$a_j > B_k a_n, \quad \text{where } B_k = \frac{r^k(r-1)}{1+\cot(\pi - k\theta)}.$$

Assume $a_j \leq B_k a_n$ for all $j \in \{0, 1, \ldots, n-1\}$. Set

$$\gamma = \frac{a_n}{1+\cot(\pi - k\theta)} \quad \text{and} \quad k' = \left\lfloor \frac{\pi}{2\theta} \right\rfloor.$$

Then $k' < k$. Also,

$$j\theta \in (0, \pi/2] \quad \text{for } j \in \{1, 2, \ldots, k'\}$$

and

$$j\theta \in (\pi/2, \pi) \quad \text{for } j \in \{k'+1, k'+2, \ldots, k\}.$$

Since

$$\begin{aligned} \alpha^{-j} = r^{-j} e^{-ij\theta} &= r^{-j} \left(\cos(-j\theta) + i \sin(-j\theta)\right) \\ &= r^{-j} \left(\cos(j\theta) - i \sin(j\theta)\right), \end{aligned}$$

we can conclude that

$$\operatorname{Re}(\alpha^{-j}) \geq 0 \quad \text{for } j \in \{1, 2, \ldots, k'\}, \tag{3.1}$$

$$\operatorname{Re}(\alpha^{-j}) < 0 \quad \text{for } j \in \{k'+1, k'+2, \ldots, k\} \tag{3.2}$$

and

$$\operatorname{Im}(\alpha^{-j}) < 0 \quad \text{for } j \in \{1, 2, \ldots, k\}. \tag{3.3}$$

Since

$$0 < \pi - k\theta \leq \pi - j\theta < \frac{\pi}{2} \quad \text{for } j \in \{k'+1, k'+2, \ldots, k\},$$

we obtain

$$0 < \tan(\pi - k\theta) \leq \tan(\pi - j\theta) \quad \text{for } j \in \{k'+1, k'+2, \ldots, k\}.$$

Now, we derive an inequality relating the imaginary and real parts of α^{-j}. For $j \in \{k'+1, k'+2, \ldots, k\}$, we have

$$\begin{aligned} \left|\operatorname{Im}(\alpha^{-j})\right| &= r^{-j} \sin(j\theta) = r^{-j} \sin(\pi - j\theta) \\ &= r^{-j} \tan(\pi - j\theta) \cos(\pi - j\theta) \\ &= \tan(\pi - j\theta) \left|\operatorname{Re}(\alpha^{-j})\right| \\ &\geq \tan(\pi - k\theta) \left|\operatorname{Re}(\alpha^{-j})\right|. \end{aligned} \tag{3.4}$$

Motivated by the approach in [8, b. 2, VIII, 128], we consider

$$\left|\frac{f(\alpha)}{\alpha^n}\right| = \left|a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k}}{\alpha^k} + \sum_{j=k+1}^{n} \frac{a_{n-j}}{\alpha^j}\right|,$$

where, in the case $k > n$, we interpret a_{n-j} to be zero for all $j > n$. We consider two possible cases.

Case 1: $\left|\mathrm{Re}\left(\dfrac{a_{n-k'-1}}{\alpha^{k'+1}} + \cdots + \dfrac{a_{n-k}}{\alpha^k}\right)\right| \le a_n - \gamma.$

In this case, we use that

$$\begin{aligned}
\left|\frac{f(\alpha)}{\alpha^n}\right| &\ge \left|a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k}}{\alpha^k}\right| - \sum_{j=k+1}^{n} \left|\frac{a_{n-j}}{\alpha^j}\right| \\
&\ge \left|a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k}}{\alpha^k}\right| - \sum_{j=k+1}^{n} \frac{a_n B_k}{r^j} \\
&> \left|\mathrm{Re}\left(a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k}}{\alpha^k}\right)\right| - \sum_{j=k+1}^{\infty} \frac{a_n B_k}{r^j} \\
&\ge \left|\mathrm{Re}\left(a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k'}}{\alpha^{k'}}\right)\right| \\
&\qquad - \left|\mathrm{Re}\left(\frac{a_{n-k'-1}}{\alpha^{k'+1}} + \cdots + \frac{a_{n-k}}{\alpha^k}\right)\right| - \sum_{j=k+1}^{\infty} \frac{a_n B_k}{r^j}.
\end{aligned}$$

From (3.1), we have

$$\left|\mathrm{Re}\left(a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k'}}{\alpha^{k'}}\right)\right| = \mathrm{Re}\left(a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k'}}{\alpha^{k'}}\right) \ge a_n.$$

Combining this with the condition of the case we are considering and summing the geometric series $\sum_{j=k+1}^{\infty} 1/r^j$, we deduce

$$\left|\frac{f(\alpha)}{\alpha^n}\right| > a_n - (a_n - \gamma) - \frac{a_n B_k}{r^k(r-1)} = \gamma - \frac{a_n B_k}{r^k(r-1)} = 0.$$

Case 2: $\left|\mathrm{Re}\left(\dfrac{a_{n-k'-1}}{\alpha^{k'+1}} + \cdots + \dfrac{a_{n-k}}{\alpha^k}\right)\right| > a_n - \gamma.$

In this case, we use that

$$\begin{aligned}
\left|\frac{f(\alpha)}{\alpha^n}\right| &\ge \left|a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k}}{\alpha^k}\right| - \sum_{j=k+1}^{n} \left|\frac{a_{n-j}}{\alpha^j}\right| \\
&\ge \left|a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k}}{\alpha^k}\right| - \sum_{j=k+1}^{n} \frac{a_n B_k}{r^j} \\
&> \left|a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k}}{\alpha^k}\right| - \sum_{j=k+1}^{\infty} \frac{a_n B_k}{r^j} \\
&\ge \left|\mathrm{Im}\left(a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k}}{\alpha^k}\right)\right| - \sum_{j=k+1}^{\infty} \frac{a_n B_k}{r^j}.
\end{aligned}$$

As a consequence of (3.2), (3.3) and (3.4), we have

$$\begin{aligned}
&\left|\mathrm{Im}\left(a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k}}{\alpha^k}\right)\right| \\
&\qquad = \left|\mathrm{Im}\left(a_n + \frac{a_{n-1}}{\alpha} + \cdots + \frac{a_{n-k'}}{\alpha^{k'}}\right)\right| + \left|\mathrm{Im}\left(\frac{a_{n-k'-1}}{\alpha^{k'+1}} + \cdots + \frac{a_{n-k}}{\alpha^k}\right)\right| \\
&\qquad \geq \left|\mathrm{Im}\left(\frac{a_{n-k'-1}}{\alpha^{k'+1}} + \cdots + \frac{a_{n-k}}{\alpha^k}\right)\right| \\
&\qquad \geq \tan(\pi - k\theta)\left|\mathrm{Re}\left(\frac{a_{n-k'-1}}{\alpha^{k'+1}} + \cdots + \frac{a_{n-k}}{\alpha^k}\right)\right|.
\end{aligned}$$

Note that

$$a_n - \gamma = a_n - \frac{a_n}{1 + \cot(\pi - k\theta)} = \frac{a_n \cot(\pi - k\theta)}{1 + \cot(\pi - k\theta)}.$$

The condition of the current case under consideration now implies

$$\begin{aligned}
\left|\frac{f(\alpha)}{\alpha^n}\right| &> \tan(\pi - k\theta)(a_n - \gamma) - \sum_{j=k+1}^{\infty} \frac{a_n B_k}{r^j} \\
&= \tan(\pi - k\theta)\left(\frac{a_n \cot(\pi - k\theta)}{1 + \cot(\pi - k\theta)}\right) - \frac{a_n B_k}{r^k(r-1)} \\
&= \gamma - \frac{a_n B_k}{r^k(r-1)} = 0.
\end{aligned}$$

Therefore, in both Case 1 and Case 2, we conclude that $\left|\frac{f(\alpha)}{\alpha^n}\right| > 0$, contradicting that α is a root of $f(x)$. As a consequence, our assumption was incorrect so that there exists a $j \in \{0, 1, \ldots, n-1\}$ for which $a_j > B_k a_n$, completing the proof. $\square$

We explain how we make use of Lemma 3.1. Our goal here is to show the following.

Corollary 3.2. *Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ be such that $f(10)$ is prime. If*

$$0 \leq a_j \leq (1.169 \cdot 10^{34})\, a_n \qquad \text{for } 0 \leq j \leq n-1,$$

then either $f(x)$ is irreducible or $f(x)$ is divisible by at least one of $x^2 - 20x + 101$, $x^2 - 19x + 91$ and $x^2 - 21x + 111$.

Let θ and θ' be real numbers satisfying $0 \leq \theta < \theta' \leq \tan^{-1}(2/23)$. We consider the set of points $\mathcal{R}(\theta, \theta')$ in $\mathcal{R}$ that lie 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. More precisely, we define

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

Recall that we are interested in the case that $f(x)$ has a factor $g(x)$ with a root $\beta \in \mathcal{R}$. As we have seen, we may take $\beta = x_0 + iy_0$ for some $(x_0, y_0) \in \mathcal{R}$ with $y_0 > 0$. Also, as shown after the proof of Lemma 2.1, the region $\mathcal{R}$ is below the line

$y = (2/23)x$. To make use of Lemma 3.1, we will specify θ_ℓ, where $\ell \in \{0, 1, \dots, 221\}$ and where

$$0 = \theta_0 < \theta_1 < \cdots < \theta_{220} < \theta_{221} = \tan^{-1}(2/23).$$

Then

$$(x_0, y_0) \in \bigcup_{\ell=0}^{220} \mathcal{R}(\theta_\ell, \theta_{\ell+1}).$$

The idea is then to use Lemma 3.1 to find a bound $B'(\theta_\ell, \theta_{\ell+1})$ so that the conclusion $a_j > B'(\theta_\ell, \theta_{\ell+1})\, a_n$ for some $j \in \{0, 1, \dots, n-1\}$ holds if $(x_0, y_0) \in \mathcal{R}(\theta_\ell, \theta_{\ell+1})$. Since $(x_0, y_0) \in \mathcal{R}(\theta_\ell, \theta_{\ell+1})$ for some $\ell \in \{0, 1, \dots, 220\}$, we can then deduce that some coefficient of $f(x)$ exceeds

$$\min_{0 \le \ell \le 220} \{B'(\theta_\ell, \theta_{\ell+1})\} \cdot a_n. \tag{3.5}$$

We will choose the θ_ℓ in such a way that each $B'(\theta_\ell, \theta_{\ell+1}) > 1.169 \cdot 10^{34}$. Then we can deduce that some coefficient of $f(x)$ exceeds $1.169 \cdot 10^{34} a_n$.

As a simple example, consider

$$k = \left\lfloor \frac{25\pi}{26\theta} \right\rfloor \quad \text{where} \quad 0 \le \theta \le \tan^{-1}\left(\frac{4}{49}\right).$$

Observe that $k \in (\pi/(2\theta), \pi/\theta)$ since $k\theta \le 25\pi/26 < \pi$ and

$$k\theta > \left(\frac{25\pi}{26\theta} - 1\right)\theta \ge \frac{25\pi}{26} - \theta \ge \frac{25\pi}{26} - \tan^{-1}\left(\frac{4}{49}\right) > \frac{\pi}{2}.$$

Also,

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

which implies

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

From the definition of k and the range of θ, we see that

$$k = \left\lfloor \frac{25\pi}{26\theta} \right\rfloor \ge \left\lfloor \frac{25\pi}{26} \div \tan^{-1}\left(\frac{4}{49}\right) \right\rfloor = 37.$$

Recall that each $z \in \mathcal{R}$ satisfies $\mathrm{Re}(z) \ge 8.383$. Hence, each $z = re^{i\theta} \in \mathcal{R}$ satisfies $r = |z| \ge 8.383$. For such z, we deduce that

$$\frac{r^k(r-1)}{1 + \cot(\pi - k\theta)} \ge \frac{8.383^{37}(8.383 - 1)}{1 + \cot(\pi/26)} > 1.17 \cdot 10^{34}.$$

From Lemma 3.1, with $\theta_0 = 0$ and $\theta_1 = \tan^{-1}(4/49)$, we see that we can take

$$B'(\theta_0, \theta_1) = B'(0, \tan^{-1}(4/49)) = 1.17 \cdot 10^{34}. \tag{3.6}$$

There is a bit of freedom on how we choose the values of θ_ℓ, but we give some explanation as to our choice of θ_ℓ. To help with using Lemma 3.1, we will want to know where the line $y = (\tan\theta_\ell)\,x$ intersects $\mathcal{R}$. Since the boundary of $\mathcal{R}$ consists of points (x, y) where $P(x, y) = 0$, we would like to determine the real numbers x satisfying $P(x, (\tan\theta_\ell)\,x) = 0$. The polynomial $P(x, (\tan\theta_\ell)\,x)$ has degree 40, and we will have to settle for approximations to these real roots. What we want to avoid is basing our results on finding approximations to the real roots of a polynomial whose coefficients themselves are only approximations. To do this, we set $r_\ell = \tan\theta_\ell$ where r_ℓ is a specific rational number, we find a close lower bound rational approximation x_ℓ to the minimum real root of the polynomial $P(x, r_\ell\,x) = 0$, and then we use a Sturm sequence to verify that $P(x, r_\ell\,x)$ has no roots in $(-\infty, x_\ell]$. As both r_ℓ and x_ℓ are rational numbers, the latter verification can be done with exact arithmetic. Thus, we can be assured that x_ℓ is a lower bound for the minimal root of $P(x, (\tan\theta_\ell)\,x) = 0$.

Our precise values for $r_\ell = \tan\theta_\ell$ are as follows.

$$
\begin{gathered}
r_0 = 0,\ r_1 = 4/49,\ r_2 = 76/897,\ r_3 = 297/3493,\ r_4 = 61/716,\\
r_5 = 47/551,\ r_6 = 7/82,\ r_7 = 67357/788600,\ r_8 = 13476627/157720000,\\
r_{8+j} = r_8 + (j/100000) \ \text{ for } j \in \{1, 2, \dots, 8\},\\
r_{16+j} = r_{16} + (j/250000) \ \text{ for } j \in \{1, 2, \dots, 10\},\\
r_{26+j} = r_{26} + (j/500000) \ \text{ for } j \in \{1, 2, \dots, 10\},\\
r_{36+j} = r_{36} + (j/1000000) \ \text{ for } j \in \{1, 2, \dots, 20\},\\
r_{56+j} = r_{56} + (j/2500000) \ \text{ for } j \in \{1, 2, \dots, 120\},\\
r_{176+j} = r_{176} + (j/1000000) \ \text{ for } j \in \{1, 2, \dots, 31\},\\
r_{207+j} = r_{207} + (j/250000) \ \text{ for } j \in \{1, 2, \dots, 8\},\\
r_{216} = 338/3943,\ r_{217} = 122/1423,\ r_{218} = 65/758,\\
r_{219} = 38/443,\ r_{220} = 23/268 \ \text{ and } \ r_{221} = 2/23.
\end{gathered}
$$

We give a brief reason for the apparent small differences $r_{\ell+1} - r_\ell$ for ℓ in certain ranges above. At and around $\theta = 0.085424$, the left-most point (x, y) on the line $y = \tan(\theta)\,x$ and $\mathcal{R}$ satisfies $x + iy = re^{i\theta}$ where r is slightly greater than 9. One checks that the value of the maximum given in Lemma 3.1 is $1.169258\ldots \cdot 10^{34}$. This means that we cannot obtain a better lower bound than $1.169258\ldots \cdot 10^{34}$ for $B'(\theta_\ell, \theta_{\ell+1})$ if $0.085424 \in [\theta_\ell, \theta_{\ell+1})$. To show $B'(\theta_\ell, \theta_{\ell+1}) > 1.169 \cdot 10^{34}$ for θ_ℓ near 0.085424, we consequently need $\theta_{\ell+1} - \theta_\ell$ to be rather small. This then is what motivates the small differences $r_{\ell+1} - r_\ell$ in some choices of ℓ above.

To finish the proof of Corollary 3.2, we fix $\ell \in \{1, 2, \dots, 220\}$ and explain how we obtained a value for $B'(\theta_\ell, \theta_{\ell+1})$. Recall that we have already explained how to obtain a verifiable lower bound x_ℓ for the first coordinate of the left-most point (x, y) on the intersection of the line $y = \tan(\theta_\ell)\,x$ and $\mathcal{R}$. Consider

$$\alpha = x' + iy' = re^{i\theta} \qquad \text{where } (x', y') \in \mathcal{R}(\theta_\ell, \theta_{\ell+1}). \tag{3.7}$$

We claim that both $x_\ell \le x'$ and $\tan(\theta_\ell)\,x_\ell \le y'$. Assume $x' < x_\ell$. Let (x'', y'') denote the point where $y = (\tan\theta)\,x$ intersects $\mathcal{R}$ with x'' minimal. Then (x'', y'') is on the boundary of $\mathcal{R}$ and, hence, $y'' = \rho(x'')$. Also, $x'' \le x' < x_\ell$ and, by Lemma 2.1 (a), $x'' \ge 10 - a$. By Lemma 2.1, the function

$$\rho_0(x) = \rho(x) - r_\ell\, x$$

is a continuous function such that $\rho_0(10-a) < 0$. On the other hand, since (x'', y'') is in $\mathcal{R}(\theta_\ell, \theta_{\ell+1})$, it lies above $y = \tan(\theta_\ell)\, x$. Thus,

$$\rho(x'') = y'' = \tan(\theta)\, x'' \ge \tan(\theta_\ell)\, x'' = r_\ell\, x''$$

so that $\rho_0(x'') \ge 0$. By the Intermediate Value Theorem, there is a $u \in [10-a, x'']$ such that $\rho_0(u) = 0$. Thus, $\rho(u) = r_\ell\, u$, which implies $P\big(u, r_\ell\, u\big) = 0$. Since

$$u \le x'' \le x' < x_\ell,$$

we obtain a contradiction to the definition of x_ℓ. Thus, our assumption is wrong, and $x_\ell \le x'$. To see that $\tan(\theta_\ell)\, x_\ell \le y'$, we simply use now that

$$y' = (\tan\theta)\, x' \ge (\tan\theta_\ell)\, x' \ge (\tan\theta_\ell)\, x_\ell.$$

Letting R_ℓ denote a lower bound approximation of $\sqrt{1 + r_\ell^2}\, x_\ell$, we see that

$$r = \sqrt{(x')^2 + (y')^2} \ge \sqrt{1 + \tan^2\theta_\ell}\, x_\ell \ge R_\ell.$$

The above holds for any $\alpha = re^{i\theta}$ as in (3.7).

For a fixed $\ell \in \{1, 2, \dots, 220\}$, we let k_1 be the largest integer $< \pi/\theta_{\ell+1}$. Set $k_2 = k_1 - 1$. We verified that

$$\frac{\pi}{2\theta_\ell} + 10^{-10} \le k_2 \quad \text{and} \quad k_1 \le \frac{\pi}{\theta_{\ell+1}} - 10^{-10}$$

based on 60 digit approximations to $\pi/(2\theta_\ell)$ and $\pi/\theta_{\ell+1}$. It follows that for any $\theta \in [\theta_\ell, \theta_{\ell+1}]$, we have

$$\frac{\pi}{2\theta} \le \frac{\pi}{2\theta_\ell} < k_2 < k_1 < \frac{\pi}{\theta_{\ell+1}} \le \frac{\pi}{\theta},$$

so both k_1 and k_2 are in the interval $\big(\pi/(2\theta), \pi/\theta\big)$. Further, for such θ, we computed $c(k_1)$ and $c(k_2)$ such that

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

Lemma 3.1 now implies that we may take

$$B'(\theta_\ell, \theta_{\ell+1}) = \max\left\{ \frac{R_\ell^{k_1}(R_\ell - 1)}{1 + c(k_1)}, \frac{R_\ell^{k_2}(R_\ell - 1)}{1 + c(k_2)} \right\}.$$

Recall we are considering the case that $g(x)$ has a root $\beta = x_0 + iy_0$ with $(x_0, y_0) \in \mathcal{R}$, which occurs whenever $f(x)$ is reducible and not divisible by one of $\Phi_3(x-10)$, $\Phi_4(x-10)$ and $\Phi_6(x-10)$. Combining the estimates we obtained for $B'(\theta_\ell, \theta_{\ell+1})$ above with (3.6), we obtained the lower bound $1.169 \cdot 10^{34}\, a_n$ on at least one coefficient of $f(x)$ from (3.5). The corollary follows.

4. Bounds based on recursive relations

We are now ready to formulate another approach that bounds the coefficients of $f(x)$ in the case that we know $f(x)$ has a given quadratic factor. This is motivated by Corollary 3.2. Our goal is to find good lower bounds on the maximum coefficient of $f(x)$ if $f(x)$ is divisible by one of $x^2-20x+101$, $x^2-19x+91$ and $x^2-21x+111$. The bound we obtain will depend on the quadratic considered.

Fix positive integers A and B. Let $b_0, \dots, b_s$ be integers such that

$$(b_0x^s + b_1x^{s-1} + \cdots + b_{s-1}x + b_s)(x^2 - Ax + B) \tag{4.1}$$

is a polynomial of degree $s+2$ with non-negative coefficients. In the setting of this paper, we will want A and B chosen so that the quadratic on the right is one of $x^2-20x+101$, $x^2-19x+91$ and $x^2-21x+111$. With $f(x) = g(x)h(x)$ as before and $g(x)$ being the quadratic, we view the polynomial factor on the left in (4.1) as $h(x)$ and further $n = \deg f = s+2$. 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 (4.1) is expanded, we obtain $f(x)$ so that the resulting coefficients are ≥ 0.

For convenience, we define $b_j = 0$ for all $j < 0$ and all $j > s$. Since the coefficients of $f(x)$ are ≥ 0, we deduce that

$$b_0 \geq 1 \quad \text{and} \quad b_j \geq Ab_{j-1} - Bb_{j-2} \ \text{ for all } j \in \mathbb{Z}. \tag{4.2}$$

In particular, $b_1 \geq Ab_0$. For each integer j, define

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

so the β_j satisfy a recursive relation for $j \geq 0$. In particular, $\beta_1 = A$ and $\beta_2 = A^2 - B$. Of some significance to our problem, the values of β_j may vary in sign and will do so for the choices of A and B that interest us. Let J be a positive integer for which

$$\beta_j \geq 0 \quad \text{for } j \leq J. \tag{4.3}$$

Then for $1 \leq j \leq J+1$, we have

$$\begin{aligned} b_j &\geq Ab_{j-1} - Bb_{j-2} \geq A\big(Ab_{j-2} - Bb_{j-3}\big) - Bb_{j-2} \\ &\geq \beta_2 b_{j-2} - B\beta_1 b_{j-3} \geq \beta_2\big(Ab_{j-3} - Bb_{j-4}\big) - B\beta_1 b_{j-3} \\ &\geq \beta_3 b_{j-3} - B\beta_2 b_{j-4} \geq \beta_3\big(Ab_{j-4} - Bb_{j-5}\big) - B\beta_2 b_{j-4} \\ &\geq \beta_4 b_{j-4} - B\beta_3 b_{j-5} \geq \cdots \geq \beta_{j-1} b_1 - B\beta_{j-2} b_0 \geq \beta_j b_0. \end{aligned} \tag{4.4}$$

We deduce the inequality

$$b_j \geq \beta_j b_0 \quad \text{for all integers } j \leq J+1. \tag{4.5}$$

Let

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

Since $b_j = 0$ for $j > s$, we have the trivial bound $L \leq 0$. We can obtain rather precise information about U and L for specific A and B by making use of (4.5), and we do so now. Below is a table indicating the A and B of interest to us. The value of J we used in (4.5) corresponds to the least J for which $\beta_{J+1} < 0$. Thus, (4.3) holds. From (4.5), we obtain $\beta_J b_0$ as a lower bound for U. In the table, the value of β_J is given.

A	B	J	β_J
20	101	30	604861792550624708513466396499
19	91	33	117704722514097750900952684327901
21	111	37	12146960414965144431227887762494414381

Table 1

Recall that we are interested in considering A and B such that $f(x)$ is divisible by $x^2 - Ax + B$. We consider an $f(x)$ with non-negative coefficients as before but with the largest coefficient as small as possible. Let $M = M(A, B)$ denote the maximum coefficient for such an $f(x)$. In the way of an important example, we recall the polynomial given after the statement of Theorem 1.3 in the introduction. It is divisible by $x^2 - 20x + 101$, so we can conclude

$$M(20, 101) \leq 49598666989151226098104244512919. \tag{4.6}$$

Let $k \geq 0$ and $\ell \geq 1$ be integers. We take a weighted average of ℓ consecutive coefficients of $f(x)$. More precisely, define $\tilde{a}_j = b_j - Ab_{j-1} + Bb_{j-2}$ for all integers j so that $\tilde{a}_j$ is the coefficient of x^{s+2-j} in $f(x)$ for $0 \leq j \leq s+2$. Suppose $b_k \neq 0$, and define t_j by

$$b_{k+j} = t_j b_k \quad \text{for } j \in \mathbb{Z}. \tag{4.7}$$

Thus,

$$\tilde{a}_{k+j+2} = (t_{j+2} - At_{j+1} + Bt_j)b_k \quad \text{for } j \in \mathbb{Z}.$$

We consider the weighted average of $\tilde{a}_j$ given by

$$W(k, \ell) = \sum_{j=0}^{\ell-1} \mu_j \tilde{a}_{k+j+2}, \quad \text{where } 0 \leq \mu_j \leq 1 \text{ for } 0 \leq j \leq \ell - 1 \text{ and } \sum_{j=0}^{\ell-1} \mu_j = 1.$$

Observe that $W(k,\ell) = W_0(k,\ell)b_k$, where

$$W_0(k,\ell) = \sum_{j=0}^{\ell-1} \mu_j\big(t_{j+2} - At_{j+1} + Bt_j\big)$$
$$= \mu_0 Bt_0 + \big(-\mu_0 A + \mu_1 B\big)t_1 + \sum_{j=2}^{\ell-1} \big(\mu_{j-2} - \mu_{j-1}A + \mu_j B\big)t_j$$
$$+ \big(\mu_{\ell-2} - \mu_{\ell-1}A\big)t_\ell + \mu_{\ell-1}t_{\ell+1}.$$

The idea is to choose the μ_j so that the coefficients of $t_1, t_2, \dots, t_{\ell-1}$ are all zero above. In other words, we want to choose the μ_j so that the matrix equation

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 \\ -A & B & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 1 & -A & B & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & -A & B & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -A & B & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & B & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & -A & B & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & -A & B & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & -A & B \end{pmatrix} \begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \\ \mu_3 \\ \mu_4 \\ \vdots \\ \mu_{\ell-4} \\ \mu_{\ell-3} \\ \mu_{\ell-2} \\ \mu_{\ell-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

holds. Note that the above corresponds to a system of ℓ equations in the ℓ unknowns μ_j where $0 \le j \le \ell - 1$. The system of equations depends only on A, B and ℓ, and not on k. The first equation in this system guarantees that the condition $\sum_{j=0}^{\ell-1} \mu_j = 1$ holds. It is not the case that the solution of this system necessarily satisfies $0 \le \mu_j \le 1$ for every $j \in \{0, 1, \dots, \ell - 1\}$. There is no reason to concern ourselves with this or whether even a solution exists; we will specify A, B and ℓ shortly and be able to explicitly solve the system of equations and obtain the information we need.

Let the μ_j be a fixed solution to the above system of equations. Since A and B are integers, we deduce that there are computable rational numbers a, b and c, independent of k, for which

$$W_0(k,\ell) = at_0 + bt_\ell + ct_{\ell+1}.$$

These a, b and c will be positive for our choices of A, B and ℓ. Recall that the definition of t_j in (4.7) depends on k. We consider first the case where k is chosen so that $b_k = U$. Since the maximum coefficient of $f(x)$ is M, we deduce from (4.7) that

$$\begin{aligned} M \ge W(k,\ell) = W_0(k,\ell)b_k &= at_0 b_k + bt_\ell b_k + ct_{\ell+1} b_k \\ &= ab_k + bb_{k+\ell} + cb_{k+\ell+1} \ge aU + bL + cL. \end{aligned} \tag{4.8}$$

Next, consider the case where k is chosen so that $b_k = L$. Since each coefficient of $f(x)$ is ≥ 0, we deduce similarly that

$$0 \leq W(k,\ell) = W_0(k,\ell)b_k = ab_k + bb_{k+\ell} + cb_{k+\ell+1} \leq aL + bU + cU. \tag{4.9}$$

Multiplying through (4.8) by a and through (4.9) by $-(b+c)$ and adding, we obtain

$$aM \geq (a^2 - (b+c)^2)U. \tag{4.10}$$

Multiplying through (4.8) by $b+c$ and through (4.9) by $-a$ and adding, we obtain

$$(b+c)M \geq (a^2 - (b+c)^2)(-L), \tag{4.11}$$

where we have written the above with $-L$ to emphasize that $L \leq 0$.

Now, we are ready to apply the above information to the cases that are of interest to us. For $A = 20$ and $B = 101$, we take $\ell = 31$. We calculate the values of $\mu_0, \mu_1, \ldots, \mu_{30}$ from the system of equations above and verify directly that each μ_j is in $[0,1]$. We solve for a, b and c and find

$$a = \frac{136132740448623470709137757482287529203605725945483260999653101}{1660155371324676472062655579052362650636003496484865073642560},$$

$$b = \frac{3433386491427782823015669 51}{10172520657626694069011369969683594673014727306892555 5983},$$

and

$$c = \frac{604861792550624708513466396499}{1660155371324676472062655579052362650636003496484865073642560}.$$

The value of $a^2 - (b+c)^2$ is positive. From our upper bound for $M = M(20,101)$ in (4.6) and from (4.10), we deduce

$$U \leq \frac{a}{a^2 - (b+c)^2} \cdot M(20,101) \leq 604861792550624708513466396499.039779\ldots.$$

Observe that the lower bound $\beta_J b_0$ for U given by Table 1 now implies $b_0 = 1$ (i.e., the polynomial $h(x)$ is monic) and

$$U = U(20,101) = 604861792550624708513466396499.$$

From (4.11), we similarly obtain

$$-L \leq \frac{b+c}{a^2 - (b+c)^2} \cdot M(20,101) \leq 0.02758\ldots.$$

Since $L \leq 0$, we deduce $L = 0$.

For $A = 19$ and $B = 91$, we want similar information. To get an estimate for $M(19,91)$, we make use of the following example of a polynomial $f(x)$ with non-negative coefficients, divisible by $x^2 - 19x + 91$, and satisfying $f(10)$ is prime:

$$\begin{aligned} x^{68} &+ 1009277144826970719448830127272551\,x^{34} \\ &+ 8592444743529135815769545955936773\,x^{33} \\ &+ \cdots + 8592444743529135815769545955936773\,x^{5} \\ &+ 8592444743529135815769545955936774\,x^{4} \\ &+ 8592444743529135815769545955936773\,x^{3} \\ &+ 8592444743529135815769545955936611\,x^{2} \\ &+ 8592444743529135815769545955936450\,x \\ &+ 7583167598702165096320715828674049, \end{aligned}$$

where the missing terms of degrees $6, 7, \ldots, 32$ each have the same coefficient as the coefficient for the terms of degrees 3, 5 and 33. The coefficient of x^4 is the largest coefficient above, so we can conclude

$$M(19, 91) \leq 8592444743529135815769545955936774. \tag{4.12}$$

We take $\ell = 34$ in this case. Following an analogous analysis to the case $A = 20$ and $B = 101$ above, we obtain here that

$$U = U(19, 91) = 117704722514097750900952684327901$$

and $L = 0$ in this case.

We do not need to do as much in the case $A = 21$ and $B = 111$. We take $\ell = 38$, check that the μ_j are in $[0, 1]$ and compute a, b and c as before. Table 1 gives us a lower bound for $U = U(21, 111)$. Using (4.10), we see that

$$M = M(21, 111) \geq \frac{a^2 - (b+c)^2}{a} U \geq 1.10537 \cdot 10^{39}.$$

This implies that any polynomial $f(x)$ with non-negative coefficients divisible by $x^2 - 21x + 111$ must have a coefficient as large as $1.10537 \cdot 10^{39}$. We easily deduce as a consequence of Corollary 3.2 that if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is such that $f(10)$ is prime and

$$0 \leq a_j \leq 1.169 \cdot 10^{34} \quad \text{for } 0 \leq j \leq n,$$

then either $f(x)$ is irreducible or $f(x)$ is divisible by either $x^2 - 20x + 101$ or $x^2 - 19x + 91$.

Along similar lines, we can use (4.10) to obtain a lower bound for $M = M(A, B)$ in the case that $f(x)$ is divisible by $x^2 - Ax + B$ where $(A, B) \in \{(20, 101), (19, 91)\}$ by making use of the precise values just obtained for $U(A, B)$. We deduce that

$$M(20, 101) \geq 49598666989151226098104244512916$$

and

$$M(19, 91) \geq 8592444743529135815769545955936771.$$

To clarify, we rounded up in these estimates since M and U being integers in (4.10) implies that

$$M \geq \left\lceil \frac{a^2 - (b+c)^2}{a} \cdot U \right\rceil.$$

Note that these lower bounds for $M(A, B)$ are each 3 less than the upper bounds obtained in (4.6) and (4.12). Combining the above information with Corollary 3.2, we see that to complete a proof of Theorem 1.4 it suffices to show that the upper bounds obtained for $M(A, B)$ are the actual values of $M(A, B)$.

5. Finishing touches to Theorem 1.4

We are interested in the case that $f(x) = g(x)h(x)$ where $g(x) = x^2 - Ax + B$ with $(A, B) \in \{(20, 101), (19, 91)\}$ and where $f(x)$ has maximal coefficient equal to $M(A, B)$. In the previous section, we established that $h(x)$ must be monic, that all of its coefficients must be non-negative (i.e., $L = 0$) and that its largest coefficient corresponds to the value of β_J indicated in Table 1. To finish the proof of Theorem 1.4, one checks that it suffices to show $M(A, B) = (1 - A + B) \cdot \beta_J + 1$ for each $(A, B) \in \{(20, 101), (19, 91)\}$. We fix $(A, B) \in \{(20, 101), (19, 91)\}$ and assume to the contrary that

$$M(A, B) \leq (1 - A + B) \cdot \beta_J. \tag{5.1}$$

We want then to obtain a contradiction for each $(A, B) \in \{(20, 101), (19, 91)\}$.

To obtain a contradiction, we will first want more information about the structure of $h(x)$. As in the previous section, we consider

$$h(x) = b_0 x^s + b_1 x^{s-1} + \cdots + b_{s-1} x + b_s,$$

where we now know $b_0 = 1$. As before, we define $b_j = 0$ if $j < 0$ or $j > s$. We consider J as in Table 1 so that (4.5) holds. We claim now that, with $h(x)$ as above, the inequality in (4.5) can be replaced by equality for $j \leq J$. In other words, since $b_0 = \beta_0 = 1$, we claim that

$$b_j = \beta_j \quad \text{for all integers } j \leq J. \tag{5.2}$$

Recall that (4.2) holds for the b_j. To justify (5.2), it suffices to show that

$$b_j = A b_{j-1} - B b_{j-2} \ \text{ for all } j \in \{1, 2, \ldots, J\}.$$

Assume that at least one of these equations for b_j does not hold. Taking $j = J$ and following the string of inequalities (4.4) that led to (4.5), we see that $b_J > \beta_J$. This contradicts that the largest coefficient of $h(x)$ is β_J. Therefore, (5.2) holds.

For the coefficients b_j with $j > J$, we will obtain a different structure. As noted earlier, the J in Table 1 satisfy $\beta_{J+1} < 0$, so indeed $b_{J+1} \neq \beta_{J+1}$. Let t denote the maximal non-negative integer for which

$$b_{J+1} = b_{J+2} = \cdots = b_{J+t} = \beta_J.$$

Thus, $b_{J+t+1} < \beta_J$. We claim next that

$$b_{J+t+j+1} = \beta_J - \beta_j \quad \text{for } j \in \{0, 1, \dots, J\}. \tag{5.3}$$

Define

$$\gamma_j = \begin{cases} \beta_J - b_{J+t+j+1} & \text{for } j \geq 0 \\ 0 & \text{for } j \leq -1. \end{cases}$$

Note that

$$\gamma_{-1} = 0 = \beta_J - \beta_J = \beta_J - b_{J+t}.$$

Since the expansion of (4.1) gives us coefficients of $f(x)$, we deduce from our assumption (5.1) that, for $j \geq 1$,

$$\begin{aligned}(1 - A + B)\beta_J - \gamma_j + A\gamma_{j-1} - B\gamma_{j-2} \\ &= b_{J+t+j+1} - Ab_{J+t+j} + Bb_{J+t+j-1} \\ &\leq M(A, B) \leq (1 - A + B)\beta_J.\end{aligned}$$

Since $b_{J+t+1} < \beta_J$, it follows that

$$\gamma_0 \geq 1 \quad \text{and} \quad \gamma_j \geq A\gamma_{j-1} - B\gamma_{j-2} \quad \text{for all } j \in \mathbb{Z}.$$

Observe that this is (4.2) with the b_j's replaced by γ_j's. We deduce, as we did there, that (4.5) holds but now with the b_j's replaced by γ_j's. So we have

$$\gamma_j \geq \beta_j \gamma_0 \qquad \text{for all integers } j \leq J + 1.$$

As in the argument for (5.2), we either have equality for each $j \leq J$ or else $\gamma_J > \beta_J \gamma_0$. This latter inequality is impossible since the b_j are all ≥ 0 which implies

$$\beta_J - \gamma_J = b_{2J+t+1} \geq 0.$$

Since $\gamma_J \geq \beta_J \gamma_0$, the above inequality also implies $\gamma_0 = 1$. Thus, we have $\gamma_j = \beta_j$ for all $j \leq J$. This implies (5.3).

A direct computation using the values of A, B and J from Table 1 shows that $\beta_{J-1} < \beta_J$. From (5.3), we deduce

$$b_{2J+t} > 0 \qquad \text{and} \qquad b_{2J+t+1} = 0.$$

Beginning with $j = -1$ and increasing j, the numbers b_j start at 0, go up to β_J, possibly remain there for awhile and then come back down to 0. It is possible that there are more non-zero b_j with $j > 2J + t + 1$. But we get a kind-of carousel effect here, where if there are more non-zero b_j with $j > 2J + t + 1$, then again they will go up in the same pattern as before to β_J, possibly linger at β_J for awhile and then come back down to 0 again. The increases in the numbers b_j are largely due to the condition that the coefficients of $f(x)$ are ≥ 0; the decreases in the coefficients are largely due to the assumption on the upper bound for the coefficients of $f(x)$ given by (5.1). We explain this in some more detail next.

Suppose we know that $b_{k-1} = 0$ and $b_k \neq 0$ for some integer k. In particular, perhaps $k = 2J + t + 2$. We have already seen that the coefficients of $h(x)$ are ≥ 0. Hence, $b_k \geq 1$. Define

$$b'_j = \begin{cases} b_{k+j} & \text{for } j \geq 0 \\ 0 & \text{for } j < 0. \end{cases}$$

Since $b_k \geq 1$, we have $b'_0 \geq 1$. From (4.2),

$$b'_1 = b_{k+1} = Ab_k - Bb_{k-1} = Ab_k = Ab'_0 - Bb'_{-1}.$$

Also, from (4.2), we deduce

$$b'_j \geq Ab'_{j-1} - Bb'_{j-2} \quad \text{for all integers } j \geq 2.$$

The definition of b'_j also implies

$$b'_j \geq Ab'_{j-1} - Bb'_{j-2} \quad \text{for all integers } j \leq 0.$$

We deduce that condition (4.2) holds with the b_j's replaced by b'_j's. Thus, based on our previous arguments with b_j, we deduce here that

$$b'_j = \begin{cases} \beta_j & \text{for } j \in \{0, 1, \dots, J\} \\ \beta_J & \text{for } j \in \{J+1, J+2, \dots, J+t'\} \\ \beta_J - \beta_{j-J-t'-1} & \text{for } j \in \{J+t'+1, J+t'+2, \dots, 2J+t'+1\}, \end{cases}$$

where t' denotes some non-negative integer. Thus, $h(x)$ can be written as a sum over some non-negative integers k of polynomials which are x^k times

$$\begin{aligned}&\big(\beta_0 x^J + \beta_1 x^{J-1} + \cdots + \beta_J\big)x^{J+t'} + \big(x^{J+t'-1} + x^{J+t'-2} + \cdots + x^J\big)\beta_J \\ &\quad + (\beta_J - \beta_0)x^{J-1} + (\beta_J - \beta_1)x^{J-2} + \cdots + (\beta_J - \beta_{J-1}),\end{aligned} \tag{5.4}$$

where $t' = t'(k)$ is a non-negative integer. We note that the k cannot be arbitrary since we do not want overlapping terms for different k and we want the coefficient of each such x^{k-1} in $h(x)$ to be 0.

We are ready to wrap up our proof of Theorem 1.4. Observe that Theorem 1.2 implies that we may restrict to $\deg f > 31$, and we do so. Under the assumption (5.1), we have shown that $h(x)$ has a very particular form. We consider the case that $A = 20$ and $B = 101$. If we take the polynomial expression in (5.4) that is multiplied by x^k and appears in $h(x)$, we see that it is congruent modulo β_J to

$$\big(\beta_0 x^{J-1} + \beta_1 x^{J-2} + \cdots + \beta_{J-1}\big)\big(x^{J+t'+1} - 1\big).$$

A direction computation shows that if the substitution $x = 10$ is made into the left polynomial factor above, we obtain

$$\beta_0 10^{J-1} + \beta_1 10^{J-2} + \cdots + \beta_{J-1} \equiv 0 \pmod{373}.$$

One checks that 373 divides β_J, so we deduce that $h(10)$ is divisible by 373. Since $\deg f \geq 32$ and $f(x)$ has non-negative coefficients, we deduce that $f(10)$ is an integer that is $\geq 10^{32}$ and divisible by 373. Thus, $f(10)$ is not prime, contradicting the condition $f(10)$ is prime in Theorem 1.4. This contradiction shows that (5.1) does not hold for $A = 20$ and $B = 101$.

Now, consider the case $A = 19$ and $B = 91$. We will show here that taking $x = 10$ in (5.4) always leads to an integer divisible by 37. On the other hand, 37 is not a divisor of β_J in this case, so our approach must vary from what was done above for $A = 20$ and $B = 101$. One checks directly that

$$\beta_0 10^J + \beta_1 10^{J-1} + \cdots + \beta_J \equiv 32 \pmod{37}$$

and

$$(\beta_J - \beta_0)10^{J-1} + (\beta_J - \beta_1)10^{J-2} + \cdots + (\beta_J - \beta_{J-1}) \equiv 5 \pmod{37}.$$

Also,

$$10^J = 10^{33} \equiv 1 \pmod{37} \quad \text{and} \quad \beta_J \equiv 8 \pmod{37}.$$

Thus, letting $x = 10$ in (5.4) gives us

$$32 \cdot 10^{t'} + \frac{10^{t'} - 1}{9} \cdot 8 + 5 \equiv \frac{296 \cdot 10^{t'} + 37}{9} \equiv 0 \pmod{37}$$

for all non-negative integers t'. We deduce then that $h(10)$ is divisible by 37. As before, we get a contradiction since then $f(10)$ is $\geq 10^{32}$, divisible by 37 and cannot be prime. Thus, (5.1) does not hold for $A = 19$ and $B = 91$, and Theorem 1.4 follows.

6. Closing arguments

We begin this section by supplying a proof of Theorem 1.3. Let

$$M = 6109104104761309555986010605548 8.$$

Then one checks that M is less than the bound

$$8592444743529135815769545955936773$$

appearing in Theorem 1.4. We deduce that if $f(x)$ satisfies the conditions of Theorem 1.3 and $f(x)$ is reducible, then it must be divisible by $x^2 - 20x + 101$. In this case, $f(x)$ is of the form given in (4.1) with $s = 30$, $A = 20$ and $B = 101$. From (4.5), with $J = 30$ as in Table 1, we deduce that the constant term of $h(x)$ is

$$b_{30} \geq \beta_{30} b_0 \geq 60486179255062470851346639649 9\, b_0.$$

Since the constant term of $g(x)$ is 101, we see that the constant term of $f(x)$ must be at least b_0 times

$$604861792550624708513466396499 \cdot 101 = 61091041047613095559860106046399.$$

Note that this number differs from M by 9089, so we still have some work to do but can deduce that $b_0 = 1$. For $A = 20$ and $B = 101$, the non-zero values of β_j occurring in (4.5) begin with

$$\beta_0 = 1, \quad \beta_1 = 20, \quad \beta_2 = 299, \quad \beta_3 = 3960, \quad \beta_4 = 49001. \tag{6.1}$$

Further the β_j continue to increase up until $j = 30$, where β_j has the value indicated in Table 1. Define

$$\kappa_j = b_j - Ab_{j-1} + Bb_{j-2}.$$

For u a non-negative integer, define

$$\kappa'_u = \sum_{j=0}^{u} \beta_j \kappa_{30-j}.$$

Along the lines of the inequalities in (4.4), we deduce the equalities

$$\begin{aligned} b_{30} &= Ab_{29} - Bb_{28} + \kappa_{30} \\ &= A\big(Ab_{28} - Bb_{27} + \kappa_{29}\big) - Bb_{28} + \kappa_{30} \\ &= \beta_2 b_{28} - B\beta_1 b_{27} + \kappa_{30} + \beta_1 \kappa_{29} \\ &= \cdots = \beta_{28} b_2 - B\beta_{27} b_1 + \kappa'_{27} \\ &= \beta_{29} b_1 - B\beta_{28} b_0 + \kappa'_{28} \\ &= \beta_{30} b_0 + \kappa'_{29} = \beta_{30} + \kappa'_{29}. \end{aligned}$$

The advantage here is that we have a formulation of how far the constant term b_{30} of $h(x)$ is from β_{30}. Since the constant term of $f(x)$ is $101b_{30}$, we deduce

$$\beta_{30} + \sum_{j=0}^{29} \beta_j \kappa_{30-j} = b_{30} \le \frac{M}{101}.$$

Given that $101\beta_{30}$ differs from M by 9089 and the increasing values of β_j start as in (6.1), we see that

$$\kappa_1 = \kappa_2 = \cdots = \kappa_{28} = 0, \quad \kappa_{29} \le \left\lfloor \frac{9089}{2020} \right\rfloor = 4, \quad \text{and} \quad \kappa_{30} \le \left\lfloor \frac{9089}{101} \right\rfloor = 89.$$

Some savings can be obtained by using, instead of these last two inequalities, that $20\kappa_{29} + \kappa_{30} \le 9089/101$. In any case, we see that by considering the different non-negative integers κ_{29} and κ_{30} with the above restrictions, we are left with ≤ 450 possible $h(x)$ to consider. Of the 450 polynomials $h(x)$ satisfying the conditions on the κ_j above, exactly four satisfy $f(10) = h(10)$ is prime. These four however each have at least one coefficient larger than M. The example given before the statement of Theorem 1.3 corresponds to $\kappa_{29} = 4$ and $\kappa_{30} = 10$.

Now, let

$$M' = 10711129748782895331986694273844450.$$

After Corollary 2.4, we gave an example of a polynomial $f(x)$ with non-negative integer coefficients each $\le M' + 1$ satisfying $\deg f = 35$, $f(10)$ is prime and $f(x)$ is divisible by $x^2 - 19x + 91$. As noted there, we can show that there is no such example with coefficients bounded instead by M'. Since the argument is similar to the argument just given, we only make some brief remarks on the proof. Here,

$$b_{33} \ge \beta_{33} b_0 \ge 117704722514097750900952684327901\, b_0,$$

and the constant term of $g(x)$ is 91. Thus, the constant term of $f(x)$ must be at least b_0 times

$$\begin{aligned} &117704722514097750900952684327901 \cdot 91 \\ &\qquad = 10711129748782895331986694273838991. \end{aligned}$$

This number differs from M' by 5459. We deduce that $b_0 = 1$. Setting $\kappa_j = b_j - Ab_{j-1} + Bb_{j-2}$ as before, but now for $0 \le j \le 33$, $A = 19$ and $B = 91$, we obtain here that

$$\beta_{33} + \sum_{j=0}^{32} \beta_j \kappa_{33-j} = b_{33} \le \frac{M'}{91}$$

and

$$\kappa_1 = \kappa_2 = \cdots = \kappa_{31} = 0, \quad \kappa_{32} \le \left\lfloor \frac{5459}{1729} \right\rfloor = 3, \quad \text{and} \quad \kappa_{33} \le \left\lfloor \frac{5459}{91} \right\rfloor = 59.$$

Of the $4 \cdot 60 = 240$ polynomials $h(x)$ satisfying these conditions on the κ_j, exactly three satisfy $f(10) = h(10)$ is prime. These three each have at least one coefficient larger than M'. The example given after Corollary 2.4 corresponds to $\kappa_{32} = 3$ and $\kappa_{33} = 3$.

References

[1] J. Alexander, *Irreducibility criteria for polynomials with non-negative coefficients*, Masters thesis, University 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] M. Filaseta, *A further generalization of an irreducibility theorem of A. Cohn*, *Canad. J. Math.*, 34 (1982), 1390–1395.

[5] M. Filaseta, *Irreducibility criteria for polynomials with nonnegative coefficients*, Canad. J. Math., 40 (1988), 339–351.

[6] M. Mignotte, AMS Mathematical Review MR0678678 of [4].

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

[8] G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis.*, Springer-Verlag, Berlin, 1964.

[9] W. Rudin, Principles of mathematical analysis, International Series in Pure and Applied Mathematics, McGraw-Hill Book Co., New York, 1976.