POLYNOMIALS IN BASE x AND THE PRIME-IRREDUCIBLE AFFINITY

FUSUN AKMAN

ABSTRACT. Arthur Cohn's irreducibility criterion for polynomials with integer coefficients and its generalization connect primes to irreducibles, and integral bases to the variable x. As we follow this link, we find that these polynomials are ready to spill two of their secrets: (i) There exists a unique "base-x" representation of such polynomials that makes the ring $\mathbb{Z}[x]$ into an ordered domain; and (ii) There is a 1-1 correspondence between positive rational primes p and certain infinite sets of irreducible polynomials $f(x)$ that attain the value p at sufficiently large x, each generated in finitely many steps from the pth cyclotomic polynomial. The base-x representation provides practical conversion methods among numeric bases (not to mention a polynomial factorization algorithm), while the prime-irreducible correspondence puts a new angle on the Bouniakowsky Conjecture, a generalization of Dirichlet's Theorem on Primes in Arithmetic Progressions.

1. INTRODUCTION

The fact that X is the Roman numeral for 10, a common base, whereas x is a routine variable for polynomial expressions, is hardly a symbolic conspiracy worthy of the time of Robert Langdon [3]. Neither would Dr. Langdon spare a smirk for the timeworn joke "let x be a number, and 10 be a letter." However, consider the following.

1.1. **Two Analogies and a Conjecture.** Let $\mathbb{Z}$ and $\mathbb{N}$ denote the sets of integers and positive integers, respectively. Polynomials in one variable, x, with integer coefficients, and representations of positive integers in a given base, b, are reasonably analogous. Also, we not only think of prime numbers and irreducible polynomials in $\mathbb{Z}[x]$ as playing similar roles in their respective domains, but expect irreducible polynomials to attain some prime values as well. A concrete connection between these analogies is given by Arthur Cohn's Irreducibility Criterion (CIC) [12], where the decimal representation of a positive rational *prime p* is converted into an *irreducible*

F. AKMAN

polynomial by replacing the base 10 with x, which, in turn, takes the value p at $x = 10$.

Theorem 1.1 (CIC). *If a prime p is expressed as $p = [a_n \cdots a_1 a_0]_{10}$ in base 10, where the integers a_i are digits between 0 and 9, then the polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is irreducible in $\mathbb{Z}[x]$.*

For example, since $p = 1187$ is prime, the polynomial $f(x) = x^3 + x^2 + 8x + 7 \in \mathbb{Z}[x]$ is irreducible. Note that the set of irreducibles in $\mathbb{Z}[x]$ is the union of the rational primes and the non-constant polynomials that cannot be written as a product of two polynomials of smaller degree. It is a mystery why this amazingly simple result is not as well-known as, say, the Eisenstein criterion for irreducibility.

Cohn's Irreducibility Criterion was generalized to any base $b \geq 2$ by Brillhart, Filaseta, and Odlyzko [2] (also see Ram Murty's exposition and simpler proof [10]); we will call this result "Generalized Cohn's Irreducibility Criterion," or, GCIC.

Theorem 1.2 (GCIC). *If a prime p is expressed as $p = [a_n \cdots a_1 a_0]_b$ in some base $b \geq 2$, where the integers a_i are between 0 and $b - 1$, then the polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is irreducible in $\mathbb{Z}[x]$.*

Does any polynomial that takes a prime value have to be irreducible? Clearly, this is too much to ask. However, it is true that any polynomial that takes distinct prime values infinitely many times has to be irreducible, since one of its factors in any given factorization in $\mathbb{Z}[x]$ must in turn take one of the values ± 1 infinitely many times, and hence, be a constant. Some irreducible polynomials in $\mathbb{Z}[x]$ cannot attain infinitely many prime values: for instance, the prime 2 divides all values of the irreducible polynomial $f(x) = x^2 - x + 4$ at $x \in \mathbb{Z}$.

Let $f(x) \in \mathbb{Z}[x]$ be a non-constant polynomial. We will call f *proper* if its values at integers are relatively prime, and *improper*, otherwise. Note that constant polynomials are in neither class by definition. We will also use the common expressions *content* and *primitive polynomial* to mean the greatest common divisor of all coefficients of a polynomial in $\mathbb{Z}[x]$ and a polynomial with content 1, respectively.

An improper polynomial $f(x)$ with all values divisible by a prime p must have a homomorphic image $\bar{f}(x) \in \mathbb{Z}_p[x]$ that is divisible by $x^p - x$, as all elements of the field $\mathbb{Z}_p$ are roots of $\bar{f}$. It follows that $p \leq \deg \bar{f} \leq \deg f$; hence, the number of such primes is limited by the degree of f. Moreover, Dirichlet's Theorem on Primes in Arithmetic Progressions asserts that every primitive *linear* polynomial in $\mathbb{Z}[x]$ with positive coefficients takes prime values infinitely many times. The Russian mathematician Viktor Bouniakowsky [1] made the following conjecture for irreducible polynomials

of all degrees in 1857, generalizing Dirichlet's Theorem. We will refer to it as the "Bouniakowsky Hypothesis," or (BH), from now on. This conjecture, widely believed to be true by those in the know, is also conspicuously absent from standard algebra textbooks.

Conjecture 1.3 (BH: Bouniakowsky Hypothesis). *Let $f(x) \in \mathbb{Z}[x]$ be a proper irreducible polynomial with a positive leading coefficient. Then $f(n)$ takes prime values infinitely many times for $n \in \mathbb{N}$.*

As Ribenboim [13] points out, (BH) is equivalent to the following statement: *Let $f(x) \in \mathbb{Z}[x]$ be a proper irreducible polynomial with a positive leading coefficient. Then $f(n)$ takes a prime value for some $n \in \mathbb{N}$.* We shall give yet another equivalent statement to (BH) in Theorem 4.4. To date, the only family of polynomials for which the Bouniakowsky Hypothesis is known to be true is the set of linear primitive polynomials in Dirichlet's Theorem. In fact, not even one proper irreducible polynomial of degree at least two has been shown to have infinitely many prime values. The case $x^2 + 1$ is one of "Landau's four problems," which were mentioned by Edmund Landau at the 1912 International Congress of Mathematicians as "unattackable at the present state of science" [11].

The GCIC construction necessarily gives rise to proper irreducible polynomials.

Proposition 1.4. *Let $f(x) \in \mathbb{Z}[x]$ be a non-constant irreducible polynomial obtained from some base-b expansion of a prime p as described in Theorem 1.2. Then $f(x)$ is proper.*

Proof. If $f(x) = \sum a_i x^i$ with $a_i \geq 0$, then $f'(x) > 0$ for all $x \in \mathbb{N}$, and f is strictly increasing for $x \in [1, \infty)$. Moreover, f has no zeros in $\mathbb{N}$. Let $b \geq 2$ be the base in which p is expressed. Then $0 < f(b-1) < f(b) = p$, and p, the only candidate for a common prime divisor, cannot divide all values of $f(x)$ at integers. $\square$

Definition 1.5. Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ has positive values for $x \geq k$ for some $k \in \mathbb{Z}$, that is, if it has a positive leading coefficient, then we will call f *positive*, and write $f > 0$. A positive, proper, and irreducible polynomial will be called a PPI-polynomial for short. These polynomials are non-constant by definition of "proper."

Hence, a nonzero polynomial with nonnegative integer coefficients, such as a GCIC polynomial, is positive. Other examples of positive polynomials include the *cyclotomic polynomials* $\Phi_k(x)$ for $k \geq 1$. With this background, and after defining base-x representations of polynomials, we will attach an easily-computable infinite family $\mathcal{F}_p$ that is partly made up of PPI-polynomials, including the ones arising from the GCIC construction, to

each rational prime p. The defining property of the family will be that each member takes the value p at a sufficiently large value of x. It will then be a simple matter to show that this correspondence is 1-1.

1.2. **A Case for a Base.** The GCIC construction is an example of a broader phenomenon: it is a well-known trick that a non-constant polynomial with nonnegative integer coefficients can be reconstructed from only two of its values, $f(c) = b$ and $f(f(c)) = f(b)$ (as long as $b \geq 2$), for some positive integer c. For example, suppose that we want to recover the polynomial $f(x) = 3x^2 + 5x + 7$ from its values $f(1) = 15$ and $f(15) = 757$. We write 757 in base 15, and use the digits as coefficients for the polynomial:

$$757 = [357]_{15} \implies f(x) = 3x^2 + 5x + 7.$$

The reason why we can do this is that the given polynomial provides a *model* for the representation of any positive integer in base $b > \max\{3, 5, 7\}$. Since we are not supposed to know the coefficients, the value $b = f(1)$, which is the sum of the positive coefficients, or else the values $f(2)$, $f(3)$, ..., which are even larger, will satisfy this condition. Let us go even further. What if we have a positive polynomial with some negative coefficients?

Example. *Consider the positive polynomial*

$$f(x) = 2 - x - x^3 + 2x^4 - x^5 + x^6 - x^7 + x^8 - x^9 + x^{10} - x^{11} + x^{12}.$$

We will soon show that any positive polynomial has a unique representation in "base x" with constant and linear "digits" that will work for any sufficiently large base b. Indeed, when we write our particular polynomial in the form

$$f(x) = 2 + (x-1)x + (x-1)x^2 + (x-2)x^3 + x^4 + (x-1)x^5 + (x-1)x^7$$
$$+ (x-1)x^9 + (x-1)x^{11}$$
$$= [(x-1)(0)(x-1)(0)(x-1)(0)(x-1)(1)(x-2)(x-1)(x-1)(2)]_x,$$

we find that

$$f(3) = [202020211222]_3, \quad f(4) = [303030312332]_4, \quad f(5) = [404040413442]_5.$$

While some digits are repeated as is, others are always one less than or two less than the base, exactly as indicated by the "coefficients" of the x^i. However, since 2 is a coefficient itself, it is too small to serve as a base, and we do not expect $f(2) = [101010111000]_2$ to conform to this shape.

These numerical experiments then suggest that a base-x representation of a positive polynomial can be obtained simply by writing two values $f(b_1)$ and $f(b_2)$ in bases $b_1, b_2 \geq 2$, respectively, where the integers b_i are sufficiently greater than the largest absolute value of the coefficients of f (see Theorem 2.5 for an application of this idea to factorization of polynomials,

and the proof of Theorem 2.1, where we use it to establish uniqueness). However, this is hardly necessary in practice. In the next section, we will describe how to compute the base-x representation of any positive polynomial algorithmically, using countably many digits that form a chain with minimum and maximum elements, and show that $\mathbb{Z}[x]$ naturally becomes an ordered domain. This representation arguably provides the most compelling analogy between $\mathbb{Z}[x]$ and $\mathbb{Z}$.

2. Representation in Base x

2.1. **Existence and Uniqueness.** The example above prompts us to give the following definitions. Let $f(x)$ be a positive polynomial. We will call the nonnegative integer coefficients a_i the *constant digits*, and the linear coefficients of the form $(x - a_i)$ the *linear digits* in a base-x representation of $f(x)$. These infinitely many digits form our *polynomial alphabet*.

Theorem 2.1 (Base-x representation). *Let $f(x) \in \mathbb{Z}[x]$ be a positive polynomial. Then there exists a unique least positive integer a and a unique base-x representation of $f(x)$ as follows:*

$$f(x) = b_0(x)\, 1 + b_1(x)\, x + b_2(x)\, x^2 + \cdots + b_m(x)\, x^m,$$

with

$$b_i(x) \in \{0, 1, \ldots, a-1\} \cup \{x-1, \ldots, x-a\}, \quad b_m(x) \neq 0.$$

In particular, the unique representation of $f(b) \in \mathbb{N}$ in base b for all $b \geq a$ is given by

$$f(b) = [b_m(b) \cdots b_1(b)\, b_0(b)]_b.$$

Proof. We start the construction with the constant term and work our way towards higher powers of x. At any step, if a_i is a negative coefficient of x^i, then we replace it by the linear digit $(x - |a_i|)$, and add the term $-x^{i+1}$ to balance it out. If the original coefficient of x^{i+1} in f is positive, then it will be reduced by one and will not affect the coefficient of x^{i+2}. However, if $a_{i+1} \leq 0$, then the new "coefficient" of x^{i+1} will be the linear digit $(x - |a_{i+1}| - 1)$, and will cause a new term $-x^{i+2}$ to appear, etc. We can see that positive coefficients remain the same or are reduced by one, whereas negative coefficients a_i are eventually replaced by $(x - |a_i|)$ or $(x - |a_{i+1}| - 1)$. This rule also applies to the last (positive) coefficient of $f(x)$, and the original highest power will now have a smaller positive coefficient, or else vanish. The base-b representations of $f(b)$ in $\mathbb{Z}$ follow for $b \geq a$. Now suppose that there are two distinct base-x representations of the same polynomial. Pick any $b > \max\{a_i + b_i\}$ in $\mathbb{N}$ so that the nonnegative integers a_i and b_i that appear in the ith constant or linear digits of the two forms of the polynomial f always result in a pair of distinct values

$\{a_i, b - b_i\}$ and a pair of distinct values $\{b_i, b - a_i\}$. Then the positive integer $f(b)$ must have two distinct base-b representations, as we shall see: let the ith digits be distinct in the two base-x expressions for some fixed i. They cannot both be constant digits or both be linear digits, because these would immediately give us different integers in base b upon substitution of b. Due to the choice of b, the two values will be different even in the case of a pair of opposite-type ith digits. $\qquad\square$

Given any positive polynomial $f(x) = \sum a_i x^i \in \mathbb{Z}[x]$, we will call the unique least positive integer a described in Theorem 2.1, the *minimum base* of f, and denote it by $a = \mathrm{MB}(f)$. We will also define $H(f) = \max |a_i|$ as the *height* of f. By construction, it is clear that $H(f) \leq \mathrm{MB}(f) \leq H(f)+1$.

Example. *We compute the base-x representation of*

$$f(x) = -7 + 2x^2 - x^3 + x^4 \tag{2.1}$$
$$= (x - 7)1 - x + 2x^2 - x^3 + x^4 \tag{2.2}$$
$$= (x - 7)1 + (x - 1)x - x^2 + 2x^2 - x^3 + x^4 \tag{2.3}$$
$$= (x - 7)1 + (x - 1)x + x^2 - x^3 + x^4 \tag{2.4}$$
$$= (x - 7)1 + (x - 1)x + x^2 + (x - 1)x^3 - x^4 + x^4 \tag{2.5}$$
$$= (x - 7)1 + (x - 1)x + x^2 + (x - 1)x^3 \tag{2.6}$$
$$= [(x - 1)(1)(x - 1)(x - 7)]_x. \tag{2.7}$$

We find that the minimum base of f is $\mathrm{MB}(f) = 7 = H(f)$. By contrast, the polynomial $g(x) = 7 + 2x^2 + x^3 + x^4$ has minimum base $\mathrm{MB}(g) = 8 = H(g) + 1$.

2.2. **A Natural Linear Ordering on $\mathbb{Z}[x]$.** The following statement is indisputable, yet somewhat surreal.

Theorem 2.2 (Linear Ordering)**.** *The linear ordering*

$$(0) < (1) < \cdots < (n) < \cdots < (x - n) < \cdots < (x - 2) < (x - 1)$$

on the polynomial alphabet extends to a natural linear ordering on the positive polynomials and to one on $\mathbb{Z}[x]$ by symmetry. We have

$$[(0)]_x \tag{2.8}$$
$$< [(1)]_x < \cdots < [(x - 1)]_x < [(1)(0)]_x \tag{2.9}$$
$$< [(1)(1)]_x < \cdots < [(1)(x - 1)]_x < [(2)(0)]_x \tag{2.10}$$
$$\vdots \tag{2.11}$$
$$< [(x - 2)(1)]_x < \cdots < [(x - 2)(x - 1)]_x < [(x - 1)(0)]_x \tag{2.12}$$

$$< [(x-1)(1)]_x < \cdots < [(x-1)(x-1)]_x < [(1)(0)(0)]_x \qquad (2.13)$$
$$< [(1)(0)(1)]_x < \cdots . \qquad (2.14)$$

Every polynomial in $\mathbb{Z}[x]$ has a successor and a predecessor obtained by adding or subtracting $[(1)]_x$, respectively.

Note that the largest digit plus 1 is equal to the base, x, written $[(1)(0)]_x$, and that the subset of positive elements of $\mathbb{Z}[x]$ is not well-ordered. If $m > n > 0$, then a positive polynomial with m digits is strictly greater than one with n digits. If two positive polynomials have the same number of digits, then the lexicographic order determines which one is larger.

Corollary 2.3. *The ordering on $\mathbb{Z}[x]$ makes it an ordered integral domain. In particular, $f > g$ if and only if $f - g$ is positive in the sense that we have defined. If $f > g$, then the following properties hold:*

(i) $f + h > g + h$ for all h, and (ii) $fh > gh$ for all $h > 0$.

The field of fractions of $\mathbb{Z}[x]$, and its subring $\mathbb{Q}[x]$, are also ordered according to the rule

$$\frac{f}{g} > 0 \iff f \text{ and } g \text{ are both positive or both negative.}$$

In fact, the set of rational functions in x over any ordered field $\mathbb{F}$ is an ordered field itself, whose order relation is compatible with the one on $\mathbb{F}$. However, this fact is more commonly used in analysis as an example of a non-Archimedean field: no natural number n satisfies $n \cdot 1 > x$ (e.g., see Example 3.2.6 and Exercise 3.16 of Lay [8]). In algebra and number theory, on the other hand, we can make use of this ordering to establish a more natural version of the Division Algorithm, as we shall see below.

Theorem 2.4 (Division Algorithm for a Monic Divisor)**.** *Let $f(x)$ be any polynomial and $g(x)$ be a monic polynomial in $\mathbb{Z}[x]$. Then there exist unique polynomials $q(x), r(x) \in \mathbb{Z}[x]$ such that*

$$f(x) = q(x)g(x) + r(x), \quad 0 \le r(x) < g(x).$$

Proof.

Existence. Long division gives us the correct form $f = qg + r$, but the second condition is replaced by "$r = 0$ or $\deg r < \deg g$". If $r \ge 0$, then we are done, as a larger degree means a larger polynomial when both are positive. However, if $r < 0$, then $q(x) - 1$ as the quotient and $g(x) + r(x)$ as the remainder will yield the desired result by judicious applications of Corollary 2.3. In the latter case, the degree of the remainder will be equal to the degree of g.

Uniqueness. Suppose that we have $f(x) = q_1(x)g(x) + r_1(x)$ and $f(x) = q_2(x)g(x) + r_2(x)$, with $0 \leq r_1(x), r_2(x) < g(x)$. Then $[q_1(x) - q_2(x)]g(x) = r_2(x) - r_1(x)$. If both sides are zero, then we are done. Suppose not. Thus, $\deg(r_2 - r_1) \geq \deg g$ by the additivity of degrees in polynomial multiplication over an integral domain. However, we also know that $\deg(r_2 - r_1) \leq \deg g$ (neither remainder can have a degree larger than that of g), and hence, we must have $\deg(r_2 - r_1) = \deg g$. This leads us to $\deg(q_1 - q_2) = 0$. Without loss of generality, say $q_1(x) = q_2(x) + a$ for some $a \in \mathbb{N}$. Hence, we conclude that

$$a\,g(x) = r_2(x) - r_1(x) \implies r_2(x) = r_1(x) + a\,g(x) \geq 0 + 1\,g(x) = g(x)$$

by Corollary 2.3, a contradiction. $\qquad\square$

Arithmetic operations on positive polynomials written in base x, including digital division by a monic divisor, are covered in Appendix A (see the last example). Unfortunately, we cannot extend the statement and the proof to any polynomial ring $\mathbb{F}[x]$, where $\mathbb{F}$ is a generic ordered domain or field, because not every ordered domain is *discrete*: there may be positive elements between 0 and 1.

2.3. **Polynomial Factorization via Base Patterns.** Factorization of integers into prime factors and of polynomials in $\mathbb{Z}[x]$ into irreducible factors in finitely many steps is theoretically possible. The reader can consult Knuth ([6], pp. 420–436) for a compendium of polynomial factorization algorithms and their history. Our method of factorization of positive polynomials is a variant of *Kronecker's Method*; according to Knuth (p. 431), Isaac Newton had described a method to factorize polynomials in $\mathbb{Z}[x]$ in *Arithmetica Universalis* (1707). Newton's method was then generalized into a general, finite algorithm by the astronomer Friedrich von Schubert in 1793 (see the account of the mathematics historian M. Cantor [4], pp. 136–137), and Kronecker rediscovered the method independently about 90 years later [7]. The complete description of Kronecker's algorithm can be found in van der Waerden [14], pp. 97–98. The algorithm relies on the facts that (1) if $g(x)$ divides $f(x)$, then for all $a \in \mathbb{Z}$, $g(a)$ either is zero or divides $f(a)$; (2) knowing sufficiently many values of a polynomial of bounded degree, we can reconstruct it using Lagrange's or Newton's interpolation formulas; (3) hence, there are finitely many candidates for polynomial factors; and (4) the division algorithm for rational numbers can be applied to see whether a suspected factor is an actual factor. This algorithm is too costly for computer applications and needs to be enhanced or replaced by other techniques such as looking for a rational root first, or reduction modulo a few primes. Similarly, the procedure that we are going to describe is computationally

expensive, but fun to implement by hand. A slight improvement over Kronecker's method is that only two values of the polynomial are required, so that fewer cases need to be considered. Moreover, interpolation formulas are replaced by base-x representations.

We recall that for $f(x) = \sum a_i x^i \in \mathbb{C}[x]$, the ℓ_2-*norm* of f is defined as

$$||f|| = \left(\sum |a_i|^2 \right)^{1/2}.$$

We will also use the traditional divisibility notation, $g|f$, for both polynomials and integers. If $f(x) \in \mathbb{Z}[x]$ is positive, then it has finitely many positive divisors $g(x) \in \mathbb{Z}[x]$, and we define the *minimum factor base* of f to be

$$\mathrm{MFB}(f) = \max\{\mathrm{MB}(g) : g|f, \ g > 0\}.$$

Note that $\mathrm{MFB}(f) = \mathrm{MB}(f)$, when f is irreducible. Although the exact value of $\mathrm{MFB}(f)$ is obviously unknown in a factorization problem, upper bounds for the height of any divisor entirely in terms of f are known. For example, a corollary of Theorem 4 in Mignotte [9] (namely, that $||g|| \leq 2^{\deg g}||f||$) implies the following bound for g dividing f:

$$H(g) \leq ||g|| \leq 2^{\deg g}||f|| \leq 2^{\deg f}||f||.$$

We will not be concerned with the best known upper bound for heights of divisors, but make a note of the fact that they do exist, and depend entirely on f itself. This, in turn, provides us with an upper bound on the minimal bases of all positive divisors of f. In what follows, let $\overline{\mathrm{MFB}}(f)$ denote such an absolute upper bound for $\mathrm{MFB}(f)$, which is not unique.

Theorem 2.5. *It is possible to factor a positive polynomial $f(x) \in \mathbb{Z}[x]$ into irreducible polynomials in $\mathbb{Z}[x]$ in finitely many steps by factorizing two values $f(b_1)$ and $f(b_2)$ of f into primes for distinct natural numbers $b_i > \overline{\mathrm{MFB}}(f) + 1$.*

Proof. Given a positive polynomial $f(x)$, we factor out its content first. Assume that f is primitive. Let $f(x) = g(x)h(x)$ be an unspecified factorization into positive and necessarily primitive polynomials in $\mathbb{Z}[x]$. Let $a = \overline{\mathrm{MFB}}(f)$, so that all integers of the form $f(b)$, as well as their unknown factors $g(b)$ and $h(b)$ for $b \geq a$, have unique representations in base b that match the base-x representations of the corresponding polynomials. We first factor $f(a + 2)$ and $f(a + 3)$ into primes, and compute all positive divisors of these two numbers. By comparing all possible divisor pairs of $f(a + 2)$ and $f(a + 3)$, we can uncover a common base pattern that is repeated as in the last example of the Introduction (Section 1). Any observed base pattern can be converted into a positive polynomial and be verified or ruled out as a divisor. We can then start testing the quotients for divisors in turn.

We remark that (1) two substitutions are necessary to decide whether a digit in the given base (substituted value) corresponds to a fixed or variable digit in base x, and (2) it is possible to choose even larger numbers b such that $f(b)$ has fewer factors. However, the latter course requires additional computations, which may be undesirable.

Why can't we just use $\overline{\text{MFB}}(f)$ as the least possible value for b, instead of $\overline{\text{MFB}}(f) + 2$? The only thing that could potentially go wrong in the first paragraph's scenario is that there may be additional non-constant polynomial factors of $f(x)$ that attain the value $+1$ at b_1 and b_2; however, if a divisor $g(x)$ is not constant, then it has at least one term of the form ux^j $(u, j \geq 1)$ or $(x - u)x^j$ $(u \geq 1, j \geq 0)$ in its base-x representation, making $\text{MFB}(f) \geq \text{MB}(g) \geq u + 1$ or u, respectively. Therefore, $g(x)$ cannot attain the value 1 when evaluated at an $x = b_i \geq \overline{\text{MFB}}(f) + 2 \geq \text{MFB}(f) + 2 \geq u + 2$, because in this case, at least one of its terms in the base-x representation $(ux^j$ or $(x - u)x^j)$ will achieve a value greater than or equal to 2, and the possibility of an invisible non-constant factor is avoided. $\qquad\square$

Example. *Let us factor a polynomial given in an exercise of van der Waerden [14]:* $f(x) = x^5 + x^4 + x^2 + x + 2$. *We compute*

$$||f|| \approx 2.828 \ \ and \ \ H(g) \leq 2^5||f|| \approx 90.496 \ \ for \ any \ g|f.$$

Hence, we may take $\overline{\text{MFB}}(f) = 90 + 1 = 91$, *and evaluate*

$$f(93) = 7\,031\,697\,638 = 2^1 \cdot 7^1 \cdot 1\,249^1 \cdot 402\,133^1$$

and

$$f(94) = 7\,417\,124\,052 = 2^2 \cdot 3^1 \cdot 13^2 \cdot 229^1 \cdot 15\,971^1.$$

By trial and error, we find that the factors of $8\,743 = 7 \cdot 1\,249$ *and* $8\,931 = 3 \cdot 13 \cdot 229$ *of* $f(93)$ *and* $f(94)$, *respectively have the base representations*

$$8\,743 = 93^2 + 93 + 1 = [111]_{93} \ \ and \ \ 8\,931 = 94^2 + 94 + 1 = [111]_{94}.$$

That is, $g(x) = x^2 + x + 1$ *is a plausible factor, which is irreducible. We divide* $f(x)$ *by* $g(x)$ *to find the exact quotient* $h(x) = x^3 - x + 2$. *By the rational root theorem,* $h(x)$ *is irreducible as well, and* $f(x) = g(x)h(x)$ *is the full factorization of* $f(x)$ *into irreducibles.*

Now, if we had tried the factors

$$804\,266 = 2 \cdot 402\,133 = 92 \cdot 93^2 + 92 \cdot 93 + 2 = [(93 - 1)(93 - 1)(2)]_{93}$$

and

$$830\,492 = 2^2 \cdot 13 \cdot 15\,971 = 93 \cdot 94^2 + 93 \cdot 94 + 2 = [(94 - 1)(94 - 1)(2)]_{94}$$

of $f(93)$ *and* $f(94)$, *respectively, we would have decided that*

$$[(x - 1)(x - 1)(2)]_x = (x - 1)x^2 + (x - 1)x + 2 = x^3 - x + 2$$

might be a factor, and we would have been correct.

Every polynomial factorization algorithm serves as an irreducibility test as well. The following corollary is a generalization of GCIC, where all coefficients are not necessarily positive.

Corollary 2.6. *Let $f(x)$ be a non-constant positive polynomial and $a = \overline{MFB}(f)$. If $f(b) = p$, a prime, for some integer $b > a + 1$, then $f(x)$ is proper and irreducible in $\mathbb{Z}[x]$.*

Proof. The polynomial f must be proper since it is increasing for $x \geq a$, and $f(a)$ cannot be divisible by p. $\square$

Remark. *It has been pointed out to us that the bounds in Theorem 2.5 and Corollary 2.6 can be improved in several ways, for example, by using ideas from Murty's paper [10]. Murty proves the following: if $f(x) = a_m x^m + \cdots + a_0$ and $f(b)$ is prime for some $b \geq \max_{0 \leq i \leq m-1} |a_i / a_m| + 2$, then $f(x)$ is irreducible (which falls just short of proving Cohn's Irreducibility Criterion). The statement and proof of Theorem 2.5 can also be fine-tuned. However, we feel that the pedagogical value of the last two statements is in the novelty and simplicity of their proofs that make use of a polynomial base, with no explicit need to consider complex roots, and where the only additional ingredient is Mignotte's inequality (or similar results bounding the height). We do not see our factorization method, and indeed the base conversion algorithms in the next section, as being competitive with established computer algorithms. Small examples are just fun and instructive to compute by hand.*

3. Polynomial and Numeric Bases

3.1. Polynomial Representatives of Positive Integers in Base b.
Since base-x representations of polynomials are central to our paper, we introduce special notation and terminology for the polynomials that represent base-b expansions of natural numbers. Let $c \in \mathbb{N}$.

(1) The polynomial

$$f_c^{(1)}(x) = \frac{x^c - 1}{x - 1} = x^{c-1} + \cdots + x + 1$$

will be called the *polynomial representative of c in base 1.*

(2) Let $b \in \mathbb{N}$, with $b \geq 2$. If $c = [a_k \cdots a_1 a_0]_b$ is the unique expansion of c in base b, with digits a_i between 0 and $b-1$, then the polynomial

$$f_c^{(b)}(x) = a_k x^k + \cdots + a_1 x + a_0$$

will be called the *polynomial representative of c in base b.*

In both of these cases, we have $f_c^{(b)}(b) = c$.

Table 1 below exhibits all polynomial representatives $f_{17}^{(b)}(x)$ of the prime 17 in bases $b \geq 1$. The first one is irreducible since it is the 17th cyclotomic

polynomial, and the rest are irreducible as a result of GCIC. We will show how to generate this table for any $c \in \mathbb{N}$ in a systematic way starting from $f_c^{(1)}(x)$ in the next Proposition.

Table 1. Polynomial representatives of $p = 17$

Base b	$f_{17}^{(b)}(x)$	Base b	$f_{17}^{(b)}(x)$
1	$x^{16} + \cdots + x + 1 = \Phi_{17}$	11	$x + 6$
2	$x^4 + 1 = \Phi_8(x)$	12	$x + 5$
3	$x^2 + 2x + 2 = \Phi_4(x+1)$	13	$x + 4$
4	$x^2 + 1 = \Phi_4(x)$	14	$x + 3$
5	$3x + 2$	15	$x + 2$
6	$2x + 5$	16	$x + 1 = \Phi_2(x)$
7	$2x + 3$	17	x
8	$2x + 1$	18	17
9	$x + 8$	19	17
10	$x + 7$	20	17

3.2. Base Conversions.

Proposition 3.1 (Base conversions). *Let $a, b, c \in \mathbb{N}$, $f(x) \in \mathbb{Z}[x]$ be either a nonzero polynomial with nonnegative coefficients $\leq b - 1$, where $b \geq 2$ and $f(b) = c$, or $f(x) = (x^c - 1)/(x - 1)$ (in which case we set $b = 1$). Then $f(x) = f_c^{(b)}(x)$, and the following hold.*

(1) *If $c = p$, a prime, then $f_c^{(b)}$ is a PPI-polynomial for all $b \geq 1$.*
(2) *(Descent) To convert $f(x) = f_c^{(b)}(x)$ into $f_c^{(b-a)}(x)$, where $b - a \in \mathbb{N}$ as well, follow these steps:*
   (a) *Substitute $x + a$ for x and expand $f(x + a)$ in powers of x. This polynomial will have all positive coefficients. The indeterminate x now represents the base $b - a$.*
   (b) *If all coefficients of the new polynomial are strictly less than $b - a$, stop. Otherwise, proceed to the next step. (If $b - a = 1$, then the stopping point is reached when all coefficients are 1.)*
   (c) *Replace all coefficients by their base-$(b - a)$ expansions; substitute x for each $b - a$; simplify. Go to Step (b).*
(3) *(Ascent) To convert $f(x) = f_c^{(b)}(x)$ into $f_c^{(b+a)}(x)$, follow these steps:*
   (a) *Substitute $x - a$ for x and simplify $f(x - a)$. The indeterminate x now represents the base $b + a$.*
   (b) *Convert the positive part of each coefficient to base $b + a$; substitute x for $b + a$; simplify.*

    (c) *If the absolute value of each coefficient in the new polynomial is strictly less than $b + a$, go on to the next step. Otherwise, return to Step (b).*

    (d) *Write the polynomial in base x; replace any digit of the form $x - j$ by $b + a - j$; simplify.*

(4) *The ascent and descent procedures are inverses of each other.*

(5) *If $1 \leq b < b'$ and $b \leq c$, then $f_c^{(b)} > f_c^{(b')}$. For $b > c$, both polynomial representatives are equal to the constant c.*

Proof. Part (1) follows from the properties of cyclotomic polynomials and Proposition 1.4. In Parts (2) and (3), we are simply performing naive base conversions by starting with an approximate expansion and making corrections as necessary: the unique expression is independent of the method. The only point that may not be immediately obvious is conversion from base 2 to base 1, or, to the unary system. Why do we always obtain the lowest c nonnegative powers of x and not just any c distinct powers? This is proven in the following Lemma. Part (4) is clear by uniqueness of base expansions. Finally, Part (5) can be seen in the details of the descent procedure, where x is replaced by $x + a$ and $b - a$ is replaced by x; all other terms and factors are nonnegative, and we can apply properties of ordered domains. $\square$

In computing, the convention for the unary representation of a positive integer c is c consecutive digits of 1, with no zeros in between or outside. Here is a good reason why.

Lemma 3.2. *Let $c \in \mathbb{N}$, and*
$$f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x],$$
with $a_i \in \{0, 1\}$. Moreover, let $f(2) = c$. Then $f(x) = f_c^{(2)}(x)$, and the descent process in Proposition 3.1 Part (2) gives us
$$f_c^{(1)}(x) = x^{c-1} + \cdots + x + 1.$$

Proof. By induction. After $f(x)$ is replaced by the larger polynomial
$$g(x) = f(x + 1) = (x + 1)^k + a_{k-1}(x + 1)^{k-1} + \cdots + a_1(x + 1) + a_0,$$
all coefficients of $g(x)$ up to the leading one become strictly positive, and the constant term becomes $g(0) = f(1) = 1 + a_{k-1} + \cdots + a_1 + a_0$. As instructed, we replace all coefficients a of g by $x^{a-1} + \cdots + x + 1$, and obtain a larger polynomial. If $f(1)$ is not already equal to 1, then it will be replaced by $[x^{f(1)-1} + \cdots + x] + 1$, where the rest of the polynomial $g(x)$ is $O(x)$. Therefore, the constant term permanently becomes 1, and no powers of x in g up to the largest one will ever vanish. Let $a \in \mathbb{N}$ be the coefficient of x in g. If $a > 1$, then the next step brings the term $(x^{a-1} + \cdots + x + 1)x$

in addition to the constant term 1, and the rest of the polynomial is now $O(x^2)$. In this manner, we guarantee that the smallest two terms of the evolving polynomial will be $x + 1$ for the rest of the procedure, and so on, until we reach $x^{c-1} + \cdots + x + 1$, which gives us the value c at $x = b = 1$. □

Example. *Let us verify a few examples from Table 1. In ascending order, we have $17 = [10001]_2$, giving us $f_{17}^{(2)}(x) = x^4 + 1$. The next base is $b = 3 = 2 + 1$. We compute $f(x-1) = x^4 - 4x^3 + 6x^2 - 4x + 2$, then replace $4 = b + 1$ by $x + 1$ and $6 = 2b$ by $2x$, and obtain the polynomial*

$$x^3 - x^2 - x + 2 = (x-2)x^2 + (x-1)x + 2.$$

A final substitution of $b = 3$ into the digits only gives us $f_{17}^{(3)}(x) = x^2 + 2x + 2$. In descending order, we know that $f_{17}^{(17)}(x) = x$, and $f_{17}^{(16)} = f_{17}^{(17)}(x+1) = x + 1$ (no change needed). Let us pick up the sequence at $f_{17}^{(9)}(x) = x + 8$. The next base is $b = 8 = 9 - 1$. Hence,

$$f_{17}^{(9)}(x+1) = x + 9 = x + (8+1) \mapsto x + (x+1) = 2x + 1 = f_{17}^{(8)}(x).$$

4. Families of Irreducibles with the Same Prime Value at Large Integers

The GCIC construction as well as Corollary 2.6 make it clear that only the prime values of polynomials for large $n \in \mathbb{N}$ are significant for characterizing irreducibility. Given a positive rational prime p, let us define a family $\mathcal{F}_p \subset \mathbb{Z}[x]$ that consists of the constant polynomial p and the PPI-polynomials with this property.

Definition 4.1. Given a positive rational prime p, consider the constant polynomial p, the cyclotomic polynomial $\Phi_p(x)$, and any PPI-polynomial $g(x) \in \mathbb{Z}[x]$ such that $g(b) = p$ for some $b \geq \mathrm{MB}(g)$. This collection, which includes all $f_p^{(b)}(x)$ for $b \geq 1$, will be denoted by $\mathcal{F}_p$ and called the *family of irreducible polynomials associated with p*.

Theorem 4.2. *Given any positive rational prime p, the family $\mathcal{F}_p$ of irreducible polynomials associated with p can be generated from the seed polynomial $\Phi_p(x)$ by the following rules.*

(1) *The ascent procedure described in Proposition 3.1;*
(2) *Replacing selected coefficients a_i of a polynomial $f_p^{(b)}(x)$ by the linear digit $x - (b - a_i)$. Note that this can be done for finitely many zero coefficients as well, including those that are associated with x^n, where $n > \deg f_p^{(b)}(x)$.*

Proof. Proposition 3.1 and the last example show us how to obtain all $f_p^{(b)}(x)$ for $b \geq 2$ from $f_p^{(1)}(x) = \Phi_p(x)$. Let $g(x)$ be any PPI-polynomial

such that $g(b) = p$ for some $b \geq \mathrm{MB}(g)$. If all coefficients of g are non-negative, then $g(x) = f_p^{(b)}(x)$, and we are done. If at least one coefficient of g is negative, then we write $g(x) = \sum b_i(x)x^i$ in base x, and replace all $b_i(x)$ by $b_i(b)$. The resulting polynomial, $f(x)$, also satisfies the property $f(b) = p$, as well as $b \geq \mathrm{MB}(f)$ (some $(x - a_i)$'s in $g(x)$ become $(b - a_i)$'s, where $b > b - a_i$). Moreover, its coefficients are nonnegative, which makes $f = f_p^{(b)}$. Therefore, any PPI-polynomial $g \in \mathcal{F}_p$ can be obtained from some $f_p^{(b)}(x)$ by the reverse procedure: (i) splitting the coefficients of $f_p^{(b)}$ into two finite subsets, indexed by I and J, and (ii) replacing all a_i with $i \in I$ with the linear digits $x - (b - a_i)$. It is not guaranteed that each such procedure will always give us an irreducible (hence, PPI) polynomial. For example, we cannot change *all* coefficients of the base-1 polynomial $f_p^{(1)}(x) = \Phi_p(x)$, which would give us a factor of $x - (p - 1)$, nor can we re-place the coefficient 1 in $f_p^{(p)}(x) = x$ with the factor $x - (p - 1)$. However, we can check whether $g(x)$ is irreducible or not by applying Theorem 2.5. □

Corollary 4.3. *For each positive rational prime p, the set $\mathcal{F}_p$ is infinite, and always contains*

$$\{x + 1, \, x, \, x - 1, \, x - 2, \, x - 3, \, \ldots, p\}.$$

Proof. For bases $b > p$, the polynomial representative of p is p itself, and we may replace it with the linear polynomial $g(x) = x - (b - p)$. In addition, for $b = p$ we have x, and for $b = p - 1$ we have $x + 1$. □

Example. *Let us compute some of the elements of $\mathcal{F}_2$ of degree ≤ 2. We start with the set in Corollary 4.3:*

$$\{x + 1, \, x, \, x - 1, \, x - 2, \, x - 3, \, \ldots, 2\}.$$

The distinct base polynomials for $p = 2$ are 2 $(b \geq 3)$, x $(b = 2)$, and $x + 1$ $(b = 1)$. The constant polynomial 2 has already been replaced by $x - (3 - 2) = x - 1$, $(x - (4 - 2) = 2$, etc. What if we also include the zero coefficient in $0x + 2$? Here are some of the additional polynomials to be considered:

b	0-replacement	2-replacement	result	PPI?
3	$x - (3 - 0)$	2	$x^2 - 3x + 2$	no
3	$x - (3 - 0)$	$x - (3 - 2)$	$x^2 - 2x - 1$	yes
4	$x - (4 - 0)$	2	$x^2 - 4x + 2$	yes
4	$x - (4 - 0)$	$x - (4 - 2)$	$x^2 - 3x - 2$	no
5	$x - (5 - 0)$	2	$x^2 - 5x + 2$	no
5	$x - (5 - 0)$	$x - (5 - 2)$	$x^2 - 4x - 3$	yes
⋮	⋮	⋮	⋮	⋮

There are potentially infinitely many quadratics in $\mathcal{F}_2$ to be obtained in this manner. Next, we consider the base polynomial $x = x + 0$. We have observed that we cannot replace the coefficient 1 by $x - (2 - 1)$ and still obtain an irreducible polynomial. But if we put the constant term 0 into the mix, then we obtain

$$(x - (2 - 1))x + (x - (2 - 0)) = x^2 - 2 \ \text{ and } \ x + (x - (2 - 0)) = 2x - 2,$$

where the first polynomial is PPI and the second is not. For the last base polynomial, $x + 1$, we cannot change both coefficients, but can try to do so one at a time. We have

$$(x - (1 - 1))x + 1 = x^2 + 1 \ \text{ and } \ x + (x - (1 - 1)) = 2x,$$

where once again $x^2 + 1$ is PPI, but $2x$ is not. Technically, we cannot include $x^2 + 1$ in $\mathcal{F}_2$, since we need to substitute $b = 1 < \mathrm{MB}(x^2 + 1) = 2$. Hence, we have the following polynomials of degree ≤ 2 in $\mathcal{F}_2$, where the unknown quadratic polynomials are of the form $(x - b)x + 2$ or $(x - b)x + (x - (b - 2))$ for $b \geq 6$.

$$\{x^2 - 2,\, x^2 - 2x - 1,\, x^2 - 4x + 2,\, x^2 - 4x - 3, \dots,$$
$$x + 1,\, x,\, x - 1,\, x - 2,\, x - 3,\, \dots,\, 2\}.$$

The degree of polynomials in $\mathcal{F}_2$, or in any $\mathcal{F}_p$, do not a priori *have an upper bound, as we are allowed to change the zero coefficients of large powers of x in a base polynomial. For example, for $b = 6$, we have*

$$(x - (6 - 0))x^2 + 2 = x^3 - 6x^2 + 2 \in \mathcal{F}_2.$$

Finally, we have the following summary. Part (2) especially shows how restrictive $\mathcal{F}_p$ is, although it is infinite.

Theorem 4.4. *Let p and q be positive rational primes. Then*

(1) *$\mathcal{F}_p = \mathcal{F}_q$ if and only if $p = q$.*
(2) *Given any prime p, there exist infinitely many PPI-polynomials f that attain the value p at some integer, but no translation of $f(x-b)$, $b \in \mathbb{Z}$, is in $\mathcal{F}_p$.*
(3) *(BH) holds if and only if every PPI-polynomial f belongs to $\mathcal{F}_p$ for some prime p.*

Theorem 4.2 gives us finitely many rules of membership in $\mathcal{F}_p$, which may be helpful in studying (BH).

Proof. As the only constant polynomial in $\mathcal{F}_p$ is p itself, the first part is straightforward. For Part (2), consider the irreducible polynomial $f(x) = x^m + p$ for any $m \geq 2$, which is PPI, but not in $\mathcal{F}_p$. The value p is attained only at $x = 0$, and any translate $g(x) = f(x - b)$ would attain the same value only at $x = b$, which needs to be positive for eligibility.

Let us fix $b \geq 1$ and $m \geq 2$. Since $g(x) = x^m - mb\,x^{m-1} + O(x^{m-2})$, we have $b < mb \leq H(g) \leq \mathrm{MB}(g)$. As for Part (3), any PPI-polynomial f would have infinitely many prime values past $x = \mathrm{MB}(f)$ under (BH). The converse is also clear by the equivalent statement to Conjecture 1.3. $\qquad\square$

5. Conclusion

Rational primes and irreducible polynomials with integer coefficients serve the same purpose of being multiplicative building blocks in their respective structures. Moreover, both integers and polynomials have unique representations in various bases that mirror each other; the base-x representation of polynomials not only highlights the analogy, but also allows us to uniquely associate to each prime a finitely generated family of irreducible polynomials that attain the prime value. We hope that the results and techniques in the article will make a new generation of mathematicians take a closer look at the Bouniakowsky Hypothesis with fresh eyes. Considering that it is a generalization of Dirichlet's Theorem, though, we suggest that the proof not be assigned as homework; not every student can be a George Dantzig [5]!

Appendix A. Arithmetic in Base x.

Table 2. Addition of digits in base x

The rule for **addition** of digits in base x is given by Table 2, where each carried digit is at most 1 (indicated by (c)).

$i, j \geq 0$	$i > j \geq 0$	$j \geq i > 0\ (c)$	$i, j > 0\ (c)$
$[(i)]_x$	$[(x-i)]_x$	$[(x-i)]_x$	$[(x-i)]_x$
$[(j)]_x$	$[(j)]_x$	$[(j)]_x$	$[(x-j)]_x$
$[(i+j)]_x$	$[(x-(i-j))]_x$	$[(1)(j-i)]_x$	$[(1)(x-(i+j))]_x$

Consider the positive polynomials

$$f(x) = 2x^3 - x^2 + 5x - 6 = [(1)(x-1)(4)(x-6)]_x$$

and

$$g(x) = x^3 - x - 1 = [(0)(x-1)(x-2)(x-1)]_x.$$

Direct polynomial addition and conversion into base x gives us

$$f(x) + g(x) = 3x^3 - x^2 + 4x - 7 = [(2)(x-1)(3)(x-7)]_x.$$

Digital addition is equally easy.

$carry$	1	1	1	
	(1)	$(x-1)$	(4)	$(x-6)$
$+$	(0)	$(x-1)$	$(x-2)$	$(x-1)$
	(2)	$(x-1)$	(3)	$(x-7)$

The rules for **subtraction** of digits, given in Table 3 below, similarly require at most a borrowed digit of 1 from the left (indicated by (b)), which amounts to adding x to the top digit. The analogy is borrowing 1 from the left and adding 10, the base, to the digit that comes up short in ordinary decimal subtraction. If a nonzero digit is to be subtracted from (0), which may itself be preceded by a string of (0)'s, then we borrow (1) from the first nonzero digit to the left of the string of zeros, send it down the line, and never have to borrow from that lender again, as x is larger than any digit. In short, any digit lends 1 to the right at most once.

Table 3. Subtraction of digits in base x

$i \geq j \geq 0$	$j > i \geq 0 \ (b)$	$i > 0, j \geq 0$
$[(i)]_x$	$[(1)(i)]_x$	$[(x-i)]_x$
$[(j)]_x$	$[(j)]_x$	$[(j)]_x$
$[(i-j)]_x$	$[(x-(j-i))]_x$	$[(x-(i+j))]_x$
$i \geq 0, j > 0 \ (b)$	$j \geq i > 0$	$i > j > 0 \ (b)$
$[(1)(i)]_x$	$[(x-i)]_x$	$[(1)(x-i)]_x$
$[(x-j)]_x$	$[(x-j)]_x$	$[(x-j)]_x$
$[(i+j)]_x$	$[(j-i)]_x$	$[(x-(i-j))]_x$

Let us subtract the same two polynomials directly, noting that $f > g$:

$$f(x) - g(x) = x^3 - x^2 + 6x - 5 = [(x-1)(5)(x-5)]_x.$$

Contrast with digital subtraction:

borrow	-1	-1	-1	
	(1)	$(x-1)$	(4)	$(x-6)$
$-$	(0)	$(x-1)$	$(x-2)$	$(x-1)$
	(0)	$(x-1)$	(5)	$(x-5)$

Multiplication in base x is done one digit at a time, followed by staggered addition. Table 4 shows the rules for digit multiplication.

Table 4. Multiplication of digits in base x

$i, j \geq 0$	$i, j > 0$	$i, j > 0$
$[(i)]_x$	$[(x-i)]_x$	$[(x-i)]_x$
$[(j)]_x$	$[(j)]_x$	$[(x-j)]_x$
$[(ij)]_x$	$[(j-1)(x-ij)]_x$	$[(x-(i+j))(ij)]_x$

For the same polynomials f and g as in the last two examples, we find

$$f(x)g(x) = 6 + x - 4x^2 - 7x^3 + 3x^4 - x^5 + 2x^6 \qquad (A.1)$$
$$= [(1)(x-1)(2)(x-8)(x-4)(1)(6)]_x. \qquad (A.2)$$

The first one-digit multiplication is done as follows (the carry digits on top are to be added to the product, as is usual).

		$(x-2)$	(4)	$(x-7)$	
		(1)	$(x-1)$	(4)	$(x-6)$
$\times$					$(x-1)$
	(1)	$(x-3)$	(5)	$(x-11)$	(6)

The second one-digit multiplication is

		$(x-3)$	(4)	$(x-8)$	
		(1)	$(x-1)$	(4)	$(x-6)$
$\times$					$(x-2)$
	(1)	$(x-5)$	(6)	$(x-16)$	(12)

Multiplication by the last digit of g is the same as the first. Finally, we stagger the results and add them.

			(1)	$(x-1)$	(4)	$(x-6)$	
$\times$				$(x-1)$	$(x-2)$	$(x-1)$	
			(1)	$(x-3)$	(5)	$(x-11)$	(6)
		(1)	$(x-5)$	(6)	$(x-16)$	(12)	(0)
$+$	(1)	$(x-3)$	(5)	$(x-11)$	(6)	(0)	(0)
	(1)	$(x-1)$	(2)	$(x-8)$	$(x-4)$	(1)	(6)

Division by a monic polynomial is always possible in $\mathbb{Z}[x]$. (See the Division Algorithm, Theorem 2.4.) For example, for

$$f(x) = 2x^4 - 5x^3 + 7x - 1 = [(1)(x-5)(0)(6)(x-1)]_x$$

and

$$g(x) = x^2 + x - 3 = [(1)(0)(x-3)]_x,$$

we have the long-division quotient and remainder

$$q(x) = 2x^2 - 7x + 13 \text{ and } r(x) = -27x + 38,$$

where $r(x)$ is not positive, but its degree (resp., its "absolute value") is still strictly less than the degree of $g(x)$ (resp., $g(x)$ itself). Hence, we may subtract 1 from the quotient and add $g(x)$ to the remainder, which will immediately give us a positive expression. The adjusted quotient and remainder are then

$$q(x) = 2x^2 - 7x + 13 - 1 = 2x^2 - 7x + 12 = [(1)(x-7)(12)]_x$$

and

$$0 \leq r(x) = (-27x+38)+(x^2+x-3) = x^2-26x+35 = [(x-26)(35)]_x < g(x).$$

F. AKMAN

Digital division yields the result directly, as shown below:

$$
\begin{array}{r}
\quad (1)\quad (x-7)\quad (12) \\
\hline
(1)\,(0)\,(x-3)\,\,\big)\;\;(1)\;(x-5)\quad (0)\quad (6)\quad (x-1) \\
(1)\quad (0)\quad (x-3)\quad (0)\quad (0) \\
\hline
(0)\,(x-6)\quad (3)\quad (6)\quad (x-1) \\
(x-7)\,(x-10)\,(21)\quad (0) \\
\hline
(0)\quad (12)\,(x-15)\,(x-1) \\
(12)\quad (11)\quad (x-36) \\
\hline
(0)\quad (x-26)\quad (35)
\end{array}
$$

REFERENCES

[1] V. Bouniakowsky, *Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs*, Mém. Acad. Sc. St. Pétersbourg, **6** (1857), 305–329.

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

[3] D. Brown, *The Da Vinci Code*, Doubleday, New York, 2003.

[4] M. Cantor, *Vorlesungen über Geschichte der Mathematik*, Vol. 4, B. G. Teubner, Leipzig, 1908, 136–137.

[5] R. Cottle, E. Johnson, and R. Wets, George B. Dantzig (1914–2005), *Notices of the AMS*, **54** (2007), 344–362.

[6] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, 2nd ed., Addison-Wesley, 1981.

[7] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. Reine Angew. Math, **92** (1882), 1–122.

[8] S. R. Lay, *Analysis With An Introduction to Proof*, 5th ed., Pearson, 2013.

[9] M. Mignotte, *Some useful bounds*, Computer Algebra: Symbolic and Algebraic Computation, B. Buchberger et al. (eds.), 259–263, Springer, 1983.

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

[11] J. Pintz, *Landau's problems on primes*, Journal de Théorie des Nombres de Bordeaux, **21.2** (2009), 357–404. `https://eudml.org/doc/10886`.

[12] G. Pólya and G. Szegö, *Problems and Theorems in Analysis*, Vol. 2, Springer-Verlag, 1976, Problem VIII.128.

[13] P. Ribenboim, *The Little Book of Big Primes*, Springer-Verlag, 1991.

[14] B. L. van der Waerden, *Algebra: Volume I*, translated by F. Blum and J. R. Schulenberger, Springer-Verlag, 1991.

MSC2010: 11A41, 11A63, 11N32, 11Y05

DEPARTMENT OF MATHEMATICS, ILLINOIS STATE UNIVERSITY, NORMAL, IL 61790-4520

E-mail address: akmanf@ilstu.edu