Prime Numbers and Irreducible Polynomials

M. Ram Murty

The similarity between prime numbers and irreducible polynomials has been a dominant theme in the development of number theory and algebraic geometry. There are certain conjectures indicating that the connection goes well beyond analogy. For example, there is a famous conjecture of Buniakowski formulated in 1854 (see Lang [**3**, p. 323]), independently reformulated by Schinzel, to the effect that any irreducible polynomial $f(x)$ in $\mathbb{Z}[x]$ such that the set of values $f(\mathbb{Z}^+)$ has no common divisor larger than 1 represents prime numbers infinitely often. In this instance, the theme is to produce prime numbers from irreducible polynomials. This conjecture is still one of the major unsolved problems in number theory when the degree of f is greater than one. When f is linear, the conjecture is true, of course, and follows from Dirichlet's theorem on primes in arithmetic progressions.

It is not difficult to see that the converse of the Buniakowski conjecture is true; namely, if a polynomial represents prime numbers infinitely often, then it is an irreducible polynomial. To see this, let us try to factor $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ of positive degree. The fact that $f(x)$ takes prime values infinitely often implies that either $g(x)$ or $h(x)$ takes the value ± 1 infinitely often. This is a contradiction, for a polynomial of positive degree can take a fixed value only finitely often.

There is a stronger converse to Buniakowski's conjecture that is easily derived (see Theorem 1). To be specific, if a polynomial $f(x)$ belonging to $\mathbb{Z}[x]$ represents a single prime number for some sufficiently large integer value of x, then the polynomial is irreducible. A classical result of A. Cohn (see Pölya and Szegö [**5**, p. 133]) states that, if we express a prime p in base 10 as

$$p = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0,$$

then the polynomial

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

is necessarily irreducible in $\mathbb{Z}[x]$. This problem was subsequently generalized to any base b by Brillhart, Filaseta, and Odlyzko [**1**]. We will give a proof of this fact that is conceptually simpler than the one in [**1**], as well as study the analogue of this question for function fields over finite fields. More precisely, let $\mathbb{F}_q$ denote the finite field of q elements, where q is a prime power. Fix a polynomial $b(t)$ in $\mathbb{F}_q[t]$. Given an irreducible polynomial $p(t)$ in $\mathbb{F}_q[t]$, we write it in "base $b(t)$" as

$$p(t) = a_m(t)b(t)^m + \cdots + a_1(t)b(t) + a_0(t).$$

The analog of Cohn's theorem to be proved in what follows is that

$$f(x) = a_m(t)x^m + \cdots + a_1(t)x + a_0(t)$$

is irreducible in $\mathbb{F}_q[t, x]$. The proof in the function field case is much simpler and is motivated by the following elementary result, which can be viewed as somewhat of a strong converse to the conjecture of Buniakowski.

Theorem 1. *Let* $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ *be a polynomial of degree* m *in* $\mathbb{Z}[x]$ *and set*

$$H = \max_{0 \le i \le m-1} |a_i/a_m|.$$

If $f(n)$ *is prime for some integer* $n \ge H + 2$, *then* $f(x)$ *is irreducible in* $\mathbb{Z}[x]$.

The proof will be based on the following elementary lemma.

Lemma 1. *Let* $f(x) = a_m x^m + \cdots + a_1 x + a_0$ *be of degree* m *and have* α *in* $\mathbb{C}$ *as a root. Then*

$$|\alpha| < H + 1,$$

where H *is defined as in Theorem 1.*

Proof. Clearly,

$$-a_m \alpha^m = a_{m-1}\alpha^{m-1} + \cdots + a_1 \alpha + a_0,$$

so

$$|\alpha|^m \le H\left(|\alpha|^{m-1} + \cdots + |\alpha| + 1\right) = H\left(\frac{|\alpha|^m - 1}{|\alpha| - 1}\right). \tag{1}$$

If $|\alpha| \le 1$, then $|\alpha| < H + 1$ and the conclusion of the lemma is trivial. If $|\alpha| > 1$, then multiplying (1) by $|\alpha| - 1$ we deduce that

$$|\alpha|^{m+1} - |\alpha|^m < H|\alpha|^m,$$

from which $|\alpha| < H + 1$ follows. ∎

The theorem can now be proved using this lemma.

Proof of Theorem 1. If $f(x)$ is reducible in $\mathbb{Z}[x]$, write $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ are of positive degree. Since $f(n)$ is prime, we must have either $g(n)$ or $h(n)$ equal to ± 1. Without loss of generality, we may suppose that it is $g(n)$. We can express g in the manner

$$g(x) = c\prod_i (x - \alpha_i),$$

where c is the leading coefficient of g and the product is over a subset of the complex zeros of f. In view of Lemma 1,

$$|g(n)| \ge \prod_i (n - |\alpha_i|) > \prod_i (n - (H + 1)) \ge 1,$$

which is a contradiction. ∎

Theorem 1 offers a simple irreducibility criterion that is applicable when most traditional tests fail. An example is given by $f(x) = x^4 + 6x^2 + 1$. We leave as an exercise

for the reader to verify that $f(x)$ is reducible modulo p for every prime p (see Lee [**4**]). On the other hand, a simple computation shows that $f(8) = 4481$, a prime, from which the irreducibility of $f(x)$ follows by Theorem 1.

Theorem 1 is not quite adequate to establish Cohn's theorem. In that context, the largest possible value of H is 9, so Theorem 1 would require that n be at least 11 in order for the theorem to be applicable: the fact that $f(10)$ is prime would not be sufficient to ensure irreducibility. Moreover, Theorem 1 is "best possible." Indeed, the polynomial $f(x) = (x-9)(x^2+1) = x^3 - 9x^2 + x - 9$ is reducible with all its coefficients of absolute value at most 9, yet $f(10) = 101$ is prime. This example shows that the positivity of coefficients must enter in a vital way into Cohn's theorem. Indeed, Filaseta extends Cohn's theorem by proving that, if $f(x) = \sum_{j=0}^{n} a_j x^j$ is a polynomial in $\mathbb{Z}[x]$ such that $0 \le a_j \le a_n 10^{30}$ for $0 \le j \le n-1$ and if $f(10)$ is prime, then $f(x)$ is irreducible [**2**].

On the other hand, it is clear that every number can be represented as

$$a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10 + a_0$$

with $-1 \le a_i \le 8$, for the integers belonging to the interval $[-1, 8]$ form a complete set of residue classes modulo 10. If we write our prime p in this "skewed" base 10 notation, then the resulting polynomial is irreducible by our theorem. This remark applies for any base $b \ge 3$. The same reasoning shows that a similar result can be stated for any "balanced" base b representation with

$$p = a_r b^r + a_{r-1} b^{r-1} + \cdots + a_1 b + a_0,$$

where $|a_i| \le b/2$.

We will prove that a slight refinement of Lemma 1 suffices to establish Cohn's theorem. After showing how this can be done, we discuss the case of function fields over finite fields. It turns out that a function field version of Lemma 1 is enough to prove the asserted analogue of the Cohn result.

We begin by indicating how Lemma 1 must be modified in order to obtain Cohn's theorem.

Lemma 2. *Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ belong to $\mathbb{Z}[x]$. Suppose that $a_n \ge 1$, $a_{n-1} \ge 0$, and $|a_i| \le H$ for $i = 0, 1, \ldots, n-2$, where H is some positive constant. Then any complex zero α of $f(x)$ either has nonpositive real part or satisfies*

$$|\alpha| < \frac{1 + \sqrt{1 + 4H}}{2}. \tag{2}$$

Proof. If $|z| > 1$ and $\Re(z) > 0$, we observe that

$$\begin{aligned}
\left|\frac{f(z)}{z^n}\right| &\ge \left|a_n + \frac{a_{n-1}}{z}\right| - H\left(\frac{1}{|z|^2} + \cdots + \frac{1}{|z|^n}\right) \\
&> \Re\left(a_n + \frac{a_{n-1}}{z}\right) - \frac{H}{|z|^2 - |z|} \\
&\ge 1 - \frac{H}{|z|^2 - |z|} = \frac{|z|^2 - |z| - H}{|z|^2 - |z|} \ge 0
\end{aligned}$$

whenever

$$|z| \geq \frac{1+\sqrt{1+4H}}{2}. \tag{3}$$

Consider an arbitrary complex zero α of $f(x)$. If $|\alpha| \leq 1$, (2) holds trivially. Assume that $|\alpha| > 1$. Either $\Re(\alpha) \leq 0$ or (3) must fail for $z = \alpha$, since $|f(z)/z^n|$ is positive whenever $\Re(z) > 0$ and (3) holds. Thus, either $\Re(\alpha) \leq 0$ or α satisfies (2). ∎

We apply Lemma 2 to solve a problem suggested in Pólya-Szegö [**5**, p. 133].

Theorem 2. *Let $b > 2$ and let p be a prime with b-adic expansion*

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0.$$

Then the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is irreducible over $\mathbb{Q}$.

Remark. Theorem 2 is also true for $b = 2$, as follows from Lemma 3 and the discussion following the proof of Theorem 2.

Proof. By a celebrated lemma of Gauss (see Lang [**3**, p. 181]), it suffices to consider reducibility over $\mathbb{Z}[x]$. If $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ nonconstant polynomials in $\mathbb{Z}[x]$, then $f(b) = p$ implies either $g(b) = \pm 1$ or $h(b) = \pm 1$. Without loss of generality we may assume that $g(b) = \pm 1$. As in the proof of Theorem 1, we write

$$g(x) = c \prod_i (x - \alpha_i),$$

where the α_i range over a certain subset of the zeros of f and c is a nonzero integer (namely, the leading coefficient of $g(x)$). By Lemma 2, every zero α of f either has nonpositive real part or has absolute value less than

$$\frac{1+\sqrt{1+4(b-1)}}{2}.$$

In the former case, we plainly have $|b - \alpha| \geq b$; in the latter case, the fact that b is at least 3 gives

$$|\alpha| < \frac{1+\sqrt{1+4(b-1)}}{2} \leq b - 1,$$

as is easily checked. In particular, $|b - \alpha_i| > 1$ for each i, from which we deduce that $|g(b)| > 1$, a contradiction. ∎

A few remarks are in order. First, the proof of Theorem 2 breaks down for $b = 2$. But not all is lost. Since when $b = 2$ the coefficients of the polynomial $f(x)$ are either 0s or 1s and $f(2)$ is prime, we must have $a_0 = 1$. If $f(x)$ has any rational roots, they can only be ± 1. Clearly, $x = 1$ is not a root. If $x = -1$ is a root, then $0 = f(-1) \equiv f(2) \equiv p \pmod 3$, implying that $p = 3$ and $f(x) = x + 1$, which is irreducible. Thus, when $p > 3$, $f(x)$ does not have any rational roots. This itself suffices to confirm the irreducibility of $f(x)$ for $b = 2$ and primes p smaller than 16, since for these primes

the degree of the polynomial is at most 3. To handle the case $b = 2$ in general, a bit more analysis is needed. Suppose that all the roots of $f(x)$ satisfy $\Re(\alpha) < v$. Then it is readily seen that the coefficients of the polynomial

$$g(x + v) = c \prod_i (x + v - \alpha_i)$$

are all nonnegative. Indeed, if α_i is real, the linear polynomial $x + v - \alpha_i$ has nonnegative coefficients. If α_i is not real, we pair it with its complex conjugate and notice that

$$(x + v - \alpha_i)(x + v - \overline{\alpha_i}) = x^2 + 2\Re(v - \alpha_i)x + |v - \alpha_i|^2 \tag{4}$$

has nonnegative coefficients. Observe that $g(x)$ is a polynomial with real coefficients and therefore, if α is a root of $g(x)$, so is $\overline{\alpha}$. As v is real, the same property applies to the polynomial $g(x + v)$. Because $g(x + v)$ is a product of polynomials of type (4), it is a polynomial in x with nonnegative coefficients. Hence $g(-x + v)$ is a polynomial with alternating coefficients. Thus, for any $x > 0$, we have $\pm g(-x + v) < g(x + v)$. Therefore, $|g(-x + v)| < g(x + v)$. If $v < b$, then we set $x = b - v$ to deduce that $|g(-b + 2v)| < g(b)$. If v can be chosen to be $3/2$, then we obtain $|g(1)| < g(2)$. As $g(1) \neq 0$ and this number is an integer, we get $|g(2)| > 1$. The proof of Theorem 2 then applies to establish the irreducibility of $f(x)$. However, the bound given by Theorem 1 is $(1 + \sqrt{5})/2 > 3/2$. This suggests the following refinement of Lemma 2. It is all that is required to extend the proof of Theorem 2 so as to cover the case $b = 2$.

Lemma 3. *Suppose that α is a complex root of a polynomial*

$$f(x) = x^m + a_{m-1}x^{m-1} \cdots + a_1 x + a_0$$

with coefficients a_i equal to 0 or 1. If $|\arg \alpha| \leq \pi/4$, then $|\alpha| < 3/2$. Otherwise $\Re(\alpha) < (1 + \sqrt{5})/(2\sqrt{2})$.

Proof. The cases $m = 1$ and $m = 2$ can be verified directly. Assuming that $m \geq 3$, we compute for $z \neq 0$:

$$\left|\frac{f(z)}{z^m}\right| \geq \left|1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right| - \left(\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^m}\right).$$

For z satisfying $|\arg z| \leq \pi/4$ it is true that $\Re(1/z^2) \geq 0$, so for such z we have

$$\left|\frac{f(z)}{z^m}\right| > 1 - \frac{1}{|z|^2(|z| - 1)} = \frac{|z|^3 - |z|^2 - 1}{|z|^2(|z| - 1)}.$$

The polynomial $f(x) = x^3 - x^2 - 1$ has exactly one real root, and this root is less than $3/2$. Indeed, the derivative of this function is $3x^2 - 2x = x(3x - 2)$, revealing that $x^3 - x^2 - 1$ has negative slope only for x in $(0, 2/3)$. Since the value of $x^3 - x^2 - 1$ at $x = 3/2$ is positive, the one real root lies in the open interval $(2/3, 3/2)$. Therefore, $|f(z)| > 0$ for $|z| \geq 3/2$ and $|\arg z| \leq \pi/4$, whence the first part of the lemma is established. For the second part, we consider the two conditions $|\alpha| < (1 + \sqrt{5})/2$ and $|\arg \alpha| > \pi/4$. It is not difficult to see that these conditions force $\Re(\alpha)$ to be smaller than $(1 + \sqrt{5})/(2\sqrt{2})$. This completes the proof. ∎

The foregoing proof of Theorem 2 is really a motivated account of the proof in [**1**], where the authors adapted the method indicated in [**5**, p. 133] to deal with the general base. Our approach has been more naive and slightly different. The point is that the naive approach to Lemma 1 and Theorem 1 works in the function field case.

There is a natural generalization of Cohn's theorem to the case of function fields over finite fields. Indeed, let $\mathbb{F}_q$ denote the field of q elements with q a prime power. Let K be the field of rational functions $\mathbb{F}_q(t)$. One defines a norm on this field by setting $|f(t)/g(t)| = q^{\deg f - \deg g}$ whenever $f(t)$ and $g(t)$ are polynomials with coefficients in $\mathbb{F}_q$. One considers the completion L of $\mathbb{F}_q(t)$ with respect to this norm, and shows that the norm extends in a natural way to L. If α is algebraic over K, we may take its norm from $L(\alpha)$ to L and thus get an element in L whose norm is well-defined. Then we take the dth root of this norm, where $d = [L(\alpha) : L]$, and define this to be the norm of α. (See Lang [**3**, p. 474] for details.)

It is easy to see that the counterpart of Lemma 1 carries over *mutatis mutandis* to this setting. If we fix a polynomial $b(t)$ of positive degree, then an irreducible polynomial $p(t)$ can be "written in base $b(t)$" via the Euclidean algorithm:

$$p(t) = a_m(t)b(t)^m + \cdots + a_1(t)b(t) + a_0(t).$$

In analogy with the theorem of Cohn, we can inquire if the polynomial

$$f(x) = a_m(t)x^m + \cdots + a_1(t)x + a_0(t)$$

is irreducible in $K[x]$. By factoring the polynomial over the algebraic closure $\overline{K}$ of K, we see as before that any nontrivial factor $g(x)$ of $f(x)$ can be factored as

$$g(x) = c(t)\prod_i (x - \alpha_i(t))$$

for some polynomial $c(t)$. Now

$$|g(b(t))| \geq \prod_i (|b(t)| - |\alpha_i(t)|) > \prod_i (q^{\deg b} - (q^{\deg b - 1} + 1)) \geq 1$$

unless $q = 2$ and $\deg b = 1$. The "fringe" case can be handled very easily by observing that if $\deg b = 1$, then $f(x)$ is the same as $p(x)$ after a linear change of variable. Therefore, we have irreducibility in this case.

As an illustration of the result in the function field case, consider the irreducible polynomial $p(t) = t^4 + t + 1$ over the finite field of two elements. We can expand this in base $b(t) = t^2 + 1$ as $(t^2 + 1)^2 + t$. In this instance, we have $f(x) = x^2 + t$, which is clearly irreducible over $\mathbb{F}_2(t)$.

ACKNOWLEDGEMENTS. I would like to thank David Pollack for bringing Cohn's problem to my attention, and Hershy Kisilevsky, Yu-Ru Liu, and the referee for useful remarks on a preliminary version of this paper.

REFERENCES

1. J. Brillhart, M. Filaseta, and A. Odlyzko, On an irreducibility theorem of A. Cohn, *Canadian J. Math.* **33** (1981) 1055–1059.
2. M. Filaseta, Irreducibility criteria for polynomials with non-negative coefficients, *Canadian J. Math.* **40** (1988) 339–351.

3. S. Lang, *Algebra*, 3rd ed., Addison-Wesley, Reading, MA, 1993.
4. M. A. Lee, Some irreducible polynomials which are reducible mod p for all p, *Amer. Math. Monthly* **76** (1969) 1125.
5. G. Pólya and G. Szegö, *Problems and Theorems in Analysis*, vol. 2, Springer-Verlag, New York, 1976.

M. RAM MURTY is Professor of Mathematics and Queen's National Scholar at Queen's University in Kingston, Ontario, Canada. He received his Ph.D. from MIT in 1980 under the supervision of Harold Stark. He was a member of the Institute for Advanced Study and the Tata Institute of Fundamental Research on numerous occasions. He was E.W.R. Steacie Fellow (1991–93), Killam Research Fellow (1998–2000), and elected Fellow of the Royal Society of Canada (1990). His monograph *Nonvanishing of L-Functions and Applications*, written jointly with V. Kumar Murty and published by Birkhäuser-Verlag, won the 1996 Balaguer Prize.
Queen's University, Kingston, Ontario, K7L 3N6, Canada
murty@mast.queensu.ca