Prime-Producing Cubic Polynomials

JOE L. MOTT, Florida State University, Tallahassee, Florida
KERMIT ROSE, Florida State University, Tallahassee, Florida

Dedicated to Jim Huckaba on the occasion of his retirement

1. Famous Prime-Producing Polynomials

Suppose $f(x)$ denotes a polynomial of degree d with integer coefficients. A basic problem of long standing fascination is that of discovering those polynomials that produce infinitely many prime values. Euclid proved that for the polynomial $f(x) = x$ the sequence

$$f(n) = n, \quad n = 0, 1, 2, \ldots$$

contains an infinite number of primes. Dirichlet's theorem on primes in arithmetic progressions extends Euclid's theorem to polynomials of the form $f(x) = ax + b$ where a and b are relatively prime integers and $a > 0$. Along this line of questioning, not much is known for arbitrary polynomials of degree at least two. Iwaniec [Iwan] proved that if $g(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ where $a > 0$ and c is odd, then there exist infinitely many integers x such that $g(x)$ is either prime or a product of two primes. For more discussion on this type of problem, consult the papers [Bo], [Ga], [Fo], [Sc], [Si], and Chapter 6 of [Ri2].

A second problem concerns polynomials (especially those of degree $d = 2$) that produce *consecutive* prime values for all integers x in some interval. Leonard Dickson traced the early history of research on this problem in Chapter XVIII of [Di1, p.420]. In 1772, Euler [Eu] noted that

$$E(x) = x^2 - x + 41 \text{ produces 40 distinct primes}$$
$$\text{for integers } x = 1, \ldots, 40.$$

Similarly, in 1798, Legendre [Leg] observed that $L(x) = x^2 + x + 41$, $2x^2 + 29$, and $x^2 - x + 17$ produce distinct primes for all integers x in the intervals $[0, 39]$, $[0, 28]$, and $[0, 16]$, respectively. Moreover, Legendre gave a method for finding other prime-producing polynomials.

In retrospect, it is not surprising that $L(x)$ generates numerous primes since $L(x) = E(x+1)$. Indeed the close connection of these two polynomials may explain why $L(x)$ has come to be called *Euler's polynomial* (see, for example [AC], [Ri1], or [Sc]).

In 1899, Escott [Es] noted that $L(x)$ produces primes not only for $x = 0, 1, \ldots, 39$, but also for $x = -1, -2, \ldots, -40$. Hence, replacing x by $x - 40$ gives the polynomial $x^2 - 79x + 1601$ which produces primes over the interval $[0, 79]$. Then in 1912, Miot

[Mio] stated that the polynomial $x^2 - 2999x + 2248541$ is prime for each integer x in the segment $[1460, 1539]$. Miot's polynomial is just $L(x - 1500)$. While these two polynomials generate 80 consecutive prime values, the number 40 of the *distinct* prime values remains the same as for $L(x)$. Recently Mollin [Mo1] listed an infinite family of polynomials $g_n(x) = L(3x - 39 - 3n)$ where each $g_n(x)$ generates forty, consecutive distinct prime values. The polynomial $g_0(x) = 9x^2 - 231x + 1523$ is the one discovered by Higgins [Hi] in 1982. Other polynomials can be obtained from Euler's polynomial by a change of variables (see Mollins's paper [Mo1] or his book [Mo2, p.105]. In any case, many have noted that the prime-producing capacity of these polynomials has less to do with their *form* than with their *discriminant*.

Table 1

Polynomial	discriminant
Euler	-163
Legendre	-163
Escott	-163
Miot	-163
Higgins	$-3^2(163)$

DEFINITION. When polynomials produce a sequence of distinct primes for a string of values starting with $x = 0$, then the sequence is called an *initial string of distinct primes*.

2. The Relationship of Prime-Producing Quadratic Polynomials to Class Numbers

Out of these investigations came the third problem of characterizing those prime integers p for which

$$f_p(x) = x^2 + x + p \text{ produces an initial string of distinct primes}$$
$$\text{for integers } x \in [0, p-2].$$

Since $f_p(p-1) = p^2$, these polynomials are optimally prime-producing. Kaplansky and Herstein [KH, p.38] called such integers p *lucky numbers*. Euler had discovered that the primes $p = 2, 3, 5, 11, 17, 41$ are lucky. In fact, if an integer p is a lucky number, then p must be the first of a pair of twin primes and if $p > 5$, then $p \equiv 1 \pmod 2$, $p \equiv 2 \pmod 3$, and $p \equiv 1 \text{ or } 2 \pmod 5$; other congruence conditions can be added as well so one should expect that lucky numbers are rare. Dickson reports that H. LeLasseur verified in 1879 that there are no lucky numbers between 41 and 54000 and that Escott in 1910 examined values for p much beyond 54000 without finding a lucky prime. Then in 1936 D. H. Lehmer [LeD] showed that if there were any other lucky numbers they would have to exceed 1250000000. Continued investigation revealed no new lucky numbers. Then the question became: *Are* *these six the only lucky numbers?* The answer remained a mystery until 1966 when Baker [B1] and Stark [Star1] showed it was yes. The story has been told many times about how this fact is intimately linked to the solution of what is now referred to as *Gauss' class number one problem for imaginary quadratic fields*; we repeat part of it here to set the stage for our later discussion; see Goldfeld's excellent article [Gol] for a more complete history.

THEOREM 1. Let p be a prime integer. Then the following are equivalent:

(1) $p = 2, 3, 5, 11, 17, 41$.

(2) p is a lucky number.

(3) The ring of algebraic integers R_p in $F_p = \mathbb{Q}(\sqrt{1-4p})$ is a unique factorization domain.

Let us review some basic facts. First, it is well known that the ring R of algebraic integers in any finite extension field over the rational field $\mathbb{Q}$ is a Dedekind domain and R is a unique factorization domain if and only R is a principal ideal domain if and only if the class number of R is one. Second, a polynomial $f(x) \in R[x]$, where R is an integral domain, is *irreducible* if and only if its only divisors in $R[x]$ are units and associates [unit multiples of $f(x)$].

Sketch of the proof of Theorem 1. As we have seen, (1) implies (2) is a simple verification. Moreover, (3) is an easy consequence of (2) since $f_p(x)$ is irreducible modulo q for each prime q that is bounded above by the *Minkowski bound* $M(F_p)$ for the field F_p [Lan, p.119]. This means that these primes q generate prime ideals in the ring of integers R_p and this fact implies that R_p is a principal ideal domain (see [ST, p. 193-194]). In the year 1912, Frobenius [Fr1] and Rabinowitsch [Ra] first proved that (3) implies (2). Rabinowitsch announced his result at the Fifth International Congress of Mathematicians in 1912, and the article by Frobenius appeared in that same year. Unaware of the earlier proofs by Frobenius and Rabinowitsch, Szekeres [Sz] gave a proof in 1974. Then Ayoub and Chowla [AC] gave a short proof using only elementary properties of quadratic fields. A simple proof can be found in [Co, p. 156]; see also the articles by Ribenboim [Ri1] and Fendel [Fe].

That (3) implies (1) is contained in the following theorem.

THEOREM 2. (Gauss' Class Number One Problem for Imaginary Quadratic Fields). There are exactly nine imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ with class number one where d is a square-free integer. They correspond to $-d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

Note that for $p = 2, 3, 5, 11, 17, 41$, then $1 - 4p$ are the last six of the nine numbers in Theorem 2. Theorem 2 was proved independently by Heegner [Hee] in 1952, and Baker [B1] and Stark [Star1] in 1966. Heegner's proof contained some steps which were unclear and his proof was generally discounted at the time. Heegner died before Deuring [De] cleared up the questionable steps in 1968. All proofs of Gauss' class number one problem are quite deep; Heegner's and Stark's proofs appeal to the theory of elliptic modular functions while Baker's proof involves consideration of lower bounds on linear forms of three logarithms. Nice surveys of the solution can be found in [Star2], [Star3], or [Gol].

From 1969 to 1975 Baker [B2, B3], Stark [Star4, Star5] and Montgomery and Weinberger [MonWe] classified all 18 imaginary quadratic number fields of class number two. In the process Hendy [Hen] extended the Frobenius-Rabinowitsch result to prove that the only quadratic fields $F = \mathbb{Q}(\sqrt{D})$, with $D < 0$, having class number $h_F = 2$ are the fields of three types:

$$-D = 2p, \text{ where } p \text{ is an odd prime.} \tag{I}$$

$$-D = p, \text{ where } p \text{ is a prime, } p \equiv 1 \pmod 4. \tag{II}$$

$$-D = pq \equiv 3 \pmod 4, \text{ where } p < q \text{ are odd primes.} \tag{III}$$

For each one of the three types of fields, let

$$\begin{aligned} f_I(x) &= 2x^2 + p, \text{ where } p \text{ is an odd prime,} \\ f_{II}(x) &= 2x^2 + 2x + (p+1)/2, \text{ where } p \text{ is a prime, } p \equiv 1 \pmod 4, \\ f_{III}(x) &= px^2 + px + (p+q)/4, \text{ where } p < q \text{ are primes,} \\ &\quad pq \equiv 3 \pmod 4. \end{aligned}$$

Then, building on the work of Euler and Frobenius, Hendy showed that

$$\begin{aligned} &f_I(x) \text{ produces primes for } x = 0, 1, \ldots, p-1 \\ &\qquad \text{if and only if } p = 3, 5, 11, 29. \\ &f_{II}(x) \text{ produces primes for } x = 0, 1, \ldots, (p-3)/2 \\ &\qquad \text{if and only if } p = 5, 13, 37. \\ &f_{III}(x) \text{ produces primes for } x = 0, 1, \ldots, [(p-3)/4] - 2 \\ &\qquad \text{if and only if } (p, q) = (3, 5), (3, 17), (3, 41), (3, 89), \\ &\qquad (5, 7), (5, 23), (5, 47), (7, 13), (7, 61), (11, 17), (13, 31). \end{aligned}$$

Other investigations have centered around the relationship between quadratic polynomials producing an initial string of primes and the class number of corresponding number fields (see Chapters 4 and 5 of [Mo2] and Chapters 3 and 6 of [Ri2]). For example, in [MolWi1], Mollin and Williams transpose the Frobenius-Rabinowitsch result to the real quadratic case and obtain a characterization for the class group of certain real quadratic fields to be one.

3. Remaining Problems

Several problems about prime-producing polynomials remain. We mention three. First Problem: Are there polynomials of the form $f_p(x) = x^2 + x + p$ that generate primes for all integers in the interval $[0, B]$ where $40 \leq B < p - 2$? Lukes, Patterson, and Williams [Lu] have shown that, if p exists, then $p > 10^{18}$.

Second Problem: For quadratic polynomials of any form, are there any which produce an initial string of distinct primes of length > 40? Ribenboim reports that Ruby, Fung, and S.M. Williams discovered four quadratic polynomials that produced, respectively, an initial string of prime values of length 45, 43, 43, and 45 (see [Ri2, p.203]and [MolWi2]).

Third Problem: Determine the distribution of prime values of polynomials over intervals. Karst [K1, K2], Lehmer, Lehmer and Shanks [LLS], and Fung and Williams [Fu] formulate the problem in terms of finding polynomials which produce a "high density of primes" in an interval. Ribenboim [Ri2, p.203] formulates it in terms of finding "champion" polynomials in *prime-producing races*. Given N and $d \geq 1$, the "champion" polynomial is one, with integer coefficients and degree d, that produces the largest number of (not necessarily distinct) prime values in the interval $[0, N]$.

"High density" is like beauty; it's in the eye of the beholder. Several authors considered the case where $d = 2$ and $N = 99$. In 1936 Lehmer [LeD] found ten polynomials of the form $x^2 + x + A$ where the percentage of primes ranged from 39 to 74 in $[0, 99]$. In 1938, Beeger [Be] showed that $x^2+x+27941$ produced 77 primes in $[0, 99]$. Boston and Greenwood [BoG] showed that $E(x - 34) = x^2 - 69x + 1231$ where $E(x)$ is Euler's polynomial, represents 95 primes in the interval $[0, 99]$. Then Karst [K2] showed that $2x^2 - 199$ produced 87 primes in the range $[0, 99]$ while $x^2 + x + 41$ gave 86 primes in the same range. Boston and Greenwood leave the challenge at the end of their paper of finding quadratic polynomials which generate 100 primes in the interval $[0, 99]$.

Karst [K1] defined high density to be at least 60% in the interval $[0, 159]$ and found several such polynomials of the form x^2+x+A, where A is negative. Goetgheluck [Goe], in studying cubic polynomials, set the bar at 75% in the interval $[0, 99]$. Fung and Williams [Fu] consider the density of polynomials $f_p(x) = x^2 + x + p$ and show that $f_{27941}(x)$ and $f_{41}(x)$ produce, respectively, 286128 and 261080 primes in the interval $[0, 1000000]$.

Here we see a distinction between producing an initial string of primes and producing a high density of primes in an interval. The polynomial $f_{41}(x)$ produced an initial string of primes of length 40 while $f_{27941}(x)$ produced an initial string of length only five. Nevertheless the latter polynomial produced 25048 more primes in the interval $[0, 1000000]$.

Given any collection of primes $p_1, p_2, \ldots, p_k$, then Lagrange Interpolation will give a polynomial $f(x)$ of degree $\leq k - 1$ such that $f(i) = p_i$. But unfortunately, a polynomial constructed in this fashion need not have integer coefficients and its degree could be as large as $(k-1)$.

Chang and Lih [CL] prove that for any prime p, there exists a polynomial $h_p(x)$ with integer coefficients such that $h_p(0) = p$ and $h_p(x)$ produces $p-1$ distinct primes as x increases from 1 to $p-1$. Their result says nothing about the degree of $h_p(x)$. Let its degree be d and let $N = p$. Then for that d and N, $h_p(x)$ is certainly the "champion".

4. Prime-Producing Polynomials of Higher Degree

Ribenboim [Ri2, p. 203] asserts that polynomials of degree greater than or equal to two often have composite values. He cites [Ri2, p. 387] two important theorems, by Nagell [N] and Heilbronn [Hei], which show that $f(x)$ has "few" prime values.

We combine the two theorems into one. The first statement, Heilbronn's Theorem, is a more precise version of the second statement, the earlier theorem due to Nagell. First, we describe the notation: If $f(x)$ has degree ≥ 2 and integral coefficients, then for every number $N \geq 1$, let

$$\pi_f(N) = |\{m : 1 \leq m \leq N, \text{ absolute value of } f(m) \text{ is prime}\}|.$$

THEOREM 3 (Nagell-Heilbronn). There exists a positive constant C (depending on $f(x)$), such that

$$\pi_f(N) \leq C(N/\log N), \text{ for every } N \geq 1.$$

Hence,

$$\lim_{N\to\infty} \pi_f(N)/N = 0.$$

It would seem that the results of Nagell and Heilbronn conspire to hinder a polynomial $f(x)$ from producing a high density of distinct prime values in an interval $[0, N]$ and so certainly puts some restriction on the length of an initial string of primes. The extent of what those restrictions are for cubic polynomials is not clear at this point. Nevertheless, we have discovered several new cubic polynomials that produce strings of primes of length at most thirty-nine. We will list these polynomials in §5, but now we review the previous contribution of other authors.

4.1. History of Prime-Producing Cubic Polynomials. Dickson reports [Di1, p.420] that Escott [Es] found that $f_1(x) = x^3 + x^2 + 17$ is prime for all integers in the interval $[-14, 10]$ and if x is replaced by $x - 10$ in $f_2(x) = x^3 - x^2 - 17$, then the polynomial $f_3(x)$ is prime for all integers in the interval $[0, 24]$. Dickson's assertion is incorrect as stated but it is correct if "prime" is replaced by "noncomposite" (that is, prime or unit) because $f_1(-3) = -1$, $f_2(3) = 1$ and $f_3(13) = 1$. Actually $f_1(x)$ is prime for all integers in the interval $[-2, 10]$ and $f_2(x)$ is prime for all integers in the interval $[4, 14]$. On page 203 of [Ri2], Ribenboim lists two cubic polynomials discovered by Goetgheluck [Goe]:

$$x^3 - 34x^2 + 381x - 1511$$

and

$$2x^3 - 45x^2 + 331x - 3191$$

that assume prime values at $0, 1, \ldots, 25$. Goetgheluck lists a table of 21 cubic polynomials that produce at least 75 primes in the interval $[0, 99]$. The above two polynomials were obtained from (14) and (15) in his table by replacing x by $x + 16$ in (14) and by $x + 74$ in (15).

Goetgheluck also discovered that the absolute value of the polynomial

$$2x^3 - 83x^2 + 1157x - 4999$$

gives distinct primes at integers $x \in [0, 33]$, and in the race among his 21 prime-producing cubic polynomials with $N = 499$, the champion was

$$2x^3 - 489x^2 + 39847x - 108453$$

which assumes 267 prime values.

4.2. What Enhances Prime Production? If there are theoretical results that tend to hinder prime production, and yet prime-producing polynomials do exist, what, then, *causes* a polynomial to produce an initial string of primes of a certain length? What *enhances* prime production?

We have seen that for certain classes of quadratic polynomials (like $f_p(x) = x^2 + x + p$ where p is a lucky number or Hendy's polynomials $f_I(x) = 2x^2 + p$ for $p = 3, 5, 11, 29$, $f_{II}(x) = 2x^2 + 2x + (p + 1)/2$ for $p = 5, 13, 37$, or $f_{III}(x) = px^2 + px + (p + q)/4$ for $(p, q) = (3, 5), (3, 17), (3, 41)$, $(3, 89)$, $(5, 7)$, $(5, 23)$, $(5, 47)$, $(7, 13)$, $(7, 61)$, $(11, 17)$, $(13, 31)$), prime production is related to the class number in a corresponding number field. But are there other contributing factors? For example, in the sketch of the proof of Theorem 1, we observed that $f_p(x)$ is irreducible modulo q for each prime $q < p$, and that fact contributed to the conclusion that the class number $h = 1$ for the ring of algebraic integers in $\mathbb{Q}(\sqrt{1 - 4p})$.

Lucky primes also have other rather unusual properties. For example, each of those six lucky primes $p = 2, 3, 5, 11, 17, 41$ are such that the number $p^* = 4p - 1$ is also prime and the five odd cases for p are such that $p^* \equiv 3 \pmod 8$.

DEFINITION. For p an odd prime, let $\ell(p)$ be the least positive prime q such that the Legendre symbol $(\frac{q}{p}) = 1$.

Chowla, Cowles, and Cowles [CCC] give an elementary proof that for primes $p^* > 3$ and $p^* \equiv 3 \pmod 8$, $\ell(p^*) = (p^*+1)/4$ if and only if the class number $h(-p^*) = 1$. The results of Baker and Starks then show that the condition $\ell(p^*) = (p^*+1)/4$ means $p^* = 11, 19, 43, 67, 163$ or that $p = (p^*+1)/4 = 3, 5, 11, 17, 41$.

The question is: Can properties, analogous to any of these, be used to contribute to prime production in other classes of polynomials?

4.3. Irreducibility. We address only the irreducibility question. If $f(x)$ is a reducible polynomial of degree $d \geq 1$ with integer coefficients, we should not expect the sequence of values, $f(k)$ for k an integer, to have many noncomposite elements. For example, the reducible polynomial $(x^2+2)(x^2+3)$ is always composite. To make the idea more precise, we reproduce the proof of a well-known fact, published first by Stackel in 1918 [Stac].

THEOREM 4 (Stackel). Suppose that $f(x)$ is a reducible polynomial with integer coefficients and degree d. Then:

1. $f(x)$ produces at most $2d$ prime values, and
2. there is a bound B such that $f(x)$ is composite for all integer values x such $|x| > B$.

PROOF. If $f(x)$ is reducible, then $f(x) = g(x)h(x)$, for polynomials $g(x)$ and $h(x)$ of positive degree. For an integer k, $f(k)$ will generally be composite, since $g(k)h(k)$ represents a prime if and only if one of the factors is a prime and the other is ± 1. But there are only finitely many values of x for which one of these factors can be ± 1, namely the integral roots of the equations

$$g(x) = \pm 1 \text{ and } h(x) = \pm 1.$$

In fact, there can be at most degree $g(x)$ integral values such that $g(x) = 1$ and such that $g(x) = -1$. The proof is similar for $h(x)$. Thus, the number of integral roots of these four equations is at most $2d$.

For the second part of the theorem, it is clear that as soon as the absolute value of k exceeds the absolute value of the largest integral root of the equations

$$g(x) = \pm 1 \text{ and } h(x) = \pm 1,$$

$f(k)$ must be composite. □

There are several results in the literature which improve upon Stackel's Theorem. Let P_f and U_f denote, respectively, the number of primes and the number of units among the values of $f(x)$. Brown and Graham [BrG] prove:

$$\text{If } P_f + 2U_f \geq d+5, \text{ then } f(x) \text{ is irreducible.}$$

In particular, $f(x)$ is irreducible if $f(m)$ is prime for at least $d+5$ values of m (see [O] and [BrG]). Thus, a cubic polynomial is irreducible in $\mathbb{Z}[x]$ if it produces at least eight prime values.

In fact, under certain conditions, we can conclude that $f(x)$ is irreducible if it produces just one prime. We mention Polya and Szego's Theorem [PS, p.350, Theorem 127]. They prove that $f(x)$ is irreducible if it satisfies these three conditions:

$$f(k) \text{ is a prime for some integer } k, \tag{1}$$

$$\text{the zeros of } f(x) \text{ lie in the half-plane } \mathbb{R}x < k - 1/2, \text{ and} \tag{2}$$

$$f(k-1) \neq 0. \tag{3}$$

Other results can be found in Brillhart, Filaseta, and Odlyzko [BFO] and [Mona].

APPLICATION. One interesting application of Polya-Szego's Theorem is credited to A. Cohn [PS, p.350]. Let the prime p be expressed in its decimal form $p = \sum_{k=0}^{n} a_k 10^k$, where $0 \le a_k \le 9$. Then the polynomial $f(x) = \sum_{k=0}^{n} a_k x^k$ is irreducible in $\mathbb{Z}[x]$.

We give an elementary application in terms of the sum of the coefficients of $f(x)$.

THEOREM 5. Let $f(x) = Ax^3 + Bx^2 + Cx + D$ where the coefficients are positive integers and $BC > AD$. If the sum of the coefficients $A + B + C + D$ is prime, then $f(x)$ is irreducible.

PROOF. The conditions on the coefficients mean that $f(x)$ satisfies the Routh-Hurwitz criterion [Mig, p.210] so that all the roots of $f(x)$ have negative real part. Since f(1) is prime, Polya-Szego's Theorem implies that $f(x)$ is irreducible. □

EXAMPLES. The polynomials $f(x) = x^3 + 3x^2 + 4x + 5$ and $g(x) = 623x^3 + 200x^2 + 5x + 1$ are irreducible since $f(1) = 13$ and $g(1) = 829$ are primes. In fact, given any positive A, C, D, then there exists infinitely many B such that $f(x) = Ax^3 + Bx^2 + Cx + D$ is irreducible. Moreover, this idea can be extended to polynomials of degree greater than 3.

Now we return to the general discussion. We know that if $f(x)$ produces at least $d + 5$ distinct prime values, then $f(x)$ is irreducible in $\mathbb{Z}[x]$. But, as you might suspect, irreducibility alone is not enough to guarantee that $f(x)$ will produce any primes at all, much less, an initial string of prime values. For example, the irreducible polynomial $f(x) = x^2 + x + 4$ is such that its values are even for every integral x and never equals ± 2.

Indeed, since the "average" polynomial of degree d is irreducible [Bro], there must be other properties that contribute to the ability to produce primes. Thus, we pose the question in reverse: *If $f(x)$ is irreducible, what additional properties must $f(x)$ satisfy in order to produce a high density of primes in an interval and, in particular, what properties will insure that $f(x)$ will produce an initial string of primes, say, of length at least $d + 5$?*

Of course, in order to produce an initial string of primes certain *extrinsic* properties must be satisfied. For example, if $f(x) = x^3 + Px + Q$ is to generate an initial string of primes, then the sequence of initial values

$$Q,\ 1+P+Q,\ 8+2P+Q,\ \text{etc., must all be prime.}$$

Thus, the coefficients of $f(x)$ must satisfy certain specific relationships in order to produce an initial string of primes. But are there also certain *intrinsic* properties that $f(x)$ must satisfy in order to produce a high density of primes in an interval? Or negatively: What intrinsic properties prevent the production of strings of primes?

4.4. Existence of Prime Divisors. Specifically, if $f(x)$ produces enough primes to be irreducible in $\mathbb{Z}[x]$, does it follow that $f(x)$ is irreducible modulo q for certain primes q? In medical terms, if producing at least $d+5$ primes is the "disease", and irreducibility in $\mathbb{Z}[x]$ is the "infection", does the "infection" spread to the polynomial ring over the integers modulo q for some primes q? The answer is no; in fact, it may happen that $f(x)$ is reducible modulo q for every prime q.

EXAMPLE. The polynomial

$$\begin{aligned} f(x) = x^{15} &+ 6x^{13} + 7x^{11} - 21x^{10} - 109x^8 - 17x^7 - 144x^6 \\ &- 355x^5 - 48x^4 + 103x^3 + 5x^2 - 56x + 29 \end{aligned}$$

produces 31 primes from $x = -50$ to 70, and, in particular, a string of primes from -3 to 5. Thus, $f(x)$ is irreducible in $\mathbb{Z}[x]$. But $f(x)$ is reducible modulo every prime q [Bra]. But of the primes q between 2 and 97, $f(x)$ has a root modulo q only for $q = 23$, 29, 31, 61, 67, 71, and 97.

Suppose that a prime q divides $f(b)$ for some integer b. If $f(b) \neq \pm q$, then $f(b)$ is composite, and $f(x)$ *cannot* produce an initial string of primes of length greater than $b-1$. Moreover, other values of $f(x)$ are known to be composite; for, q also divides $f(b_1)$ for any b_1 in the residue class of b in $\mathbb{Z}_q$. Therefore, $f(b+kq)$ will be composite, for $k \in \mathbb{Z}$, if $f(b+kq) \neq \pm q$. If the leading coefficient of $f(x)$ is positive, then the possibility that $f(b+kq) \neq \pm q$ can be settled at the outset since $f(x)$ is an increasing function to the right of the maximal real part of its zeros.

DEFINITION. We say that a prime q is a *prime divisor* of $f(x)$ if any of the following equivalent conditions are satisfied for some integer b:

1. q divides $f(b)$
2. $f(b) \equiv 0 \pmod{q}$
3. $f(x) \equiv (x-b)g(x) \pmod{q}$
4. the residue class of b modulo q is a root of $f(x)$ considered as a polynomial in $\mathbb{Z}_q[x]$, where $\mathbb{Z}_q$ is the ring of integers modulo q.

Of course, if q is a prime divisor, then we may assume that $0 \leq b < q$.

Therefore, the existence of prime divisors (rather than reducibility modulo q *per se*) will prevent long strings of prime values. Then on the heels of that deduction comes this new question: Is it possible that some polynomials $f(x)$ have no roots modulo q for *every* prime q? Frobenius [Fr2] proved in 1896 that the answer to this question is also no. Schur proved a special case of it in 1912; see [GB] for a simple proof of Schur's version.

THEOREM 6 (Frobenius). Every nonconstant polynomial $f(x) \in \mathbb{Z}[x]$ has an infinite number of prime divisors q for which $f(x)$ splits completely modulo q.

We recently learned the following Theorem 7 and its proof from Robert Gilmer who, in turn, learned it from Dennis Estes. But, after searching the literature, we discovered that the result dates back to a previous generation. Iwata [Iwat] gave simple proofs of Theorems 6 and 7 in 1971, and in his review of [Iwat], Gerst attributes both results to Frobenius [Fr2].

THEOREM 7 (Frobenius). Suppose $f(x) \in \mathbb{Z}[x]$ is an irreducible polynomial of degree $d \geq 2$. Then $f(x)$ fails to have a root modulo q for infinitely many primes q.

PROOF. The proof depends on the classical Frobenius Density Theorem. Suppose there are only finitely many primes q such that $f(x)$ fails to have a root modulo q. Then that set of primes is a set of Dirichlet density 0. Then Corollary 16.6.2 of [Ma, p.153] implies that $f(x)$ is reducible. $\square$

4.5. Irreducibility of Polynomials of Degree Two or Three in $\mathbb{Z}_q[x]$. The polynomial $f(x) = 2x^2 + 3$ is such that modulo 2, we get the constant polynomial 1, and then the discussion of reducibility or irreducibility is meaningless. But if $f(x)$ has degree 2 or 3 and the degree of $f(x)$ modulo q is at least 2, then $f(x)$ is reducible modulo q if and only if $f(x)$ has a root modulo q. Applying the above theorems of Frobenius to the case of polynomials of degree 2 or 3, we get:

COROLLARY 8. Suppose $f(x) \in \mathbb{Z}[x]$ is an irreducible polynomial of degree 2 or 3. Then there exist infinitely many primes q such that $f(x)$ is irreducible modulo q and infinitely many primes q^* such that $f(x)$ has a root modulo q^*.

PROOF. We might as well consider those primes q for which the leading coefficient is nonzero modulo q. Then the result is immediate.

$\square$

On the basis of Corollary 8, we make two observations:

OBSERVATION 1. Suppose the degree of $f(x) \in \mathbb{Z}[x]$ is 2 or 3 and for each prime q such that $2 \le q \le B$, the degree of $f(x)$ modulo q is at least 2. Suppose $|f(x)|$ is a prime $> B$ for each integer $x \in [0, B]$. Then $f(x)$ must be irreducible modulo q for primes q such that $2 \le q \le B$. This is because if $f(x) \equiv (x-b)g(x) \pmod q$ for a prime q such that $2 \le q \le B$ and $0 \le b < q$, then $f(b) = qt$, for some integer t, and $f(b)$ is an associate of a prime so t is a unit. But then $|f(b)| = q$ is not greater than B.

OBSERVATION 2. Suppose B is a positive integer and $f(x) = Px^3+Qx^2+Rx+S \in \mathbb{Z}[x]$ is increasing and positive over the interval $[0, B]$. Suppose $f(x)$ modulo q is irreducible of degree at least 2 for each prime $q < PB^3 + QB^2 + RB + S$. Then $f(x)$ is noncomposite for each integer $x \in [0, B]$. This is because if $f(b)$ is composite, for $b \in [0, B]$, then $f(b) = Pb^3+Qb^2+Rb+S = qt \le PB^3+QB^2+RB+S$ for some prime q. But $f(b)$ composite implies t is not ± 1, and $f(x)$ positive implies t is positive so $q < PB^3+QB^2+RB+S$. Yet $f(x) \equiv (x-b)g(x) (\mathrm{mod}\ q)$, where degree $g(x)$ is at least 1, means $f(x)$ is not irreducible modulo q.

In topological terms, the "local" result of the existence of a prime divisor for $f(x)$ is something that prevents the "global" result of long strings of primes. Therefore irreducibility modulo q for many small primes q, at least for polynomials of degree 2 or 3, is a finger of truth pointing in the direction of prime production.

The conditions of Observations 1 and 2 are not vacuous.

EXAMPLES. (1) Consider the polynomial $f(x) = x^3 + x^2 + 17$. Then $f(x)$ is prime greater than 17 for each integer $x \in [0, 10]$ so let $B = 10$. The first prime for which $f(x)$ is reducible is 13.

(2) The polynomials $f_p(x) = x^2 + x + p$, for p a lucky prime, satisfy the conditions of Observation 1 where $B = p - 2$.

(3) Let $f(x) = 98x^3 - 257x^2 + 175x + 1$. The $f(x)$ is irreducible modulo all primes $q \le 13$, and by taking derivatives, we see that $f(x)$ is increasing for $x \ge 0$ and $f(0) = 1$ so $f(x)$ is positive for $x \ge 0$. Furthermore, $f(0) = 1$, $f(1) = 17$, so the conditions of Observation 2 are satisfied for $B = 1$.

(4) Nevertheless, there are situations not covered by Observation 2. For example, $f(x) = x^3 - x^2 - 17$ is such that $f(x)$ is noncomposite for each integer $x \in [0, 14]$ but $f(x)$ is not positive nor increasing in $[0, 14]$ and $f(x)$ is reducible modulo 13.

4.6. Quadratic Residues. Suppose $f(x) \in \mathbb{Z}[x]$ has degree two. It is well known that the number of roots of $f(x)$ modulo a prime q can be reformulated in terms of the Legendre symbol. In fact, $f(x)$ has repeated, two distinct, or zero roots modulo a prime q according as the Legendre symbol $(\frac{D}{q}) = 0, 1, -1$, where D is the discriminant of $f(x)$. Therefore, a quadratic polynomial $f(x)$ is irreducible modulo q if and only D is a quadratic nonresidue modulo q or equivalently if the Legendre symbol $(\frac{D}{q}) = -1$.

Suppose further that $f(x)$ is monic and irreducible in $\mathbb{Z}[x]$, F is the quadratic field extension obtained by adjoining a root of $f(x)$ to $\mathbb{Q}$, and R is the integral closure of $\mathbb{Z}$ in F. If Δ is the discriminant of an integral basis for R, then $D = s^2\Delta$, where s is an integer, and the prime decomposition of qR is completely determined by the Legendre symbol $(\frac{\Delta}{q})$: q splits, ramifies, or is inert if and only if $(\frac{\Delta}{q})$ is, respectively, 1, 0, -1.

Considerable research about quadratic polynomials $f(x)$ modulo a prime q has been formulated in terms of quadratic residues. We will mention four items.

First, Euler hit upon the remarkable fact that the polynomials $f_p(x) = x^2 + x + p$, where p is one of the 6 lucky numbers 2, 3, 5, 11, 17, 41, are such that $(\frac{D}{q}) = -1$ for each prime q between 2 and $p - 2$. Thus, $x^2 + x + 41$ is irreducible modulo q for every prime q between 2 and 37 since $(\frac{-163}{q}) = -1$ for each such prime.

Second, it has long been known that there is a strong connection between the class number of quadratic fields and the distribution of quadratic residues. This connection is exemplified, for instance, by Dirichlet's class number formula [BS, p.342-347], which formed the basis of much of the work on the subject of class numbers.

Third, Mollin and Williams [MolWi3] show that for three classes of quadratic polynomials $f_d(x) = -x^2 + x + (d-1)/4$, $-2x^2 + d/2$, $-2x^2 + 2x + (d-1)/2$, prime production in a certain interval is equivalent to the fact that $(d/p) = -1$ for all primes p less than, respectively, $(\sqrt{d-1})/2$, $(\sqrt{d})/2$, $(\sqrt{d-2})/2$. (The number d satisfies certain restrictions as well.)

Finally, regarding the number of prime values of a quadratic polynomial, Hardy and Littlewood [HL] formulated their Conjecture F in terms of quadratic residues.

4.7. Point of View. In considering the density of primes for polynomials $f_p(x) = x^2 + x + p$, Lehmer [LeD], Lehmer, Lehmer, and Shanks [LLS], and Fung and Williams [FW] accept Conjecture F's prediction and require $(\frac{D}{q}) = -1$ for as many small primes q as possible, where $D = 1 - 4p$ is the discriminant of $f(x)$. Their point of view is that if $(\frac{D}{q}) = -1$, then q cannot divide the composite values of $f_p(x)$, and, thus, the values that $f_p(x)$ can assume are considerably restricted and, therefore, should frequently be prime.

Using their work on polynomials $f_p(x)$ as a template, we take the same point of view and impose the criterion that a polynomial $f(x)$ of arbitrary degree be irreducible for all primes q between 2 and B. Then we expect that criterion should increase the density of primes assumed over $[0, B]$ and, therefore, increase the chances that $f(x)$ will produce an initial string of prime values.

4.8. Probability. From this perspective, we give a heuristic argument that the probability is quite small that a randomly selected cubic polynomial is irreducible modulo q for the first k primes where $k \geq 5$. Thus, we believe that while an "average" cubic polynomial in $\mathbb{Z}[x]$ is irreducible, it is not likely that it is irreducible modulo the first k primes.

Let F be the Galois field with q elements. Define $\mathbb{N}_q(d)$ = the number of monic irreducible polynomials of degree d in $F[x]$. If Prob(d, irred; q) denotes the probability that a monic polynomial of degree d is irreducible in $F[x]$, then

$$\mathrm{Prob}(d,\ \text{irred}; q) = \mathbb{N}_q(d)/q^d.$$

Let F_i be the Galois field with q_i elements and let

$$\mathrm{Prob}(d, \text{irred}; q_1, \ldots, q_k)$$

denote the probability that an integral monic polynomial of degree d is irreducible in each $F_i[x]$, for $i = 1, 2, \ldots, k$. Then, assuming that the events are independent,

$$\mathrm{Prob}(d,\ \text{irred}; q_1, \ldots, q_k) = \prod_{i=1}^{k} \mathbb{N}_{q_i}(d)/(q_i^d).$$

It is well known [LN, p.93] that $\mathbb{N}_q = (1/3)(q^3 - q)$. Therefore,

$$\begin{aligned}\mathrm{Prob}(3,\ \text{irred}; q) &= \mathbb{N}_q(3)/q^3 = (1/3)(q^3 - q)/q^3 \\ &= (1/3)(q^2 - 1)/q^2, \\ 1/4 \leq \mathrm{Prob}(3,\ \text{irred}; q) &< 1/3,\end{aligned}$$

and (assuming the events are independent)

$$\begin{aligned}\mathrm{Prob}(d,\ \text{irred}; q_1, \ldots, q_k) &= \prod_{i=1}^{k} \mathbb{N}_{q_i}(3)/(q_i^3) \\ &= (1/3)^k \prod_{i=1}^{k} (q_i^2 - 1)/q_i^2.\end{aligned}$$

Table 2 shows that it is rare that an average monic cubic polynomial will be irreducible modulo the first five primes.

Table 2

primes $q_1, \ldots, q_k$	$\mathrm{Prob}(d, \text{irred}; q_1, \ldots, q_k)$
2	.25
3	.296
5	.3306
7	.3265
11	.3305
2, 3	.074
2, 3, 5	.0237
2, 3, 5, 7	.0077
2, 3, 5, 7, 11	.0076

4.9. Strategies for Finding Irreducible Cubic Polynomials. When we started work on this paper, we wanted a simple analytical condition, like that for quadratic polynomials, which would determine the number of roots a cubic polynomial $f(x)$ has modulo q and, in particular, determine when $f(x)$ is irreducible modulo q. Then we could search for irreducible cubics that produce numerous primes in much the same way that Lehmer, Shanks, Fung and Williams did for quadratics. Here, of course, we would apply Hardy and Littlewood's Conjecture H which is formulated in terms of the number of solutions of $f(x) \equiv 0 \pmod q$. At that time, we knew of no such condition that would provide what we wanted, but soon discovered what we considered an impractical one by Redei [Red, p.703]. So our research proceeded in a different direction. Recently we discovered a criterion by Dickson [Di2] which we believe will be useful in the future. Since Dickson's and Redei's Theorems are apparently not familiar, we include them here.

First, we start with the Stickelberger's Parity Theorem ([Red, p.663] or [Ch, p.282]), which determines the parity of the number of irreducible factors for any polynomial $f(x) \in F[x]$ where F is a finite field of odd characteristic.

THEOREM 9 (Stickelberger). Suppose F is a Galois field of odd characteristic, and suppose $f(x) \in F[x]$ is a monic polynomial of degree d with discriminant $D \neq 0$ in F. Let r be the number of irreducible factors of $f(x)$ in $F[x]$. Then $r \equiv d \pmod 2$ if and only if D is a square in F.

For cubic polynomials $f(x)$, Stickelberger's Theorem implies that $f(x)$ has exactly one root in F iff D is not a square in F, and $r = 1$ or 3 iff D is a square in F iff $f(x)$ has 0 or 3 roots in F iff $f(x)$ is either irreducible or has 3 linear factors. To distinguish the last two cases we need Dickson's or Redei's Theorem.

Apparently unaware of Stickelberger's Theorem, Dickson included the special case for cubic polynomials in his theorem. Here the characteristic of F is greater than 3 so we need only consider cubics $f(x)$ of the form $x^3 + ax + b$. Further $f(x)$ has no squared factors if the discriminant $D = -4a^3 - 27b^2 \neq 0$. If D is a square in F, write $D = 81c^2$ for $c \in F$, and let w denote a root of $y^2 + 3$ so that $w \in F$ if $q \equiv 1 \pmod 3$ and $w \in L$, a quadratic extension of F, if $q \equiv 2 \pmod 3$. Also in this case, we consider whether or not the element $(\frac{1}{2})(-b + cw)$ is a cube in either F or L according as $q \equiv 1 \pmod 3$ or $q \equiv 2 \pmod 3$.

If $f(x)$ factors in $F[x]$ as a product of three linear factors we write $f(x) = (1, 1, 1)$, if $f(x)$ factors as a product of a linear factor and an irreducible quadratic factor we write $f(x) = (1, 2)$, and finally if $f(x)$ is itself irreducible over F[x] we write $f(x) = (3)$. With these preliminaries, we state Dickson's Theorem.

THEOREM 10 (Dickson). Suppose F is a Galois field with q elements and characteristic > 3 and suppose L is the quadratic extension of F described above. The factorizations of $f(x) = x^3 + ax + b \in F[x]$ (with discriminant $D = -4a^3 - 27b^2 \neq 0$) are characterized as follows:

1. $f(x) = (1,1,1)$ if and only if D is a square in F and $(\frac{1}{2})(-b+cw)$ is a cube in either F if $q \equiv 1 \pmod 3$ or L if $q \equiv 2 \pmod 3$,

2. $f(x) = (1,2)$ if and only if D is not a square in F,

3. $f(x) = (3)$ if and only if D is a square in F, and $(\frac{1}{2})(-b+cw)$ is not a cube in either F if $q \equiv 1 \pmod 3$ or L if $q \equiv 2 \pmod 3$.

Redei formulates his criterion somewhat differently.

THEOREM 11 (Redei). Suppose F is a Galois field with q elements and characteristic > 3. Let n denote the integer nearest to $q/6$. Let $f(x) = x^3 + ax + b \in F[x]$ with discriminant $D = -4a^3 - 27b^2 \neq 0$. Suppose D is a square in F. If $g(-27b^2D^{-1}) = 0$, where $g(x) = C(2n,1) + C(2n,3)x + C(2n,5)x^2 + \ldots + C(2n,2n-1)x^{n-1}$, then $f(x)$ has exactly 3 roots in F. In the remaining case, $f(x)$ is irreducible in $F[x]$.

Thus, the irreducibility of $f(x)$ in $\mathbb{Z}_q[x]$, where q is a prime, is not completely determined by $(\frac{D}{q})$ as was the case for quadratic polynomials. But Dickson's and Redei's Theorems come to the rescue and give an irreducibility criterion for cubics.

Bateman and Horn [BH1, p. 129] chose eight polynomials:

$$\begin{array}{cccc} x^3-2, & x^3+2, & 2x^3-1, & 2x^3+1, \\ x^3-3, & x^3+3, & 3x^3-1, & 3x^3+1 \end{array}$$

for numerical investigation of their prime production. They apply a criterion, due to Emma Lehmer [LeE], which makes it easy to determine for polynomials of these eight types whether they have 0, 1, or 3 roots in $\mathbb{Z}_q$ for a prime q.

4.10. A Method of Constructing Irreducible Cubics. At this point, we restrain ourselves from attempting to see the connection between Lehmer's and Stickelberger-Dickson-Redei's criteria, and instead turn our attention to discussing another method of constructing irreducible cubic polynomials.

Here is the idea. Suppose that for $i = 1, 2, \ldots, k$, the integers P_i and Q_i are such that $f_i(x) = x^3 + P_i\, x + Q_i$ is irreducible modulo a prime q_i. Then we use the Chinese Remainder Theorem to select positive integers P and Q where P and Q satisfy the system of congruences:

$$P \equiv P_i \pmod{q_i}, \text{ and } Q \equiv Q_i \pmod{q_i} \text{ for } i = 1, 2, \ldots, k \text{ and}$$
$$P \text{ and } Q \text{ are unique modulo the product } q_1q_2\cdots q_k.$$

Then $f(x) = x^3 + Px + Q$ will be irreducible modulo q_i for $i = 1, 2, \ldots, k$.

There may be many possibilities for the P_i and Q_i so we narrow the focus a bit. Experimenting with the computer algebra systems, Maple and Mathematica, we noticed the frequency that for $P \neq 0$, $f(x) = x^3 + Px + 1$ was irreducible modulo a prime q. The following theorem confirms it in general.

THEOREM 12. (a) Let q be any prime. Then there is an integer $P \not\equiv 0 \pmod{q}$ such that $x^3 + Px + 1$ is irreducible modulo q.

(b) Let q be any prime different from 3. Then there is an integer $Q \not\equiv 0 \pmod{q}$ such that $x^3 + x + Q$ is irreducible modulo q.

PROOF. (a) Define the map $\theta : U \to \mathbb{Z}_q$ where U is the group of units of $\mathbb{Z}_q$, by $\theta(a) = (-a^3 - 1)/a$. This makes sense because $a \neq 0$. A set with $q - 1$ elements is mapped into a set with q elements so the complement of the range of θ is nonempty. Choose the residue class $[P] \in \mathbb{Z}_q$ not in the range of θ. Note that $\theta(1) = 0$, so $[P] \neq 0$.

Part (b) is a special case of a theorem by Carlitz [Ca]. □

DEFINITION. For h a positive integer and q a prime, let $Q(h,q) = h(q^*) + 1$ where q^* is the product of the primes up to q. Then if $Q(h,q)$ is prime, we say it is a *generalized Euclidean prime*. If $Q(1,q)$ is prime, it is customary to call it a *Euclidean prime*.

For a given prime q, Dirichlet's Theorem on arithmetic progressions implies that there are infinitely many h such $Q(h,q)$ is prime.

THEOREM 13. For a given positive integer k, there is a polynomial $f(x) = x^3 + Px + Q$, with P and Q both nonzero integers, $f(x)$ is irreducible modulo each prime up to the k-th prime q, and $f(0) = Q$ is prime.

PROOF. We repeat the above idea with more precision. Let q_i be the i-th prime and $q = q_k$. By Theorem 12, we can choose a nonzero P_i so that $f_i(x) = x^3 + P_i x + 1$ is irreducible modulo q_i, for each i. Apply the Chinese Remainder Theorem to find $P \equiv P_i \pmod{q_i}$, for $i = 1, 2, \ldots k$. Clearly P is nonzero. Then let $Q = Q(h,q)$ be a generalized Euclidean prime. Then $Q \equiv 1 \pmod{q_i}$ for each prime q_i for each $i = 1, 2, \ldots, k$ and the polynomial $f(x) = x^3 + Px + Q$ is irreducible modulo each prime q_i for $i = 1, 2, \ldots, k$. Moreover, $f(0) = Q$ is a prime. □

Later in Table 5, we will apply Theorem 13 to build some specific examples of cubic polynomials that are irreducible modulo the first several primes. For these examples, we decided to choose P_i and Q_i from the values listed in Table 3.

Table 3

q	P_i	Q_i	q	P_i	Q_i
2	1	1	37	5	1
3	2	1	41	1	1
5	1	1	43	9	1
7	1	1	47	5	1
11	4	1	53	3	1
13	4	1	61	3	1
17	3	1	67	5	1
19	1	1	71	1	1
23	3	1	73	7	1
29	4	1	79	2	1
31	3	1	83	3	1

Then in Table 4, we let q^* be the product of the first k primes where q is the k-th prime. Then P is the unique positive integer $< q^*$ such that $P \equiv P_i \pmod{q_i}$, for $i = 1, 2, \ldots, k$. Secondly, we list the smallest h such that $Q(h, q)$ is prime and set $Q = Q(h, q)$. Then we can form $f(x) = x^3 + Px + Q$.

Table 4

q	P	Q	h
2	1	3	1
3	5	7	1
5	11	31	1
7	71	211	1
11	2171	2311	1
13	29891	600601	2
17	150011	4084081	8
19	2702561	106696591	11
23	128798531	892371481	4
29	5259934541	7116662551	11
31	167002265291	200560490131	1
37	4579333048151	29682952539241	4
41	264305167766501	2129751844690471	7
43	8783312546528381	78496567990020181	6
47	191941971189908801	8608456956238879741	14

4.11. Irreducibility's Failures. Our point of view has been that if we build polynomials $f(x)$ that are irreducible for primes $2, 3, 5, \ldots, q$, then the number of possible small divisors of composite values of $f(x)$ are considerably restricted. We might expect that such a polynomial would have an improved chance of generating a long sequence of consecutive prime values. As we have said, this seems to be the reason behind the initial string of prime values in the case of the polynomials $f_p(x) = x^2 + x + p$, where p is one of the six lucky numbers 2, 3, 5, 11, 17, 41. It may be the reason for the initial string of prime values in the following example.

EXAMPLE. Let $f(x) = x^3 + 2171x + 7$. Then $f(x)$ is irreducible modulo 2, 3 (and other primes like 11, 13 as well). But $f(x)$ is reducible modulo 5, and $f(x)$ produces primes for $x = 0, 1, 2, 3$.

Nevertheless, things can go wrong. As we have said in §4.3, for an integer $m, f(m)$ may be composite regardless of the irreducibility of $f(x)$. Also it may be that $f(x)$ is irreducible modulo q for primes $q \leq B$, and yet q divides $f(b)$ for some integer $b < B$, and it may happen that for a prime $r > B$, $f(x)$ may have a root b modulo r, where $b < B$ and then r divides $f(b)$. We illustrate the point by several examples from Table 5.

In Table 5 the integers a, b, c are the numbers of primes in the intervals $[0, 99]$, $[0, 999]$ and $[0, 9999]$, respectively.

EXAMPLES. (a) Let $a(x) = x^3 + 71x + 211$. Then $a(x)$ is irreducible modulo 2, 3, 5, 7; produces a string of 8 primes in the interval $[-6, 1]$ and produces 46 primes in the interval $[0, 99]$.

(b) Let $b(x) = x^3 + 2171x + 2311$. Then $b(x)$ is irreducible modulo all primes up to 13 with 17 its smallest prime divisor. It produces 3 primes in $[0, 2]$, 16 consecutive primes in $[-39, -24]$, 7 consecutive primes in $[-71, 65]$ and $[-13, -7]$, and 112 primes in $[-100, 99]$ so 56% of its values in $[-100, 99]$ are prime.

(c) Let $c(x) = x^3 + 264305167766501x + 1$. Then $c(x)$ is irreducible modulo q for each prime $q \leq 41$, hence 43 is its smallest prime divisor. But $c(x)$ produces only 13 primes in $[0, 99]$.

(d) Let $d(x) = x^3 + 264305167766501x + 2129751844690471$. Then, just as for $c(x)$, $d(x)$ is irreducible modulo all primes up to 41 and produces only 25 primes in $[0, 99]$.

(e) Let $e(x) = x^3 + 287709034191671 + 1$. Then $e(x)$ is irreducible modulo q for every prime $q \leq 41$ except for 13. Perhaps it is worthwhile to describe how we constructed $e(x)$. We chose $P_{13} = 1$ and all other P_q for primes q between 2 and 41 as in Table 4. So 13 and 43 are the lowest prime divisors of $e(x)$. Moreover, $e(x)$ is composite for each integer x in the interval $[0, 31]$ and produces only 11 primes in the interval $[0, 99]$.

Table 5 gives a mixed bag of results, but still we can make two tentative conclusions and two observations:

1. It seems that we can control the smallest prime divisor of $f(x) = x^3 + Px + Q$ by choosing the minimum line q of Table 4 from which P and Q are found.

2. We can even control the second smallest prime divisor; see $e(x)$ above. But a relatively large smallest prime divisor does not guarantee that many prime values are produced, rather it seems that only the divisors of the composite values are restricted.

3. Not many strings of consecutive prime values of length 8 or more, and certainly no initial strings of that length, were produced.

4. It is interesting that the ratios c/b and b/a range between 6 and 10 except for $x^3 + 29891x + 2129751844690471$ where $c/b = 11.02$ and $b/a = 11.83$; $x^3 + 264305167766501x + 1$

where $b/a = 14$; $x^3+264305167766501x+211$ where $b/a = 24.75$; $x^3+287709034191671x+1$ where $b/a = 14.04$; and $x^3 + 2171x + 2129751844690471$ where $c/b = 11$.

Table 5

Polynomial	3 Smallest Prime Divisors	# of primes		
		a	b	c
$x^3 + 71x + 1$	$13, 23, 29$	51	317	2233
$x^3 + 71x + 211$	$11, 13, 17$	46	264	1941
$x^3 + 71x + 2311$	$13, 19, 23$	50	298	2121
$x^3 + 71x + 600601$	$13, 17, 23$	34	270	1969
$x^3 + 71x + 2129751844690471$	$13, 23, 29$	14	131	1263
$x^3 + 2171x + 1$	$13, 17, 19$	29	211	1528
$x^3 + 2171x + 211$	$11, 13, 17$	44	262	1908
$x^3 + 2171x + 2311$	$17, 29, 41$	30	235	2807
$x^3 + 2171x + 600601$	$13, 19, 29$	35	261	1853
$x^3 + 2171x + 2129751844690471$	$13, 17, 19$	12	94	1034
$x^3 + 29891x + 1$	$17, 19, 23$	41	295	2073
$x^3 + 29891x + 211$	$11, 13, 23$	29	245	1690
$x^3 + 29891x + 2311$	$13, 17, 19$	30	235	1673
$x^3 + 29891x + 600601$	$17, 37, 41$	39	309	2318
$x^3 + 29891x + 2129751844690471$	$17, 19, 23$	12	142	1565
$x^3 + 264305167766501x + 1$	$43, 59, 61$	13	182	1559
$x^3 + 264305167766501x + 211$	$11, 13, 17$	4	99	992
$x^3 + 264305167766501x + 2311$	$13, 19, 31$	15	140	1328
$x^3 + 264305167766501x + 600601$	$17, 19, 23$	14	114	1026
$x^3 + 287709034191671x + 1$	$13, 43, 47$	11	155	1522
$x^3 + 287709034191671x + 211$	$11, 13, 17$	11	89	800
$x^3 + 287709034191671x + 2311$	$13, 19, 31$	15	130	1242
$x^3 + 287709034191671x + 600601$	$13, 17, 19$	11	96	948
$x^3 + 191941971189908801x$	$53, 61, 71$	19	169	1537
$+8608456956238879741$	$53, 61, 71$	19	169	1537

4.12. An Open Problem. In the above examples, we have been able to control the smallest prime divisor, but we have not been able to prevent a "large" prime q having a "small" root b modulo q so that $f(b)$ is divisible by q and then the length of initial primes is bounded above by b. Therefore, we have hit upon a third facet of truth that affects prime production. If $f(x)$ is to produce an initial string of primes of length B, then $f(x)$ is irreducible and has no "small" prime divisors, and for "large" prime divisors q the root b modulo q is such that $B \leq b$.

EXAMPLE. Let $f(x) = x^3 - x^2 + 66x + 457$. Then $f(x)$ produces a string of consecutive primes of length 33 over the interval $[-17, 15]$. Its first few prime divisors are such that its roots modulo those primes are relatively large. For instance, it roots modulo 23, 53, 59, 67, and 71 are 18, 16, 39, 45, and 53. Also $f(-5) = -23$.

We know of no conditions, beyond our Observation 2 above, that can guarantee the existence of "large" roots modulo a prime q. We pose this as an open problem and turn to the method of exhaustive search.

5. Our List of Prime-producing Cubic Polynomials and the Method of Computation

In this section we exhibit some cubic polynomials $f(x) \in \mathbb{Z}[x]$ which produce a string of consecutive primes and explain how these polynomials were discovered. In Table 6 we consider polynomials of the form $f(x) = x^3 - x^2 + Cx + D$. The idea is that we wanted to imitate the form of polynomials $E_p(x) = x^2 - x + p$, where $E_{41}(x)$ is Euler's polynomial, and one of Escott's polynomials, $x^3 - x^2 + 17$. We list some polynomials that produce strings of consecutive primes in different intervals $[S, T]$ containing 0 and we calculate the class numbers h_F for the integral closure of $\mathbb{Z}$ in the field extension F of $\mathbb{Q}$ obtained by adjoining a root of $f(x)$. In calculating the class numbers, we used a package, `Kant V4` Software, copyrighted by Prof. Dr. M. E. Pohst, Technische Universitaet, Berlin. Then we list the percentage of primes produced in the interval $[0, 255]$.

Table 6

seq.#	L	A	B	C	D	S	T	h_F	%
1	27	1	−1	−74	−89	−11	15	1	42
2	28	1	−1	−20	−131	−10	17	1	48
3	28	1	−1	−60	223	−12	15	1	41
4	28	1	−1	−66	−101	−13	14	1	44
5	28	1	−1	−86	199	−13	14	1	46
6	28	1	−	−92	−59	−13	14	1	45
7	28	1	−1	−250	1373	−8	19	1	51
8	30	1	−1	−44	181	−14	15	1	40
9	30	1	−1	−82	−109	−14	15	1	49
10	30	1	−1	−294	1861	−12	17	1	56
11	33	1	−1	66	457	−17	15	3	57

If we allow the values to be noncomposite, then we include the polynomials in Table 7. Observe that the class numbers in Tables 6 and 7 are all small, but, at this stage, we cannot make a general conjecture.

Table 7

seq.#	L	A	B	C	D	S	T	h_F	%
12	27	1	−1	30	−167	−8	18	6	48
13	28	1	−1	−82	−151	−13	14	1	44
14	29	1	−1	−114	241	−14	14	2	45
15	30	1	−1	−70	−1	−12	17	3	44

In Table 8 we consider polynomials of the general form $f(x) = Ax^3 + Bx^2 + Cx + D$ that produce consecutive primes over the interval $[S, T]$. For our algorithm, we write

$$f(x) = \sum_{k=1}^{3} b_k \frac{(x!)}{(x-k)!}.$$

Then we search for polynomials under the stipulations that

$$\text{each } b_i \text{ is a positive integer,}$$

and

$$\begin{gathered} 1 \le b_3 + b_2 + b_1 \le \pi^*(b_0),\ \pi^*(N) = 1 + \pi(N), \\ \text{where } b_0 \text{ is a noncomposite } < 20000, \text{ and} \\ \text{where } \pi(N) \text{ is the number of primes } \le N. \end{gathered}$$

Moreover, if we write

$$f(x) = [[[b_3\,(x-2) + b_2]\,(x-1) + b_1]\,(x) + b_0],$$

then we know that $f(x)$, being the sum and products of increasing functions, is increasing. We require that b_0, $b_1 + b_0$, $2b_2 + 2b_1 + b_0$, $6b_3 + 6b_2 + 3b_1 + b_0$, etc. are all prime. Finally, we choose a value for L and exclude all polynomials that produce a string of primes of length less than L. At the end we solve for the coefficients A, B, C, D. We also list the percentage of primes in $[0, 255]$.

Each cubic prime producing polynomial in Tables 6 and 7 is such that its discriminant is not a square; in fact, each discriminant is either a prime or a product of two primes except in the one case, number 2 of Table 6, where the discriminant is a product of three primes. Therefore, the integral basis for the integral closure of $\mathbb{Z}$ is monogenic and the Galois group for each polynomial is *nonabelian.* The polynomials in Table 8 are not squares either (though sometimes they have square factors) so their Galois groups are also nonabelian. Also the three polynomials of Goetgheluck, the eight of Bateman and Horn, and Escott's cubic polynomials are all nonabelian. We might suppose that every prime-producing cubic polynomial is nonabelian. But such is not the case as there are several abelian examples from Shank's list of simplest cubic fields that produce fairly long initial strings of primes. We turn next, then, to describing his paper [Sh1].

Table 8

seq.#	L	A	B	C	D	S	T	%
16	27	8	−15	31	107	−6	20	42
17	27	8	9	25	131	−7	19	42
18	27	17	−30	13	701	−7	19	41
19	29	10	−8	14	73	−7	21	49
20	29	10	22	28	89	−8	20	49
21	34	2	−5	13	409	−13	20	49
22	34	2	1	9	419	−14	19	49
23	34	2	7	17	431	−15	18	49
24	35	4	25	−7	229	−16	18	57
25	36	2	−5	121	151	−17	18	56
26	39	6	−8	60	331	−20	18	56

5.1. The Simplest Cubic Fields. Let us compare and contrast a cubic number field K with quadratic fields. The discriminant D of K can be written in a unique way in the form $D = (d)N^2$ where d is a discriminant of a quadratic field or is equal to one. Accordingly there are two distinct types of cubic fields determined by whether or not d equals one. Quadratic fields are always normal with cyclic Galois group (of order 2), but cubic fields are normal only in the case where the discriminant is a square $D = N^2$ and only then is the Galois group cyclic (of order 3). In the non-normal case, when d is not 1, the normal closure L of the cubic field is a sextic field, with Galois group the symmetric group $\mathcal{S}_3$, and L contains the quadratic field $k = Q(\sqrt{d})$ of index 3 in L.

Real quadratic fields have one fundamental unit whereas real cubic fields have two. The integral closure of $\mathbb{Z}$ in a quadratic field always has a monogenic integral basis but that need not be the case for cubic fields (see Dedekinds classical example $x^3 + x^2 - 2x + 8$ [W, p.170] or [A]).

Moreover, the study of cubic fields is complicated by two additional facts:

(1) The discriminant uniquely determines quadratic fields, but not so for cubic fields. Borevic and Shafarevich [BS, p.94, exercise 21] list 3 non-isomorphic cubic fields with the same discriminant 22356. Even in the case when $D = N^2$, if N is not 9 or a prime, there will be more than one cubic field with discriminant D. In fact, it can be shown by class field theory [Has2, p.10] that abelian cubic fields of discriminant $C = N^2$ are enumerated as follows: There is a single field with $N = 9$ or $N = q_0$ and there are for $t \geq 1$ exactly 2^t

fields with $N = q_0 q_1 \cdots q_t$ or $N = 9q_1 \cdots q_t$, where the q_i are primes $\equiv 1 \pmod 6$. These fields are subfields of the field of the Nth roots of unity.

(2) The splitting of primes q in the ring of algebraic integers, even in the case of cyclic cubic fields (see [Sh2] and [Has1]), is more difficult than in quadratic fields where splitting is determined by $(\frac{D}{q})$.

But these two complications may be avoided if N is restricted to certain primes. This is what Shanks does. He studied a class of cubic fields $K = Q(\alpha)$ where α is a root of $f(x) = x^3 - ax^2 - (a+3)x - 1$. The discriminant of $f(x)$ is $D = (a^2+3a+9)^2 = P^2$ where $P = P(a) = a^2 + 3a + 9$ is a prime. Thus, K is normal, and the polynomial $f(x)$ is abelian. Here fundamental units are easily calculated, and therefore the regulator and the class number are easily determined. Note $P \equiv 1 \pmod 3$, and for all primes $q \neq P$, the polynomial $f(x)$ splits completely or is irreducible modulo q according as:

$$q^{(P-1)/3} \equiv 1 \pmod P.$$

Shanks generates a table of fields K where a ranges between -1 and 410 and calculates P and the class number h. We list the first eight from his table, all of the cases where $h = 1$. We list the first prime q_1 where $f(x)$ is reducible modulo q and we give the length L of a string of prime values of $f(x)$ starting at $x = 1$.

Shanks' Modified Table 9

a	P	q_1	L
-1	7	7	5
1	13	5	5
2	19	5	1
4	37	11	8
7	79	17	14
8	97	19	16
10	139	23	20

References

[A] A.A. Albert, A determination of the integers of all cubic fields, *Ann. of Math.* **31** (1930), 550–556.

[AC] R.G. Ayoub and S. Chowla, On Euler's polynomials, *J. No. Th.* **13** (1981), 443–445.

[B1] A. Baker, Linear forms in the logarithms of algebraic numbers, *Mathematika* **13** (1966), 204–216.

[B2] ——, A remark on the class number of quadratic fields, *Bull. London Math. Soc.* **1** (1969), 98–102.

[B3] ——, Imaginary quadratic fields with class number two, *Ann. of Math.* **94** (1971), 139–152.

[BH] P.T. Bateman and R.A. Horn, Primes Represented by Irreducible Polynomials in One Variable, *Theory of Numbers* (Proc. Symp. Pure Math. Vol. VIII), 119–132.

[Be] N.G.W.H. Beeger, *Liste des Nombres Premiers de Onzième Million (Plus Precisement de 10006741 a 10999997) dápres les Tables Manuscrites de J. Ph. Kulik*, L. Poletti et R.J. Porter, Amsterdam 1951.

[BS] Z.I. Borevic and I. Shafarevich, *Number Theory*, Academic Press, Vol. 20 of *Pure and Applied Math.*, 1966.

[BoG] N. Boston and M.L. Greenwood, Quadratics representing primes, *Amer. Math. Monthly* **102** (1995), 595–599.

[Bo] V. Bouniakowsky, Sur les diviseurs numeriques invariables des functions rationalles entieres, *Mem. Acad. Sci. St. Petersburg* **6** (1857), 305–329.

[Bra] R. Brandl, Integer polynomials that are reducible modulo all primes, *Amer. Math. Monthly* **93** (1986), 286–288.

[BFO] J. Brillhart, M. Filaseta and A. Odlyzko, An Irreducibility Theorem of A. Cohn, *Canad. J. Math.* **33** (1981), 1055–1059.

[Bro] W.S. Brown, Reducibility properties of polynomials over the rationals, *Amer. Math. Monthly* **70** (1963), 965–969.

[BrG] W.S. Brown and R.L. Graham, An irreducibility criterion for polynomials over the integers, *Amer. Math. Monthly* **76** (1969), 795–797.

[Ca] L. Carlitz, A note on irreducible cubics (mod p), *K. Norske Vidensk. Selsk. Forh.* **40** (1967), 25–30.

[CL] G. Chang and K.W. Lih, Polynomial representation of primes, *Tamkang J. Math.* **8** (1977), no. 2, 197–198.

[Chi] L. Childs, *A Concrete Introduction to Higher Algebra*, Springer-Verlag, New York, 1979.

[CCC] S. Chowla, J. Cowles and M. Cowles, The least prime quadratic residue and the class number, *J. Number Th.* **22** (1986), 1–3.

[Co] H. Cohn, *A Second Course in Number Theory*, John Wiley and Sons, Inc., New York, 1962.

[De] M. Deuring, Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins, *Invent. Math.* **5** (1968), 169–179.

[Di1] L.E. Dickson, *History of the Theory of Numbers*, reprinted by Chelsea 1952.

[Di2] ——, Criteria for the irreducibility of functions in a finite field, *Bull. Amer. Math. Soc.* **13** (1906), 1–8.

[Do] H.L. Dorwart, Irreducibility of polynomials, *Amer. Math. Monthly* **42** (1935), 369–381.

[Es] E.B. Escott, Responses 1133, Formule d'Euler $x^2 + x + 41$ et formules analogues, *L'intermediare des Math* **6** (1899), 10–11.

[Eu] L. Euler, Extrait d'une lettre de M. Euler le père á M. Bernoulli concernant le memoire imprimé parmi ceux de 1771, Nouveaux Memoire de l'Academe des Sciences de Berlin 1772 (1774), p. 381.

[Fe] D. Fendel, Prime-producing polynomials and principal ideal domains, *Math. Mag.* **58** (1985), 204–210.

[Fo] R. Forman, Sequences with many primes, *Amer. Math. Monthly* **99** (1992), 548–557.

[Fr1] F.G. Frobenius, Über quadratische Formen, die Primzahlen darstellen, Sitzungsber. d. Königl. Akad. d. Wiss. zu Berlin, (1912), 966–980. (Reprinted in *Gesammelte Abhandlungen*, Vol. III, 573–587, Springer-Verlag, Berlin, 1968.

[Fr2] ——, S-B Presses. Akad. Wiss. Phys Mat. Kl. I (1896), 689–703; Jahrbuch 27, 91. (Reprinted in *Gesammelte Abhandlungen*, Vol. II, 719–733, Springer-Verlag, Berlin, 1968.

[FW] G.W. Fung and H.C. Williams, Quadratic polynomials which have a high density of prime values, *Math. Comp.* **55** (1990), 345–353.

[Ga] B. Garrison, Polynomials with large numbers of prime values, *Amer. Math. Monthly* **97** (1990), 316–317.

[GB] I. Gerst and J. Brillhart, On the prime divisors of polynomials, *Amer. Math. Monthly* **78** (1971), 250–266.

[Goe] P. Goetgheluck, On cubic polynomials giving many primes, *Elem. Math.* **44** (1989), 70–73.

[Gol] D. Goldfield, Gauss' class number problem for imaginary quadratic fields, *Bull. Amer. Math. Soc.* **13** (1985), 23–37.

[HL] G.H. Hardy and J.E. Littlewood, Partitio numerorum III: On the expression of a number as a sum of primes, *Acta. Math.* **44** (1923), 1–70.

[Has1] N. Hasse, Arithmetische Theorie der Kubischen Zahlkorper auf Klassenkorper theoretischen Grundage, *Math. Zeit.* **31** (1930), 565–582.

[Has2] ——, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkorpern, Berlin, 1950.

[Hee] K. Heegner, Diophantine analysis and modelfunkten, *Math. Zeit.* **56** (1952), 227–253.

[Hei] H. Heilbronn, Über die Verteilung der Primzahlen in Polynomen, *Math. Ann.* **104** (1931), 794–799.

[Hen] M.D. Hendy, Prime quadratics associated with complex quadratic fields of class number two, *Proc. Amer. Math. Soc.* **43** (1974), 253–260.

[Hi] O. Higgins, Another long string of primes, *J. Rec. Math.* **14** (1982), 185.

[Iwan] H. Iwaniec, Almost-primes represented by quadratic polynomials, *Inventiones Math.* **47** (1978), 171–188.

[Iwat] H. Iwata, A property of some polynomials, *Bull. Fac. Sci. Ibaraki Univ. Ser. A*, No. 3 (1971), 21–24, (MR 54#6790).

[KH] I. Kaplansky and I.N. Herstein, *Matter's Mathematical*, Harper and Row (1974).

[K1] E. Karst, The congruence $2^{p-1} \equiv 1 (\mathrm{mod}\ p^2)$ and quadratic forms with high density of primes, *Elem. Math.* **22** (1967), 85–88.

[K2] ——, New quadratic forms with high density of prime, *Elem. Math.* **28** (1973), 116–118.

[La] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Massachusetts, 1971.

[Leg] A.M. Legendre, *Thèorie des nombres*, *Libraire Scientifique*, A. Herman, Paris (1798), 69–76; 2nd ed. (1808), 3rd ed. (1830), 72–80.

[LeD] D.H. Lehmer, On the function of $X^2 + X + A$, *Sphinx* **6** (1936), 212–214 and *Sphinx* **7** (1937), 40.

[LLS] D.H. Lehmer, E. Lehmer, and D. Shanks, Integer sequences having prescribed quadratic character, *Math. Comp.* **24** (1970), 433–451.

[LeE] E. Lehmer, Criteria for cubic and quartic residuacity, *Mathematika* **6** (1958), 20–29.

[LN] R. Lidr and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Massachusetts, 1983.

[Lu] R.F. Lukes, C.D. Patterson, and H.C. Williams, Numerical Seiving Devices: Their History and Some Applications. *Nieuw Archief voor Wiskunde* **13** (1995), 113–139.

[Ma] H. Mann, *Introduction to Algebraic Number Theory*, The Ohio State University Press, Columbus, Ohio, 1955.

[Mig] M. Mignotte, *Mathematics for Computer Algebra*, Springer-Verlag, New York, 1992.

[Mio] E. Miot, (title of article unavailable), *L'intermediare des math* **19** (1912), 36.

[Mo1] R.A. Mollin, Prime-producing quadratics, *Amer. Math. Monthly* **104** (1997), 529–544.

[Mo2] ——, *Quadratics*, CRC Press, 1996.

[MolWi1] R.A. Mollin and H.C. Williams, On prime valued polynomials and class numbers of real quadratic fields, *Nagoya Math. J.* **112** (1988), 143–151.

[MolWi2] ——, Class number problems for real quadratic fields, in *Number Theory and Cryptography* (J.H. Loxton, ed.) London Math. Soc. Lecture Note Series **154** (1990), 177–195.

[MolWi3] ——, Quadratic non-residues and prime-producing polynomials, Canad. Math. Bull. **32(4)** (1989), 474–478.

[Mona] M.B. Monagan, A heuristic irreducibility test for univalent polynomials, *J. Symbolic Comput.* **13** (1992), 47–57.

[MonWe] H.L. Montgomery and P.J. Weinberger, Notes on small class numbers, *Acta Arith.* **24** (1974), 529–542.

[N] T. Nagell, Zur Arithmetik der Polynome, *Abhandl. Math. Sein. Univ. Hamburg* **1** (1922), 179–194.

[O] O. Ore, Einige Bernerkungen über Irreduzibilität, *Jahresbericht der Deutschen Math.* Ver. **44** (1934), 146–151.

[PS] G. Polya and G. Szego, *Aufbau und Lehrsatze aus der Analysis die Grundlehren der Mathematische Wissenschaften in Anzeldarstellungen*, Vol. 20, Springer-Verlag, Berlin, 1954.

[Ra] G. Rabinowitsch, Eindeutig der Zerlegung in Primzahlfactoren in quadratischen Zahlkörpern, *J. Reine Angew. Math.* **142** (1913), 153–164.

[Re] L. Redei, *Algebra*, Vol. 1, Pergamon Press, New York, 1st ed., 1967.

[Ri1] P. Ribenboim, Euler's famous prime generating polynomial and the class number of imaginary quadratic fields, *L'Enseignment Math.* **34** (1988), 23–42.

[Ri2] ——, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

[Sc] A. Schultz, Inseln der Ordnung unter den Primzahlen-Primzahlsenien in Polynomen, *Elem. Math.* **54** (1999), 64–79.

[Sh1] D. Shanks, The simplest cubic fields, *Math. Comp.* **28** (1974), 1137–1152.

[Sh2] ——, A survey of quadratic, cubic and quartic algebraic number fields, *Cong. Numer.* **17** (1976), 15–42.

[Si] W. Sierpinski, Les binômes $x^2 + n$ les numbres premiers, *Bull. Soc. Royale Sciences Liege* **33** (1964), 259–260.

[Stac] Stäckel, (title of article unavailable), *Journal f. Math.* **48** (1918), 101.

[Star1] H. Stark, A complete determination of complex quadratic fields of class number one, *Mich. Math. J.* **14** (1967), 1–27.

[Star2] ——, Class-number problems of quadratic fields, *Proc. Internat'l Congress of Math.* 1970, Vol. 1, 511–518.

[Star3] ——, Class-numbers of complex quadratic fields, Springer Lecture Notes, No. 320, 152–1, (1973).

[Star4] ——, A transcendence theorem for class number problems, *Ann. of Math.* **94** (1971), 153–173.

[Star5] ——, On complex quadratic fields with class number two, *Math. Comp.* **29** (1975), 289–302.

[ST] I.N. Stewart and D.O. Tall, *Algebraic Number Theory*, 2nd ed. Chapman and Hall, New York, 1987.

[Sz] G. Szekeres, On the number of divisors of $x^2 + x + A$, *J. Number Th.* **6** (1974), 434–442.

[W] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.