Artin prime producing quadratics

Pieter Moree

Abstract

Fix an integer g. The primes p such that g is a primitive root for p are called *Artin primes*. Using a mixture of heuristics, well-known conjectures and rigorous arguments an algorithm is given to find quadratics that produce many Artin primes. Using this algorithm Y. Gallot has found a g and a quadratic f such that the first 31082 primes produced by f have g as a primitive root. There is a connection with finding integers d such that $L(2,(d/.))$ is small.

1 Introduction

Given a non-zero integer g, let $\mathcal{P}(g)$ denote the set of primes p such that g is a primitive root modulo p. Put $G := \{g \in \mathbb{Z} : g \neq -1 \text{ and } g \neq b^2,\ b \in \mathbb{Z}\}$. In 1927 Emil Artin conjectured that if g is in G, then the set $\mathcal{P}(g)$ is infinite. This conjecture is commonly known as the *Artin primitive root conjecture*. Under the Generalized Riemann Hypothesis (GRH) this was proved by C. Hooley in 1967.

A natural question that arises is to find an easy way to generate primes in $\mathcal{P}(g)$. In this paper we study to which extent quadratic polynomials are suitable for this. This problem goes back to the mathematical amateur Raymond Griffin who in 1957 thought that all primes of the form $10X^2+7$ belong to $\mathcal{P}(10)$. (Note that the primes in $\mathcal{P}(10)$ can be alternatively characterized as those primes p for which the decimal expansion of $1/p$ has period $p-1$.) Having a computer at his/her disposal the modern number theorist immediately disposes of Griffin's assertion: the first 16 primes p of the form $10X^2+7$ have indeed decimal period $p-1$, but this is not true for $p = 7297$, the 17th such prime. Nevertheless, one can wonder whether there exists a quadratic polynomial such that the prime values amongst $f(0), f(1), f(2), \cdots$ are all in $\mathcal{P}(g)$ (we call this *Griffin's dream*). To avoid trivialities one wants f to be such that, assuming the Bateman-Horn conjecture (see next section), f assumes infinitely many distinct prime values.

D.H. Lehmer [14] was the first to seriously investigate Griffin's dream (inspired by a letter Griffin wrote him). He found the candidate $326X^2+3$ for $g = 326$. At

P. Moree: Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Deutschland, e-mail: moree@mpim-bonn.mpg.de

Mathematics Subject Classification (2000). 11Y55, 11A07, 11B83

the time he did not have enough computational resources to find, as is trivial these days, that 326 is a primitive root for the first 206 primes of the form $326X^2+3$ (they satisfy $0 \le X \le 2374$), but is not for $p = 1838843753 = 326 \cdot 2375^2 + 3$.

In contrast to the polynomials of Griffin and Lehmer, Euler's polynomial X^2+X+41 enjoys cult status as virtually every number theorist is aware of the fact that $f(0), \ldots, f(39)$ are all prime and that this is related to the celebrated class number one problem. As will be worked out in some detail in this paper, the problems of finding *Artin prime producing quadratics* (i.e. quadratics producing many Artin primes) and *prime producing quadratics* (i.e. quadratics producing many primes) are closely related. Indeed, since the latter quadratics are so well-researched some of the results obtained on them can be used to our advantage.

The starting idea in finding prime producing quadratics is to choose $f(X) \in \mathbb{Z}[X]$ in such a way that for many small primes q the equation

$$f(X) \equiv 0 (\mathrm{mod}\ q) \tag{1}$$

does not have a solution and that the values assumed by f do not grow too quickly. Note that if q is odd the equation (1) does not have a solution iff $\chi_\Delta(q) := (\frac{\Delta}{q}) \neq 1$, where Δ denotes the discriminant of f and $(\frac{\Delta}{q})$ denotes the Legendre symbol. Thus we are led to try to find a Δ such that $|\Delta|$ is small and $\chi_\Delta(q) \neq 1$ for many consecutive odd primes q. Let us for simplicity assume that $\Delta < 0$. This then forces

$$\frac{\pi h(\Delta)}{w\sqrt{|\Delta|}} = L(1, \chi_\Delta) = \sum_{n=1}^{\infty} \frac{\chi_\Delta(n)}{n} = \prod_q \frac{1}{1 - \chi_\Delta(q)/q} \tag{2}$$

to be small, where $h(\Delta)$ is the class number of $\mathbb{Q}(\sqrt{\Delta})$ and w the number of roots of unity in this quadratic field. Thus we should find Δ such that $h(\Delta)$ is small. Indeed, for Euler's polynomial we have $\Delta = -163$ and $h(\Delta) = 1$ and it turns out that (1) does not have a solution for the primes $q = 2, 3, \ldots, 37$.

Define $r_p(g) := [(\mathbb{Z}/p\mathbb{Z})^* : \langle g \rangle]$ to be the residual index of $g(\mathrm{mod}\ p)$, that is the index of the subgroup generated by g in $(\mathbb{Z}/p\mathbb{Z})^*$. Since the residual index is usually small, one way to produce Artin prime producing quadratics f is to search for quadratics such that $q \nmid r_p(g)$ for many consecutive primes q, where p runs over the primes produced by f. For $q = 2$ we can ensure this if we can find a quadratic f such that $(\frac{g}{p}) = -1$ for the primes p produced by f. This leads to the question of studying the fraction of primes p of the form $p = f(X)$ that are inert in a prescribed quadratic number field (a problem of some interest by itself, it seems). Using character sums this question is studied in Section 5.

Now let q be an odd prime. Since $r_p(g) | p-1$ we can ensure that $q \nmid r_p(g)$ by choosing $f(X)$ in such a way that the equation $f(X) \equiv 1 (\mathrm{mod}\ q)$ has no solution. If Δ_1 denotes the discriminant of the polynomial $f(X) - 1$, then by a reasoning similar to the one for prime producing polynomials, we are interested in those Δ_1 for which $L(1, \chi_{\Delta_1})$ is small. The polynomial of Lehmer is in this way related to the quadratic number field $\mathbb{Q}(\sqrt{-163})$. The primes p it produces have the property that if $q | r_p(g)$, then $q \ge 41$. A more refined, partially heuristic, analysis suggests that one should rather look for Δ_1 such that $L(2, \chi_{\Delta_1})$ is small. Since these values being small are not unrelated, one can use values for which $L(1, \chi_{\Delta_1})$

is small (exhaustively investigated) to produce values for which $L(2, \chi_{\Delta_1})$ is small (little investigated).

In order to briefly describe the contents of this paper, we have to be a little bit more precise.

Definition 1 *Given integers g and $f(X) \in \mathbb{Z}[X]$, let $p_1(g, f), p_2(g, f), \ldots$ be the sequence of primes that is obtained on going through the sequence $f(0), f(1), \ldots$ and writing down the primes not dividing g as they appear. We let r be the largest integer r (if this exists) such that g is a primitive root mod p for all primes $p_j(g, f)$ with $1 \le j \le r$. We let $c_g(f)$ be the number of distinct primes amongst $p_j(g, f)$ with $1 \le j \le r$.*

Thus, for example, $c_{326}(f) = 206$, with $f(X) = 326X^2 + 3$.

Problem 1 *(Griffin's dream). Find g and f such that $c_g(f)$ is unbounded.*

A more modest variant of this problem is as follows:

Problem 2 *Find g and quadratic f such that $c_g(f)$ is as large as possible.*

Alternatively one could ask, given a prescribed integer g in G, to find a quadratic f such that $c_g(f)$ is as large as possible. Since this is an easy variant of Problem 2, we will only discuss it briefly in the sequel.

By the Chinese Remainder Theorem we know that given any finite set of odd primes one can find g such that g is a primitive root for each of these primes. Thus one should require g to be small in comparison with the coefficients of f. We say g is small in this context if $|g| < 10^{c_g(f)/3}$ (see Section 3 for an explanation).

It will be shown (Theorem 2), using some ideas due to A. Granville, that under the prime k-tuplets conjecture (see next section), for every g in G and real number m, there exists a quadratic f such that $c_g(f) > m$. Based on a mixture of heuristics, well-known conjectures and rigorous arguments an algorithm is proposed in Section 8 to find f producing many Artin primes. This algorithm has been implemented by Y. Gallot. Using it he found g and f producing many Artin primes such that $c_g(f) = 31082$ (the current record). Finally, some arguments are presented that suggest that Griffin's dream will be forever a dream for quadratic polynomials...

Of course there is no need to restrict to quadratic polynomials, but this is what we shall do in this paper (even less theoretical tools seem to be available in the higher degree case). Since at present it is not even known whether $n^2 + 1$ is prime infinitely often, we can only expect to gain some insight on assuming certain conjectures. In the next section we briefly recall some relevant conjectures.

As the words 'lemma' and 'proposition' do not have a universal definition, I like to state that I use them to mean 'intermediary result that is being used further on to prove a theorem' and 'final result, deemed not deep or important enough to be called theorem'.

Y. Gallot and A. Granville kindly permitted me to state their results. They appear here for the first time in print.

2 Prerequisites on two conjectures

Let $f(X)$ be an irreducible polynomial of content 1 in $\mathbb{Q}[X]$ with integer coefficients. By a special case of a conjecture due to Bateman and Horn [2] $\pi_f(x)$, the number of integers $0 \le n \le x$ such that $f(n)$ is prime, should satisfy, as x tends to infinity,

$$\pi_f(x) \sim \frac{H(f)}{\deg(f)} \frac{x}{\log x}, \text{ where } H(f) = \prod_p \frac{p - N_p(f)}{p-1},$$

and $N_p(f) = \#\{n(\text{mod } p) : f(n) \equiv 0(\text{mod } p)\}$. We say a congruence class modulo an integer m is *allowable* if for any number r in it we have $(f(r), m) = 1$ and thus, e.g., $p - N_p(f)$ denotes the number of allowable congruence classes modulo p.

Let $\mathcal{F}$ be the set of quadratic polynomials $aX^2 + bX + c$ with $a > 0$, b, c integers such that $\gcd(a, b, c) = 1$, $d = b^2 - 4ac$ is not a square and $a + b$ and c are not both even. Then, as x tends to infinity, Hardy-Littlewood's Conjecture F [10], a special case of the Bateman-Horn conjecture, asserts that

$$\pi_f(x) \sim \epsilon \frac{x}{\log x} \prod_{\substack{p>2 \\ p|(a,b)}} \frac{p}{p-1} \prod_{\substack{p>2 \\ p\nmid a}} \left(1 - \frac{(\frac{d}{p})}{p-1}\right), \tag{3}$$

where $\epsilon = 1$ if $a + b$ is even and $\epsilon = 1/2$ otherwise. For $f \in \mathcal{F}$ it is easily shown that

$$\frac{a}{\varphi(a)L(1, (d/.))} \ll H(f) \ll \frac{a}{\varphi(a)L(1, (d/.))}. \tag{4}$$

For our purposes the following weaker conjecture, which is implied by Hardy-Littlewood's Conjecture F, will suffice.

Conjecture 1 *Let $m \ge 2$ be an integer. Suppose that $f(X) \in \mathbb{Z}[X]$ represents infinitely many primes, then the n for which $f(n)$ is prime are asymptotically equidistributed over the allowable congruence classes modulo m.*

Proof that Hardy-Littlewood's conjecture F implies Conjecture 1. This can be done by direct computation from (3), but this computation turns out to be a bit messy. Instead we use the formula for $H(f)$. Let $r(\text{mod } m)$ be an allowable congruence classes modulo m. We put $f_r(X) = f(mX + r)$ and will show that $H(f_r)$ does not depend on r. If $p \nmid m$, then $N_p(f_r) = N_p(f)$ as the map $X \to mX + r$ induces a permuation of $\mathbb{Z}_p$ then. If $p|m$, then $f(mX + r) \equiv f(r) \not\equiv 0(\text{mod } p)$ (since by assumption r is not allowable) and thus $N_p(f_r) = 0$ in this case. It follows that

$$H(f_r) = \prod_p \frac{p - N_p(f_r)}{p-1} = \prod_{p|m} \frac{p}{p-1} \prod_{p\nmid m} \frac{p - N_p(f)}{p-1} = \frac{m}{\varphi(m)} \prod_{p\nmid m} \frac{p - N_p(f)}{p-1},$$

which is a constant not depending on r. □

Finally we recall the prime k-tuplets conjecture (TC(k)). This conjecture seems to be due to Dickson (1904).

Conjecture 2 *Let $k \geq 1$ and let $A_1, \ldots, A_k, B_1, \ldots, B_k$ be integers with $A_j > 0$ for $j = 1, \ldots, k$. Suppose that for each prime p there exists an integer n_p such that p does not divide $\prod_{j=1}^{k}(A_j n_p + B_j)$, then there exist infinitely many integers n such that $A_j n + B_j$ is prime for $1 \leq j \leq k$.*

3 On the likelihood of finding $c_g(f) = m$

Let $p_1 < \cdots < p_s$ be distinct primes and put $P = \prod_{i=1}^{s} p_i$. There are $\prod_i^s \varphi(p_i - 1)$ residue classes modulo P such that if g is in any of them it is a primitive root for every prime dividing P. Assuming equidistribution we expect that the smallest of them is roughly of size $Q := \prod_{i=1}^{s}(p_i - 1)/\varphi(p_i - 1)$. It is an easy exercise in analytic number theory to evaluate the average value of $(p-1)/\varphi(p-1)$. To this end note that

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu(d)^2}{\varphi(d)},$$

whence we infer that

$$\sum_{p \leq x} \frac{p-1}{\varphi(p-1)} = \sum_{p \leq x} \sum_{d|p-1} \frac{\mu(d)^2}{\varphi(d)} = \sum_{d \leq x} \frac{\mu(d)^2}{\varphi(d)} \pi(x; d, 1),$$

where $\pi(x; d, 1)$ denotes the number of primes $q \leq x$ such that $q \equiv 1 (\mathrm{mod}\ d)$ and we swapped the order of summation in the double sum. Proceeding as in the proof of Lemma 1 of [20] one then finds that for every $C > 1$ one has

$$\sum_{p \leq x} \frac{p-1}{\varphi(p-1)} = B\mathrm{Li}(x) + O(\frac{x}{\log^C x}), \text{ with } B = \prod_{q \text{ prime}} \left(1 + \frac{1}{(q-1)^2}\right),$$

where the implied constant may depend on C and $\mathrm{Li}(x)$ denotes the logarithmic integral. This improves on an estimate due to Murata [21]. Expressing B in terms of zeta values, cf. [5, 19], one finds $B = 2.826419997067\ldots$. Thus Q is roughly of size $B^s \approx 10^{0.45s}$. This motivates the definition of small g in the introduction.

Likewise one can wonder about the probability that a given g is a primitive root for our finite set of primes. An estimate for this is given by $1/Q$ and should be roughly $10^{-0.45s}$. Thus a measure for the likelihood of having $c_g(f) = m$ (by random choice of f and g) is $10^{-m/2}$.

4 Lehmer's polynomial reconsidered

In their celebrated book Ireland and Rosen [12] write (p. 47): 'Lehmer discovered the following curious result. The first prime of the form $326n^2 + 3$ for which 326 is not a primitive root must be bigger than 10 million. He mentions other results of the same nature. It would be interesting to see what is responsible for this strange behavior'. What is responsible is the class number one phenomenon (see introduction) in combination with the fact that $(\frac{326}{p})=-1$ for all primes p represented by Lehmer's polynomial (Proposition 1). In this section this will be worked out in further detail.

In this context the following trivial result will play an important role.

Lemma 1 *Let $\alpha \ge 0$ be an integer. Let p be a prime and g an integer coprime with p. Define $r_p(g) := [(\mathbb{Z}/p\mathbb{Z})^* : \langle g \rangle]$ (the residual index of $g(\text{mod } p)$). Let d_1, d_2 be positive integers. Let p be a prime of the form $2^\alpha d_1 n^2 + d_2 2^\alpha + 1$. If q is an odd prime with $(\frac{-d_1 d_2}{q}) \ne 1$ and $q \nmid d_2$, then $q \nmid r_p(g)$.*

Proof. The equation $2^\alpha d_1 X^2 + d_2 2^\alpha + 1 = 1$ is solvable mod q if and only if $(\frac{-d_1 d_2}{q}) = 1$ or $q | d_2$. Since by assumption $(\frac{-d_1 d_2}{q}) \ne 1$ and $q \nmid d_2$, it follows that $p \not\equiv 1(\text{mod } q)$. From this and $r_p(g)|p-1$, it then follows that $q \nmid r_p(g)$. □

Using Lemma 1 it is easy to deduce the following proposition.

Proposition 1 *Let k be a non-zero integer. Let $g \in \{-163, -3, 6, 326\}$. If p is a prime not dividing kg and $p = 326n^2 + 3$, then $(r_p(k^2 g), 2 \cdot 3 \cdots 37) = 1$.*

Proof. Using quadratic reciprocity one deduces that $(\frac{k^2 g}{p}) = -1$ and hence $2 \nmid r_p(k^2 326)$. Let q be an odd prime not exceeding 37. It is easy to check (using e.g. quadratic reciprocity) that $(\frac{-163}{q}) = -1$ and thus, by Lemma 1, $q \nmid r_p(k^2 g)$. □

Put $L(X) = 326X^2 + 3$. The latter result shows that if 326 is not a primitive root modulo a prime $p = L(n)$, then $r_p(326) \ge 41$. Since this is rather unlikely to happen, we expect to find a reasonably long string of primes of the form $L(n)$ before we find a prime p for which 326 is not a primitive root mod p. This is precisely what happens: we have to wait until $n = 2375$ and hence $p = 1838843753$, for 326 not to be a primitive root mod p (we have $r_p(326) = 83$).

Supposing $p = L(n)$ to be prime, one can wonder about the probability that $r_p(326) > 1$. For this to happen $r_p(326)$ must be divisible by some odd prime q such that $(\frac{-163}{q}) = 1$. In this case n has to be in one of two residue classes mod q and, moreover, we need to have $326^{\frac{p-1}{q}} \equiv 1(\text{mod } p)$. Since $326^{\frac{p-1}{q}}$ is merely one out of the q solutions of $x^q \equiv 1(\text{mod } p)$, one heuristically expects that $326^{\frac{p-1}{q}} \equiv 1(\text{mod } p)$ with probability $1/q$. We thus expect that with probability

$$\prod_{(\frac{-163}{q})=1} \left(1 - \frac{2}{q^2}\right) = 0.99337\ldots \tag{5}$$

a prime of the form $p = L(n)$ will have 326 as a primitive root. This argument is taken from Lehmer's paper. He implicitly assumes that the n for which $f(n)$ is prime are asymptotically equally distributed over the congruence classes modulo q, instead of over the allowable congruence classes modulo q. On correcting for this one arrives at a probability of

$$p_1 := \prod_{(\frac{-163}{q})=1} \left(1 - \frac{2}{q(q-1-(\frac{-978}{q}))}\right) = 0.99323\ldots. \tag{6}$$

For $0 \leq n \leq 5 \cdot 10^6$ there are 240862 primes $p = L(n)$ of which 239239 have 326 as a primitive root. Note that $239239/240862 \approx 0.99326\ldots$.

Instead of taking 326 as base, Proposition 1 suggests we could take $k^2 326$ as a base and vary over k. Assuming that each prime $p = L(n)$ has a probability p_1 of having $k^2 326$ as a primitive root we might expect that

$$\lim_{x\to\infty} \frac{1}{x} \sum_{k\leq x} g_{k^2 326}(f) \approx \sum_{j=1}^{\infty} j p_1^j (1-p_1) = \frac{p_1}{1-p_1},$$

that is equals about 150 (note that the 'probability' that $g_{k^2 326}(f) = j$ equals $p_1^j - p_1^{j+1} = p_1^j(1-p_1)$). For $k \leq 5000$ it turns out that the average is around 180. Note that in the averaging process there is a very strong bias towards the smallest primes of the form $p = L(n)$. This might explain the observed discrepancy.

The most interesting quantity for our purposes is $\max_{1\leq k\leq s} g_{k^2 326}(L)$. Since one expects the probability that $\max_{1\leq k\leq s} g_{k^2 326}(L) \leq j$ to be $(1-p_1^{j+1})^s$, one arrives at

$$M(p_1, s) := \sum_{j=1}^{\infty} j \left((1-p_1^{j+1})^s - (1-p_1^j)^s\right).$$

It is not difficult to show that, as s tends to infinity,

$$M(p_1, s) \sim \frac{\log s}{\log(1/p_1)}, \tag{7}$$

and that this holds more generally for any value of p_1 satisfying $0 < p_1 < 1$ [18]. By more subtle techniques [4, 22] it can be shown that

$$M(p_1, s) \approx \frac{1}{\log(1/p_1)} \sum_{r=1}^{s} \frac{1}{r} - \frac{1}{2},$$

where the approximation is remarkably good and $0 < p_1 < 1$. The interpretation of the latter result is somewhat disappointing: if one has found $M(s) := \max_{1\leq k\leq s} g_{k^2 326}(L)$ with $s = 10^6$, say, then in order to find a k such that $g_{k^2 326}(L) \geq 2M$ one expects to have to compute $g_{k^2 326}(L)$ for all k up to around 10^{12} in order to achieve this. The numerics seem to confirm the slow growth of $M(s)$. For example, $M(350) = 1123$ and $M(25000) = 1614$.

One can wonder how 'special' it is to find a given value of $c_{k^2 326}(L)$. An obvious measure for this is the smallest integer s such that $M(p_1, s) = c_{k^2 g}(L)$. For 1614 for example this is around 32500, i.e., one would expect to try around 32500 values of k before finding $c_{k^2 326}(L) \geq 1614$.

Griffin's and Lehmer's polynomial for $g = 10$, respectively $g = 326$ show that there are quadratic polynomials f and integers g such that $(\frac{g}{p}) \neq 1$ for all primes of the form $f(n)$, i.e. all the primes $p = f(n)$ are inert in $\mathbb{Q}(\sqrt{g})$. In the next section we investigate this situation further.

5 On the splitting of primes $p = f(n)$ in a quadratic field

This section is devoted to a conditional result on the splitting behaviour of primes of the form $p = f(n)$ in a prescribed quadratic field K. In the case where f is quadratic we will make this result more explicit.

Let $d > 1$ be an odd squarefree integer. Put

$$a_d(f) = \frac{\sum_{r (\mathrm{mod}\ d)} \left(\frac{f(r)}{d}\right)}{\#\{r (\mathrm{mod}\ d) : (f(r), d) = 1\}}. \tag{8}$$

Note that $-1 \le a_d(f) \le 1$. By the Chinese Remainder Theorem and the multiplicative property of the Jacobi symbol the quantity $a_d(f)$ is seen to be a multiplicative function on odd squarefree integers d. Thus $a_d(f) = \prod_{p|d} a_p(f)$. Note that if $p > 2$ and $N_p(f)$ is even, then $a_p(f)$ is odd and hence $a_p(f) \ne 0$.

Theorem 1 *Let D be a fundamental discriminant. Suppose that $f(n)$ is prime for infinitely many n and that the n for which $f(n)$ is prime are equidistributed over the residue classes $a (\mathrm{mod}\ D)$ with $(f(a), D) = 1$. The proportion $\tau_D^-(f)$ of primes p satisfying $p = f(n)$ for some n that are, moreover, inert in a quadratic field of discriminant D exists and is a rational number. Let D_1 be the largest odd prime divisor of D and assume that $D_1 > 1$. For $j = 1, 3, 5$ and 7 put*

$$\alpha_j = \frac{\#\{s (\mathrm{mod}\ 8) : f(s) \equiv j (\mathrm{mod}\ 8)\}}{4\#\{s (\mathrm{mod}\ 2) : f(s) \equiv 1 (\mathrm{mod}\ 2)\}}.$$

We have

$$2\tau_D^-(f) = \begin{cases} 1 - a_{D_1}(f) & \text{if } D \text{ is odd;} \\ 1 + (\alpha_3 + \alpha_7 - \alpha_1 - \alpha_5) a_{D_1}(f) & \text{if } D \equiv 4 (\mathrm{mod}\ 8); \\ 1 + (\alpha_3 + \alpha_5 - \alpha_1 - \alpha_7) a_{D_1}(f) & \text{if } D \equiv 8 (\mathrm{mod}\ 32); \\ 1 + (\alpha_5 + \alpha_7 - \alpha_1 - \alpha_3) a_{D_1}(f) & \text{if } D \equiv 24 (\mathrm{mod}\ 32). \end{cases}$$

Moreover, $a_{D_1}(f) = \prod_{p|D_1} a_p(f)$, with

$$a_p(f) = \frac{\sum_{j=0}^{p-1} \left(\frac{f(j)}{p}\right)}{p - N_p(f)}.$$

Proof. Let us consider the case where $D > 1$ and $D \equiv 1 (\mathrm{mod}\ 4)$ first. Note that p is inert in K iff $(\frac{D}{p}) = -1$. Since $D \equiv 1 (\mathrm{mod}\ 4)$, we have $(\frac{D}{p}) = (\frac{p}{D})$ and thus only the value of $p (\mathrm{mod}\ D)$ matters. By assumption the corresponding values of n are equidistributed asymptotically. Therefore $\tau_D^-(f)$, the proportion of primes of the form $f(n)$ which are inert in K, satisfies

$$\tau_D^-(f) = \frac{\#\{r (\mathrm{mod}\ D) : (\frac{D}{f(r)}) = -1\}}{\#\{r (\mathrm{mod}\ D) : (f(r), D) = 1\}} = \frac{\#\{r (\mathrm{mod}\ D) : (\frac{f(r)}{D}) = -1\}}{\#\{r (\mathrm{mod}\ D) : (f(r), D) = 1\}}.$$

Let us denote the corresponding proportion of split primes by $\tau_D^+(f)$. We have $\tau_D^-(f) + \tau_D^+(f) = 1$ and $\tau_D^+(f) - \tau_D^-(f) = a_D(f)$, whence $\tau_D^-(f) = (1 - a_D(f))/2$, as required.

In case $2|D$ we consider the various congruence classes modulo 8 separately. Each of them can then be dealt with as before (this involves quadratic reciprocity). We find that

$$2\tau_D^-(f) = \begin{cases} \tau_{D_1}^-(f)\{\alpha_1 + \alpha_5\} + \tau_{D_1}^+(f)\{\alpha_3 + \alpha_7\} & \text{if } D \equiv 4 (\mathrm{mod}\ 8); \\ \tau_{D_1}^-(f)\{\alpha_1 + \alpha_7\} + \tau_{D_1}^+(f)\{\alpha_3 + \alpha_5\} & \text{if } D \equiv 8 (\mathrm{mod}\ 32); \\ \tau_{D_1}^-(f)\{\alpha_1 + \alpha_3\} + \tau_{D_1}^+(f)\{\alpha_5 + \alpha_7\} & \text{if } D \equiv 24 (\mathrm{mod}\ 32). \end{cases}$$

The remaining details are left to the interested reader. $\square$

`Remark` 1. Note that under the assumption of Hardy-Littlewood's Conjecture F the hypothesis of the result is satisfied. (For then Conjecture 1 holds true.)

`Remark` 2. Notice that the condition that $f(n)$ represents infinitely many primes ensures that α_j exists for $j = 1, 3, 5$ and 7. These numbers can be explicitly evaluated, but this requires a lot of case distinctions.

`Remark` 3. In case $\tau_D^-(f) = 1$, then it is *unconditionally* true that, with finitely many exceptions, all primes represented by f are inert in $\mathbb{Q}(\sqrt{D})$. In this case we have that $(\frac{D}{f(r)}) = -1$ for all allowable congruence classes $r(\text{mod } D)$. Since there are at most finitely many primes represented by f for r that are not allowable, the assertion follows. Similarly, if $\tau_D^-(f) = 0$, then it is unconditionally true that, with finitely many exceptions, all primes represented by f split completely in $\mathbb{Q}(\sqrt{D})$.

5.1 The case where f is quadratic

Before we state the main result of this section (Proposition 2), we need some preliminaries on certain simple character sums.

The following two lemmas are well-known, see [9, p. 79]. The proof of Lemma 2 given here (suggested by I. Shparlinski) is more natural than the one in [9, p. 79].

Lemma 2 *Let p be an odd prime. Then*

$$\sum_{m=0}^{p-1} \left(\frac{m^2+a}{p}\right) = \begin{cases} p-1 & \text{if } p|a; \\ -1 & \text{otherwise.} \end{cases}$$

Proof. Let $\nu_j(p)$ denote the number of $0 \le m \le p-1$ such that $(\frac{m^2+a}{p}) = j$. The sum under consideration equals $\nu_1(p) - \nu_{-1}(p)$ and so the result follows once we compute $\nu_1(p)$ and $\nu_{-1}(p)$. If $p|a$ the assertion is trivial. Next assume that $(\frac{-a}{p}) = -1$. Let us count the number of pairs (m, y) with $0 \le m, y \le p-1$ such that $m^2 + a \equiv y^2(\text{mod } p)$. Note that $y = 0$ does not occur. Equivalently we want to have $a \equiv (y-m)(y+m)(\text{mod } p)$. Write $u = y - m$ and $v = y + m$. There are $p-1$ pairs (u, v) satisfying $a \equiv uv(\text{mod } p)$. Using that the pairs (u, v) are in bijection with the pairs (m, y) and that with each pair (m, y) there is a pair $(m, p-y)$, we infer that $\nu_1(p) = \frac{p-1}{2}$. On noting that $\nu_0(p) = 0$, we infer that $p = \nu_{-1}(p) + \nu_0(p) + \nu_1(p) = \nu_{-1}(p) + \frac{p-1}{2}$ and hence $\nu_{-1}(p) = \frac{p+1}{2}$. Thus $\nu_1(p) - \nu_{-1}(p) = -1$ and the result follows in this case. In the remaining case $(\frac{-a}{p}) = 1$ a similar argument shows that $\nu_{-1}(p) = \frac{p-1}{2}$, $\nu_0(p) = 2$ and $\nu_1(p) = \frac{p-3}{2}$ and thus that $\nu_1(p) - \nu_{-1}(p) = -1$ again. $\square$

Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial. Put $d = b^2 - 4ac$ and

$$T_p(f) = \sum_{m=0}^{p-1} \left(\frac{f(m)}{p}\right).$$

Lemma 3 *Let p be an odd prime. Then*

$$T_p(f) = \begin{cases} -(\frac{a}{p}) & \text{if } p \nmid ad; \\ p(\frac{c}{p}) & \text{if } p|(a,d); \\ (p-1)(\frac{a}{p}) & \text{otherwise.} \end{cases}$$

Proof. If $p \nmid a$, then

$$(\frac{a}{p})T_p(f) = (\frac{4a}{p})T_p(f) = \sum_{m=0}^{p-1} \left(\frac{(2am+b)^2 - d}{p} \right) = \sum_{m=0}^{p-1} \left(\frac{k^2 - d}{p} \right),$$

where $k = 2am + b$. The proof is easily completed on invoking the previous lemma. (For more details see, e.g., [9, p. 79], see also [1]). □

`Remark`. S. Arms, Á. Lozano-Robledo and S.J. Miller [1] use Lemma 2 and 3 in their method of constructing elliptic curves over $\mathbb{Q}(T)$ with moderate rank.

Lemma 4 *Let p be an odd prime. Then*

$$a_p(f) = \begin{cases} \frac{-(\frac{a}{p})}{p-1-(\frac{d}{p})} & \text{if } p \nmid ad; \\ 0 & \text{if } p|a,\ p \nmid d; \\ (\frac{a}{p}) & \text{if } p \nmid a,\ p|d; \\ (\frac{c}{p}) & \text{if } p|(a,d). \end{cases}$$

Proof. The denominator in (8) is easily evaluated in prime arguments. On combining this computation with Lemma 3 the result follows. □

The next result in the case where $(D, a, d) = 1$ was first established by Andrew Granville (with a different proof).

Proposition 2 *Let $D_1 > 0$ be an odd squarefree integer. We have*

$$a_{D_1}(f) = \begin{cases} \left(\frac{c}{(D_1, a, d)} \right) \left(\frac{a}{D_1/(D_1, a)} \right) \prod_{\substack{q|D_1 \\ q \nmid ad}} \frac{-1}{q - 1 - (\frac{d}{q})} & \text{if } (D_1, a)|d; \\ 0 & \text{if } (D_1, a) \nmid d. \end{cases}$$

Alternatively,

$$a_{D_1}(f) = \left(\frac{c}{(D_1, a, d)} \right) \left(\frac{a}{D_1/(D_1, a, d)} \right) \prod_{\substack{q|D_1 \\ q \nmid ad}} \frac{-1}{q - 1 - (\frac{d}{q})}.$$

Proof. Note that $a_{D_1}(f) = \prod_{p|D_1} a_p(f)$. Then invoke the previous lemma. □

Let $\mathcal{F}$ be as in Section 2. The latter result in combination with Theorem 1 gives:

Proposition 3 *Assume Conjecture* 1. *Let $f \in \mathcal{F}$ and D be its discriminant.*
1) *If $\tau_D^-(f) \neq 0, 1$, then $1/3 \leq \tau_D^-(f) \leq 2/3$.*
2) *If $\tau_D^-(f) = 0$ or $\tau_D^-(f) = 1$, then $D|24ad$.*

Remark 1. We have $\tau_5^-(3X^2+7)=1/3$ and $\tau_5^-(X^2+1)=2/3$ (thus the bounds in part 1 are sharp). One computes that $\tau_{-3}^-(X^2+5)=1$ and thus $D|24ad$ in part 2 cannot be replaced by $D|8ad$.
Remark 2. It can happen for a given $f\in\mathcal{F}$ that there is no discriminant D for which $\tau_D^-(f)=1$, e.g. for $f(X)=X^2+X+41$.

The latter proposition strongly suggests that in order to find large $c_g(f)$ we have to ensure that $\tau_D^-(f)=1$, where D denotes the discriminant of $\mathbb{Q}(\sqrt{g})$. This highly restricts the possible choices of D. For Lehmer's polynomial L, for example, one finds that $\tau_D^-(L)=1$ iff $D=-163,-3,24$ or 1304.

5.2 Higher degree f

If f induces a permutation of $\mathbb{F}_p$ (that is, is a permutation polynomial), then clearly $a_p(f)=0$. E.g. if $f(X)=X^n+k$ and $(p-1,n)=1$, then f induces a permutation of $\mathbb{F}_p$ and hence $a_p(f)=0$.

Suppose that $Y^2=f(X)$ is the Weierstrass equation of an elliptic curve E having conductor N_E. Hasse's inequality yields $|a_p(f)|\le 2\sqrt{p}/(p-3)$ for $p>3$. It is well-known that $\sum_{j=0}^{p-1}(\frac{f(j)}{p})$ is the trace of Frobenius over $\mathbb{F}_p$. In the remainder of this section it is assumed that the conditions of Theorem 1 are satisfied, so that Theorem 1 can be invoked. It follows that if $D\equiv 1(\mathrm{mod}\ 4)$ and $(N_E,D)=1$, then $\tau_D^-(f)=1/2$ iff there is prime p dividing D such that E is supersingular at p. Since Deuring it is known that the number of supersingular primes $p\le x$ in case of a CM curve E grows asymptotically as $\pi(x)/2$ and hence for almost all quadratic fields of odd discriminant D one has in this case $\tau_D^{-1}(f)=1/2$ (again under the conditions of Theorem 1). On the other hand, if E does not have complex multiplication one finds using the result of Serre that the number of supersingular primes $p\le x$ is then bounded by $\ll x(\log x)^{-5/4+\epsilon}$ that for a positive proportion of the fundamental discriminants $D\equiv 1(\mathrm{mod}\ 4)$ one has $\tau_D^-(f)=1/2$.

6 Heuristics for the proportion of primitive roots

In the previous section we gave an heuristic for the proportion $\tau_D^-(f)$ of primes $p=f(n)$ such that $(\frac{g}{p})=-1$. In this section we do the same but with the more stringent condition that g should be a primitive root modulo p. Numerical work suggests the truth of:

Conjecture 3 *Suppose that $f(X)\in\mathbb{Z}[X]$ represents infinitely many primes. Then the quotient of*

$$\#\{p\le x : f(m)=p \text{ for some } m \text{ and } g \text{ is a primitive root mod } p\}$$

and $\#\{p\le x : f(m)=p$ for some $m\}$ tends to a limit as x tends to infinity, that is the relative proportion of primes p such that g is a primitive root mod p and moreover p is represented by $f(x)$ exists. Let us denote this conjectural density by $\delta_g(f)$.

In the remainder of this section it is assumed that the latter conjecture holds true. It is also supposed that g is not an hth power of an integer for any $h \geq 2$.

Suppose that g is such that $\tau_D^-(f) = 1$, where D is the discriminant of $\mathbb{Q}(\sqrt{g})$ (the most relevant case for our purposes). Then, by an argument similar to that used in the derivation of (6), one is led to believe that a good approximation for $\delta_g(f)$ should be

$$\delta(f) := \prod_{q>2} \left(1 - \frac{\#\{s(\text{mod } q) : f(s) \equiv 1(\text{mod } q)\}}{q\#\{s(\text{mod } q) : f(s) \not\equiv 0(\text{mod } q)\}}\right). \tag{9}$$

In case $f(X) = AX^2 + B$ a short calculation shows that

$$\delta(f) = \prod_{\substack{q|(A,B-1)\\ q>2}} (1 - \frac{1}{q}) \prod_{q \nmid 2A} \left(1 - \frac{\{1 + \left(\frac{-A(B-1)}{q}\right)\}}{q(q - 1 - \left(\frac{-AB}{q}\right))}\right).$$

If $\delta(f)$ is close to 1, then

$$\delta_1(f) := \prod_{\substack{q|(A,B-1)\\ q>2}} (1 - \frac{1}{q}) \prod_{q \nmid 2A} \left(1 - \frac{\{1 + \left(\frac{-A(B-1)}{q}\right)\}}{q^2}\right),$$

yields a quite good approximation to $\delta(f)$; compare (5) with (6). Clearly the idea in finding a large value of $c_g(f)$ is to find f such that $\delta(f)$ is close to 1. For this results from the theory of prime producing quadratics can be used. Note that $\delta_1(f)$ is a rational multiple of

$$\prod_{q\geq 3} \left(1 - \frac{\{1 + (\frac{\Delta}{q})\}}{q^2}\right) = \frac{3}{4}\zeta(2) \prod_{q\geq 3} \left(1 - \frac{(\frac{\Delta}{q})}{q^2 - 1}\right), \tag{10}$$

where $\Delta = -A(B - 1)$. It is not difficult to show that for $\text{Re}(s) \geq 1$

$$\prod_{q\geq 3} \left(1 - \frac{\chi_\Delta(q)}{q^s - 1}\right) = \epsilon(s)\frac{\zeta(2s)}{L(s, \chi_\Delta)} \prod_{q|\Delta} (1 - \frac{1}{q^{2s}}) \prod_{\substack{q\geq 3\\ (\frac{\Delta}{q})=1}} \left(1 - \frac{2}{q^s(q^s - 1)}\right), \tag{11}$$

where $\epsilon(s) = 1 + 2^{-s}(\frac{\Delta}{2})$. On combining the latter two formulae one sees that the behaviour of $\delta_1(f)$ is very much determined by that of $L(2, \chi_\Delta)$.

For a general quadratic $f(X) = aX^2 + bX + c$ one finds that

$$\frac{\varphi((a, b, c - 1))}{(a, b, c - 1)L(2, (d/.))} \ll \delta(f) \ll \frac{\varphi((a, b, c - 1))}{(a, b, c - 1)L(2, (d/.))}, \tag{12}$$

where $d = b^2 - 4a(c - 1)$.

7 Prime producing quadratics

Let $f_A(X) = X^2 + X + A$, with $A > 0$ a positive integer. Euler discovered in 1772 that $X^2 + X + 41$ satisfies $\pi_{f_{41}}(39) = 40$. It can be shown that $\pi_{f_A}(A-2) = A-1$ iff $A \in \{2, 3, 5, 11, 17, 41\}$, see Mollin [17], and that this is related to the class number one problem. The connection with the class number one problem dates back to Frobenius (1912) and Rabinowitsch (1913). The discriminant of $f_A(X)$ is given by $\Delta = 1 - 4A$. Note that if A is even, then $2|f_A(x)$ and so we may assume that A is odd and hence $\Delta \equiv 5 (\mathrm{mod}\ 8)$. If for a prime q, $(\frac{\Delta}{q}) = -1$, then the values of f_A are not divisible by q. So if $(\frac{\Delta}{q}) = -1$ for many consecutive primes q, the values of f_A have a better chance of being prime, in particular if Δ is also small. Thus we want

$$L(1, \chi) = \prod_q \frac{1}{1 - \chi(q)/q}, \tag{13}$$

where $\chi_\Delta(n) = (\Delta/n)$ and $(./n)$ is the Kronecker symbol, to be small. Since with two exceptions $\pi h/\sqrt{|\Delta|} = L(1, \chi_\Delta)$, we want the class number h to be small. By (3) one should have, as x tends to infinity, $\pi_{f_A}(x) \sim C(\Delta)x/\log x$, where

$$C(\Delta) = \prod_{q \geq 3} \left(1 - \frac{(\frac{\Delta}{q})}{q-1}\right).$$

It is easy to show (using that $(\Delta/2) = -1$) that

$$C(\Delta) = \frac{\zeta(4)}{2L(1, \chi_\Delta)L(2, \chi_\Delta)} \prod_{q|\Delta} (1 - \frac{1}{q^4}) \prod_{\substack{q \geq 3 \\ (\frac{\Delta}{q})=1}} \left(1 - \frac{2}{q(q-1)^2}\right). \tag{14}$$

Shanks has computed $C(-163) = 3.3197732\ldots$ and $C(-111763) = 3.6319998\ldots$. Thus Beeger's [3] polynomial $X^2 + X + 27941$ should produce asymptotically more primes than Euler's. One computes that $\pi_{f_{41}}(10^6) = 261080$ and $\pi_{f_{27941}}(10^6) = 286128$. On the other hand $\pi_{f_{41}}(39) = 40$, whereas $\pi_{f_{27941}}(39) = 30$. The constant $C(\Delta)$ can become arbitrarily large: for every $\epsilon > 0$ there are infinitely many Δ such that

$$(1/2 + \epsilon)e^\gamma \log\log|\Delta| < C(\Delta) < (1 + \epsilon)e^\gamma \log\log|\Delta|,$$

where γ denotes Euler's constant (see [13, p. 511-512]).

Quadratics that produce too many primes contradict the Generalized Riemann Hypothesis. If there are lots of Siegel zeros this can be used to infer results on the growth of $\pi_f(x)$. This is akin to Heath-Brown's result that if there are many Siegel zeros, then the twin primes behave as expected. For more on the analytic aspects of prime-producing polynomials, see [8].

In order to find Δ with $(\frac{\Delta}{q}) = -1$ for many consecutive primes q, special purpose devices have been built (some even involving bicycle chains !). For a nice account of this see Lukes, Patterson and Williams [15].

In searching for good prime producing quadratics it is thus tantamount to find Δ for which $C(\Delta)$ is large. Similarly, for Problem 2 we want $\delta(f)$ to be close to 1. Equation (14) shows that finding a large value of $C(\Delta)$ amounts to finding

Δ such that $L(1, \chi_\Delta)$ is small. For $s = 1$ identity (11) gives an expression for $C(\Delta)$ and for $s = 2$ we obtain an expression closely related to $\delta_1(f)$ (which on its turn gives a good approximation to $\delta(f)$). However, in case $s = 1$ the latter product in the expression does not converge very well and preference is to be given to expression (14). In contrast, in case $s = 2$ the expression (11) is quite usable. The special value $L(2, \chi_\Delta)$ involved can be evaluated with high precision, see [13].

Let $\alpha \geq 1$. If $f(X)$ is a prime producing quadratic, then $g_\alpha(X) = 2^\alpha f(X) + 1$ is likely to be Artin prime producing for those g satisfying $\tau_D^-(g_\alpha) = 1$, with D the discriminant of $\mathbb{Q}(\sqrt{g})$. Conversely, if $g(X)$ is a Artin prime producing quadratic, then we can write $g(X) - 1 = 2^\alpha(aX^2 + bX + c)$ with $\alpha \geq 0$ and $(a, b, c) = 1$. Write $h(X) = aX^2 + bX + c$. If $N_2(h) = 0$, then h is likely to be prime producing. Thus the connection between Artin prime producing and prime producing quadratics is rather intimate.

8 Finding Artin prime producing quadratics

In general an approach to Problem 2 is to find an integer d such that $|d|$ is small and $(\frac{d}{q}) \neq 1$ for as many small odd primes q as possible. Thus we hope to ensure that $\delta(f)$ (the quality of f) is very close to 1. We factorize d as $d_1 d_2$ and choose a small α. Then we consider primes p of the form $2^\alpha d_1 n^2 + 2^\alpha d_2 + 1$. Since we want $(\frac{g}{p}) \neq 1$ for all primes of the latter form, the choice of g is rather restricted: under Conjecture 1 the discriminant $\mathbb{Q}(\sqrt{g})$ has to be a divisor of $24 d_1(2^\alpha d_2 + 1)$ by Proposition 3. It can happen that no suitable g can be found and then α can be adjusted. If g has the required property, so has $k^2 g$ for every integer k. Now we vary over k in the hope of finding a large value of $c_{k^2 g}(2^\alpha d_1 X^2 + 2^\alpha d_2 + 1)$. Another variation option we have is to consider primes p of the form $2^\alpha d_1 r_1 n^2 + 2^\alpha d_2 r_2 + 1$ with $r_1 r_2$ a square and with $r_1 r_2$ having only large prime factors. The corresponding value of $\delta(f)$ changes little by this and again we can search for a large value of $c_g(2^\alpha d_1 r_1 X^2 + 2^\alpha d_2 r_2 + 1)$. (In this variation g remains fixed and thus it can be used in dealing with the variation of Problem 2 discussed in the introduction.) Since we want $(\frac{g}{p}) \neq 1$ usually some mild congruence conditions on r_1 and r_2 have to be imposed. A further variation possibility is to replace n by $\gamma n + \delta$. However, computational practice suggests this is only effective when $\gamma = 1$.

The asymptotic (7) suggests that it is crucial to get a large value of $\delta(f)$: if this value is not close enough to 1, then there is not much to be gained by letting k run over a large range (note that in general $p_1 = \delta_g(f)$).

`Example 1`. The number $d = 4472988326827347533$ satisfies $(d/p) = -1$ for the primes $p = 3, \ldots, 283$ by Table 4.3 of [13]. A factor of d is $d_1 = 252017$. Let $d_2 = d/d_1$. Let $f(X) = 1008068X^2 + 16921429448X + 15753313937$. (This is $4d_1(X + 8393)^2 - 4d_2 + 1$.) The first 'bad' prime equals 432050978399143373. It turns out that $c_{170363492}(f) = 22779$. One finds that $\delta(f) \approx 0.999453$ and that $M(\delta(f), 145700) \approx 22779$.

`Example 2`. (Y. Gallot). We let d be as in Example 1, $d_1 = 230849$ and $d_2 = d/d_1$. Let $f(X) = 64d_1(X + 728069)^2 - 64d_2 + 1$ and $g = 17^2 \cdot 230849 = 66715361$. Then $c_g(f) = 25581$. This is the presently largest known value of $c_g(f)$ for an f having positive discriminant. One finds that $\delta(f) \approx 0.999453$ and that $M(\delta(f), 675200) \approx 25581$.

Let $f(X) = 64d_1(X + 56943)^2 - 64d_2 + 1$. Then $d_{24}(f) = 21690$. This is the record for $c_g(f)$ with $|g| < 100$.

`Example 3`. The number $d = 9828323860172600203$ satisfies $(-d/p) = -1$ for the primes $p = 3, \ldots, 277$ by Table 4.1 of [13]. A factor of d is $d_1 = 54151$. Let $d_2 = d/d_1$. Let $f(X) = 866416X^2 + 2903975582404049$. (This is $16d_1X^2 + 16d_2 + 1$.) It turns out that $c_{23731350844}(f) = 18176$. Let $f_1(X) = f(X + 599206)$. One computes that $c_{72922}(f_1) = 29083$. Let $f_2(X) = d_1(X + 1484224)^2 + d_2 + 1$. Then $c_{17431902}(f_2) = 31082$. This is the presently largest known value of $c_g(f)$ for an f having negative discriminant and was discovered by Yves Gallot. One finds that $\delta(f_2) \approx 0.999535$ and that $M(\delta(f_2), 1066000) \approx 31082$.

9 On the (un)boundedness of $c_g(f)$

A tool in investigating this is an extension of a criterion of Chebyshev which is discussed in the next section.

9.1 Extension of a primitive root criterion of Chebyshev

It is an old result of Chebyshev that if $p_1 \equiv 1 (\mathrm{mod}\ 4)$ is prime and $p_2 = 2p_1 + 1$ is also prime, then $g = 2$ is a primitive root modulo p_2. Under TC(2) it then follows that 2 is a primitive root for infinitely many primes. Unconditionally it is not known whether there are infinitely many primes satisfying Chebyshev's criterion, but it can be shown that there are infinitely many primes satisfying a somewhat weaker version of it. This can then be used to show, e.g., that at least one of the numbers $2, 3$ and 5 is a primitive root for infinitely many primes [11].

Already in the 19th century Chebyshev's criterion was extended to some numbers other than 2, see e.g. [23]. In this section an analogue of Chebyshev's criterion is derived for every integer g in G. This criterion plays a keyrole in the proof of Theorem 2.

Lemma 5 *Let $g \geq 3$ be an odd squarefree integer. There exists an integer a such that $(a, g) = 1$ and $(\frac{8a+1}{g}) = -1$.*

Proof. It is easy to see that the result holds true in case g is an odd prime. In case $g \geq 5$ is an odd prime, likewise there exists an integer b such that $(b, g) = 1$ and $(\frac{8b+1}{g}) = 1$. From these two observations the result follows on invoking the Chinese Remainder Theorem. □

Lemma 6 *Suppose that $g \in G$. Write $g = {g_0}^2 g_1$ with g_1 squarefree. Let $g_2 = |g_1|$ if g_1 is odd and $g_2 = |g_1/2|$ otherwise.*

For parts 1 and 2 it is assumed that $g_1 \neq \pm 2$.

1) Let a be any integer such that $(a, g_2) = 1$ and $(\frac{8a+1}{g_2}) = -1$ (by Lemma 5 at least one such integer exists). If p_1 is a prime of the form $g_2 k + a$ such that $p_2 := 8p_1 + 1$ is also a prime and $g^8 \not\equiv 0, 1 (\mathrm{mod}\ p_2)$, then g is a primitive root modulo p_2.

2) Under TC(2) *there are infinitely many primes p_1 satisfying the conditions of part 1.*

3) Assume that $g_1 = \pm 2$. If p_1 is a prime and $p_2 := 2p_1 + 1$ is a prime, then g is a primitive root modulo p_2 if $p_1 \equiv \mathrm{sgn}(g) (\mathrm{mod}\ 4)$ and $g^2 \not\equiv 0, 1 (\mathrm{mod}\ p_2)$. If TC(2) *holds true, there are infinitely many primes p such that g is a primitive root modulo p.*

Proof. 1) The assumption $g^8 \not\equiv 0, 1 (\mathrm{mod}\ p_2)$ ensures that the order of g modulo p_2 exists and is a multiple of p_2. Since

$$(\frac{g}{p_2}) = (\frac{g_1}{p_2}) = (\frac{g_2}{p_2}) = (\frac{p_2}{g_2}) = (\frac{8a+1}{g_2}) = -1,$$

and $-1 = (\frac{g}{p_2}) \equiv g^{4p_1} (\mathrm{mod}\ p_2)$, the order must be $8p_1 = p_2 - 1$.
2) We have to show that for each prime p there exists k for which

$$(g_2 k + a)(8g_2 k + 8a + 1) \not\equiv 0 (\mathrm{mod}\ p). \tag{15}$$

For $p = 2$ this is clear. In case $p|g_2$ this follows since we have $(a, g_2) = 1$ and $(8a + 1, g_2) = 1$. For the remaining primes p there are at least $p - 2 \geq 1$ choices of $0 \leq k < p$ such that (15) is satisfied.
3) Similar to the proof of parts 2 and 3. □

Corollary 1 *Artin's primitive root conjecture is true, assuming* TC(2).

Another generalisation of Chebyshev's criterion is in the direction of cubic reciprocity. For example, if p is an odd prime such that $q = 1 + 6p$ is a prime then 3 is not a primitive root mod q iff we can write $4p = n^2 + 243m^2$ with n, m integers. This criterion is due to Fueter [6].

9.2 A conditional result on $c_g(f)$

Lemma 6 will be used in the proof of the following theorem, the basic idea of which is due to Andrew Granville.

Theorem 2 *Let $N \geq 1$ be an integer. Assume* TC($2N$). *Suppose that $g \in G$. Then there exist integers A_1 and C_1 such that $A_1 n^2 + C_1$ is prime for $n = 1, \ldots, N$ and g is a primitive root for each of these primes.*

Here and in the sequel A_1 and C_1 are allowed to depend on N.

Corollary 2 *Assume* TC($2N$) *for every $N \geq 1$. Let $g \in G$ be fixed. The number $c_g(AX^2 + C)$ can be larger than any prescribed number.*

Remark. Let $N \geq 1$ be an integer and $g \in G$. Perhaps it is possible to show under TC that there exist integers A_1 and C_1 such that $A_1 n^2 + C_1$ is prime for $n = 1, 2, \ldots, N+1$ and g is a primitive root for the first N of these primes, but not for the $(N+1)$th. This would show that $c_g(AX^2 + C)$ can assume any prescribed natural number as value under TC.

Proof of Theorem 2. We adopt the notation of Lemma 6 and assume that $g_1 \neq \pm 2$ (the remaining case being similar).

Let $A = \prod_{p \leq 2N} p$ and C be the smallest integer $> 2N$ with $C \equiv a(\text{mod } g_2)$ for which C and $8C+1$ are both primes (C exists by part 2 of Lemma 6). Consider the $2N$-tuplet of numbers $g_2 At + C + g_2 An^2$ for $n = 1, \ldots, N$ and $8g_2 At + 8C + 1 + 8g_2 An^2$ for $n = 1, \ldots, N$ for integer t. TC($2N$) predicts that there will be infinitely many t for which these are all prime, provided there is no obstruction modulo a prime p (i.e. it is not true that for every t at least one of the forms is divisble by p). (We will take $A_1 = 8g_2 A$ and $C_1 = 8g_2 At + 8C + 1$ above for one of these t's such that, moreover, none of the primes $p(n)$ of the form $A_1 n^2 + C_1$ with $n = 1, \ldots, N$ satisfies $g^8 \equiv 0, 1(\text{mod } p(n))$). Now for $p \leq 2N$, we see that $p|A$ and $p \nmid C(8C+1)$, so p never divides any of the forms. If $p|g_2$ the first N forms are $\equiv a(\text{mod } p)$ and the second N forms are $\equiv 8a+1(\text{mod } p)$. The conditions on a ensure that $a(8a+1) \not\equiv 0(\text{mod } p)$. In general there are at most $2N$ values of t for which at least one of our $2N$ linear forms is divisible by p, so if $p > 2N$ and $p \nmid g_2$, there exists an integer t such that none of them is divisible by p.

Let $p(n) = A_1 n^2 + C_1$. Now for $1 \leq n \leq N$ each $p(n)$ is a prime for which $(p(n)-1)/8$ is also a prime and satisfies the conditions of part 1 of Lemma 6 and hence g is a primitive root modulo $p(n)$. □

Lemma 7 *Suppose that* $g_i \neq -1$ *for* $i = 1, \ldots, s$ *and that*

$$(\frac{g_1}{p}) = \ldots = (\frac{g_s}{p}) = -1 \tag{16}$$

for infinitely many primes $p \equiv 2(\text{mod } 3)$*, then there exists* $1 \leq m \leq 2$*,* a *and* f *with* $(a, f) = 1$*, such that for every prime* q *satisfying* $q \equiv a(\text{mod } f)$ *for which* $q_1 = 2^m q + 1$ *is also a prime and* $g_i^{2^m} \not\equiv 0, 1(\text{mod } q_1)$ *for* $i = 1, \ldots, s$*, then the integers* $g_1, \ldots, g_s$ *are simultaneously primitive roots modulo* q_1*.*

Proof. Let $Q = \{q_1, \ldots, q_t\}$ be the set of odd primes dividing the discriminant of $\mathbb{Q}(\sqrt{g_i})$ for some $1 \leq i \leq s$. Let $A_{+1}(q)$ be the set of non-zero quadratic residues modulo q and $A_{-1}(q)$ the set of quadratic non-residues. It is a consequence of quadratic reciprocity that there exist $\epsilon_i \in \{-1, 1\}$ with the property that for each choice of elements $\alpha(\epsilon_i) \in A_{\epsilon_i}(q)$, there are infinitely many primes p satisfying (16) such that, moreover, $p \equiv \alpha(\epsilon_i)(\text{mod } q_i)$ for $1 \leq i \leq t$. The condition that $p \equiv 2(\text{mod } 3)$ now ensures that we can pick $\alpha(\epsilon_i) \neq 1$. The argument can easily be extended to take the behaviour at the prime two into account. One sees one can pick $\beta \in \{3, 5, 7\}$ such that there are infinitely many primes p satisfying (16) such that $p \equiv \beta(\text{mod } 8)$ and $p \equiv \alpha(\epsilon_i)(\text{mod } q_i)$ for $1 \leq i \leq t$. Setting $f = 8q_1 \cdots q_t$, one then finds that a with $2^m a + 1 \equiv \beta(\text{mod } 8)$ and $2^m a + 1 \equiv \alpha(\epsilon_i)(\text{mod } q_i)$ for $1 \leq i \leq t$ exists and satisfies the requirement $(a, f) = 1$, provided we set $m = 2$

if $\beta = 5$ and $m = 1$ otherwise. The proof is then finished by an argument as used in the proof of Lemma 6. $\square$

The following result generalizes Theorem 2.

Theorem 3 *Let $s \geq 1$ be an integer and let $g_1, \ldots, g_s$ be integers $\neq -1, 0, 1$. Let $0 \leq e_1, \ldots, e_s \leq 1$. Suppose that $\prod_{i=1}^{s} g_i^{e_i}$ is not a square if $e_1 + \ldots + e_s$ is odd. Suppose furthermore that the discriminant of each of the fields $\mathbb{Q}(\sqrt{g_i})$ is not divisible by 3. Then there exist integers A and C such that $p(j) = Aj^2 + C$ is prime for $1 \leq j \leq n$ and each of the g_i is a primitive root modulo $p(j)$.*

Proof. Using the argument at p. 37 of Heath-Brown [11], one easily infers that the conditions of Lemma 7 are satisfied. Thus there exist numbers a, f and m as in that lemma. Now proceed as in the proof of Theorem 2. Thus take C to be the smallest integer $> 2N$ with $C \equiv a(\text{mod } f)$ and replace $8C + 1$ by $2^m C + 1$. The rest of the argument is left as a (copy) exercise to the interested reader. $\square$

`Remark`. I do not see how to prove this result with for example $g_1 = -25$ and $g_2 = 3$, although in this case under GRH it can be shown that there are infinitely many primes p such that both are primitive roots [16]. In essence the question amounts to this one: for each $N \geq 1$ are there A and C such that $p(j) = Aj^2 + C \equiv 7(\text{mod } 12)$ are all prime and 3 is a primitive root mod $p(j)$ for $1 \leq j \leq N$? One seems to be forced to use cubic reciprocity, cf. Fueter's criterion (Section 9.1).

10 Conclusion

The above arguments and experiments suggest the following conjecture.

Conjecture 4
1) *For quadratic f Griffin's dream cannot be realized, i.e. $c_g(f) < \infty$.*
2) *Let $m \geq 1$ be arbitrary. For $g \in G$ there exist f such that $c_g(f) > m$.*

I base part 1 on the following proposition and the observation that if an event occurs with positive probability it will eventually occur (after enough repetition).

Proposition 4 *Let $f \in \mathbb{Z}[X]$ be quadratic. Then $\delta(f) < 1$.*

Proof. Suppose that $\delta(f) = 1$. Then from (9) one infers the existence of a fundamental discriminant Δ such that $(\frac{\Delta}{q}) = -1$ for all but finitely many primes q. Since $\prod_{p \leq x}(1 + 1/p) \sim e^{\gamma} \log x / \zeta(2)$ by a result of Mertens (1874), it then follows from (13) that $L(1, \chi_\Delta) = 0$. However, $L(1, \chi_\Delta) > 0$ by (2). $\square$

The motivation for part 2 of Conjecture 4 is provided by Theorem 2. If the prime k-tuplets conjecture holds true, then by Theorem 2 part 2 of the conjecture also holds true. Whereas the problem of finding prime producing polynomials amounts to finding D for which $L(1, \chi_D)$ is small (cf. the estimate (4)), the problem of finding Artin prime producing polynomials amounts to finding D for which $L(2, \chi_D)$ is small (cf. the estimate (12)).

Acknowledgement. I'd like to thank Bruce Berndt for pointing out reference [9] in relation with Lemma 2 and Steven J. Miller for correspondence related to his joint paper [1]. Igor Spharlinski kindly sketched a proof of Lemma 2. As so often Yves Gallot and Paul Tegelaar kindly provided computational assistance. The terminology 'Artin prime producing quadratics' was suggested by the referee.

Special thanks are due to Andrew Granville, if it were not for him the paper would have looked quite differently: especially Section 9 would not have been there. Thanks are also due to Richard Mollin for passing on a question of mine to Andrew.

References

[1] S. Arms, Á. Lozano-Robledo and S.J. Miller, Constructing elliptic curves over $\mathbb{Q}(T)$ with moderate rank, preprint, arXiv:math.NT/0406579.

[2] P.T. Bateman and R.A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962), 363–367.

[3] N.G.W.H. Beeger, Report on some calculation of prime numbers, *Nieuw Archief Wisk.* **20** (1939), 48–50.

[4] O. Bottema and S.C. van Veen, Calculation of probabilities in the game of billiards. II. (Dutch), *Nieuw Arch. Wiskunde* (2) **22** (1946), 123–158.

[5] H. Cohen, High precision computation of Hardy-Littlewood constants, Draft of a preprint (see his homepage).

[6] R. Fueter, Über primitive Wurzeln von Primzahlen, *Comment. Math. Helv.* **18** (1946), 217–223.

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

[8] A. Granville and R.A. Mollin, Rabinowitsch revisited, *Acta Arith.* **96** (2000), 139–153.

[9] E. Grosswald, *Topics from the theory of numbers*, Second edition, Birkhäuser Boston, Inc., Boston, MA, 1984. xv+335 pp..

[10] 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.

[11] D.R. Heath-Brown, Artin's conjecture for primitive roots, *Quart. J. Math. Oxford Ser.* **37** (1986), 27–38.

[12] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Second edition, Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.

[13] M.J. Jacobson and H.C. Williams, New quadratic polynomials with high densities of prime values, *Math. Comp.* **72** (2003), 499–519.

[14] D.H. Lehmer, A note on primitive roots, *Scripta Math.* **26** (1963), 117–119.

[15] R.F. Lukes, C.D. Patterson and H.C. Williams, Numerical sieving devices: their history and some applications, *Nieuw Arch. Wisk* **13** (1995), 113–139.

[16] K.R. Matthews, A generalization of Artin's conjecture for primitive roots, *Acta Arith.* **29** (1976), 113-146.

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

[18] P. Moree, Problem 1097, *Elem. Math.* **50** (1995), p. 82. (Solution **51** (1996), pp. 81-82.)

[19] P. Moree, Approximation of singular series and automata, *Manuscripta Math.* **101** (2000), 385–399.

[20] P. Moree, Asymptotically exact heuristics for (near) primitive roots, *J. Number Theory* **83** (2000), 155–181.

[21] L. Murata, On the magnitude of the least prime primitive root, *J. Number Theory* **37** (1991), 47–66.

[22] S.C. van Veen, Probability problems in throwing dice. (Dutch), *Nieuw Arch. Wiskunde* **17** (1932), 120–136, 209–239.

[23] G. Wertheim, Primitiven Wurzeln der Primzahlen von der Form $2^x q^\lambda + 1$, in welcher $q = 1$ oder eine ungerade Primzahl ist, *Acta Math.* **20** (1895), 143–152.