ACTA ARITHMETICA
XCVI.2 (2000)

Rabinowitsch revisited

by

ANDREW GRANVILLE (Athens, GA) and
RICHARD A. MOLLIN (Calgary)

1. Introduction. In the late eighteenth century both Euler and Legendre noticed that n^2+n+41 is prime for $n = 0, 1, \ldots, 39$, and remarked that there are few polynomials with such small degree and coefficients that give such a long string of consecutive prime values. Rabinowitsch, at the 1912 International Congress of Mathematicians [22], showed that $n^2 + n + A$ is prime for $n = 0, 1, \ldots, A-2$ if and only if $4A-1$ is squarefree and the ring of integers of the field $\mathbb{Q}(\sqrt{1-4A})$ has just one equivalence class of ideals (that is, class number one). In 1934 Heilbronn [15] proved that there are only finitely many such fields, and in 1952 Heegner [14] that there are just seven such fields ([1]), corresponding to $A = 1, 2, 3, 5, 11, 17$ and 41.

One can generalize Rabinowitsch's criterion to other polynomials, and to other fields; for example, Mollin and Williams proved the following for real quadratic fields: $n^2 + n - A$ is prime for all positive $n < \sqrt{A} - 1$ if and only if the field $\mathbb{Q}(\sqrt{4A+1})$ has class number one where either $A = 4$, or $A \geq 5$ is odd and is of the form m^2 or $m^2 + m \pm 1$ for some integer m (see [21, pp. 352–354]).

One can develop a similar criterion for the case when the class number is 2, or 3, or any fixed number (see [19, 20]). The idea in all of these proofs is that if a large proportion of the values of a quadratic polynomial of discriminant d are prime then there cannot be many small primes p for which $(d/p) = 1$ (else those small primes would divide the values of the given quadratic polynomial, preventing it from being prime very often). If that is

---

2000 *Mathematics Subject Classification*: Primary 11N32, 11E41; Secondary 11N36, 11R44, 11D85, 11R29.

The first author is a Presidential Faculty Fellow supported, in part, by the National Science Foundation. The second author is a Killam Fellow, supported in part by NSERC (Canada).

([1]) $\mathbb{Q}(\sqrt{-4})$ and $\mathbb{Q}(\sqrt{-8})$ also have class number one, but do not correspond to such polynomials.

the case then the value of $L(1,(d/\cdot))$ will be surprisingly small ([2]), which is equivalent to having $h(d)$, the class number, small if $d<0$, and to having both $h(d)$ and ε_d, the fundamental unit, small ([3]) if $d>0$. We remark that ε_d is "small" if and only if the continued fraction for $(1+\sqrt{d})/2$ or $\sqrt{d}/2$ (as $d\equiv 1$ or $0 \pmod 4$) is short, that is, if d is a value of one of several special forms. Siegel [26] showed that $L(1,(d/\cdot)) \gg 1/|d|^{o(1)}$ and Tatuzawa [27] made Siegel's argument explicit, excluding at most one d, a presumably hypothetical counterexample to the Generalized Riemann Hypothesis ([4]). Using Tatuzawa's result, Mollin [19, 20] gives many explicit criteria "with one possible exception".

One might ask whether it is possible to find quadratic polynomials with arbitrarily long strings of consecutive prime values (though we do not necessarily constrain ourselves to a string almost as long as the largest coefficient of the polynomial, as we did above); that is whether, for any given N can we find A for which n^2+n+A is prime for $n=0,1,\dots,N$? This is an open question, though in Section 2A we will show that such polynomials exist assuming the *prime k-tuplets conjecture.*

In this paper we are primarily interested in further developing the theory of quadratic polynomials for which many of the small values are prime (rather than "all" as in Rabinowitsch's result). It is well known (see [5]) that if the class number of some imaginary quadratic field with large discriminant is one then we will have an egregious counterexample to the Generalized Riemann Hypothesis (that is, a zero of the associated Dirichlet L-function which is very close to 1). Thus Rabinowitsch's result can be informally stated as "n^2+n+A is prime for $n=0,1,\dots,A-2$ and $A>41$ if and only if the Generalized Riemann Hypothesis is very badly false for some quadratic Dirichlet L-function". One might guess that if n^2+n+A is prime for very many of the numbers $n=0,1,\dots,A-2$ (though not all) then perhaps still the Generalized Riemann Hypothesis is false, though perhaps not with a zero quite so close to 1. This is indeed the case:

COROLLARY 1. *There exists a constant $\kappa_1>0$ such that if there are more than $\kappa_1 N\log\log|A|/\log N$ primes amongst the integers n^2+A or n^2+n+A for $n=0,1,\dots,N$ for some N then the Generalized Riemann Hypothesis is false.*

([2]) Here $L(s,(d/\cdot)) := \sum_{n\ge 1}(d/n)/n^s$ when $\mathrm{Re}(s)>1$, and is then analytically continued to the rest of the complex plane.

([3]) One has $h(d)\ge 1$ and $\varepsilon_d \ge (1+\sqrt{d})/2$, so that $L(1,(d/\cdot))$ is small if and only if $h(d)$ and ε_d are both small by virtue of Dirichlet's formula $\sqrt{d}L(1,(d/\cdot)) = h(d)\log\varepsilon_d$.

([4]) The Generalized Riemann Hypothesis claims that all non-trivial zeros of $L(s,(d/\cdot))$ are on the line $\mathrm{Re}(s)=1/2$.

Our next result shows that Corollary 1 cannot be improved (other than in giving a precise value for the constant κ_1).

PROPOSITION 1. *There is a constant $\kappa_2 > 0$ such that there are infinitely many positive integers A for which there are more than $\kappa_2 N \log\log A/\log N$ primes amongst the integers $n^2 + n + A$ for $n = 0, 1, \dots, N$ with $N = \sqrt{A}$.*

We now discuss how our results relate to the predicted number of such primes: For a given quadratic polynomial $f(x) = ax^2 + bx + c$ with integer coefficients, define the *discriminant* $d = b^2 - 4ac$. For each prime p, define $\omega(p) = \omega_f(p)$ to be the number of $n \pmod p$ for which $f(n) \equiv 0 \pmod p$. There are two obvious reasons why there might not be many prime values of $f(n)$. The first is that $f(x)$ is reducible over the rationals, which is equivalent to d being a square. The second that prime p might divide $f(n)$ for every integer n, which is equivalent to $\omega(p) = p$. Schinzel and Sierpiński's "Hypothesis H" [24] implies that if f is irreducible, and $\omega(p) < p$ for all primes p then there are infinitely many integers n for which $f(n)$ is prime (a conjecture which is due to Bouniakovsky, see [23]), and Bateman and Horn [3] gave the explicit conjecture that

$$\pi_f(N) := \#\{n \le N : |f(n)| \text{ is prime}\} \sim c_f \frac{N}{D \log N}, \tag{1.1}$$

$$\text{where} \quad c_f := \prod_p \left(1 - \frac{\omega(p)}{p}\right) \Big/ \left(1 - \frac{1}{p}\right)$$

as $N \to \infty$, where $D = 2$. (Moreover they conjecture that this holds for polynomials of arbitrary degree D.)

If we fix the degree D then, by the fundamental lemma of the sieve [10, Theorem 2.5], we have, uniformly,

$$\pi_f(N) \ll \prod_{p \le N} \left(1 - \frac{\omega(p)}{p}\right) N. \tag{1.2}$$

If $\sum_{p>N}(1 - \omega(p))/p \ll 1$ then (1.2) becomes $\pi_f(N) \ll c_f N/(D \log N)$, uniformly.

Henceforth assume that f has degree 2, with $f(x) = ax^2 + bx + c$. At the beginning of Section 5, we show that

$$c_f \asymp L(1, (d/\cdot))^{-1} \frac{a}{\phi(a)}. \tag{1.3}$$

By determining when $\sum_{p>N}(1 - \omega(p))/p \ll 1$ we deduce

THEOREM 1. *Fix $\tau > 0$. Uniformly for all quadratic polynomials $f(x) = ax^2 + bx + c$, if $N > |d|^\tau + \log|a|$ then*

$$\pi_f(N) \ll L(1, (d/\cdot))^{-1} \frac{a}{\phi(a)} \cdot \frac{N}{\log N} \asymp c_f \frac{N}{\log N}. \tag{1.4}$$

Moreover (1.4) *holds uniformly for* $N > \log|ad|$ *if the Riemann Hypothesis for* $L(s,(d/\cdot))$ *is true.*

Littlewood's bounds [16] imply that $(a/\phi(a))L(1,(d/\cdot))^{-1} \ll \log\log|ad|$ assuming the Generalized Riemann Hypothesis (see Section 5A). Corollary 1 thus follows from Theorem 1.

One can show unconditionally, in a certain range, that many of the polynomials x^2+x+A take on roughly the number of prime values predicted by (1.1):

THEOREM 2. *For large* R *and* N *in the range* $R^\varepsilon < N < R^{1/2}$ *we have*

$$\#\{n \le N : n^2+n+A \text{ is prime}\} \asymp \frac{N}{\log N} L(1,((1-4A)/\cdot))^{-1}$$

for at least a positive proportion of the integers A *in the range* $R < A < 2R$.

We wish to establish some kind of converse result to Corollary 1, in the spirit of Rabinowitsch. To do so we will need to be more precise about what we mean by "the Generalized Riemann Hypothesis is false" in Corollary 1, and so we shall now define "*Siegel zeros*": If χ is a Dirichlet character modulo q and $L(s,\chi)$ is the corresponding L-function, then (see [5, Chapter 14]) $L(\sigma+it,\chi) \ne 0$ for $\sigma \ge 1 - c/\log(q(|t|+2))$ (for some explicit $c>0$), except possibly when χ is real and $t=0$. These are the "Siegel zeros" and if they do not exist then one can prove many of the conjectured results of analytic number theory (in other words, there are many arguments in which one does not need the full strength of the Generalized Riemann Hypothesis, but rather this weaker requirement). Following the notation of Heath-Brown [11] we shall denote this zero by β if it exists, and assume

$$\eta := \frac{1}{(1-\beta)\log q} \ge 3$$

(and we know that $\eta \ll q$). It is well known [7, 8] (and see below) that if $d = 1-4A$ and $h(d)=1$ with A sufficiently large then we have a Siegel zero $L(\beta,(d/\cdot))=0$ with $1-\beta \sim 6/(\pi\sqrt{d})$. For convenience we will take $\eta=1$ if there is no such Siegel zero.

Hecke [13] proved that if $L(s,(d/\cdot))$ has no Siegel zero then $L(1,(d/\cdot))^{-1} \ll \log|d|$ (which we reprove in Section 5B). We therefore deduce from Theorem 1:

COROLLARY 1′. *There exists a constant* $\kappa_3 > 0$ *such that if there are more than* $\kappa_3 N\log|ad|/\log N$ *primes amongst the integers* an^2+bn+c *for* $n = 0,1,\dots,N$ *for some* N *then the* L*-function* $L(s,(d/\cdot))$ *has a Siegel zero, where* $d = b^2-4ac$.

We can also prove a result that comes close to being a converse to Corollary 1′:

THEOREM 3. *Suppose that the L-function $L(s,(d/\cdot))$ with $d = 1-4A$ has a "Siegel zero" β with $1-\beta \le 1/\log^3|d|$, that is, $\eta \ge \log^2|d|$. Then there exists an integer N such that there are more than $\kappa_3 N \log|A|/\log N$ primes amongst the integers $|n^2+n+A|$ with $n = 0,1,\dots,N$. If $d = -4A$ above then we have the same conclusion for the polynomial $|n^2+A|$.*

By Rabinowitsch's Theorem one knows that if $h(d) = 1$ with $d < 0$ (which gives $\eta \sim (\pi/6)\sqrt{|d|}/\log|d|$) then $\pi_f(N) = N$ where $N = (|d|-7)/4$. This might lead one to hope that whenever η is large enough, one can get a *very precise* estimate for $\pi_f(N)$. We now show that one can get accurate estimates, in a certain range, whenever $\eta \ge \log|d|$:

THEOREM 4. *Suppose that there is a Siegel zero for $L(s,(d/\cdot))$ with $\eta \ge \log|d|$, where $d \equiv 1 \pmod 4$. Then for $f(x) = x^2+x+(1-d)/4$ we have*

$$\pi_f(N) \sim \varrho_d N, \qquad \text{where} \qquad \varrho_d := \prod_{p \le \sqrt{d}} \left(1 - \frac{\omega(p)}{p}\right),$$

uniformly in the range $d^{10} \le N \le d^{o(\eta)}$. If $d \equiv 0 \pmod 4$ above then the same conclusion holds with $f(x) = x^2 - d/4$.

One can prove results similar to Theorems 3 and 4 for non-monic quadratic polynomials of the same discriminant.

One can give a good estimate for ϱ_d in terms of c_f and η:

PROPOSITION 2. *Suppose that there is a Siegel zero for $L(s,(d/\cdot))$ with $\eta \to \infty$ as $|d| \to \infty$. Then*

$$\varrho_d \sim \frac{c_f}{\log(|d|^\eta)}.$$

Our results are not the first of this nature. It is known that if the Generalized Riemann Hypothesis is true then one can obtain very sharp estimates for the distribution of primes in arithmetic progressions [5] in a wide range. Surprisingly if the Generalized Riemann Hypothesis is very wrong, in that there is a Siegel zero, then we are also able to obtain sharp estimates in a wide range (though at first quite different estimates). This phenomenon is well known and most precisely explored by Heath-Brown [12] and Shiu [25].

In [1], Ankeny and Chowla show that the connection between class numbers and primes in arithmetic progressions can be made without resorting to any analysis (see Section 2B below).

In [11], Heath-Brown uncovered a new and quite remarkable phenomenon: If there are Siegel zeros then, at least in a certain range depending on the Siegel zero, one can show that there are roughly the expected number of twin primes. Thus if there are a surprisingly large number of Siegel zeros the twin prime conjecture is true! Heath-Brown's theorem is the result in the literature which is most similar to Theorem 4: Both results allow us

to determine that there are primes in sequences which we cannot approach by other means. Moreover both are proved by sieve methods relying on the fact that the set of primes one is sieving with is very sparse (the primes p with $(d/p) = 1$). However Heath-Brown's theorem lies far deeper in that our polynomial is connected to the Siegel zero in an obvious way, whereas this is evidently not the case for twin primes, and so the proof of his result seems to require far more substantial techniques.

Mahler [17] made precise the connection between class number and Siegel zeros when $d < 0$, as follows: Define $h'(d) := h(d)/\sum_a 1/a$ where the sum runs over the minimal norms of ideals, one from each equivalence class. If $h'(d) \ll \sqrt{|d|}/\log|d|$ then $L(s,(d/\cdot))$ has a Siegel zero. Conversely if $L(\beta,(d/\cdot)) = 0$ for real $\beta > 1 - c/\log|d|$ for some sufficiently small constant $c > 0$ then $h'(d) \ll \sqrt{|d|}/\log|d|$. (Note that this is not exactly an "if and only if" condition since the constants may be different in the two statements.) Let us note that $h(d) \geq h'(d) \geq 1$ for all $d < 0$. Theorem 3 of [9] states that for any fundamental discriminant $d < 0$ we have

$$h'(d) \sim \frac{\pi}{3}\left(1 + \frac{2}{\log|d|} \cdot \frac{L'(1,(d/\cdot))}{L(1,(d/\cdot))}\right)^{-1} \frac{\sqrt{|d|}}{\log|d|}.$$

In [9] it is noted that $L'(1,(d/\cdot))/L(1,(d/\cdot)) \ll \log\log|d|$ if the Generalized Riemann Hypothesis is true so that $h'(d) \sim (\pi/3)\sqrt{|d|}/\log|d|$. One deduces, unconditionally, that $h'(d) \asymp \sqrt{|d|}/(\eta\log|d|)$. If there is a Siegel zero β with $\eta \to \infty$ then $h'(d) \sim (\pi/(6\eta))\sqrt{|d|}/\log|d|$. Note that

$$\varrho_d \asymp 1\Big/\sum_a \frac{1}{a} = h'(d)/h(d) \gg 1/\log^2|d|.$$

We end the introduction by giving a version of Theorem 4 avoiding mention of zeros:

COROLLARY 2. *Suppose that* $h(d) \leq \sqrt{|d|}/\log^2|d|$, *with* d *a fundamental, negative discriminant. Let* $f(x) = x^2 + x + (1-d)/4$ *if* $d \equiv 1 \pmod 4$, *and* $f(x) = x^2 - d/4$ *if* $d \equiv 0 \pmod 4$. *Then* $\pi_f(N) \sim \varrho_d N$ *uniformly in the range* $|d|^{10} \leq N \leq |d|^{o(\sqrt{|d|}/h(d))}$.

In Section 7 we give an entirely elementary proof of a weak version of this result: if $h(d) = o(\sqrt{|d|}/\log^3|d|)$ then we have the asymptotic formula if $\log N/\log|d| \to \infty$ and $\log N = o(\sqrt{|d|}/(h(d)\log^2|d|))$.

2. Elementary arguments

2A. *Long strings of prime values of a high degree polynomial.* A set of integers $a_1 < \ldots < a_k$ is called *admissible* if, for every prime p, there exists an integer n such that p does not divide $n + a_i$ for any i. A consequence of

Hardy and Littlewood's prime k-tuplets conjecture is that if $a_1 < \ldots < a_k$ is admissible then there exist infinitely many integers n for which each $n+a_i$ is prime (though this conjecture was actually due to Dickson, see [24]).

Fix integer $D \geq 2$. Let $a_i = i^D - i$ for $i = 0, 1, \ldots, k$. We claim that this set of integers is admissible, for if not then for every $n \pmod p$ there exists $i \pmod p$ with $i^D - i \equiv -n \pmod p$. But then the map $g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defined by $g(i) = i^D - i$ is onto, and so is a bijection since the domain is the same size as the range. However this is false since $g(0) = g(1) = 0$. Therefore, by the prime k-tuplets conjecture, there exist infinitely many integers n such that $f_n(i) = i^D - i + n = a_i + n$ is prime for $i = 0, 1, \ldots, k$.

The nearest unconditional theorem to this is Balog's beautiful result [2] that there exist infinitely many polynomials of degree D having prime values at $2D + 1$ consecutive integers.

2B. *A connection between class number and prime count.* The following argument is a slight improvement of that in Ankeny and Chowla [1], which in turn looks very similar to the proof of Dirichlet's class number formula in [5], though with a different conclusion:

The reduced quadratic forms $ax^2+bxy+cy^2$ of fundamental discriminant $d < 0$ all satisfy $a, |b|, c < \sqrt{|d|}$. Every prime p is represented $1 + (d/p)$ times by such forms. Thus

$$\sum_{p \leq x} (1 + (d/p)) \leq \sum_i \#\{(m,n) : f_i(m,n) \leq x\},$$

where the f_i run through the reduced binary quadratic forms of discriminant d. Now if $x > |d|$ then $\#\{(m,n) : f_i(m,n) \leq x\} \ll x/\sqrt{|d|}$ and so the above gives

$$\sum_{p \leq x} (1 + (d/p)) \ll h(d)x/\sqrt{|d|} \ll L(1, (d/\cdot))x.$$

Thus, if $\pi(x; d, a) \leq (2 - \varepsilon)\pi(x)/\phi(|d|)$ for some $x \geq |d|$, for all a with $(d/a) = -1$, then $L(1, (d/\cdot)) \gg \varepsilon/\log x$.

3. Linnik's Theorem. By equations (13) and (14) of Section 19 of [5], we have, for $x \geq T \geq |d| \geq 1$ where d is not a square,

$$\sum_{p \leq x} \left(\frac{d}{p}\right) \log p + \frac{x^\beta}{\beta} \ll \frac{x \log^2 x}{T} + x^{1/2} + \sum_{|\gamma| < T} x^{\mathrm{Re}\varrho}, \tag{3.1}$$

where the "x^β/β" occurs only if there is a Siegel zero β of $L(\beta, (d/\cdot))$, and the sum is over all other zeros $\varrho = \sigma + i\gamma$ of this L-function. By the proof of Linnik's Theorem in [4] on pages 54–55, we find that for fixed $C > 9$, there

exists a small constant $c > 0$ such that if $x \geq T^C$ then

$$\sum_{|d|\leq T} \sum_{|\gamma|<T} x^{\mathrm{Re}\varrho} \ll x^{1/2}T^3 + \delta x^{1-c/\log T}, \tag{3.2}$$

where $\delta = (1-\beta)\log T$ if there is a Siegel zero, and $\delta = 1$ otherwise. Here we sum over the zeros of $L(s,(d/\cdot))$, with d squarefree, and of $\zeta(s)$ when $d = 1$. Note that we have improved "T^5" to "T^3" in (3.2) from what appears in [4], though this follows easily from the proof there by noting that $L(s,(d/\cdot))$ with $|d| \leq T$ has $\ll T^2$ zeros with $|\gamma| < T$.

Fix $C > 9$. Inserting (3.2) into (3.1) with $T = |d|\log^3 x$ gives, for $x > |d|^C$,

$$\sum_{p\leq x} \left(\frac{d}{p}\right)\log p + \frac{x^\beta}{\beta} \ll \frac{x}{|d|\log x} + \frac{x^{1-c/\log|d|}}{\eta} \tag{3.3}$$

(after some calculations when $x > e^d$).

Let $\sum'$ be a sum over squarefree integers d such that $L(s,(d/\cdot))$ has no Siegel zero. Thus we get, for $x > D^C$ with $T = D\log^3 x$, by summing (3.1) and then applying (3.2),

$$\sum_{D<|d|\leq 2D}{}' \left|\sum_{p\leq x}\left(\frac{d}{p}\right)\log p\right| \ll \frac{x}{\log x} + \frac{x^{1-c/\log D}}{\eta}. \tag{3.4}$$

By partial summation we thus deduce, for $x > D^A$,

$$\sum_{D<|d|\leq 2D}{}' \left|\sum_{p\geq x}\frac{(d/p)}{p}\right| \ll \frac{1}{\log D} + \frac{1}{\eta} \ll 1. \tag{3.5}$$

4. Maier's method: The proofs of Proposition 1 and Theorem 2. Our idea is to use Maier's method [18] as explained in [6]: Fix large N and $\varepsilon > 0$. Let M be the product of all of the primes $\leq y := \varepsilon\log N$. If there is a Siegel zero modulo M, let q be the conductor of the character whose Dirichlet L-function has this zero. Not only does q divide M but we can also show that its largest prime factor p must be larger than any given bound once N is sufficiently large. In this case let $m = M/p$ (thus guaranteeing that q does not divide m); if there had been no Siegel zero then let $m = M$. Now there is no Siegel zero modulo m, and we see that $m = N^{\varepsilon+o(1)}$ and that there exists an absolute constant $B > 2$ such that $\pi(5t/4,m,a) - \pi(t,m,a) \gg \pi(t)/\phi(m)$ for $t > m^B$ provided $(a,m) = 1$ (by Linnik's Theorem [4]). Here $\pi(t)$ denotes the number of primes $\leq t$, and $\pi(t,m,a)$ the number of primes $\leq t$ which are $\equiv a \pmod m$.

For each prime $p \leq y$ we select $\delta_p = -1, 0$ or 1. Now select odd $a \pmod{4m}$ so that $((1-4a)/p) = \delta_p$ for all primes $p \leq y$ (this is easily accomplished using the Chinese Remainder Theorem). We shall select integer R, divisible by $4m$, so that $N^{O(1)} > R \geq N^2$, and we choose $\varepsilon < 1/B$ so

that $R > m^B$. Now, by swapping the order of summation we get

$$(4.1)\qquad \sum_{\substack{R<A\le 2R\\ A\equiv a \,(\mathrm{mod}\, 4m)}} \#\{n \le N : n^2+n+A \text{ is prime}\}$$

$$= \sum_{n\le N} \{\pi(2R+(n^2+n);4m,n^2+n+a) - \pi(R+(n^2+n);4m,n^2+n+a)\}$$

$$\gg \sum_{\substack{n\le N\\ (n^2+n+A,4m)=1}} \frac{1}{\phi(4m)}\cdot\frac{R}{\log R}$$

$$\gg \frac{1}{\phi(m)}\cdot\frac{R}{\log N} N \prod_{p\le y}\left(1-\frac{1+\delta_p}{p}\right) \gg \frac{R}{m}\cdot\frac{N}{\log N}\prod_{p\le y}\left(1-\frac{\delta_p}{p}\right)$$

since each $n^2+n \le 2R$.

Proof of Proposition 1. Let us take each $\delta_p = -1$ and $R = N^2$. Then the maximum value of $\#\{n \le \sqrt{A} : n^2+n+A \text{ is prime}\}$ for $R < A \le 2R$ with $A \equiv a \pmod{4m}$, is larger than the average in the sum above, which is $\gg N \log\log N/\log N$.

Proof of Theorem 2. Select

$$B > \sum_{N^{1/4}<p\le R^{10}} \frac{1}{p} \ge \left|\sum_{N^{1/4}<p\le R^{10}} \frac{(d/p)}{p}\right|,$$

and so that B is bigger than the bound implicit in (3.5).

Now for any A included in the above sum, and $d = 1-4A$, we have $\delta_p = (d/p)$ for all $p \le y$. Write $d = kl^2$ where k is squarefree. We apply (3.5) with $d = k, x = R^{10}$ and $D = 4R/l^2$. Thus $|\sum_{p>R^{10}}(d/p)/p| < B$ unless k is the modulus of a Siegel zero. There are $O(\sqrt{R})$ such A (at most one for each l).

Also

$$\sum_{\substack{4R<-d\le 8R\\ d\equiv 1-4a \,(\mathrm{mod}\, 16m)}} \left|\sum_{y<p\le N^{1/4}} \frac{(d/p)}{p}\right|^2$$

$$\ll \sum_{\substack{4R<-d\le 8R\\ d\equiv 1-4a \,(\mathrm{mod}\, 16m)}} \sum_{y<p\le N^{1/4}} \frac{1}{p^2} + \sum_{y<p<q\le N^{1/4}} \frac{1}{pq}\left|\sum_{\substack{4R<-d\le 8R\\ d\equiv 1-4a \,(\mathrm{mod}\, 16m)}} \left(\frac{d}{pq}\right)\right|$$

$$\ll \frac{R}{my} + N^{1/2} \ll \frac{R}{m\log N}.$$

Therefore $|\sum_{y<p\le N^{1/4}}(d/p)/p| < B$ for all but $O(R/(m\log N))$ values of A in this range. Let S be this set of values of A together with those A which gave rise to k, the modulus of a Siegel zero, above. Then S has $O(R/(m\log N))$ elements.

Now suppose $A \in S$. By the small sieve we have

$$\#\{n \le N : n^2+n+A \text{ is prime}\} \le \#\{n \le N : (n^2+n+A, m) = 1\} \ll \frac{N}{\log y}\prod_{p\le y}\left(1-\frac{\delta_p}{p}\right),$$

so that the contribution of all elements of S to the left side of (4.1) is

$$\ll (R/m)(N/(\log N \log\log N))\prod_{p\le y}(1-\delta_p/p),$$

which is negligible compared to the right side of (4.1). Therefore (4.1) may be rewritten as

$$\frac{1}{R/m}\sum_{\substack{R<A\le 2R\\ A\equiv a \,(\mathrm{mod}\, 4m)\\ A\notin S}} \#\{n \le N : n^2+n+A \text{ is prime}\} \gg \frac{N}{\log N}\prod_{p\le y}\left(1-\frac{\delta_p}{p}\right). \tag{4.2}$$

If $A \notin S$ then, by the definition of S,

$$\prod_{p\le y}\left(1-\frac{\delta_p}{p}\right) \asymp \prod_{p\le N}\left(1-\frac{(d/p)}{p}\right) \asymp L(1,(d/\cdot))^{-1}. \tag{4.3}$$

By (1.2) we deduce that

$$\#\{n \le N : n^2+n+A \text{ is prime}\} \ll \frac{N}{\log N}\prod_{p\le N}\left(1-\frac{(d/p)}{p}\right) \ll \frac{N}{\log N}\prod_{p\le y}\left(1-\frac{\delta_p}{p}\right).$$

Inserting this into (4.2) we find that

$$\#\{n \le N : n^2+n+A \text{ is prime}\} \gg \frac{N}{\log N}\prod_{p\le y}\left(1-\frac{\delta_p}{p}\right)$$

for a positive proportion of $A \notin S$, and the result follows from (4.3).

5. Estimating the Euler product in (1.2). First note that

$$\omega(p) = \begin{cases} 1+(d/p) & \text{if } p \text{ does not divide } a,\\ (d/p) & \text{if } p \text{ does divide } a.\end{cases}$$

As $\prod_{p\le N,\, p\mid a} p/(p-1) \sim a/\phi(a)$ if $N \ge \log a$, we deduce that

$$\prod_{p\le N}\left(1-\frac{\omega(p)}{p}\right) \asymp \frac{1}{\log N}\cdot\frac{a}{\phi(a)}\prod_{p\le N}\left(1-\frac{(d/p)}{p}\right), \tag{5.1}$$

which implies (1.3).

5A. *Assuming the Generalized Riemann Hypothesis.* Littlewood [16] showed, assuming the Generalized Riemann Hypothesis, that for any non-principal character χ of modulus d, we have

$$\prod_{\log^2 d<p\le x}(1-\chi(p)/p) = 1+o(1), \tag{5.2}$$

and so we deduce (1.4) from inserting (5.1) and then (5.2) into (1.2). We also deduce from Littlewood's estimate $L(1,\chi)\sim \prod_{p\le \log^2 d}(1-\chi(p)/p)^{-1}$ that $1/\log\log d \ll L(1,\chi) \ll \log\log d$, since $1-1/p \le |1-\chi(p)/p| \le 1+1/p$.

5B. *Assuming that there is no Siegel zero.* By (3.3) and partial summation, for $d^{2C} \le y < x$, we obtain

$$\prod_{y<p\le x}\left(1-\frac{(d/p)}{p}\right) = \exp\left(O\left(\frac{1}{d}+\frac{1}{y^{c/\log d}}\right)\right). \tag{5.3}$$

Taking $y = d^{2C}$, we deduce that $L(1,(d/\cdot)) \asymp \prod_{p\le y}(1-(d/p)/p)^{-1}$. Thus $1/\log|d| \ll L(1,(d/\cdot)) \ll \log|d|$.

Proof of Theorem 1 (when there is no Siegel zero). By (5.3) and (5.1) we deduce from (1.2) that (1.4) holds uniformly when $x > d^{2C}$. The result follows since $\prod_{d^\tau<p\le d^{2C}}(1-(d/p)/p) \asymp 1$.

5C. *Assuming that there is a Siegel zero.* If $x > d^\eta$ then by (3.3) we get

$$\sum_{p\le x}(d/p)\log p \ll x\exp\left(-\frac{\log x}{\log d^\eta}\right)+\frac{x}{\log x},$$

and so, by partial summation we then deduce

$$\prod_{d^\eta<p\le x}\left(1-\frac{(d/p)}{p}\right) \asymp 1. \tag{5.4}$$

If $d^\eta > x \ge d^C$ then by (3.3) and (3.2) (where we sum over the zeros of $\zeta(s)$) we get

$$\sum_{p\le x}(1+(d/p))\log p \ll \left(x-\frac{x^\beta}{\beta}\right)+\frac{x}{|d|\log x}+\frac{x^{1-c/\log|d|}}{\eta} \ll \frac{x\log x}{\log(d^\eta)}.$$

By partial summation we obtain for $d^\eta > x > y \ge d^C$

$$\prod_{y<p\le x}\left(1-\frac{1+(d/p)}{p}\right)=1+O\left(\frac{\log x}{\log(d^\eta)}\right). \tag{5.5}$$

Proof of Theorem 1 (when there is a Siegel zero). Fix $c>0$. By (5.4), (5.5) and (5.1) we find that for any $x>|d|^c+\log|a|$,

$$\prod_{p\le x}\left(1-\frac{\omega(p)}{p}\right)\asymp\prod_{p\le xd^\eta}\left(1-\frac{\omega(p)}{p}\right)\asymp\frac{a}{\phi(a)}\cdot\frac{L(1,(d/\cdot))^{-1}}{\log(xd^\eta)}$$
$$\ll\frac{a}{\phi(a)}\cdot\frac{L(1,(d/\cdot))^{-1}}{\log x},$$

by (5.4). Theorem 1 follows from inserting this into (1.2).

Note that if $p\,|\,a$ then $\omega(p)=(d/p)=0$ or 1. In Lemma 3 of [11] it is shown that $\sum_{p\le d^{500}}(1+(d/p))(\log p)/p\ll\log d/\sqrt{\log\eta}$, and so

$$\sum_{p\le d^{500}}\omega(p)\frac{\log p}{p}\ll\frac{\log d}{\sqrt{\log\eta}}.$$

Taking $y=d^{10}$ gives

$$\prod_{z<p\le y}\left(1-\frac{\omega(p)}{p}\right)=1+O\left(\frac{1}{\log z}\cdot\frac{\log d}{\sqrt{\log\eta}}\right). \tag{5.6}$$

Combining (5.5) and (5.6) we find that, for any $\varepsilon>0$ with $\varepsilon\sqrt{\log\eta}\to\infty$, provided $\sum_{p|a,\ p\le y}1/p=o(1)$,

$$\prod_{d^\varepsilon<p\le x}\left(1-\frac{\omega(p)}{p}\right)=1+o(1) \tag{5.7}$$

where $x=d^{o(\eta)}$. We also note that this implies that, for any a,

$$\varrho_d:=\prod_{p\le\sqrt{d}}\left(1-\frac{\omega(p)}{p}\right)\ge\prod_{p\le\sqrt{d}}\left(1-\frac{1+(d/p)}{p}\right) \tag{5.8}$$
$$\gg\prod_{p\le d^{1/\sqrt{\log\eta}}}\left(1-\frac{2}{p}\right)\gg\frac{\log\eta}{\log^2 d}.$$

6. Prime values of a quadratic polynomial

6A. *Sieving.* First note that if $f(x)=x^2+x+A$ or x^2+A for some integer A, and if $f(n)$ is composite for $n\le N$, with $N\gg\sqrt{A}$, then there exists a prime $q\ll N$ for which q divides $f(n)$. Therefore, by the fundamental lemma of the sieve, if $y=N^{o(1)}$ then, for $m=\prod_{p\le y}p$, we have

$$\pi_f(N)=\#\{n\le N:(f(n),m)=1\}$$
$$+O\Big(\sum_{y<q\ll N}\#\{n\le N:q\,|\,f(n)\text{ and }(f(n),m)=1\}\Big) \tag{6.1}$$

$$= \{1+o(1)\}N\prod_{p\le y}\left(1-\frac{\omega(p)}{p}\right)$$
$$+O\Big(\sum_{y<q\ll N}\frac{\omega(q)N}{q}\prod_{p\le N/q}\left(1-\frac{\omega(p)}{p}\right)\Big).$$

Here, the implied constants are independent of A.

6B. *Estimates assuming there is a Siegel zero (The proofs of Theorems 3 and 4)*

Proof of Theorem 4. We assume that $\eta\to\infty$ as $d\to\infty$ to simplify our calculations. We use the estimates of Section 5C. In (6.1) we suppose that $d^{10}<N<d^{o(\eta)}$ and $y=d^{\varepsilon}$ where $\varepsilon=\tau/(\log\eta)^{1/2}$ with $\tau\to\infty$ as $d\to\infty$.

If $y\le q\le N/y$ then $\prod_{p\le N/q}(1-\omega(p)/p)\sim\varrho_d$ and $\sum_{y<q<N/y}\omega(q)/q=o(1)$ by (5.7), and so (6.1) becomes

(6.2) $$\pi_f(N)$$
$$=\varrho_d N\Big\{1+o(1)+O\Big(\sum_{N/y<q\le N}\frac{\omega(q)}{q}\prod_{N/q<p\le y}\left(1-\frac{\omega(p)}{p}\right)^{-1}\Big)\Big\}.$$

We note that, for $N/y\le q\le N$, we have

$$\prod_{N/q<p\le y}\left(1-\frac{\omega(p)}{p}\right)^{-1}\ll\min\{1/\varrho_d,(\log y/\log(N/q))^2\}.$$

Now $\sum_{x<p<2x}\omega(p)/p\ll 1/\log(d^{\eta})$ for $x>d^{C}$, by (5.5). Combining these last two bounds to estimate the error term in (6.2), after some calculation, gives

$$\ll\frac{\log y}{\varrho_d^{1/2}\log(d^{\eta})}=\frac{\varepsilon}{\eta\varrho_d^{1/2}}\ll\frac{\tau\log d}{\eta\log\eta}$$

using (5.8). If $\eta>\log d$, we take $\tau=\sqrt{\log\eta}$ to deduce Theorem 4.

Proof of Theorem 3. If $\eta>\log^2 d$ then take $\log N=\log^3 d/\sqrt{\log\log d}$. Then N is in the range of Theorem 4. Moreover $\log d/\log N\ll\log\log d/\log^2 d\ll\varrho_d$ by (5.8). Thus we have proved Theorem 3.

7. An elementary approach. It is possible to get results like Corollary 2 without recourse to any complex analysis (that is, the results of Section 3). For simplicity we will work with fundamental discriminants $d<0$:

In Section 2B we saw that the number of primes $p\le x$ with $(d/p)=0$ or 1 is $\ll L(1,(d/\cdot))x$, when $x>|d|$. Take $m=\prod_{p\le|d|}p$ and N so that $\log N/\log|d|\to\infty$. The fundamental lemma of the sieve thus gives

$$\pi_f(N) = \#\{n \le N : (f(n), m) = 1\} + O\Big(\sum_{|d|<p\ll N} (1 + (d/p))N/p\Big)$$
$$= \{1 + o(1)\}N \prod_{p\le|d|}\left(1 - \frac{\omega(p)}{p}\right) + O(NL(1, (d/\cdot))\log N).$$

We thus get

$$\pi_f(N) \sim N \prod_{p\le|d|}\left(1 - \frac{\omega(p)}{p}\right)$$

provided $\log N = o(1/(L(1, (d/\cdot))\log^2|d|))$, which gives a non-trivial range for N provided $h(d) = o(\sqrt{|d|}/\log^3|d|)$. Since this is weaker than Corollary 2 we do not pursue this further.

8. The value of ϱ_d: Proof of Proposition 2. Write $T = d^{\eta/C}$ and $U = d^{\eta C}$ where $C \to \infty$ slowly. Then, by definition,

$$c_f/\varrho_d \sim \prod_{p\le T}\left(1 - \frac{1}{p}\right)^{-1} \prod_{\sqrt{d}<p\le T}\left(1 - \frac{\omega(p)}{p}\right)\prod_{p>T}\left(1 - \frac{(d/p)}{p}\right)$$
$$\sim e^{\gamma}\log U \prod_{U<p\le T}\left(1 - \frac{\omega(p)}{p}\right)$$

using Mertens' Theorem, (5.7) and (3.3), respectively. Now using (3.3) with partial summation we obtain

$$\log\Big(\prod_{U<p\le T}\left(1 - \frac{\omega(p)}{p}\right)\Big) = -\int_U^T \frac{t - t^{\beta}}{t^2\log t}\,dt + o(1)$$
$$= -\int_{1/C}^{C} \frac{1 - e^{-v}}{v}\,dv + o(1) \to -\log C - \gamma$$

as $C \to \infty$. We took $t = (d^{\eta})^v$ above, and noted that $(d^{\eta})^{1-\beta} = e$. Combining these last two estimates gives the result.

References

[1] N. C. Ankeny and S. Chowla, *The relation between the class number and the distribution of primes*, Proc. Amer. Math. Soc. 1 (1950), 775–776.

[2] A. Balog, *The prime k-tuplets conjecture on average*, in: Analytic Number Theory, B. Berndt *et al.* (eds.), Birkhäuser, Boston, 1990, 47–75.

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

[4] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque 18 (1987).

[5] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, New York, 1980.

[6] J. Friedlander and A. Granville, *Limitations to the equi-distribution of primes IV*, Proc. Roy. Soc. London 435 (1991), 197–204.
[7] D. M. Goldfeld, *An asymptotic formula relating the Siegel zero and the class number of quadratic fields*, Ann. Scuola Norm. Sup. Pisa (4) 2 (1975), 611–615.
[8] D. M. Goldfeld and A. Schinzel, *On Siegel's zero*, ibid., 571–583.
[9] A. Granville and H. M. Stark, *ABC implies no "Siegel zeros" for L-functions of characters with negative discriminant*, Invent. Math. 139 (2000), 509–523.
[10] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.
[11] D. R. Heath-Brown, *Primes twins and Siegel zeros*, Proc. London Math. Soc. 47 (1983), 193–224.
[12] —, *Siegel zeros and the least prime in an arithmetic progression*, Quart. J. Math. Oxford Ser. (2) 41 (1990), 405–418.
[13] E. Hecke, in the paper of E. Landau, *Über die Klassenzahl imaginärquadratischer Zahlkörper*, Gött. Nachr. 1918, 285–295.
[14] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. 56 (1952), 227–253.
[15] H. Heilbronn, *On the class number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. (2) 5 (1934), 150–160.
[16] J. E. Littlewood, *On the class number of the corpus* $P(\sqrt{-k})$, Proc. London Math. Soc. 27 (1928), 358–372.
[17] K. Mahler, *On Hecke's Theorem on the real zeros of the L-functions and the class number of quadratic fields*, J. London Math. Soc. 9 (1934), 298–302.
[18] H. Maier, *Primes in short intervals*, Michigan Math. J. 32 (1985), 221–225.
[19] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, 1996.
[20] —, *Prime-producing quadratics*, Amer. Math. Monthly 104 (1997), 529–544.
[21] —, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, 1998.
[22] G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, in: Proc. Fifth Internat. Congress. Math. (Cambridge), Vol. 1, 1913, 418–421.
[23] A. Schinzel, *Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"*, Acta Arith. 7 (1961), 1–8.
[24] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, ibid. 4 (1958), 185–208; Errata, ibid. 5 (1959), 259.
[25] D. Shiu, *Prime numbers in arithmetic progressions*, doctoral thesis, Oxford University, 1997.
[26] C. L. Siegel, *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), 83–86.
[27] T. Tatuzawa, *On a theorem of Siegel*, Japan. J. Math. 21 (1951), 163–178.

Department of Mathematics
University of Georgia
Athens, Georgia 30602, U.S.A.
E-mail: andrew@math.uga.edu

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta, Canada T2N 1N4
E-mail: ramollin@math.ucalgary.ca

Received on 21.12.1998
and in revised form 12.5.2000 (3530)