PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 122, Number 1, September 1994

FINITELY GENERATED GROUPS $(\mathrm{mod}\, p)$

M. RAM MURTY

(Communicated by Dennis A. Hejhal)

ABSTRACT. Given r mutually coprime natural numbers $a_1, \ldots, a_r$ greater than 1 and an irreducible polynomial $f(t)$ with integer coefficients, we investigate how the structure of the group generated by $a_1, \ldots, a_r \bmod p$ varies as the prime p varies subject to the condition that $f(t)$ splits completely $\bmod p$.

1. INTRODUCTION

A classical conjecture of Artin [1] predicts the density of primes for which a given natural number is a primitive root $(\mathrm{mod}\, p)$.

Under the generalised Riemann hypothesis, Hooley [7] proved Artin's conjecture. The work of Gupta and Murty [3] together with the refinement of Heath-Brown [6] led to the unconditional result that if a_1, a_2, and a_3 are mutually coprime natural numbers greater than unity, then at least one of them is a primitive root $(\mathrm{mod}\, p)$ for infinitely many primes p.

Recently, work of Lichtman [9] on polycyclic groups led him to raise allied questions. They can be summarised as follows. Let $f(t) \in \mathbb{Z}[t]$ be an irreducible polynomial, and suppose $a_1, \ldots, a_r$ are mutually coprime natural numbers greater than unity. We will denote by $\langle a_1, a_2, \ldots, a_r \rangle$ the multiplicative group generated by $a_1, a_2, \ldots, a_r$. For each prime p coprime to $a_1, a_2, \ldots, a_r$ we can consider the image of this group $\bmod p$.

Question 1. Are there infinitely many primes p such that

$$\langle a_1, \ldots, a_r \rangle = \langle a_1 \rangle \qquad (\mathrm{mod}\ p)$$

and $f(t)$ factors completely into linear factors $(\mathrm{mod}\, p)$?

Question 2. Are there infinitely many primes p such that $\langle a_1, \ldots, a_r \rangle$ $(\mathrm{mod}\, p)$ has prime order and $f(t)$ splits completely $\bmod p$?

Question 3. Are there infinitely many primes p such that $f(t)$ splits completely $\bmod p$ and any group of order $(p-1)$ has normal q-Sylow subgroups for odd primes q?

Received by the editors May 12, 1992 and, in revised form, November 30, 1992.
1991 *Mathematics Subject Classification.* Primary 11N36, 11S05.
Research partially supported by NSERC and FCAR grants.

0002-9939/94 $1.00 + $.25 per page

These questions are not unrelated to the Artin primitive root conjecture. For instance, the first question certainly follows from a "twisted" Artin conjecture that there are infinitely many primes p such that a given natural number $a > 1$ is a primitive root $(\mathrm{mod}\, p)$ *and* $f(t)$ splits completely $(\mathrm{mod}\, p)$. Such a conjecture would be expected to be true unless there are some "obvious" obstructions (such as the splitting field of f contains $\mathbb{Q}(\zeta_l, a^{1/l})$, where l is a prime and ζ_l denotes a primitive lth root of unity).

In this paper we address the three questions. Our first result is an affirmative answer to Question 3. The method is sieve theory. We show that the number of primes $p \leq x$ satisfying the condition of Question 3 is

$$\gg x/[(\log x)(\log\log x)].$$

For Question 2 a method of Hardy and Ramanujan, elaborated by Turan, allows us to show that the number of such primes is small. More precisely, we show that the number of such primes $p \leq x$ is

$$\ll x/[(\log x)(\log\log\log\log x)].$$

Finally, for Question 1 we answer it in the affirmative assuming the generalised Riemann hypothesis for Dedekind zeta functions of certain algebraic number fields. Our method follows Hooley [7].

Though Question 1 is related to the primitive root conjecture, it is not clear if the full strength of the Riemann hypothesis is necessary to answer it. Indeed, if $r = 2$, Lichtman showed me the following elegant argument: a classical result of Siegel [15] states that if $f(x)$ has at least three distinct roots, then $P(f(x)) \to \infty$ as $x \to \infty$, where $P(n)$ denotes the largest prime factor of n. We apply this to the polynomial $g(x) = x^3 - a_2$. Hence $P(g(a_1^n)) \to \infty$ as $n \to \infty$. In particular, there are infinitely many primes p such that $a_1^{3n} \equiv a_2 \pmod{p}$. Thus it may be possible that an alternate argument can lead to an answer to Question 1.

For the purpose of clarity and ease of exposition, we begin with Question 2. Some of the tools developed there are used in Question 3. In the final section we consider Question 1.

In the sequel we put $\Gamma = \langle a_1, \ldots, a_r \rangle$ as a subgroup of $\mathbb{Q}^\times$ and write $\Gamma_p = \Gamma \pmod{p}$.

2. Preliminary lemmas

The following two lemmas will be crucial in the discussion, and we record them here for convenience.

Lemma 1. *Let $K/\mathbb{Q}$ be a Galois extension with group G. Let C be a conjugacy class in G. Let $(a, k) = 1$ and $\pi_C(x, k, a)$ denote the number of primes $p \leq x$ which are unramified in K with Artin symbol C and $p \equiv a \pmod{k}$. There are Chebotarev densities $\delta(C, k, a) > 0$ such that for any $A > 0$*

$$\sum_{k \leq Q} \max_{(a,k)=1} \max_{y \leq x} |\pi_C(y, k, a) - \delta(C, k, a)\pi(y)| \ll \frac{x}{\log^A x}$$

for $Q = x^{\alpha - \varepsilon}$ for any fixed $\varepsilon > 0$ and $\alpha = \min(\frac{2}{n}, \frac{1}{2})$, $n = [K : \mathbb{Q}]$.

Proof. See [10, p. 244].

Lemma 2. *Let Γ be a finitely generated subgroup of $\mathbb{Q}^\times$ of rank r. Let Γ_p be the reduction $\Gamma \pmod p$ (which makes sense for p sufficiently large). The number of primes p such that $|\Gamma_p| < y$ is $O(y^{1+1/r})$.*

Proof. See [3, p. 128].

3. Orders of Γ_p

Lemma 3. *Let $v_z(p-1)$ denote the number of prime divisors of $p-1$ less than z. Then*

$$\sum_{p\le x}\{v_z(p-1)-\log\log z\}^2 = O\left(\frac{x\log\log z}{\log x}\right).$$

Proof. We will use the Bombieri-Vinogradov theorem. Let $\pi(x, q, a)$ denote the number of primes $p \le x$ such that $p \equiv a \pmod q$. For any $A > 0$ there is a $B(A) = B > 0$ such that

$$\sum_{q<x^{1/2}L^{-B}} \max_{y\le x}\max_{(a,q)=1}\left|\pi(y, q, a) - \frac{\operatorname{li} y}{\varphi(q)}\right| \ll \frac{x}{L^A},$$

where $L = \log x$. To prove the theorem, we may suppose that $z \le x^\theta$ with $\theta < \frac{1}{4}$ because

$$v_z(p-1) = v_{x^\theta}(p-1) + O(1).$$

Then

$$\sum_{p\le x} v_z(p-1) = \sum_{q\le z}\pi(x, q, 1) = \sum_{q\le z}\frac{\operatorname{li} x}{q-1} + O\left(\frac{x}{L^A}\right)$$

by an application of the Bombieri-Vinogradov theorem. Since

$$\sum_{q\le z}\frac{1}{q-1} = \log\log z + O(1),$$

we deduce

$$\sum_{p\le x} v_z(p-1) = (\operatorname{li} x)\log\log z + O\left(\frac{x}{\log x}\right).$$

In a similar way, another application of the Bombieri-Vinogradov theorem leads to

$$\sum_{p\le x} v_z^2(p-1) = (\operatorname{li} x)(\log\log z)^2 + O\left(\frac{x\log\log z}{\log x}\right).$$

Hence

$$\sum_{p\le x}\{v_z(p-1)-\log\log z\}^2 = O\left(\frac{x\log\log z}{\log x}\right).$$

This completes the proof of the lemma.

Corollary. *If $z = z(x) \to \infty$, the number of primes $p \le x$ satisfying*

$$|v_z(p-1) - \log\log z| \ge \varepsilon\log\log z \tag{1}$$

is $O_\varepsilon(x/(\log x)(\log\log z))$, where the implied constant may depend on ε.

Proof. If N is the number of primes $p \leq x$ satisfying (1), then by the lemma $\varepsilon^2 N(\log\log z)^2 = O((x\log\log z)/\log x)$, from which the assertion is immediate.

Lemma 4. *The number of primes p such that $l|(\mathbb{F}_p^\times : \Gamma_p)$ is*

$$\delta(l)\operatorname{li} x + O\left(xe^{-\sqrt{\log x}}\right)$$

uniformly for $l \leq (\log x)^\alpha$ for a suitable constant $\alpha > 0$. Moreover, $\delta(l) = O(l^{-r-1})$.

Proof. Let $L/\mathbb{Q}$ be a Galois extension of degree n and discriminant d. By Proposition 3.3 of [14] there are absolute constants C, A such that if

$$\sqrt{\log x/n} \leq C\max(\log|d|, |d|^{1/n}),$$

then the number of primes $p \leq x$ which split completely in L is

$$\operatorname{li} x/n + O\left(x\exp\left(-A\sqrt{(\log x)/n}\right)\right).$$

By [14] we know that $(\log|d|)/n \geq \log l + O(1)$ for $L_l = \mathbb{Q}(\zeta_l, a_1^{1/l}, \ldots, a_r^{1/l})$, where $O(1)$ may depend on $a_1, \ldots, a_r$. Hence $|d|^{1/n} \ll l$. Also, for sufficiently large l, $[L_l : \mathbb{Q}] = (l-1)l^r$, so $\frac{1}{n} = O(l^{-r-1})$.

It is now clear that if $l \leq (\log x)^\alpha$ for a suitably small constant $\alpha > 0$, the constraints on the discriminant d are met and the lemma follows.

Theorem 1. *Let $a_1, \ldots, a_r$ be mutually coprime natural numbers greater than unity. Let Γ be the multiplicative group generated by $a_1, \ldots, a_r$ and Γ_p its image $(\mathrm{mod}\, p)$. Then the number of primes $p \leq x$ such that Γ_p has prime order is $o(x/\log x)$.*

Remark. It is reasonable to conjecture that the number of such primes less than x is $\geq cx/\log^2 x$ for some positive constant c. Indeed, one expects an infinitude of primes p such that $p-1 = 2q$, where q is prime and $(a_i/p) = 1$. For such primes p Γ_p clearly has order q.

Proof. The proof has two steps. By Lemma 3 the number of prime divisors of $p-1$ less than z is essentially (in the sense of the previous corollary) $\log\log z$ for almost all primes $p \leq x$ and for suitable $z = z(x) \to \infty$. The second step is derived from Lemma 4. The number of primes $p \leq x$ such that $l|(\mathbb{F}_p^\times : \Gamma_p)$ is

$$\delta(l)\operatorname{li} x + O\left(xe^{-\sqrt{\log x}}\right)$$

uniformly for $l \leq (\log x)^\alpha$ with a suitable constant $\alpha > 0$. Moreover, $\delta(l) = O(l^{-r-1})$. From step 1, for all but $o(x/\log x)$ primes $p \leq x$, the number of prime factors v of $p-1$ less than $(\log x)^\alpha$ satisfies

$$(1-\varepsilon)\log\log\log x < v < (1+\varepsilon)\log\log\log x.$$

By the same result, all but $o(x/\log x)$ primes $p \leq x$ have at least

$$(1-\varepsilon)\log\log\log x - (1+\varepsilon)\log\log z(x) \tag{2}$$

prime factors l satisfying $z(x) < l < (\log x)^\alpha$. Choose $z(x) = \log\log x$. Since

$$\sum_{z(x)<l<(\log x)^\alpha} \left\{\frac{\operatorname{li} x}{l^{r+1}} + O\left(xe^{-\sqrt{\log x}}\right)\right\}$$

is $o(x/\log x)$, we can suppose that the prime divisors of $p-1$ enumerated by (2) *do not* divide the index $(\mathbb{F}_p^\times : \Gamma_p)$. They therefore divide $|\Gamma_p|$. Hence for all but $o(x/\log x)$ primes $p \le x$ the order of Γ_p is composite. This completes the proof.

Remark. For the logarithmic cognoscenti it is not difficult to see that the proof in fact gives

$$O(x/(\log x)(\log\log\log\log x)).$$

Indeed, taking the choice of $z(x) = \log\log x$ in the corollary to Lemma 3 makes this estimate apparent.

4. The sieve argument

Theorem 2. *Let $f(t) \in \mathbb{Z}[t]$ be irreducible. The number of primes $p \le x$ such that $f(t) \pmod p$ factors completely into linear factors and $(p-1)/2$ has no divisor of the form $q(qs+1)$ with q a prime is*

$$\ge Cx/(\log x)(\log\log x)$$

for some appropriate constant $C > 0$.

Remark. With a little more care it is possible to obtain an asymptotic formula for the number of such $p \le x$ as

$$\sim C_f x/(\log x)(\log\log x),$$

where C_f is a positive constant depending only on f. Note that this theorem answers Question 3 by virtue of Sylow's theorem.

Proof. The key tool is the variant of the Bombieri-Vinogradov theorem as developed by Murty [10] and given in Lemma 3. Without loss of generality let us suppose that $f(t)$ is a normal polynomial (that is, a root θ generates a Galois extension), for if not we can consider a defining polynomial associated with the normal closure of $\mathbb{Q}(\theta)$ instead of $f(t)$. Let $n =$ degree of f. Let $\pi_f(x; d)$ be the number of primes $p \le x$ such that $p \equiv 1 \pmod d$ and $f(t)$ splits completely $(\mathrm{mod}\, p)$. We know from Lemma 1 that for any $B > 0$ there is an $A > 0$ such that

$$\sum_{d \le x^{1/n}/\log^A x} \left| \pi_f(x, d) - \frac{\alpha_d \operatorname{li} x}{\phi(d)} \right| \ll \frac{x}{\log^B x}, \tag{3}$$

where α_d is an appropriate adjustment factor of the expected density. [Indeed, $\alpha_d = \frac{1}{n}$ for all d supported outside a finite set of primes.] Now let $z = \frac{1}{2n}\log x$. We apply the sieve of Eratosthenes (see [14]) to deduce that the number of primes $p \le x$ such that $f(t)$ splits completely $(\mathrm{mod}\, p)$ *and* $(p-1)/2$ has no prime factors $\le z$ is

$$\sim \frac{Cx}{\log x} \prod_{p \le z} \left(1 - \frac{1}{p}\right),$$

where C is a positive constant. By Merten's formula [5, p. 351] this is

$$\sim Ce^{-\gamma} x/(\log x)(\log\log x), \tag{4}$$

where γ is Euler's constant. The choice of z is made so that $2^{z/\log z} \le$

$x^{1/n}/\log^A x$, and we can use (3) in the sieve of Eratosthenes. Of *these* primes p, those $p-1$ having a divisor of the form $q(qs+1)$ with q prime must have $q > z$. We can apply Brun's sieve [4] to count primes $p \leq x$ such that $p \equiv 1 \pmod{d}$ and $(p-1)/2$ has no prime factors $\leq z$. This number is bounded by

$$\frac{x}{\phi(d)\log x} \cdot \prod_{2<l\leq z}\left(1-\frac{1}{l-1}\right) \ll \frac{x}{\phi(d)\log x}\cdot\frac{1}{\log\log x}.$$

For $d = q(qs+1)$ this estimate is

$$\ll \frac{x}{q(qs+1)}\cdot\frac{1}{(\log x)\log\log x}.$$

Now sum this over all s and q prime $> z$. We obtain

$$\ll \sum_{q<z}\frac{1}{q^2}\cdot\frac{x}{\log\log x} \ll \frac{x}{(\log x)(\log\log x)^2}$$

since

$$\sum_{q>z}\frac{1}{q^2} \sim \frac{1}{z\log z}.$$

Hence of the primes enumerated in (4) only

$$O(x/(\log x)(\log\log x)^2)$$

primes $p \leq x$ have the property that $p-1$ has a divisor of the form $q(qs+1)$ with q prime. Hence, the remaining do not. This completes the proof.

Theorem 3. *Let $f(t) \in \mathbb{Z}[t]$ be irreducible. For $q > C(f)$ (a constant depending on f) there are infinitely many primes p such that $f(t)$ splits completely* $\pmod{p}$ *and $|\mathbb{F}_p^\times : \langle q\rangle| = 1$ or 2.*

Remark. If q is a quadratic residue $\pmod{p}$, the index equals 2. This possibility cannot be ruled out. It is also noteworthy that if the GRH is true, then the restriction $q > C(f)$ is unnecessary.

Proof. Lemma 1 used in the proof of the previous theorem in conjunction with the lower bound sieve (see Iwaniec [8]) allows us to deduce that the number of primes $p \leq x$ such that $f(t)$ splits completely $\pmod{p}$ *and* $(p-1)/2$ has all its prime factors $> x^{1/2n-\varepsilon}$ is (for any fixed $\varepsilon > 0$)

$$\gg x/\log^2 x,$$

where the implied constant depends on ε. Now let $q_1, \ldots, q_r$ be r distinct primes. If $\langle q_1, \ldots, q_r\rangle \pmod{p}$ is a proper subgroup of $\mathbb{F}_p^\times$ and the index is not equal to two, then $|\langle q_1, \ldots, q_r\rangle \pmod{p}|$ has size $\leq x^{1-1/2n+\varepsilon}$.

By Lemma 2 the number of such primes is

$$O(x^{(1-1/2n+\varepsilon)(r+1)/r}), \tag{5}$$

which is $O(x^{1-\eta})$ with $\eta > 0$ if $r > 2n-1$. Moreover, this estimate is uniform for $q_i \leq x$. Therefore, if we remove the primes enumerated in (5) we are still left with $\gg x/\log^2 x$ primes $p \leq x$ such that $f(t)$ splits completely $\pmod{p}$ and $\langle q_1, \ldots, q_r\rangle = \mathbb{F}_p^\times$ or $(\mathbb{F}_p^\times)^2$ for $r > 2n-1$. Now suppose that conclusion of the theorem is false. For every prime q sufficiently large q is not a primitive

root for the primes enumerated above. To each prime q associate a subset of primes dividing $p-1$ that divide the order of $\langle q\rangle \pmod p$. This subset has at most $2n$ elements and corresponds to a divisor of $p-1$. Our claim is that the associated divisor should be $p-1$ or $(p-1)/2$ for *all* q sufficiently large. If not, there are $\geq \delta x/\log x$ primes $q \leq x$ that are associated to a *proper* divisor of $(p-1)/2$. Taking any r such primes contradicts the above estimate. This completes the proof.

Remark. It is to be noted that this argument works because the q_i do not enter into the first part of the result obtained by the lower bound sieve method *and* estimate (5) is uniform $q_i \leq x$. In fact, if $q_i \leq x^A$ for any fixed $A > 0$, estimate (5) is still uniform, as the method of [3] reveals.

5. Conditional results

Theorem 4. *Let $a_1, \ldots, a_r$ be mutually coprime natural numbers greater than unity, and let $\Gamma = \langle a_1, \ldots, a_r\rangle$. Assuming the generalised Riemann hypothesis (GRH), there is a positive density of prime numbers p such that $\Gamma_p = \langle a_1\rangle \pmod p$.*

Proof. We may suppose $r \geq 2$. For the sake of the simplicity we will suppose that $a_1, \ldots, a_r$ are squarefree numbers. (The general case can be treated by the method below without difficulty by noting that certain densities have to be altered appropriately.) On the GRH we will produce a positive density of primes p such that $p-1$ is squarefree and $\Gamma_p = \langle a_1\rangle \pmod p$. Indeed, if l is a given prime, when does it divide the index $[\Gamma_p : \langle a_1\rangle] \pmod p$? This happens if and only if

$$l|(\mathbb{F}_p^\times : \langle a_1\rangle)/(\mathbb{F}_p^\times : \Gamma_p).$$

Suppose that $p-1$ is squarefree. Then the latter condition is equivalent to

$$l|(\mathbf{F}_p^\times : \langle a_1\rangle) \quad \text{and} \quad l \nmid (\mathbf{F}_p^\times : \Gamma_p). \tag{6}$$

We now follow the method of [12]. The reader may find it useful to scan [13] before proceeding. We introduce a suitable parameter $y(x) \to \infty$ as $x \to \alpha$ and first consider $l \leq y(x)$. By the method of [12] the number of primes $p \leq x$ such that $p-1$ is squarefree and (6) is not satisfied for any $l \leq y(x)$ is asymptotically

$$= \frac{6}{\pi^2} \prod_l \left(1 - \frac{1}{l(l-1)} + \frac{1}{l^r(l-1)}\right) \operatorname{li} x$$

because the Chebotarev density of primes p satisfying (6) is

$$1/l(l-1) - 1/l^r(l-1).$$

From these we must remove those primes $p \leq x$ for which (6) is satisfied for some $l > y(x)$. As indicated in [12], we break the calculation into three parts

$$y(x) < l < x^{1/2}/\log^A x,$$
$$x^{1/2}/\log^A x < l < x^{1/2}\log^A x,$$
$$x^{1/2}\log^A x < l < x$$

for some appropriate $A > 0$ to be chosen later. If $l|(\mathbb{F}_p^\times : \langle a_1\rangle)$ for $l > x^{1/2}\log^A x$, then $a_1^m \equiv 1 \pmod p$ with $m < x^{1/2}\log^{-A} x$ so that p divides

the product

$$T = \prod_{m<x^{1/2}\log^{-A}x} (a_1^m - 1).$$

Since a natural number has $O(\log n)$ prime factors, the number of such p cannot exceed

$$\log T \ll \sum_{m<x^{1/2}\log^{-A}x} m \log a \ll x \log^{-2A} x.$$

This is negligible in comparison with the main term for A sufficiently large. For $x^{1/2}/\log^A x < l < x^{1/2}\log^A x$ the number of primes p satisfying (6) clearly cannot exceed

$$\sum_{x^{1/2}/\log^A x<l<x^{1/2}\log^A x} \pi(x, l, 1),$$

where $\pi(x, l, 1)$ is the number of primes $p \leq x$ satisfying $p \equiv 1 \pmod{l}$. By the Brun-Titchmarsh theorem [4] this is dominated by $\sum_l' x/l\log x$, where the dash on the summation indicates that l is in the specified range. But

$$\begin{aligned}\sum_l{}' \frac{1}{l} &= \log\log(x^{1/2}\log^A x) - \log\log(x^{1/2}\log^{-A} x) + O\left(\frac{1}{\log x}\right)\\ &= \log\left(\frac{(\log x + A\log\log x)/2}{(\log x - A\log\log x)/2}\right) + O\left(\frac{1}{\log x}\right)\\ &= O\left(\frac{\log\log x}{\log x}\right)\end{aligned}$$

by the formula in [5]. The contribution from the second interval thus cannot exceed $O((x\log\log x)/\log^2 x)$. The range $y(x) < l < x^{1/2}/\log^A x$ is dealt with by the Chebotarev density theorem with an error term implied by the generalized Riemann hypothesis [11, p. 261]. For a fixed l a prime p satisfying (6) splits completely in $\mathbb{Q}(\zeta_l, a_1^{1/l})$, where ζ_l is a primitive lth root of unity (see [12]). On the GRH the number of such primes $p \leq x$ is

$$\frac{1}{l(l-1)} \cdot \operatorname{li} x + O(x^{1/2}\log lx).$$

Summing this for l in the specified range, we get that the number of primes $p \leq x$ satisfying (6) is

$$\ll x/y(x)\log x + O(x\log^{-A+1} x).$$

We choose $y(x) = \log x$ and $A = 3$. Putting this all together, we find that the number of primes $p \leq x$ satisfying (6) $O((x\log\log x)/\log^2 x)$. This completes the proof.

Remark. It is not difficult to introduce a splitting condition for p. Suppose $f(t)$ is an irreducible polynomial in $\mathbb{Z}[t]$ and we require primes p such that $f(t) \pmod{p}$ factors completely and

$$\langle a_1, \ldots, a_r\rangle = \langle a_1\rangle \qquad (\text{mod } p).$$

If the splitting field of f does not contain $\mathbb{Q}(\zeta_l, a_1^{1/l})$ for any l, then the above method generalizes easily (by the method of [12]) to yield a positive density of primes p of the required type.

ACKNOWLEDGMENTS

I thank Professor Alexander Lichtman for inviting me to University of Wisconsin, where this work was done. I also thank Hershy Kisilevsky for his comments.

REFERENCES

1. E. Artin, *Collected papers* (S. Lang and J. Tate, eds.), Springer-Verlag, New York, 1965.
2. P. Erdös, *On the distribution of divisors of integers in the residue class* (mod d), Bull Soc. Math. Grèce (N.S.) **6** (1965), 27–36.
3. R. Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), 127–130.
4. H. Halberstam and H. E. Richert, *Sieve methods*, Academic Press, London and New York, 1974.
5. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., Clarendon Press, Oxford, 1979.
6. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), 27–38.
7. C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.
8. H. Iwaniec, *Rosser's sieve*, Acta Arith. **36** (1980), 171–202.
9. A. Lichtman, *The Tits alternative and the soluble subgroups in linear groups over rings of fractions of polycyclic group rings*. I, J. Pure Appl. Algebra **86** (1993), 231–287.
10. K. Murty and R. Murty, *A variant of the Bombieri-Vinogradov theorem* (H. Kisilevsky and J. Labute, eds.), Montreal Number Theory Conference 1985, Canad. Math. Soc. Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 243–272.
11. K. Murty, R. Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), 253–281.
12. R. Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), 147–168.
13. ____, *Artin's conjecture on primitive roots*, Math. Intelligencer. **10** (1988), 59–67.
14. R. Murty and N. Saradha, *On the sieve of Eratosthenes*, Canad. J. Math. **39** (1987), 1107–1122.
15. C. L. Siegel (under the pseudonym X), *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \cdots + k$, J. London Math. Soc. (2) **1** (1926), 66–68.

DEPARTMENT OF MATHEMATICS, MCGILL UNIVERSITY, MONTREAL, CANADA H3A 2K6
E-mail address: murty@math.mcgill.ca