Centre de Recherches Mathématiques
CRM Proceedings and Lecture Notes
Volume 19, 1999

On the Order of a (mod p)

Pál Erdös and M. Ram Murty

1. Introduction

Let a be a fixed natural number greater than unity. For each prime p not dividing a, let $f(p)$ denote the order of a (mod p). A classical conjecture of E. Artin [**1**] states that if a is a perfect square, then $f(p) = p - 1$ for infinitely many primes p. We are interested in obtaining a good lower bound for $f(p)$ for almost all prime numbers p (that is, for all but $o(x/\log x)$ prime numbers $p \leq x$).

It is easy to see that

$$f(p) > \sqrt{p}/\log p$$

for all but $o(x/\log x)$ primes $p \leq x$. Indeed, if $f(p) < z$, then p divides the product

$$V = \prod_{t<z}(a^t - 1).$$

Since a natural number has at most $O(\log n/\log\log n)$ prime factors, we find that V has at most

$$\ll \sum_{t<z} \frac{t}{\log t} \ll \frac{z^2}{\log z}$$

prime factors. Thus, the inequality $f(p) < \sqrt{p}/\log p$ can hold for at most $O(x/\log^3 x)$ primes $p \leq x$.

It seems difficult to improve this simple argument to show that $f(p) > \sqrt{p}$ for almost all primes. By a different argument, we will prove:

THEOREM 1. *Let $\epsilon(p)$ be any function tending to zero as $p \to \infty$. For all but $o(x/\log x)$ primes $p \leq x$,*

$$f(p) \geq p^{1/(2+\epsilon(p))}.$$

This theorem will be a consequence of a more general theorem concerning divisors of $p - 1$. Indeed, we prove:

1991 *Mathematics Subject Classification.* Primary 11A07, 11N35; Secondary 11R42.

This paper was written by the authors in 1987 while Pál Erdös was visiting McGill. We had planned to work on an expanded version refining Theorem 2 but neither of the authors found the time or the opportunity to continue the work. Unfortunately, Pál has passed away. It is published here in the hope that others may continue the task.

This is the final version of the paper.

THEOREM 2. *Let $\delta > 0$ and fixed. Let $\epsilon(x)$ be any function tending to zero as $x \to \infty$. The number of primes $p \le x$ such that $p-1$ has a divisor in the interval $I = (x^\delta, x^{\delta+\epsilon(x)})$ is $o(x/\log x)$.*

Since $f(p)$ divides $p-1$, Theorem 1 follows from Theorem 2 upon taking $\delta = 1/2$.

Theorem 2 is to be viewed as the $p-1$ analogue of a theorem of Erdös [**3**], who proved that the number of integers $n \le x$ having a divisor in the interval $(x^\delta, x^{\delta+\epsilon(x)})$ is $o(x)$. Our proof of Theorem 2 follows very closely to the method and notation of Erdös [**3**]. The method, however, cannot give a better estimate for the exceptional set than $o(x/\log x)$. By an alternate method, we deduce:

THEOREM 3. *There exists an $\alpha > 0$ and a $\delta > 0$ such that*

$$f(p) \ge \sqrt{p}\exp((\log p)^\delta)$$

for all but $O(x/(\log x)^{1+\alpha})$ primes $p \le x$.

In [**11**], it was proved that

$$\sum_{p\le x} \frac{1}{f(p)} \ll \sqrt{x},$$

and it was conjectured that the sum is in fact $O(x^\epsilon)$. It was also noted that if the sum is $O(x^{1/4})$, then Artin's conjecture follows. Theorem 3 allows us to obtain the following improvement.

COROLLARY. *For some $\delta > 0$,*

$$\sum_{p\le x} \frac{1}{f(p)} \ll \frac{\sqrt{x}}{(\log x)^{1+\delta}}.$$

If we assume the analogue of the Riemann hypothesis for zeta functions of certain number fields, then it is possible to prove more than Theorem 1.

THEOREM 4. *Let $\epsilon(x)$ be any function tending to zero as $x \to \infty$. For each squarefree d, let $\zeta_d(s)$ denote the Dedekind zeta function of the algebraic number field*

$$\mathbb{Q}(\exp(2\pi\sqrt{-1}/d), a^{1/d})$$

and $\zeta(s)$ the usual Riemann zeta function. If all the non-trivial zeroes of $\zeta_d(s)$ lie on $\mathrm{Re}(s) = 1/2$, then

$$f(p) \ge p/\epsilon(p)$$

for all but $o(x/\log x)$ primes $p \le x$.

It is not difficult to generalize these results to an arbitrary subgroup $\Gamma \subseteq \mathbb{Q}^*$ of rank r (say). Suppose Γ is generated by the mutually coprime numbers $a_1, a_2, \ldots, a_r$. For all primes p not dividing the denominators of $a_1, \ldots, a_r$, we can define $f_\Gamma(p)$ to be the order of Γ (mod p). The previous theorems can be viewed as the case $r = 1$. The methods are analogous. The key idea is to use an appropriate analogue of Lemma 14 of [**5**] in conjunction with Theorem 2 to deduce the following:

THEOREM 5. *Let $\epsilon(x)$ be any function tending to zero as $x \to \infty$.*
(1) *For all but $o(x/\log x)$ primes $p \le x$,*

$$f_\Gamma(p) \ge p^{r/(r+1)+\epsilon(p)}.$$

(2) *There exists an $\alpha > 0$ and a $\delta > 0$ such that*

$$f_\Gamma(p) \ge p^{r/(r+1)} \exp((\log p)^\delta)$$

for all but $O(x/(\log x)^{1+\alpha})$ primes $p \le x$.
(3) *For each squarefree number d, let $\zeta_{d,i}(s)$ denote the Dedekind zeta function of*

$$\mathbb{Q}(\exp(2\pi\sqrt{-1}/d), a_i^{1/d}).$$

If for each $1 \le i \le r$, $\zeta_{d,i}(s)$ has no zeroes in the region $\mathrm{Re}(s) > r/r+1$, then

$$f_\Gamma(p) \ge p/\epsilon(p)$$

for all but $o(x/\log x)$ primes $p \le x$.

2. Lemmas

Denote by $\pi(x)$ the number of primes $\le x$. Let us factor $p-1 = uD$ where u is a divisor of $p-1$ in the stated interval I. Set $\nu = -\log\epsilon(x)$. Now write

$$u = AB$$

where A is a number composed of primes $\le x^{\epsilon(x)}$, B is a number composed of primes $> x^{\epsilon(x)}$.

LEMMA 1. *Let A be as above. The number of primes $p \le x$ for which A is greater than $x^{\epsilon(x)\nu}$ is $O(\pi(x)/\nu)$.*

PROOF. If S is the number of primes in question, then by an analogue of Legendre's formula,

$$S\epsilon(x)\nu\log x \le \sum_{q \le x^\epsilon} \{\pi(x,q) + \pi(x,q^2) + \cdots\}\log q$$

where q denotes a prime number and $\pi(x,q^a)$ is the number of primes $\le x$ which are $\equiv 1 \pmod{q^a}$. We write the sum on the right hand side as $\sum_I + \sum_{II}$ where in the first sum $a = 1$ and in the second sum $a \ge 2$. An application of the Bombieri-Vinogradov theorem shows that the first sum is $\ll \epsilon(x)x$. For the second sum, we begin by observing

$$\sum_{q > \log^3 x} \{\pi(x,q^2) + \cdots\}\log q \ll \log x \sum_{q > \log^3 x} \frac{x}{q(q-1)}$$

obtained by using the trivial bound $\pi(x,q^a) \le x/q^a$. The contribution from these terms to the sum is seen to be $O(x/\log x)$. If $q^a \le x^{1/2}$, we can apply the Brun-Titchmarsh inequality [6] to see that

$$\sum_{\substack{q \le x^{\epsilon(x)} \\ q^a \le x^{1/2}, a \ge 2}} \{\pi(x,q^a)\}\log q \ll \frac{x}{\log x}.$$

It remains to consider the contribution to $\sum_{II}$ of the primes $q \le \log^3 x$ for which $q^a > x^{1/2}$. But in this case,

$$a \ge b = \frac{\log x}{6 \log\log x}$$

and the contribution is for some constant $c_1 > 0$,

$$\ll \sum_{\substack{q \le \log^3 x \\ a \ge b}} \frac{x}{q^{b-1}(q-1)} \log q \ll x \log^3 x \exp\left(-c_1 \frac{\log x}{\log\log x}\right),$$

which is negligible. Hence,

$$S \ll \pi(x)/\nu.$$

□

Lemma 1 implies that in trying to prove Theorem 2, we can suppose that $A \le x^{\epsilon(x)\nu}$. Thus, B lies in the interval

$$J = (x^{\delta - \epsilon(x)\nu}, x^{\delta + \epsilon(x)})$$

and all its prime factors lie in the interval $K = (x^{\epsilon(x)}, x^{\delta+\epsilon(x)})$. The next lemma allows us to confine our attention to squarefree numbers in J.

LEMMA 2. *If B is divisible by a square of a prime, the number of primes $p \le x$ such that $p-1$ is divisible by such a B is $o(x/\log x)$.*

PROOF. This is immediate from the Brun-Titchmarsh inequality. Indeed, since all the prime divisors of B are $\ge x^{\epsilon(x)}$, the number in question is bounded by

$$\sum_{q \ge x^{\epsilon(x)}} \pi(x, q^2).$$

Using the trivial bound $\pi(x, q^2) \le x/q^2$ gives

$$\sum_{x^{\epsilon(x)} \le q \le \log^2 x} \pi(x, q^2) + \sum_{q > \log^2 x} \frac{x}{q^2} = \sum_{x^{\epsilon(x)} \le q \le \log^2 x} \pi(x, q^2) + O\left(\frac{x}{\log^2 x}\right).$$

Now using the Brun-Titchmarsh inequality, the result is immediate. □

LEMMA 3. *For $\theta > 1$,*

(i) $$\sum_{k > \theta y} \frac{y^k}{k!} \le \theta^{-\theta y} e^{\theta y}$$

and for $\theta < 1$,

(ii) $$\sum_{k < \theta y} \frac{y^k}{k!} \le \theta^{-\theta y} e^{\theta y},$$

provided $y > 1$.

PROOF. We have

$$\sum_{k>\theta y} \frac{y^k}{k!} = \sum_{k>\theta y} \frac{(\theta y)^k}{k!}\theta^{-k} \le \theta^{-\theta y} e^{\theta y},$$

for $\theta > 1$. This proves (i). To prove (ii), we first note that

$$e^k \ge k^k/k!.$$

For $y > 1$, observe that $y^k/k!$ is an increasing function of k when $k < \theta y$ and $\theta < 1$. Hence,

$$\sum_{k<\theta y} \frac{y^k}{k!} \le (\theta)^{-\theta y} e^{\theta y}.$$

□

A version of Lemma 3 appears in [**10**]. We insert it here because it makes our subsequent argument easier to follow. Using the notation of [**3**], we will denote by B_i^* a number lying in the interval J which has no more than $2\nu/3$ prime factors from K. A B_i^+ will denote a number lying in J whose number of prime factors from K is at least $2\nu/3$ but less than $4\nu/3$. A $B_i^{(r)}$ will denote a number from J with exactly r prime factors in K.

LEMMA 4. *There is a positive constant c such that*

$$\sum_{i=1}^{\infty} \frac{1}{\phi(B_i^*)} \le \epsilon(x)^c,$$

where ϕ denotes Euler's function.

PROOF. First we estimate

$$\sum_{i=1}^{\infty} \frac{1}{\phi(B_i^{(r)})}.$$

If

$$B_i^{(r)} = p_1 p_2 \cdots p_r,$$

then $p_r > (B_i^{(r)})^{1/r}$ so that

$$p_1 \cdots p_{r-1} < x^{(\delta+\epsilon(x))(r-1)/r} \tag{1}$$

and so the sum of the reciprocals of $\phi(B_i^{(r)})$ of which the first $r-1$ prime factors are $p_1, \ldots, p_{r-1}$ is not greater than

$$\frac{1}{\phi(p_1 \cdots p_{r-1})} \sum{}' \frac{1}{p_r - 1}$$

where the dash on the summation means that p_r runs through the interval

$$\left(\frac{x^{\delta-\epsilon(x)\nu}}{p_1 \cdots p_{r-1}}, \frac{x^{\delta+\epsilon(x)}}{p_1 \cdots p_{r-1}}\right).$$

Since

$$\sum_{U \le p \le UV} \frac{1}{p} = \log\log UV - \log\log U + O\left(\frac{1}{\log V}\right),$$

we find

$$\sum_{U\le p\le UV}\frac{1}{p}<\frac{\log V}{\log U}+O\left(\frac{1}{\log U}\right).$$

Therefore, taking

$$U=\frac{x^{\delta-\epsilon(x)\nu}}{p_1\cdots p_{r-1}},\quad V=x^{\epsilon(x)(\nu+1)}$$

in the above estimate, we find on using (1),

$$\sum{}'\frac{1}{p_r-1}\ll\frac{r(\nu+1)\epsilon(x)}{\delta-\epsilon(x)(\nu r+r-1)}.$$

Since, $r\le 4\nu/3$, $\epsilon(x)(r\nu+r-1)\ll\epsilon(x)\nu^2$ and so

$$\sum{}'\frac{1}{p_r-1}\ll\epsilon(x)\nu^2.$$

Hence

$$\sum_{i=1}^{\infty}\frac{1}{\phi(B_i^{(r)})}\ll\frac{\epsilon(x)\nu^2}{(r-1)!}\left(\sum_{p\in K}\frac{1}{p}\right)^{r-1}$$

which is

$$\ll\frac{\epsilon(x)\nu^2}{(r-1)!}(\nu+1)^{r-1}.$$

Thus,

$$\begin{aligned}\sum_{i=1}^{\infty}\frac{1}{\phi(B_i^*)}&=\sum_{1\le r\le 2\nu/3}\sum_{i=1}^{\infty}\frac{1}{\phi(B_i^{(r)})}\\&\ll\epsilon(x)\nu^2\sum_{1\le r\le 2\nu/3}\frac{(\nu+1)^{r-1}}{(r-1)!}\\&\ll\epsilon(x)\nu^2(2/3)^{-2(\nu+1)/3}e^{2(\nu+1)/3}\end{aligned}$$

by Lemma 3. The latter quantity is easily seen to be

$$\ll\epsilon(x)^c\nu^3$$

for some positive constant $c>0$. This completes the proof. □

LEMMA 5.

$$\sum_{i=1}^{\infty}\frac{1}{\phi(B_i^+)}\ll\nu^2.$$

PROOF. As in the previous lemma, we find

$$\begin{aligned}\sum_{i=1}^{\infty}\frac{1}{\phi(B_i^+)}&\le\sum_{2\nu/3\le r\le 4\nu/3}\sum_{i=1}^{\infty}\frac{1}{\phi(B_i^{(r)})}\\&\ll\epsilon(x)\nu^2\sum_{2\nu\le r\le 4\nu/3}\frac{(\nu+1)^{r-1}}{(r-1)!}\\&\ll\epsilon(x)\nu^2e^{\nu+1}\\&\ll\nu^2.\end{aligned}$$

□

LEMMA 6. *The number of primes $p \leq x$ such that $p-1$ is divisible by more than $4\nu/3$ primes from the interval K is $o(x/\log x)$.*

PROOF. This follows from Turán's normal order method. For completeness, we give a sketch. Let $\nu_K(p-1)$ denote the number of prime factors of $p-1$ lying in K. Then, letting $\rho = \min(1/6, \delta)$, we find

$$\sum_{p \leq x} \nu_K(p-1) = \sum_{p \leq x} \left(\sum_{\substack{x^{\epsilon(x)} \leq q \leq x^{\rho} \\ q \mid p-1}} + O(1) \right)$$

which is

$$= \sum_{x^{\epsilon(x)} \leq q \leq x^{\rho}} \pi(x, q) + O(x/\log x).$$

Using the Bombieri-Vinogradov theorem, we deduce that

$$\sum_{p \leq x} \nu_K(p-1) = \pi(x)\nu + O(x/\log x).$$

Similarly, we deduce that

$$\sum_{p \leq x} \nu_K^2(p-1) = \pi(x)\nu^2 + O(\pi(x)\nu)$$

so that

$$\sum_{p \leq x} (\nu_K(p-1) - \nu)^2 = O(\pi(x)\nu).$$

Therefore, the number of primes $p \leq x$ satisfying $\nu_K(p-1) \geq (4/3)\nu$ is $O(\pi(x)/\nu)$. This completes the proof of the lemma. □

3. Proof of Theorem 2

By Lemma 1, we can suppose that $A \leq x^{\epsilon(x)\nu}$ and so $B \in J$. If B has less than $2\nu/3$ prime factors from K, then by the Brun-Titchmarsh inequality the number of primes divisible by such a B is

$$\ll \sum_{i=1}^{\infty} \frac{x}{\phi(B_i^*) \log x}.$$

This quantity is by Lemma 4,

$$\ll \frac{x}{\log x} \epsilon(x)^c = o(x/\log x).$$

If B has more than $4\nu/3$ prime factors from K, then by Lemma 6, the number of primes p such that $p-1$ is divisible by such a B is $o(x/\log x)$. Thus, in our notation, B is a B_i^+ and $p-1$ has the form

$$p - 1 = tB_i^+$$

where t has no prime factors in the interval K. Fixing B_i^+, we count the number of integers $t \leq x/B_i^+$ such that t is not divisible by any prime in the interval K and $tB_i^+ + 1$ is not divisible by any prime $\leq x^{1/2}$. Defining

$$\omega(p) = \begin{cases} 1 & \text{if } p \leq x^{\epsilon(x)} \\ 2 & \text{if } x^{\epsilon(x)} < p \leq x^{1/2} \\ 1 & \text{if } p \mid B_i^+ \end{cases}$$

we see by Brun's sieve that the number of such t is

$$\ll \frac{x}{B_i^+} \prod_{p \leq x^{1/2}} \left(1 - \frac{\omega(p)}{p}\right) \ll \frac{x}{\phi(B_i^+)} \frac{\epsilon(x)}{\log x}.$$

Summing over B_i^+ using Lemma 5 yields that the sum is

$$\ll \frac{x}{\log x} \epsilon(x) \nu^2 = o(x/\log x).$$

This completes the proof of Theorem 2.

4. Proof of Theorem 3

In view of the remarks made at the outset of the paper, it suffices to consider the size of the set

$$\mathcal{S} = \{p \leq x : \sqrt{x}/\log x < f(p) \leq \sqrt{x}\exp(\log^\delta x)\}$$

for a suitable $\delta > 0$ to be chosen later. If p is an element of this set, then $p-1$ can be written as a product of two numbers u and v, each factor approximately $\sqrt{x}$, since we can assume, without loss, $p \geq x/\log^2 x$. More precisely,

$$p - 1 = uv, \quad \sqrt{x}/\log x < u < \sqrt{x}\exp(\log^\delta x), \quad \sqrt{x}\exp(-\log^\delta x) < v < \sqrt{x}\log x.$$

We now estimate the number of such primes. Let $\Omega(n)$ denote the number of prime factors of n, counted with multiplicity. Then, if both conditions

$$\Omega(u) > \frac{2}{3}\log\log x$$

$$\Omega(v) > \frac{2}{3}\log\log x$$

hold, then $\Omega(p-1) > 1.3\log\log x$. By a classical theorem of Erdös [4], the number of such primes $p \leq x$ is

$$O\left(\frac{x}{\log^\eta x}\right)$$

for some $\eta > 0$. Therefore, we can suppose that one of the above inequalities fails. Without loss of generality, suppose that

$$\Omega(v) \leq \frac{2}{3}\log\log x.$$

Let $P(v)$ denotes the greatest prime factor of v. If

$$P(v) < \exp(\log^{1-\epsilon} x) \tag{2}$$

then by a classical theorem of de Bruijn [2], the number of such $v \le x/u$ is

$$\ll \frac{x}{u}\exp(-\log^{\epsilon} x).$$

Thus, if (2) holds, the number of elements of $\mathcal{S}$ cannot exceed

$$\sum_u{}' \frac{x}{u}\exp(-\log^{\epsilon} x)$$

where the dash on the sum indicates that u is in the specified range of $\mathcal{S}$. But

$$\sum_u{}' \frac{1}{u} \ll \log^{\delta} x$$

and so the number of primes $p \in \mathcal{S}$ satisfying (2) cannot exceed

$$x\exp(-c_2 \log^{\epsilon} x)$$

for some positive constant c_2. We may therefore suppose that

$$p - 1 = uv_1 q \tag{3}$$

where q is a prime greater than $\exp(\log^{1-\epsilon} x)$. For fixed u and v_1, the number of solutions of (3) is by Brun's sieve

$$\ll \frac{x}{uv_1 \log^2(x/uv_1)}.$$

As

$$uv_1 \le x\exp(-c_1 \log^{1-\epsilon} x)$$

the number of solutions of (3) is

$$\ll \frac{x}{uv_1 \log^{2-\epsilon} x}.$$

Since

$$\Omega(v_1) < \frac{2}{3}\log\log x$$

and the number of natural numbers satsifying this inequality is [4]

$$O\left(\frac{x}{\log^{\beta} x}\right),$$

for some $\beta > 0$, and therefore by partial summation,

$$\sum_{\Omega(v_1) < 2\log\log x/3} \frac{1}{v_1} \ll (\log x)^{1-\beta}.$$

Hence, the total number of elements of $\mathcal{S}$ cannot exceed

$$\frac{x}{(\log x)^{1+\beta-\epsilon}} \sum_u{}' \frac{1}{u} \ll \frac{x}{(\log x)^{1+\beta-\epsilon-\delta}}$$

so that if we choose $\delta < \beta$, we obtain the desired result. This completes the proof of Theorem 3.

To prove the corollary, we break the sum into three parts:

$$\sum_{f(p)\le y} + \sum_{y<f(p)\le z} + \sum_{z<f(p)\le x}.$$

By the remarks made at the outset of the paper, the number of primes p such that $f(p) \le u$ is $O(u^2/\log u)$. Hence, by partial summation, the first sum is $O(y/\log y)$. The third sum is trivially $O(x/z \log x)$. If we choose

$$y = \sqrt{x}/\log^{\beta} x, \quad z = \sqrt{x}\exp(\log^{\delta} x)$$

then Theorem 3 implies that the middle sum is

$$\ll \frac{\sqrt{x}}{(\log x)^{1+\alpha-\beta}}.$$

Choosing $\beta < \alpha$ gives the result.

5. Proof of Theorem 4

For the sake of simplicity, let us suppose a is squarefree. The proof needs slight modification otherwise. The condition

$$a^{(p-1)/d} \equiv 1 \pmod p$$

implies that p splits completely in the field $\mathbb{Q}(\exp(2\pi\sqrt{-1}/d), a^{1/d})$. The number of such primes $p \le x$ is easily calculated by the standard methods of analytic number theory (see for example [**7**] or [**9**]). Denoting $\pi_d(x)$ to be the number of such primes, we find assuming the generalised Riemann hypothesis:

$$\pi_d(x) = \frac{\text{li } x}{d\phi(d)} + O(x^{1/2}\log dx).$$

Hence, if $d = (p-1)/f(p) \ge \epsilon(x)$, then the number of primes $p \le x$ for which this can happen cannot exceed

$$\sum_{\epsilon(x)\le d \le x^{1/2}/\log^5 x} \{\frac{li\ x}{d\phi(d)} + O(x^{1/2}\log dx)\} + O(x/\log^2 x)$$

the latter term coming from the number of primes for which $f(p) < p^{1/2}/\log^5 p$. Since the series

$$\sum_{d=1}^{\infty} \frac{1}{d\phi(d)}$$

converges, the result is now immediate.

Acknowledgement. The second author would like to thank the Institute for Advanced Study for its hospitality where this work was completed.

References

1. E. Artin, *The collected papers of Emil Artin* (S. Lang and J. Tate, ed.), Addison-Wesley, 1965.
2. N.G. de Bruijn, *On the number of positive integers $\le x$ and free of prime factors $> y$*, Nederl. Akad. Wetensch. Proc. Ser. A **54** (1951), 50–60.
3. P. Erdös, *A generalization of a theorem of Besicovitch*, J. London Math. Soc. **11** (1936), 92–98.
4. ———, *On the normal number of prime factors of $p-1$ and some related questions concerning Euler's ϕ function*, Quart. J. Math. (Oxford Ser.) **6** (1935), 205–213.
5. R. Gupta and M. Ram Murty, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), 13–44.
6. H. Halberstam and H. Richert, *Sieve Methods*, Academic Press, London, 1974.
7. C. Hooley, *Applications of sieve methods*, Cambridge University, 1976.

8. M. Ram Murty, *On Artin's conjecture*, J. Number Theory, **16** (1983), 147–168.
9. M. Ram Murty, V. Kumar Murty and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. of Math. **110** (1988), 253–281.
10. M. Ram Murty and N. Saradha, *On the sieve of Eratosthenes*, Canad. J. of Math. **39** (1987), 1107–1122.
11. M. Ram Murty and S. Srinivasan, Some remarks on Artin's conjecture, Canad. Math. Bull. **30** (1987), 80–85.

Hungarian Academy of Sciences, Budapest, Hungary

Departement of mathematics and statistics, Queen's University, Kingston, Ontario, K7L 3N6, Canada
E-mail address: murty@mast.queensu.ca