The average least quadratic nonresidue modulo m and other variations on a theme of Erdős

Paul Pollack

Abstract. For each natural number $m \geq 3$, let $n_2(m)$ denote the least *quadratic nonresidue* modulo m. That is, $n_2(m)$ is the least integer $n \geq 1$ coprime to m for which the congruence $x^2 \equiv n \pmod m$ is insoluble. In 1961, Erdős showed that the mean value of $n_2(p)$, as p runs over the odd primes, is given by $\sum_{k=1}^{\infty} \frac{p_k}{2^k} \approx 3.675$, where p_k denotes the kth prime in increasing order. Our first theorem gives the mean value of $n_2(m)$ without the restriction to prime values; it is $\sum_{k=1}^{\infty} \frac{p_k - 1}{p_1 p_2 \cdots p_{k-1}} \approx 2.920$.

For each prime p, let $G(p)$ denote the least natural number n so that the subgroup generated by $\{1, 2, \dots, n\}$ is all of $(\mathbf{Z}/p\mathbf{Z})^\times$. For p odd, $n_2(p) \leq G(p) \leq g(p) < p$, where $g(p)$ is the least primitive root modulo p. Assuming the Generalized Riemann Hypothesis, we show that $G(p)$ possesses a finite mean value ≈ 3.975.

For K a quadratic extension of $\mathbf{Q}$, let n_K denote the smallest rational prime which is inert in K and r_K the least prime which is split in K. We show that if one orders quadratic fields by the absolute value of their discriminant, then r_K and n_K have the same mean value, which is ≈ 4.981.

1. Introduction

For each natural number $m > 2$, let $n_2(m)$ denote the least *quadratic nonresidue* modulo m, i.e., the smallest natural number n relatively prime to m for which the congruence $x^2 \equiv n \pmod m$ is insoluble. Such an n always exists, since the squaring map on $(\mathbf{Z}/m\mathbf{Z})^\times$ fails to be injective (as $(-1)^2 = 1^2$), and so also fails to be surjective. Set $n_2(1) = n_2(2) = 1$. The maximal order of the function $n_2(m)$ has been the object of intense study, especially in the case when the argument m is assumed to be a prime number p. Around 1920, Vinogradov conjectured that $n_2(p) \ll_\epsilon p^\epsilon$ for each $\epsilon > 0$; this remains open, the closest approximation being Burgess's result [**Bur57**] that

$$n_2(p) \ll_\epsilon p^{\frac{1}{4\sqrt{e}} + \epsilon}.$$

Short of a proof that $n_2(p)$ is never large, one could hope to show that large values are very rare. The first theorem of this type is due to Linnik [**Lin42**], who showed that for each $\epsilon > 0$, one has that

$$\#\{p \leq x : n_2(p) > x^\epsilon\} \ll_\epsilon 1 \qquad \text{(for all } x\text{)}.$$

This was an early triumph of the large sieve in analytic number theory. Borrowing ideas from this work of Linnik, Erdős [**Erd61**] showed that $n_2(p)$ has a finite mean value: As

1991 *Mathematics Subject Classification.* Primary 11A27, Secondary 11N25, 11N36.

Key words and phrases. quadratic nonresidue, mean value, quadratic field, inert prime, split prime.

$x \to \infty$,

$$\frac{1}{\pi(x)} \sum_{p \le x} n_2(p) \to \sum_{k=1}^{\infty} \frac{p_k}{2^k}, \tag{1.1}$$

where p_k denotes the kth prime in increasing order.

Our first theorem is a determination of the average value of $n_2(m)$ without the restriction to prime arguments.

THEOREM 1.1. *As $x \to \infty$, we have*

$$\frac{1}{x} \sum_{m \le x} n_2(m) \to \Gamma, \quad \text{where} \quad \Gamma := \sum_{k=1}^{\infty} \frac{p_k - 1}{p_1 \cdots p_{k-1}}.$$

REMARKS 1.2.

(i) It is easy to see that $n_2(m)$ is prime for $m > 2$. The heuristic for Erdős's theorem is that $n_2(p) = p_k$ with probability 2^{-k}. This is exactly what one would guess, since each of $p_1, \dots, p_k$ should be a quadratic residue modulo p with probability $\frac{1}{2}$, and these events should be independent. The heuristic for Theorem 1.1 is simpler; a typical m has many prime factors, and so the proportion of quadratic residues among the units is very small. Thus, one might guess that typically, the least prime not dividing m is the least quadratic nonresidue. This turns out to be the case and explains the form of Γ given above: Γ is the mean value of the least prime not dividing m.

(ii) From the expressions above, we may compute that $n_2(p)$ has average value

$$3.67464396601132877899567630908402941167779758877943\dots$$

while the average of $n_2(m)$ is

$$2.92005097731613471209256291711201946800272789932142\dots$$

For each prime p, let $g(p)$ denote the least primitive root modulo p. Then $n_2(p) \le g(p)$ for all p. The mean value of $g(p)$ was investigated by Elliott and Burgess [**BE68**] and later by Elliott and Murata. In [**BE68**], one finds the result

$$\frac{1}{\pi(x)} \sum_{p \le x} g(p) \ll (\log x)^2 (\log\log x)^4, \tag{1.2}$$

and in [**EM97**], one reads that on the Generalized Riemann Hypothesis,

$$\frac{1}{\pi(x)} \sum_{p \le x} g(p) \le (\log x)(\log\log x)^{1+o(1)},$$

as $x \to \infty$. (Throughout this article, we use the term *Generalized Riemann Hypothesis*, or GRH, to refer to the assertion that all nontrivial zeros of all Dedekind zeta functions lie on the line $\Re(s) = \frac{1}{2}$.) Under a certain technical hypothesis additional to GRH, Elliott and Murata show that $g(p)$ possesses a finite mean value, which they believe to be $4.924\dots$.

The second topic of this paper is an investigation into a function intermediate between $n_2(p)$ and $g(p)$. Let $G(p)$ denote the least natural number n so that the set $\{1, 2, \dots, n\}$ generates the full unit group modulo p. Thus, $n_2(p) \le G(p) \le g(p)$. We prove the following unconditional result, which is slightly better than what one obtains directly from (1.2) and the inequality $G(p) \le g(p)$:

THEOREM 1.3. *For $x \geq 3$, we have*

$$\frac{1}{\pi(x)} \sum_{p \leq x} G(p) \ll (\log x)^2.$$

Assuming GRH (and without any further technical hypotheses) we show that the mean value of $G(p)$ exists:

THEOREM 1.4. *Assume the Generalized Riemann Hypothesis. Then as $x \to \infty$,*

$$\frac{1}{\pi(x)} \sum_{p \leq x} G(p) \to \Delta, \quad \textit{where } \Delta = 3.97483847045631033\ldots.$$

In fact, we give a (complicated) expression for Δ as an infinite series. The proof of Theorem 1.4 rests on work of Pappalardi [**Pap97**], who studied (on GRH) the proportion of primes p for which $G(p)$ assumes a prescribed value. We note that $G(m)$ can also be defined for composite values of m and that in this case, the maximal and average orders have been investigated by Burthe [**Bur97a, Bur97b**] and Norton [**Nor98**].

The last theme we take up concerns yet another variation on (1.1). For each non-principal Dirichlet character χ, let n_χ denote the least n for which $\chi(n) \notin \{0, 1\}$. Erdős's result (1.1) gives the average of n_χ as χ runs over the characters $\left(\frac{\cdot}{p}\right)$, for $p \leq x$. Now let D be a fundamental discriminant, i.e., the discriminant of a quadratic field. Let $\chi_D := \left(\frac{D}{\cdot}\right)$ be the associated Kronecker symbol, which is a real primitive character modulo $|D|$, and let $n(D) := n_{\chi_D}$. What is the average of $n(D)$? Equivalently, what is the average size of the smallest inert prime, where the average is taken over quadratic fields ordered by discriminant? Our answer is the following:

THEOREM 1.5. *As $x \to \infty$, one has*

$$\frac{\sum_{|D| \leq x} n(D)}{\sum_{|D| \leq x} 1} \to \Theta, \quad \textit{where} \quad \Theta := \sum_{k=1}^{\infty} \frac{p_k^2}{2(p_k+1)} \prod_{i=1}^{k-1} \frac{p_i + 2}{2(p_i+1)}. \tag{1.3}$$

Here D runs over all fundamental discriminants with $|D| \leq x$. Numerically,

$$\Theta = 4.98094733961493415079132532588077528123773269658520\ldots.$$

Theorem 1.5 may be compared with the following theorem of Elliott [**Ell70**, Theorem 5]: The function $n'(a)$, defined for $a > 1$ as the least odd prime p with $\left(\frac{a}{p}\right) = -1$, possesses a finite mean value.

Elliott [**Ell68**, Theorem 2] showed that Erdős's result (1.1) holds with $n_2(p)$ replaced by $r_2(p)$, the least *prime* quadratic residue. This raises the question of the behavior of $r(D)$, defined as the least split prime in $\mathbf{Q}(\sqrt{D})$, with D a fundamental discriminant. We conclude the paper by discussing the proof of the following result:

THEOREM 1.6. *The average smallest split prime in $\mathbf{Q}(\sqrt{D})$, in the sense of Theorem 1.5, is the constant Θ defined in* (1.3)*. In other words,*

$$\frac{\sum_{|D| \leq x} r(D)}{\sum_{|D| \leq x} 1} \to \Theta \qquad (\textit{as } x \to \infty),$$

where again D runs over fundamental discriminants of absolute value $\leq x$.

Notation and conventions. The letters p and ℓ are reserved for prime numbers. We remind the reader that p_k denotes the kth prime in increasing order, so that $p_1 = 2$, $p_2 = 3$, etc. When we speak of the subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$ generated by a set of integers, we mean the group generated by (the images of) the elements coprime to p. We use $\Psi(x, y)$ for the number of *y-smooth* (also called *y-friable*) natural numbers $n \le x$, i.e., the number of $n \le x$ divisible only by primes $p \le y$. We let $\Psi_q(x, y)$ denote the counting function of the y-smooth numbers coprime to q. We write $\mathrm{Li}(x) := \int_2^x dt/\log t$ for the usual logarithmic integral.

2. Proof of Theorem 1.3

It is convenient to prove Theorems 1.3 and 1.4 before Theorem 1.1, since their proofs are shorter and conceptually simpler.

We need a few preliminary results. The following lemma, which is proved using the arithmetic large sieve (à la Linnik and Erdős), is extracted from work of Konyagin and Pomerance [**KP97**]; essentially the same lemma appears in work of Pappalardi [**Pap95**].

LEMMA 2.1. *Suppose that $2 \le y \le x$. The number of primes $p \le x$ for which the natural numbers $\le y$ fail to generate $(\mathbf{Z}/p\mathbf{Z})^\times$ is $\ll x^2/\Psi(x^2, y)$.*

The next lemma, with an explicit implied constant, appears as [**KP97**, Theorem 6.2]:

LEMMA 2.2. *Suppose that $2 \le y \le x$. The number of primes $p \le x$ with $G(p) > y$ is $\ll x^{2\log\log(x^2)/\log y}$.*

PROOF. This follows immediately from Lemma 2.1 and the following lower bound on $\Psi(X, Y)$ due to Konyagin and Pomerance [**KP97**, Theorem 2.1]: $\Psi(X, Y) > X^{1-\frac{\log\log X}{\log Y}}$ whenever $X \ge 4$ and $2 \le Y \le X$. □

The next result follows immediately from the classical Polya–Vinogradov inequality; sharper upper bounds on $G(p)$ are known but these would not be of use to us.

LEMMA 2.3. *For all primes $p \ge 2$, we have $G(p) \ll p^{1/2}\log p$.*

PROOF OF THEOREM 1.3. We split the mean value appearing in the theorem statement into three parts, according to whether (i) $G(p) > (2\log x)^5$, (ii) $(3\log x)^2 < G(p) \le (2\log x)^5$, or (iii) $G(p) \le (3\log x)^2$. By Lemmas 2.2 and 2.3, the sum over those p in (i) is

$$\ll x^{1/2}\log x \sum_{\substack{p\le x\\ G(p)>(2\log x)^5}} 1 \ll (x^{1/2}\log x)\cdot x^{2/5};$$

in particular, this contribution is $o(\pi(x))$. The sum over those p in (ii) is

$$\ll (\log x)^5 \sum_{\substack{p\le x\\ G(p)>(3\log x)^2}} 1 \ll (\log x)^5 x^{\frac{2\log\log(x^2)}{2\log\log x+\log 9}} \ll x/\exp(\frac{1}{3}\log x/\log\log x),$$

by a short computation. So this contribution is also $o(\pi(x))$. Finally, the sum over those p satisfying (iii) is trivially at most $\pi(x)(3\log x)^2$. Dividing through by $\pi(x)$ gives the theorem. □

3. Proof of Theorem 1.4

If $p > 2$, so that the unit group modulo p consists of more than one element, then $G(p)$ is a prime number. We would like an estimate on the proportion of primes p for which $G(p)$ assumes a prescribed prime value. This comes out of the next result, which is due to Hooley [**Hoo67**] when $r = 1$ and to Pappalardi (see [**Pap97**, Theorems 1, 2]) when $r > 1$.

THEOREM A. *Assume GRH. Let $x \geq 3$, and let r be a natural number satisfying*

$$r \leq \frac{1}{4}\frac{\log x}{\log\log x}. \tag{3.1}$$

The number of $p \leq x$ for which the primes $p_1, \dots, p_r$ generate the unit group modulo p is

$$\delta_r \pi(x) + O(x \log\log x (4/\log x)^{r+1}).$$

Here the constant δ_r is given by

$$\left(\prod_{\ell \text{ odd prime}} \left(1 - \frac{1}{\ell^r(\ell-1)}\right)\right) \times \left(1 - \frac{1}{2^{r+1}}\left\{\prod_{i=1}^{r-1}\left(1 - \frac{\left(\frac{-1}{p_i}\right)}{p_i^{r+1} - p_i^r - 1}\right) + \prod_{i=1}^{r-1}\left(1 - \frac{1}{p_i^{r+1} - p_i^r - 1}\right)\right\}\right). \tag{3.2}$$

REMARK 3.1. To obtain our statement from [**Pap97**, Theorems 1, 2], we use that the product of the first r primes is bounded by $x^{1/2}$ (say), for r satisfying (3.1) and x sufficiently large. We also replace $\pi(x)$ with $\mathrm{Li}(x)$, which is justified by von Koch's well-known estimate $\mathrm{Li}(x) - \pi(x) \ll x^{1/2}\log x$ (under GRH). Note that [**Pap97**, Theorem 1] allows us to remove the factor $\log\log x$ from the error term whenever $r > 1$; however, this is unimportant.

PROOF OF THEOREM 1.4. Put $\delta_0 = 0$, and for $r \geq 1$, let δ_r have the same meaning as in Theorem A. By that theorem, it is natural to expect that

$$\frac{1}{\pi(x)}\sum_{p \leq x} G(p) \to \Delta, \quad \text{where} \quad \Delta := \sum_{r=1}^{\infty} p_r(\delta_r - \delta_{r-1}), \tag{3.3}$$

provided that the series defining Δ converges. We prove convergence of this series and then we prove (3.3); after the proof, we indicate how to obtain a numerical approximation to Δ.

Convergence of the infinite series in (3.3) is easy; indeed, the first factor in (3.2) satisfies

$$\begin{aligned}\prod_{\ell > 2}\left(1 - \frac{1}{\ell^r(\ell-1)}\right) &\geq 1 - \sum_{\ell > 2}\frac{1}{\ell^r(\ell-1)} \\ &> 1 - \sum_{\ell > 2}\frac{1}{(\ell-1)^{r+1}} > 1 - \frac{1}{2^{r-1}},\end{aligned}$$

where the final sum is handled by ignoring the primality of ℓ and employing a crude integral approximation. Also, the second factor in (3.2) is at least $1 - 1/2^r$. Thus, for $r \geq 2$, we have $1 - \frac{3}{2^r} \leq \delta_r \leq 1$. This gives convergence of the series defining Δ, by comparison with the convergent series $\sum_{r=1}^{\infty} p_r/2^r$.

Now we prove the limiting relation asserted in (3.3). Referring back to the proof of Theorem 1.3, we have from the estimates in ranges (i) and (ii) that (unconditionally)

$$\frac{1}{\pi(x)} \sum_{\substack{p \le x \\ G(p) > (3\log x)^2}} G(p) = o(1) \qquad (\text{as } x \to \infty).$$

So we may focus attention on p with $G(p) \le (3\log x)^2$. When $G(p) \le \frac{1}{8}\log x$, we use Theorem A: Set $R := \pi(\frac{1}{8}\log x)$, and note that $R \le \frac{1}{4}\log x/\log\log x$ if x is large (as we may assume). From Theorem A,

$$\begin{aligned}\frac{1}{\pi(x)} \sum_{\substack{p \le x \\ G(p) \le \frac{1}{8}\log x}} G(p) &= \sum_{r \le R} p_r(\delta_r - \delta_{r-1}) + O\left(\log\log x \sum_{1 \le r < R} p_{r+1}(4/\log x)^r\right) \\ &= \sum_{r \le R} p_r(\delta_r - \delta_{r-1}) + O\left(\log\log x \sum_{1 \le r < R} (8/\log x)^r\right) \\ &= \Delta - \sum_{r > R} p_r(\delta_r - \delta_{r-1}) + O(\log\log x/\log x) = \Delta + o(1).\end{aligned}$$

Thus, it remains only to show that those primes $p \le x$ with $p_R < G(p) \le (3\log x)^2$ contribute $o(1)$ to mean value. Clearly,

$$\frac{1}{\pi(x)} \sum_{\substack{p \le x \\ p_R < G(p) \le (3\log x)^2}} G(p) \le (3\log x)^2 \left(\frac{1}{\pi(x)} \sum_{\substack{p \le x \\ G(p) > p_R}} 1\right), \tag{3.4}$$

while by Theorem A and our estimate for δ_R above,

$$\begin{aligned}\left(\frac{1}{\pi(x)} \sum_{\substack{p \le x \\ G(p) > p_R}} 1\right) &= 1 - \delta_R + O((\log\log x)(4/\log x)^R) \\ &\ll \frac{1}{2^R} + \frac{1}{x^{1/10}} \ll \exp\left(-\frac{1}{20}\log x/\log\log x\right).\end{aligned}$$

We use here that $R > \frac{1}{9}\log x/\log\log x$ (say) for large x. Thus, the right-hand side of (3.4) is $o(1)$, completing the proof of (3.3). □

To approximate Δ, we use a method of Moree [**Mor00**] (generalizing earlier work of Wrench [**Wre61**]) to evaluate the constants δ_j. The only difficult part of this computation is obtaining an approximation to the products over ℓ appearing in (3.2). These products are tailor-made for application of [**Mor00**, Theorem 1]:

THEOREM B. *Let $A(T), B(T) \in \mathbf{Z}[T]$ be monic polynomials with $\deg A \le \deg B - 2$. Let β be the modulus of a root of $B(B-A)$ of maximum modulus, and let n_0 be such that $p_{n_0+1} > \beta$. Then for $n \ge n_0$,*

$$\prod_{p > p_n} \left(1 - \frac{A(p)}{B(p)}\right) = \prod_{j=2}^{\infty} \zeta_n(j)^{b_B(j) - b_{B-A}(j)}.$$

Here the function ζ_n is defined by $\zeta_n(s) := \zeta(s)\prod_{p\le p_n}(1-p^{-s})$; also, if $C(T)\in\mathbf{Z}[T]$ and $j\ge 1$, we set

$$b_C(j) := \frac{1}{j}\sum_{d|j}\mu(j/d)s_C(d),$$

where $s_C(d)$ is the sum of the dth powers of the roots of C (appearing with multiplicity).

In our case, $A(T)=1$ and $B(T)=T^r(T-1)$. By the triangle inequality, if $|x|\ge 2$, then $(B-A)(x)\ge 1$. Thus, every root of $B(B-A)$ has absolute value <2, and we may take $n=n_0=1$ in Theorem B to estimate the first factor in (3.2). We used MATHEMATICA to carry out the computations, employing the algorithm of [**Tro06**, p. 916] to find the values of s_{B-A}. This yields

$$\Delta = 3.974838470456310338399598989789506617230936562902 89\ldots.$$

REMARKS 3.2.

(i) Without any unproved hypothesis, one can at least show that

$$\limsup_{x\to\infty}\frac{1}{\pi(x)}\sum_{p\le x}G(p)\ge\Delta. \tag{3.5}$$

To see this, first observe that rearranging the series expression in (3.3) gives

$$\Delta = 2+\sum_{r=1}^{\infty}(p_{r+1}-p_r)(1-\delta_r). \tag{3.6}$$

For each nonnegative integer r, define $\delta_r'(x)$ as the proportion of $p\le x$ with $G(p)\le p_r$, where we view $p_0=1$. Fixing R, one has that as $x\to\infty$,

$$\begin{aligned}\frac{1}{\pi(x)}\sum_{p\le x}G(p) &\ge \sum_{1\le r\le R}p_r(\delta_r'(x)-\delta_{r-1}'(x))+p_{R+1}(1-\delta_R'(x))\\ &\ge 2+o(1)+\sum_{1\le r\le R}(p_{r+1}-p_r)(1-\delta_r'(x)). \qquad (3.7)\end{aligned}$$

Pappalardi has shown (see [**Pap97**, Theorem 3.1]) that $\limsup\delta_r'(x)\le\delta_r$; comparing (3.6) and (3.7), and finally letting $R\to\infty$, gives the claim (3.5).

(ii) Brown and Zassenhaus [**BZ71**] considered the function $\kappa(p)$, defined as the least k so that $p_1,\ldots,p_k$ generate the unit group modulo p. (Thus, $\kappa(p)=k$ precisely when $G(p)=p_k$.) A small modification of our arguments gives that under GRH, $\kappa(p)$ has mean value

$$2.206082894007974060365409598582527006356291182422 05\ldots.$$

As in remark (i), the lower bound implicit in this claim holds unconditonally.

4. Proof of Theorem 1.1

For each odd prime p, the number $n_2(p)$ is a prime $<p$. We need an analogue of this fact for $n_2'(p)$, defined as the least *odd* quadratic nonresidue modulo p.

LEMMA 4.1. *Suppose $p>3$ is prime. Then $n_2'(p)$ is prime and $n_2'(p)<p$.*

PROOF. That $n_2'(p)$ is prime is clear, so it is enough to show that $n_2'(p)<p$. If this inequality fails, then each of the $\frac{p-1}{2}$ odd numbers $<p$ is a quadratic residue modulo p. Since there are precisely $\frac{p-1}{2}$ nonzero squares modulo p, every even number $<p$ must be a quadratic nonresidue. But $2^2=4<p$ and 2^2 is a quadratic residue. □

LEMMA 4.2. *Suppose $p > 3$ is prime. Then there is an odd prime $q < p$ for which $\left(\frac{p}{q}\right) = -1$.*

PROOF. Suppose first that $p \equiv 1 \pmod 4$; then by quadratic reciprocity,

$$\left(\frac{p}{n_2'(p)}\right) = \left(\frac{n_2'(p)}{p}\right) = -1,$$

and so the result in this case follows from Lemma 4.1.

Now suppose that $p \equiv 3 \pmod 4$. Assume for the sake of contradiction that there is no such q. Then the Jacobi symbol $\left(\frac{p}{m}\right) = 1$ for all odd natural numbers $1 \le m < p$. Take $m = p - 2$; by quadratic reciprocity,

$$1 = \left(\frac{p}{m}\right) = \left(\frac{m}{p}\right) = \left(\frac{-2}{p}\right),$$

and so $p \equiv 3 \pmod 8$. Now take $m = \frac{p+3}{2}$. Then $m < p$ and $m \equiv 3 \pmod 4$, so that

$$1 = \left(\frac{p}{m}\right) = -\left(\frac{m}{p}\right) = -\left(\frac{4m}{p}\right) = -\left(\frac{6}{p}\right) = -\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right),$$

Hence, $\left(\frac{p}{3}\right) = -1$, which is a contradiction. □

REMARK 4.3. The case $p \equiv 1 \pmod 4$ of Lemma 4.2 was treated by Gauss *without* invoking the law of quadratic reciprocity; see [**Gau86**, Articles 125–129]. In fact, this case of the lemma was a key ingredient in the first proof of this law [**Gau86**, Articles 130–144]. For a modernized account, see (e.g.) Brown's exposition [**Bro81**].

If $\mathscr{P}$ is a set of primes, let $S(\mathscr{P})$ denote the set of natural numbers all of whose prime divisors belong to $\mathscr{P}$. The following somewhat technical lemma should be read as saying that whenever $\mathscr{P}$ is sufficiently sparse, so is $S(\mathscr{P})$. A lemma of this type (with a different proof) has also been obtained by Gottschlich [**Got11**].

LEMMA 4.4. *Let $\mathscr{P}$ be a nonempty set of primes. Suppose that for all $t \ge 3$, one has*

$$\#\mathscr{P} \cap [1,t] \le t/(\log t)^{A(t)}, \tag{4.1}$$

where the function $A(t)$ satisfies all of the following:

- *A is defined and real-valued for all $t \ge 3$,*
- *A is bounded on each compact subinterval of $[3,\infty)$,*
- *$A(t) > 4$ for all sufficiently large values of t,*
- *$A(t)\frac{\log\log t}{\log t}$ is eventually nonincreasing.*

Then for $x \ge 3$, the number of elements of $S(\mathscr{P})$ not exceeding x is

$$\ll_{\mathscr{P},A} x/(\log x)^{\frac{2}{3}A(x)}.$$

PROOF. We use a technique of Rankin familiar from the study of smooth numbers. For any choice of $\sigma \in [1/3, 1]$ (say), the number of elements of $S(\mathscr{P})$ not exceeding x is bounded by

$$\sum_{\substack{n\ge 1\\ p\mid n \Rightarrow p\in\mathscr{P}\cap[1,x]}} \left(\frac{x}{n}\right)^{\sigma} = x^{\sigma} \prod_{\substack{p\in\mathscr{P}\\ p\le x}} \left(1 + \frac{1}{p^{\sigma}} + \frac{1}{p^{2\sigma}} + \dots\right) \ll x^{\sigma} \exp\left(O\left(\sum_{\substack{p\in\mathscr{P}\\ p\le x}} \frac{1}{p^{\sigma}}\right)\right).$$

We choose

$$\sigma = 1 - \frac{2A(x)}{3}\frac{\log\log x}{\log x}.$$

Notice that if x is large (as we may assume), then $\sigma \in [1/3, 1]$; indeed, were we to have $\sigma < 1/3$, then $A(x) > \log x/\log\log x$, contradicting (4.1) with $t = x$. Now $x^\sigma = x/(\log x)^{2A(x)/3}$. Thus, it suffices to show that $\sum_{\substack{p\in\mathscr{P}\\ p\le x}} \frac{1}{p^\sigma} \ll_{\mathscr{P},A} 1$. We have

$$\sum_{\substack{p\in\mathscr{P}\\ p\le x}} \frac{1}{p^\sigma} \ll_{\mathscr{P},A} 1 + \int_3^x \frac{dt}{t^\sigma (\log t)^{A(t)}}$$

$$= 1 + \int_3^x \frac{\exp(\frac{2A(x)}{3}\frac{\log\log x}{\log x}\log t)}{t(\log t)^{A(t)}}\,dt \ll_A 1 + \int_3^x \frac{(\log t)^{\frac{2}{3}A(t)}}{t(\log t)^{A(t)}}\,dt \ll_A 1,$$

using in the last step that $A(t) > 4$ for large t. (Of course, we could replace 4 with any constant > 3 here.) □

We also need a variant of Lemma 2.2 for $n_2'(p)$:

LEMMA 4.5. *Suppose $2 \le y \le x$. The number of odd primes $p \le x$ for which $n_2'(p) > y$ is $\ll (\log x)\cdot x^{2\log\log(x^2)/\log y}$.*

PROOF. The number of p described in Lemma 4.5 is $\ll x^2/\Psi_2(x^2, y)$; this follows from the argument given in [**KP97**] for Lemma 2.1 (cf. [**Erd61**, Lemma 2]). (Summary: One observes that if $p > 3$ is as in the lemma statement, then the odd y-smooth numbers up to x occupy $< p/2$ residue classes modulo p; one then applies the arithmetic large sieve [**IK04**, Theorem 7.14, p. 180] as in the cited papers.) Now we use the Konyagin–Pomerance lower bound $\Psi(X, Y) > X^{1-\frac{\log\log X}{\log Y}}$ and the crude lower estimate $\Psi_2(X, Y) \gg \Psi(X, Y)/\log X$, the latter proved by decomposing each Y-smooth number as the product of an odd number and a power of 2. □

The next result is a well-known consequence of the Polya–Vinogradov inequality. As was the case for Lemma 2.3, much stronger bounds are known (see, e.g., [**Nor98**]), but these are not needed here. Recall from the introduction that n_χ denotes the least natural number n with $\chi(n) \notin \{0, 1\}$.

LEMMA 4.6. *For any nonprincipal character χ modulo m, we have $n_\chi \ll_\epsilon m^{\frac{1}{2}+\epsilon}$. Consequently, $n_2(m) \ll_\epsilon m^{\frac{1}{2}+\epsilon}$.*

Note that the second half of Lemma 4.6 follows from the first upon choosing for χ any quadratic character (at least one of which exists once $m \ge 3$).

PROOF OF THEOREM 1.1. Let $\ell(m)$ denote the least prime not dividing m, and observe that by the prime number theorem, we have $\ell(m) \le 2\log x$ uniformly for $m \le x$, once x is sufficiently large. We first treat those m with $\ell = \ell(m) > 3$. In this case, Lemma 4.2 shows that there is a prime $q < \ell$ for which $\left(\frac{\ell}{q}\right) = -1$. Then m is a multiple of q, since $q < \ell$. The congruence $x^2 \equiv \ell \pmod q$ is insoluble, and so a fortiori, ℓ is a quadratic nonresidue modulo m; thus, $n_2(m) = \ell(m)$. It follows that for large x,

$$\sum_{\substack{m\le x\\ \ell(m)>3}} n_2(m) = \sum_{2<k\le\pi(2\log x)} \sum_{\substack{m\le x\\ \ell(m)=p_k}} n_2(m) = \sum_{2<k\le\pi(2\log x)} p_k \sum_{\substack{m\le x\\ \ell(m)=p_k}} 1$$

$$= \sum_{2<k\le\pi(2\log x)} p_k \left((1-1/p_k)\frac{x}{p_1\cdots p_{k-1}} + O(1)\right),$$

which, after some crude estimation, is seen to be

$$x \sum_{k=3}^{\infty} \frac{p_k - 1}{p_1 \cdots p_{k-1}} + o(x), \tag{4.2}$$

as $x \to \infty$.

We now turn our attention to those m for which $\ell(m) = 2$ (i.e., odd values of m). If 2 is a quadratic residue modulo m, then $\left(\frac{2}{p}\right) = 1$ for each prime p dividing m; so by Brun's sieve [**HR74**, Theorem 2.2, p. 68], the number of such $m \le x$ is

$$\ll x \prod_{p \le x,\ \left(\frac{2}{p}\right) = -1} \left(1 - \frac{1}{p}\right) \ll x/(\log x)^{1/2}. \tag{4.3}$$

Thus,

$$\sum_{\substack{m \le x \\ \ell(m)=2}} n_2(m) = 2\left(\frac{1}{2}x + O(x/(\log x)^{1/2})\right) + \sum_{k>1} p_k \sum_{\substack{m \le x \\ \ell(m)=2,\ n_2(m)=p_k}} 1.$$

We claim that the double sum above contributes only $o(x)$. To prove this, we split it into three parts:

(i) those k with $2 < p_k \le (\log x)^{1/3}$,
(ii) those k with $(\log x)^{1/3} < p_k \le (\log x)^{100}$, and
(iii) those k with $p_k > (\log x)^{100}$.

By (4.3), the contribution from (i) to the double sum is bounded by

$$(\log x)^{1/3} \#\{\text{odd } m \le x : n_2(m) > 2\} \ll x/(\log x)^{1/6}.$$

Suppose that m is counted in (ii). Then m cannot be divisible by any prime $p \le (\log x)^{1/3}$. To see this, suppose otherwise, and let p denote the smallest such prime divisor. Then $n_2(p) < p \le (\log x)^{1/3}$ and $n_2(p)$ is a quadratic nonresidue modulo m, contradicting that $n_2(m) > (\log x)^{1/3}$. So m is composed entirely of primes $p > (\log x)^{1/3}$. Moreover, for each prime p dividing m, we have $n_2(p) > (\log x)^{1/3}$ (otherwise, $n_2(p)$ is a nonresidue mod m, by what was just shown). Let

$$\mathscr{P} := \{p : n_2(p) > (\log p)^{1/3}\}.$$

Then m is composed entirely of primes belonging to $\mathscr{P}$. We will show that such m are rare by showing that $\mathscr{P}$ is a sparse set of primes and then invoking Lemma 4.4.

First, we count the number of elements of $\mathscr{P}$ belonging to a dyadic interval $[T, 2T]$, where T is large. If $p \in \mathscr{P} \cap [T, 2T]$, then $n_2(p) > (\log T)^{1/3}$. By quadratic reciprocity, the latter inequality forces p into one of $\varphi(M) \cdot 2^{-\pi((\log T)^{1/3})}$ residue classes modulo $M := 4\prod_{q \le (\log T)^{1/3}} q$. But $M < T^{1/100}$, say, and so by the Brun–Titchmarsh inequality, the number of $p \in \mathscr{P} \cap [T, 2T]$ is

$$\ll \frac{1}{2^{\pi((\log T)^{1/3})}} \frac{T}{\log T} \ll T/\exp((\log T)^{1/4}).$$

Summing over dyadic intervals, it follows that

$$\#\mathscr{P} \cap [1, t] \ll t/\exp((\log t)^{1/5})$$

for all $t \ge 3$. So by Lemma 4.4, the number of $m \le x$ as above is

$$\ll x/\exp((\log x)^{1/6}),$$

say. Thus, the contribution from (ii) is

$$\ll (\log x)^{100}(x/\exp((\log x)^{1/6})) = o(x) \qquad (\text{as } x \to \infty).$$

Finally, we turn to (iii). By Lemma 4.6 (with $\epsilon = \frac{1}{20}$), these m contribute

$$\sum_{\substack{m\le x\\ \ell(m)=2,\ n_2(m)>(\log x)^{100}}} n_2(m) \ll x^{0.55} \sum_{\substack{m\le x\\ \ell(m)=2,\ n_2(m)>(\log x)^{100}}} 1.$$

Arguing as in (ii), we see that each m counted in the final sum is composed entirely of primes $p > (\log x)^{100}$, each of which satisfies $n_2(p) > (\log x)^{100}$. Let

$$\mathscr{P}' := \{p : n_2(p) > (\log p)^{100}\}.$$

By Lemma 2.2, the number of $p \in \mathscr{P}' \cap [T, 2T]$ is $\ll T^{1/49}$; we use here that $n_2(p) \le G(p)$. Summing dyadically, $\#\mathscr{P}' \cap [1, t] \ll t^{1/49}$ for all $t \ge 3$. Putting this into Lemma 4.4, we find that the number of $m \le x$ counted in (iii) is $\ll x^{2/5}$ (say). Thus, the contribution from (iii) is $\ll x^{0.55}x^{0.4} \ll x^{0.95} = o(x)$.

Collecting our estimates, we have proved that

$$\sum_{\substack{m\le x\\ \ell(m)=2}} n_2(m) = (1 + o(1))x, \tag{4.4}$$

as $x \to \infty$.

It remains to treat those m with $\ell(m) = 3$, i.e., those $m \equiv 2, 4 \pmod 6$. The steps are similar to what we have just seen, and so we only sketch them. By another application of Brun's sieve, the number of such $m \le x$ for which 3 is a quadratic residue is $\ll x/(\log x)^{1/2}$. Thus,

$$\sum_{\substack{m\le x\\ \ell(m)=3}} n_2(m) = 3\left(\frac{1}{3}x + O(x/(\log x)^{1/2})\right) + \sum_{k>2} p_k \sum_{\substack{m\le x\\ \ell(m)=3,\ n_2(m)=p_k}} 1.$$

We split the double sum into the same three pieces as above, but with the condition "$2 < p_k$" in (1) replaced by "$3 < p_k$". The contribution from (i) is treated as before. To treat (ii), we first show that an m counted there has no odd prime factors $\le (\log x)^{1/3}$; if it did, and p was the least such prime divisor, then by Lemma 4.1, $n_2'(p)$ would be a quadratic nonresidue of m smaller than $(\log x)^{1/3}$ and so smaller than $n_2(m)$. Moreover, any odd prime p dividing m must satisfy $n_2'(p) > (\log x)^{1/3}$; thus, m is supported on

$$\{2\} \cup \{p : n_2'(p) > (\log p)^{1/3}\}.$$

Using quadratic reciprocity, Brun–Titchmarsh, and finally Lemma 4.4 as before, we find the contribution from (ii) is once again $o(x)$. For (iii), we argue again using Lemma 4.1 that any m appearing there has all its prime divisors from the set

$$\{2\} \cup \{p : n_2'(p) > (\log p)^{100}\}.$$

In place of Lemma 2.2, we use Lemma 4.5 to show that this is a thin of set of primes, and then Lemma 4.4 to show that there are few corresponding m. (The number of such m turns out to again be $\ll x^{2/5}$.) Carrying out the details and collecting the estimates, one obtains that

$$\sum_{\substack{m\le x\\ \ell(m)=3}} n_2(m) = x + o(x). \tag{4.5}$$

Putting together (4.2), (4.4), and (4.5), we have shown that

$$\frac{1}{x}\sum_{m\le x} n_2(m) = 2 + \sum_{k=3}^{\infty} \frac{p_k - 1}{p_1 \cdots p_{k-1}} + o(1)$$
$$= \sum_{k=1}^{\infty} \frac{p_k - 1}{p_1 \cdots p_{k-1}} + o(1),$$

as $x \to \infty$. This completes the proof. □

5. Proof of Theorems 1.5 and 1.6

Since the proofs of Theorems 1.5 and 1.6 are quite similar to Erdős's proof of (1.1), as well as our own proofs of Theorems 1.1 and 1.4, we only sketch them.

5.1. Preliminaries. We need some preparation; the following lemma is due to Cohen and Robinson [**CR63**, Theorem 1] and (independently) Schwarz [**Sch62**, Lemma 8].

LEMMA 5.1. *Let a and d be integers with $d \ge 1$, and let $x \ge 1$. The number of squarefree $n \le x$ satisfying $n \equiv a \pmod d$ is*

$$\left(\frac{1}{\zeta(2)} \frac{1}{d\prod_{p\mid d}(1-p^{-2})} \prod_{\substack{p\mid \gcd(a,d)\\ \gcd(p^2,d)\mid a}} \left(1 - \frac{\gcd(p^2,d)}{p^2}\right) \right) x + O(x^{1/2}).$$

The estimate is uniform in all of a, d, and x.

The next lemma has the feel of a classical result, but it does not seem easy to pinpoint its origins. It appears implicitly in work of Erdős, Luca, and Pomerance [**ELP08**, proof of Theorem 4] and explicitly as [**Pol11**, Lemma 4.2].

LEMMA 5.2. *Suppose $x \ge 3$. Let $q \le x$ be a natural number. The number of $n \le x$ all of whose prime factors divide q is at most $\exp(O(\log x/\log\log x))$, uniformly in q.*

The next lemma, due to Duke and Kowalski [**DK00**, eq. (1)], plays the role of Lemmas 2.1 and 2.2. The proof uses the ideas of Linnik (op. cit.) and the large sieve for character sums.

LEMMA 5.3. *Fix $A > 2$. The number of primitive characters χ of conductor not exceeding x for which $n_\chi > (\log x)^A$ is at most $x^{\frac{2}{A}+o(1)}$, as $x \to \infty$.*

REMARK 5.4. Making small changes to the proof of a theorem of Baier [**Bai06**], we could obtain Lemma 5.3 with $2/A$ replaced by $1/(A-1)$. However, we shall not need this improvement.

PROOF. Since the lemma is stated but not proved in [**DK00**], we include the proof here. For $Q \ge 1$, let $\mathscr{X}(Q)$ denote the set of primitive characters of conductor not exceeding Q. Let $N \ge 1$, and suppose that $\{a_n\}$ is any sequence of complex numbers supported on $n \le N$. By the multiplicative large sieve [**IK04**, Theorem 7.13, p. 179],

$$\sum_{\chi\in\mathscr{X}(Q)} \left|\sum_{n\le N} a_n\chi(n)\right|^2 \ll (N+Q^2)\sum_{n\le N}|a_n|^2. \tag{5.1}$$

We take $N = x^2$ and $Q = x$, and we let a_n be the indicator function of the y-smooth numbers, with $y := (\log x)^A$. If $n_\chi > y$, then χ assumes only the values 0 and 1 on the

y-smooth integers. Thus, using $*$ to denote a sum over primitive characters χ modulo q, (5.1) gives

$$\sum_{q\le x}\sideset{}{^*}\sum_{\chi:\ n_\chi>y}\Psi_q(x^2,y)^2 \ll x^2\cdot\Psi(x^2,y). \tag{5.2}$$

Each y-smooth number can be written as the product of a y-smooth number coprime to q and a number supported on the primes dividing q. By Lemma 5.2,

$$\#\{m\le x^2 : p\mid m\Rightarrow p\mid q\} = x^{o(1)},$$

uniformly for $q\le x$. Thus, $\Psi_q(x^2,y)\ge x^{o(1)}\Psi(x^2,y)$. It now follows from (5.2) that as $x\to\infty$,

$$\sum_{q\le x}\sideset{}{^*}\sum_{\chi:\ n_\chi>y} 1 \le x^{2+o(1)}/\Psi(x^2,y) \le x^{2\frac{\log\log(x^2)}{\log y}+o(1)} = x^{2/A+o(1)},$$

as claimed. □

5.2. The least inert prime (Proof of Theorem 1.5). It is well-known and easy to prove (cf. [**CDyDO06**, §2]) that the denominator in (1.3) is $\sim x/\zeta(2)$, as $x\to\infty$, so we may concentrate on estimating the numerator. We claim that uniformly for k satisfying $p_k\le(\log x)^{1/3}$,

$$\#\{D : |D|\le x, n(D)=p_k\} = \left(\frac{1}{\zeta(2)}\frac{p_k}{2(p_k+1)}\prod_{i=1}^{k-1}\frac{p_i+2}{2(p_i+1)}\right)x + O(x^{2/3}). \tag{5.3}$$

The proof of (5.3) is straightforward but somewhat tedious and so we only give the main ideas. Suppose $k>1$, as the case when $k=1$ can be checked directly. We partition the values of D counted in the left-hand side of (5.3) according to the sign of D and the residue class of D modulo 8. In this sketch, we only treat the case when $D>0$ and $D\equiv 1 \pmod 8$. If $n(D)=p_k$ for such a D, then $\chi_D(p_i)=1$ or 0 for all indices $1<i<k$; let $\mathscr{A}$ consist of those indices i of the first type and $\mathscr{B}$ consist of those of the second. For fixed $\mathscr{A}$ and $\mathscr{B}$, the condition that $n(D)=p_k$ places D into one of

$$\frac{p_k-1}{2}\prod_{i\in\mathscr{A}}\frac{p_i-1}{2} \tag{5.4}$$

residue classes modulo $4p_1\cdots p_k$; now Lemma 5.1 shows that up to an error term (to be discussed later), the number of such $D\le x$ is

$$\begin{aligned}\left(\frac{1}{\zeta(2)}\frac{1}{4p_1\cdots p_k\prod_{1\le i\le k}(1-p_i^{-2})}\prod_{i\in\mathscr{B}}\left(1-\frac{1}{p_i}\right)\right)\left(\frac{p_k-1}{2}\prod_{i\in\mathscr{A}}\frac{p_i-1}{2}\right)x \\ = \frac{x}{\zeta(2)}\left(\prod_{i=2}^{k}\frac{p_i-1}{2}\right)\frac{1}{4p_1\cdots p_k\prod_{1\le i\le k}(1-p_i^{-2})}\prod_{i\in\mathscr{B}}\frac{2}{p_i} \\ = \frac{x}{2\zeta(2)}\left(\prod_{i=1}^{k}\frac{p_i}{2(p_i+1)}\right)\left(\prod_{i\in\mathscr{B}}\frac{2}{p_i}\right),\end{aligned}$$

where in moving from the first line to the second we have used that the set $\{2,\dots,k-1\}$ is the disjoint union of $\mathscr{A}$ and $\mathscr{B}$. Now sum over subsets $\mathscr{B}$ of $\{2,\dots,k-1\}$, noting that

$$\sum_{\mathscr{B}\subset\{2,\dots,k-1\}}\prod_{i\in\mathscr{B}}\frac{2}{p_i} = \prod_{1<i<k}\left(1+\frac{2}{p_i}\right).$$

After some simplification, we find that the number of D counted above is (up to error terms)

$$\frac{x}{4}\left(\frac{1}{\zeta(2)}\frac{p_k}{2(p_k+1)}\prod_{i=1}^{k-1}\frac{p_i+2}{2(p_i+1)}\right),$$

which may be recognized as one-quarter of the main term on the right-hand side of (5.3). The error may be crudely estimated as

$$\ll x^{1/2}\cdot 2^{\pi((\log x)^{1/3})}\left(\prod_{p\le(\log x)^{1/3}} p\right)\ll x^{2/3}.$$

This completes the discussion of the contribution to (5.3) from positive $D\equiv 1 \pmod 8$; the other cases for D may be handled similarly.

Now split $\sum_{|D|\le x} n(D)$ into three parts, corresponding to

(i) $n(D)\le (\log x)^{1/3}$,
(ii) $(\log x)^{1/3} < n(D) \le (\log x)^{10}$,
(iii) $n(D) > (\log x)^{10}$.

The estimate (5.3) shows that (i) contributes $\Theta + o(1)$ to the average. For D in (ii), one has $\left(\frac{D}{p}\right)\in\{0,1\}$ for all $p\le(\log x)^{1/3}$. Thus, D avoids $\frac{p-1}{2}$ residue classes modulo p for every odd prime p in this range. By the Chinese remainder theorem, the number of such D with $|D|\le x$ is

$$\ll x\prod_{2<p\le(\log x)^{1/3}}\left(1-\frac{p-1}{2p}\right)\ll x/\exp((\log x)^{1/4}).$$

Hence, the contribution to the average from those D in (ii) is $o(1)$. Finally, we treat (iii). Note that $n(D)\ll_\epsilon |D|^{0.55}$ (say), by Lemma 4.6. So to show that the contribution from (iii) is $o(1)$, it is enough to show that the number of $D\in[-X,X]$ with $n(D)>(\log x)^{10}$ is $\ll x^{0.4}$ (say). But this follows from Lemma 5.3. This completes the proof of Theorem 1.5 apart from the estimation of Θ, which was carried out in MATHEMATICA.

5.3. The least split prime (Proof of Theorem 1.6). The proof in the split case follows precisely the same outline as that given for Theorem 1.5. However, to treat the range (iii) now requires analogues of Lemmas 4.6 and 5.3 with n_χ replaced by n'_χ, defined as the least prime p with $\chi(p)\notin\{0,-1\}$.

It is simple to obtain the desired analogue of Lemma 5.3: If $\chi(p)\in\{0,-1\}$ for all $p\le y$, where $y:=(\log x)^A$, then $\chi(n)=\lambda(n)$ (the Liouville λ-function) for all y-smooth numbers n coprime to the conductor q. Now letting a_n be the twist by $\lambda(n)$ of the characteristic function of the y-smooth numbers, the above proof of Lemma 5.3 goes through for n'_χ.

The situation for Lemma 4.6 is more complicated. When χ is the Legendre symbol modulo p, the bound $n'_\chi\ll_\epsilon p^{\frac14+\epsilon}$ was proved by Linnik and Vinogradov [**VL66**]; a more elementary proof was later given by Pintz [**Pin77**]. This result is not general enough for our purposes; however, a small modification of Pintz's proof (using the form of the Burgess bound appearing as [**IK04**, eq. (12.56), p. 326]) would show the analogous bound for every real primitive χ. For completeness' sake, we prove the following weaker (but slightly more general) result, sufficient to complete the proof of Theorem 1.6:

LEMMA 5.5. *Let $\epsilon>0$, and let χ be a quadratic character modulo q. Then $n'_\chi\ll_\epsilon q^{\frac12+\epsilon}$.*

PROOF. We largely follow Pintz (ibid.). We can assume that q is sufficiently large (larger than an absolute constant) and that $\epsilon < \frac{1}{2}$. Let us suppose for the sake of contradiction that $n'_\chi > y$, where $y := q^{\frac{1}{2}+\epsilon}$.

For each natural number n, put $R(n) := \sum_{d|n} \chi(d)$. Take a y-smooth integer n, and write $n = AB$, where A is supported on primes dividing q and $\gcd(B, q) = 1$. Then we have

$$R(n) = \prod_{p^e \| n} (1 + \chi(p) + \cdots + \chi(p^e)) = \begin{cases} 1 & \text{if } B \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases}$$

Hence,

$$\sum_{n \le y} R(n) \le \left(\sum_{\substack{B \le y \\ B \text{ is a square}}} 1 \right) \left(\sum_{A \le y:\ p|A \Rightarrow p|q} 1 \right) \le y^{1/2} \exp(O(\log q / \log\log q)), \tag{5.5}$$

using Lemma 5.2 (with $x = q$) to estimate the sum on A. On the other hand,

$$\sum_{n \le y} R(n) = \sum_{d \le y} \chi(d) \left\lfloor \frac{y}{d} \right\rfloor = y \sum_{d \le y} \frac{\chi(d)}{d} - \sum_{d \le y} \chi(d) \left\{ \frac{y}{d} \right\}.$$

By Polya–Vinogradov and partial summation,

$$\begin{aligned} \sum_{d \le y} \frac{\chi(d)}{d} &= L(1, \chi) - \sum_{d > y} \frac{\chi(d)}{d} \\ &= L(1, \chi) + O(y^{-1} \sqrt{q} \log q). \end{aligned}$$

Moreover, for any choice of $z \le y$,

$$\begin{aligned} \left| \sum_{d \le y} \chi(d) \left\{ \frac{y}{d} \right\} \right| &\le \left| \sum_{d \le z} \chi(d) \left\{ \frac{y}{d} \right\} \right| + \sum_{m \le y/z} \left| \sum_{\substack{\lfloor y/d \rfloor = m \\ d > z}} \chi(d) \left\{ \frac{y}{d} \right\} \right| \\ &\ll z + (y/z) \sqrt{q} \log q, \end{aligned}$$

where we use Abel's inequality to estimate the second right-hand sum. Choosing $z = y^{1/2} q^{1/4} \sqrt{\log q}$ to optimize this upper bound, and collecting our estimates, we find that

$$\sum_{n \le y} R(n) = y L(1, \chi) + O(\sqrt{q} \log q) + O(y^{1/2} q^{1/4} \sqrt{\log q}).$$

Comparing this with (5.5) and recalling the definition of y, we obtain

$$L(1, \chi) \ll y^{-1/2} \exp(O(\log q / \log\log q)) + O(\sqrt{q} y^{-1} \log q) + O(q^{1/4} y^{-1/2} \sqrt{\log q}) \ll q^{-\epsilon/3}.$$

But for large q, this contradicts Siegel's lower bound on $L(1, \chi)$ [**MV07**, Theorem 11.14, p. 372]. □

REMARK 5.6. In contrast with Theorems 1.5 and 1.6, it is simple to compute asymptotics for the average least ramified prime in $\mathbf{Q}(\sqrt{D})$: Taken over fundamental discriminants with $|D| \le x$, the average is asymptotic to $\frac{\zeta(2)}{2} \frac{x}{\log x}$, as $x \to \infty$. Cf. Kalecki's estimation [**Kal64**, Theorem 3] of the average least prime factor of n, as n ranges over the natural numbers.

Acknowledgements

The author thanks Greg Martin for his guidance and encouragement. He also thanks Carl Pomerance for numerous helpful comments, and in particular for suggesting simplifications incorporated in the proof of Lemma 4.2. Finally, he would like to express his gratitude to Avram Gottschlich for sharing his preprint [**Got11**].

References

[Bai06] S. Baier, *On the least n with $\chi(n) \neq 1$*, Q. J. Math. **57** (2006), no. 3, 279–283.

[BE68] D. A. Burgess and P. D. T. A. Elliott, *The average of the least primitive root*, Mathematika **15** (1968), 39–50.

[Bro81] E. Brown, *The first proof of the quadratic reciprocity law, revisited*, Amer. Math. Monthly **88** (1981), no. 4, 257–264.

[Bur57] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika **4** (1957), 106–112.

[Bur97a] R. J. Burthe, Jr., *The average least witness is* 2, Acta Arith. **80** (1997), no. 4, 327–341.

[Bur97b] ———, *Upper bounds for least witnesses and generating sets*, Acta Arith. **80** (1997), no. 4, 311–326.

[BZ71] H. Brown and H. Zassenhaus, *Some empirical observations on primitive roots*, J. Number Theory **3** (1971), 306–309.

[CDyDO06] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Counting discriminants of number fields*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 573–593.

[CR63] E. Cohen and R. L. Robinson, *On the distribution of the k-free integers in residue classes*, Acta Arith. **8** (1962/1963), 283–293.

[DK00] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, Invent. Math. **139** (2000), no. 1, 1–39.

[Ell68] P. D. T. A. Elliott, *Some notes on k-th power residues*, Acta Arith. **14** (1967/1968), 153–162.

[Ell70] ———, *On the mean value of $f(p)$*, Proc. London Math. Soc. (3) **21** (1970), 28–96.

[ELP08] P. Erdős, F. Luca, and C. Pomerance, *On the proportion of numbers coprime to a given integer*, Anatomy of integers, CRM Proc. Lecture Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008, pp. 47–64.

[EM97] P. D. T. A. Elliott and L. Murata, *On the average of the least primitive root modulo p*, J. London Math. Soc. (2) **56** (1997), no. 3, 435–454.

[Erd61] P. Erdős, *Remarks on number theory. I*, Mat. Lapok **12** (1961), 10–17 (Hungarian).

[Gau86] C. F. Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986.

[Got11] A. Gottschlich, *On positive integers n dividing the nth term of an elliptic divisibility sequence*, preprint, 2011.

[Hoo67] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[HR74] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, no. 4, Academic Press, London-New York, 1974.

[IK04] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

[Kal64] M. Kalecki, *On certain sums extended over primes or prime factors*, Prace Mat. **8** (1963/1964), 121–129 (Polish).

[KP97] S. Konyagin and C. Pomerance, *On primes recognizable in deterministic polynomial time*, The mathematics of Paul Erdős, I, Algorithms Combin., vol. 13, Springer, Berlin, 1997, pp. 176–198.

[Lin42] U. V. Linnik, *A remark on the least quadratic non-residue*, C. R. (Doklady) Acad. Sci. URSS (N.S.) **36** (1942), 119–120 (Russian).

[Mor00] P. Moree, *Approximation of singular series and automata*, Manuscripta Math. **101** (2000), no. 3, 385–399.

[MV07] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[Nor98] K. K. Norton, *A character-sum estimate and applications*, Acta Arith. **85** (1998), no. 1, 51–78.

[Pap95] F. Pappalardi, *On minimal sets of generators for primitive roots*, Canad. Math. Bull. **38** (1995), no. 4, 465–468.

[Pap97] ———, *On the r-rank Artin conjecture*, Math. Comp. **66** (1997), no. 218, 853–868.

[Pin77] J. Pintz, *Elementary methods in the theory of L-functions. VI. On the least prime quadratic residue* (mod p), Acta Arith. **32** (1977), no. 2, 173–178.

[Pol11] P. Pollack, *On the greatest common divisor of a number and its sum of divisors*, Michigan Math. J. **60** (2011), no. 1, 199–214.

[Sch62] W. Schwarz, *Über die Summe* $\sum_{n\leq x} \varphi(f(n))$ *und verwandte Probleme*, Monatsh. Math. **66** (1962), 43–54.

[Tro06] M. Trott, *The Mathematica guidebook for symbolics*, Springer, New York, 2006.

[VL66] A. I. Vinogradov and U. V. Linnik, *Hypoelliptic curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR **168** (1966), 259–261 (Russian).

[Wre61] J. W. Wrench, Jr., *Evaluation of Artin's constant and the twin-prime constant*, Math. Comp. **15** (1961), 396–398.

University of British Columbia, Department of Mathematics, Room 121, 1984 Mathematics Road, Vancouver, BC Canada V6T 1Z2

Simon Fraser University, Mathematics Department, Burnaby, BC Canada V5A 1S6
E-mail address: pollack@math.ubc.ca
URL: http://www.math.ubc.ca/~pollack/