On pseudosquares and pseudopowers

Carl Pomerance
Department of Mathematics
Dartmouth College
Hanover, NH 03755-3551, USA
carl.pomerance@dartmouth.edu

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Abstract

Introduced by Kraitchik and Lehmer, an x-pseudosquare is a positive integer $n \equiv 1 \pmod 8$ that is a quadratic residue for each odd prime $p \le x$, yet is not a square. We give a subexponential upper bound for the least x-pseudosquare that improves on a bound that is exponential in x due to Schinzel. We also obtain an equi-distribution result for pseudosquares. An x-pseudopower to base g is a positive integer which is not a power of g yet is so modulo p for all primes $p \le x$. It is conjectured by Bach, Lukes, Shallit, and Williams that the least such number is at most $\exp(a_g x/\log x)$ for a suitable constant a_g. A bound of $\exp(a_g x \log\log x/\log x)$ is proved conditionally on the Riemann Hypothesis for Dedekind zeta functions, thus improving on a recent conditional exponential bound of Konyagin and the present authors. We also give a GRH-conditional equidistribution result for pseudopowers that is analogous to our unconditional result for pseudosquares.

1 Introduction

1.1 Pseudosquares

An x-pseudosquare is a nonsquare positive integer n such that $n \equiv 1 \pmod 8$ and $(n/p) = 1$ for each odd prime $p \leq x$. The subject of pseudosquares was initiated by Kraitchik and more formally by Lehmer in [12]. It was later shown by Weinberger (see [17]) that if the Generalized Riemann Hypothesis (GRH) holds, then the least x-pseudosquare, call it N_x, satisfies $N_x \geq \exp(cx^{1/2})$ for a positive constant c. The interest in this inequality is that there is a primality test, due to Selfridge and Weinberger, for integers $n < N_x$ that requires the verification of some simple Fermat-type congruences for prime bases $p \leq x$. Thus, a large lower bound for N_x leads to a fast primality test, and in particular this result gives an alternate and somewhat simpler form of Miller's GRH-conditional polynomial-time deterministic primality test. See [17] for details.

By the GRH, we mean the Riemann Hypothesis for Dedekind zeta functions, that is, for algebraic number fields. Note that this conjecture subsumes the Extended Riemann Hypothesis (ERH), which is the Riemann Hypothesis for rational Dirichlet L-functions. The Weinberger lower bound for N_x in fact only requires the ERH.

As the concept of an x-pseudosquare is a natural one, it is also of interest to find a reasonable upper bound for N_x and also to study the distribution of x-pseudosquares. Let $M(x)$ denote the product of the primes up to x. For integers n coprime to $M(x)$, the "probability" that n satisfy $n \equiv 1 \pmod 8$ and $(n/p) = 1$ for all odd primes $p \leq x$ is $2^{-\pi(x)-1}$. Since the squares are themselves so sparsely distributed one might conjecture that if $y > 2^{(2+\varepsilon)\pi(x)}$, then in an interval of length y there should be $y/2^{(1+o(1)\pi(x)}$ x-pseudosquares. In particular, it is natural to conjecture that

$$N_x \leq 4^{(1+o(1))\pi(x)}.$$

In [16], Schinzel proves this heuristically best-possible inequality conditionally on the GRH. Unconditionally, he uses the Burgess bound [4] (see also [9, Theorem 12.6]) to show that

$$N_x \leq \exp((1/4 + o(1))x). \tag{1}$$

Here we follow Schinzel's method, but use a character sum estimate given in [9, Corollary 12.14] which dates back to work of Graham and Ringrose [5], to prove the following result. Let $\mathcal{S}_x$ be the set of x-pseudosquares.

Theorem 1. *For any interval* $(A, A+N] \subseteq (0,\infty)$*, uniformly over* $N \geq \exp(3x/\log\log x)$*, we have*

$$\#\left(\mathcal{S}_x \cap (A, A+N]\right) = (1+o(1))\frac{N}{M(x)}\#\left(\mathcal{S}_x \cap (0, M(x)]\right), \qquad x \to \infty.$$

We also show

$$\#\left(\mathcal{S}_x \cap (0, M(x)]\right) = (1+o(1))\frac{M(x)}{2^{\pi(x)+1}e^{\gamma}\log x}, \qquad x \to \infty, \tag{2}$$

so that one can rewrite Theorem 1 in a more explicit form.

In particular, we improve (1) and obtain a sub-exponential upper bound on N_x.

Corollary 2. *For large* x*,*

$$N_x \leq \exp(3x/\log\log x).$$

1.2 Pseudopowers

Let g be a fixed integer with $|g| \geq 2$. Following Bach, Lukes, Shallit, and Williams [1], we say that an integer $n > 0$ is an *x-pseudopower to base g* if n is not a power of g over the integers but is a power of g modulo all primes $p \leq x$. Denote by $q_g(x)$ the least x-pseudopower to base g.

In [1] it is conjectured that for each fixed g, there is a number a_g such that for $x \geq 2$,

$$q_g(x) \leq \exp(a_g x/\log x). \tag{3}$$

In addition, a heuristic argument is given for (3), with numerical evidence presented in the case of $g = 2$. For any g, we have (see [10]) the trivial bound $q_g(x) \leq 2M(x)+1$, where $M(x)$ is the product of the primes $p \leq x$. Thus,

$$q_g(x) \leq \exp((1+o(1))x).$$

Using an estimate for exponential sums due to Heath-Brown and Konyagin [7] and results of Baker and Harman [2, 3] on the Brun–Titchmarsh theorem on average, Konyagin, Pomerance, and Shparlinski [10] proved that

$$q_g(x) \leq \exp(0.88715x)$$

for all sufficiently large x and all integers g with $2 \le |g| \le x$. Further, it was noted in [10] that the method implied that for fixed g,

$$q_g(x) \le \exp((1/2 + o(1))x),$$

assuming the GRH. In this paper we make further progress towards (3), again assuming the GRH. Our proof makes use of the approach in Schinzel [16] for pseudosquares.

Theorem 3. *Assume the GRH. Then for each fixed integer g with $|g| \ge 2$ there is a number a_g such that for $x \ge 3$,*

$$q_g(x) \le \exp(a_g x \log\log x/\log x).$$

We are also able to prove an equidistribution result conditional on the GRH that is similar in strength to Theorem 1. Let $\mathcal{P}_x$ be the set of x-pseudopowers base g.

Theorem 4. *Assume the GRH. Let g be a fixed integer with $|g| > 1$. There is a positive number b_g such that for any interval $(A, A+N] \subseteq (0,\infty)$, uniformly over $N \ge \exp(b_g x/\log\log x)$, we have*

$$\#\left(\mathcal{P}_x \cap (A, A+N]\right) = (1+o(1))\frac{N}{M(x)}\#\left(\mathcal{P}_x \cap (0, M(x)]\right), \qquad x \to \infty.$$

We derive an asymptotic formula for $\#\left(\mathcal{P}_x \cap (0, M(x)]\right)$ in Section 3.2, see (21), so that one can get a more explicit form of Theorem 4.

We note that in [10] an unconditional version of Theorem 4 is given which however holds only for $N \ge \exp(0.88715x)$. Under the GRH, the method of [10] gives a somewhat stronger result but still requires N to be rather large, namely it applies only to $N \ge \exp\left((0.5+\varepsilon)x\right)$ for an arbitrary $\varepsilon > 0$.

As for lower bounds for $q_g(x)$, it follows from Schinzel [14, 15] that

$$q_g(x) \to \infty, \qquad x \to \infty.$$

In [1] it is shown that assuming the GRH there is a number $c_g > 0$ such that

$$q_g(x) \ge \exp(c_g\sqrt{x}(\log\log x)^3/(\log x)^2).$$

1.3 Notation

We recall that the notation $U = O(V)$ and $U \ll V$ are equivalent to the assertion that the inequality $|U| \le cV$ holds for some constant $c > 0$.

2 Distribution of pseudosquares

In this section we prove Theorem 1 by making use of the following character sum estimate, which is [9, Corollary 12.14].

Lemma 5. *Let χ be a primitive character to the squarefree modulus $q > 1$. Suppose all prime factors of q are at most $N^{1/9}$ and let r be an integer with $N^r \geq q^3$. Then for any number A,*

$$\left| \sum_{A < n \leq A+N} \chi(n) \right| \leq 4N\tau(q)^{r/2^r} q^{-1/r2^r},$$

where $\tau(q)$ is the number of positive divisors of q.

Recall that $M(x)$ is the product of the primes in $[1, x]$. Let x be a large number and let $\overline{\mathcal{S}}_x$ denote the set of positive integers $n \equiv 1 \pmod 8$ with $(n/p) = 1$ for each odd prime $p \leq x$. That is, $\overline{\mathcal{S}}_x$ consists of the x-pseudosquares and actual squares coprime to $M(x)$. In particular, $\mathcal{S}_x \subseteq \overline{\mathcal{S}}_x$. We let $M_2(x) = M(x)/2$, the product of the odd primes up to x.

Theorem 1 is routine once N is large compared with $M(x)$, so we assume that $N \leq M(x)^2$. Note that for a positive integer n with $(8n+1, M_2(x)) = 1$, we have that

$$\prod_{p | M_2(x)} \left(1 + \left(\frac{8n+1}{p}\right)\right) = \begin{cases} 2^{\pi(x)-1}, & \text{if } 8n+1 \in \overline{\mathcal{S}}_x; \\ 0, & \text{else.} \end{cases} \tag{4}$$

Thus, if A, N are positive numbers, then the sum

$$S_{A,N} := \sum_{\substack{A < 8n+1 \leq A+N \\ (8n+1, M_2(x))=1}} \prod_{p | M_2(x)} \left(1 + \left(\frac{8n+1}{p}\right)\right)$$

satisfies

$$S_{A,N} = 2^{\pi(x)-1} \#(\overline{\mathcal{S}}_x \cap (A, A+N]). \tag{5}$$

The product in (4) can be expanded, so that we have

$$\begin{aligned} S_{A,N} &= \sum_{\substack{A < 8n+1 \leq A+N \\ (8n+1, M_2(x))=1}} \sum_{f | M_2(x)} \left(\frac{8n+1}{f}\right) \\ &= \sum_{f | M_2(x)} \sum_{\substack{A < 8n+1 \leq A+N \\ (8n+1, M_2(x))=1}} \left(\frac{8n+1}{f}\right). \end{aligned} \tag{6}$$

The contribution to $S_{A,N}$ from $f = 1$ is

$$\sum_{\substack{A<8n+1\le A+N\\(8n+1,M_2(x))=1}} 1 \sim \frac{N}{4e^\gamma \log x} \tag{7}$$

uniformly for A, N with $N \ge \exp(x^{1/2})$. This estimate follows immediately from the fundamental lemma of the sieve; for example, see [6, Theorem 2.5].

Suppose now that $f \mid M_2(x)$, $f > 1$ is fixed. We can rewrite the contribution in (6) corresponding to f as

$$R_f = \sum_{d \mid M_2(x)/f} \mu(d) \sum_{\substack{A<8n+1\le A+N\\ d\mid 8n+1}} \left(\frac{8n+1}{f}\right), \tag{8}$$

where $\mu(d)$ is the Möbius function.

The Pólya–Vinogradov inequality (see [9, Theorem 12.5]) immediately implies that

$$|R_f| \le 3 \cdot 2^{\pi(x)-2}\sqrt{f}\log f < 2^{\pi(x)}\sqrt{f}\log f \tag{9}$$

for any choice of $f > 1$. We use (9) when f is not much larger than N, namely we use it when

$$f \le N^{r2^r/(r2^{r-1}+1)},$$

where r shall be chosen later. In this case it gives

$$|R_f| \le 2^{\pi(x)} N^{1-2/(r2^r+2)} \log(N^2) \le 2^{(1+o(1))\pi(x)} N^{1-2/(r2^r+2)}. \tag{10}$$

For large values of f, that is, when

$$f > N^{r2^r/(r2^{r-1}+1)}, \tag{11}$$

we use a different approach which relies on Lemma 5.

Let $r_f = (1-f^2)/8$, so that r_f is an integer and $8r_f \equiv 1 \pmod f$. Then

$$\begin{aligned} R_f &= \sum_{d\mid M_2(x)/f} \mu(d)\left(\frac{d}{f}\right) \sum_{\substack{A<dk\le A+N\\ k\equiv d \pmod 8}} \left(\frac{k}{f}\right)\\ &= \sum_{d\mid M_2(x)/f} \mu(d)\left(\frac{8d}{f}\right) \sum_{A<d(8l+d)\le A+N} \left(\frac{l+dr_f}{f}\right)\\ &= \sum_{d\mid M_2(x)/f} \mu(d)\left(\frac{8d}{f}\right) \sum_{m\in\mathcal{I}_{d,f}} \left(\frac{m}{f}\right), \end{aligned}$$

where $\mathcal{I}_{d,f} = [B_{d,f}+1, B_{d,f}+N_{d,f}]$, an interval of length

$$N_{d,f} = \frac{N}{8d} + O(1).$$

Thus,

$$|R_f| \le \sum_{d|M_2(x)/f} \left| \sum_{m\in\mathcal{I}_{d,f}} \left(\frac{m}{f}\right) \right|. \tag{12}$$

The character sums in (12) where $8d > N^{0.1}$ are trivially bounded by $N_{d,f} = O(N^{0.9})$ in absolute value, so their total contribution to R_f is

$$\sum_{\substack{d|M_2(x)/f \\ 8d>N^{0.1}}} \left| \sum_{m\in\mathcal{I}_{d,f}} \left(\frac{m}{f}\right) \right| \ll 2^{\pi(x)} N^{0.9}. \tag{13}$$

We now assume that $8d \le N^{0.1}$. Note that the conductors f of the characters which appear in (12) are squarefree. We choose r as the largest integer with

$$r2^r + 2 \le \frac{\log x}{\log\log x}$$

and apply Lemma 5 to the inner sum in (12) with this value of r. To do this we need

$$(N/(8d))^r \ge f^3 \qquad \text{and} \qquad x \le (N/(8d))^{1/9}.$$

These inequalities hold since

$$r = \left(\frac{1}{\log 2} + o(1)\right) \log\log x \qquad \text{and} \qquad N \ge \exp(3x/\log\log x), \tag{14}$$

so that

$$\left(\frac{N}{8d}\right)^r \ge N^{0.9r} \ge \exp(2.7rx/\log\log x) \ge M(x)^3 \ge f^3 \tag{15}$$

and

$$\left(\frac{N}{8d}\right)^{1/9} \ge N^{0.1} \ge \exp(0.3x/\log\log x) \ge x. \tag{16}$$

for all large x.

Thus, by Lemma 5,

$$\sum_{\substack{d|M_2(x)/f\\ 8d\le N^{0.1}}}\left|\sum_{m\in\mathcal{I}_{d,f}}\left(\frac{m}{f}\right)\right|\le 4\cdot 2^{\pi(x)-1}N2^{(\pi(x)-1)r/2^r}f^{-1/r2^r}. \tag{17}$$

We now derive from (13), (17), and (11) that

$$|R_f|\le 2^{(1+o(1))\pi(x)}N^{0.9}+2^{(1+o(1))\pi(x)}Nf^{-1/r2^r}\le 2^{(1+o(1))\pi(x)}N^{1-2/(r2^r+2)}$$

which is also the bound in (10) for those $f>1$ not satisfying (11).

Now summing on f we see that the contribution to $S_{A,N}$ from values of $f>1$ is at most

$$\begin{aligned}\sum_{\substack{f|M_2(x)\\ f>1}}|R_f|\le\ & 4^{(1+o(1))\pi(x)}N^{1-2/(r2^r+2)}\\ =\ & N^{1-2/(r2^r+2)}\exp((\log 4+o(1))x/\log x).\end{aligned}$$

Note that by our choice of r we have

$$N^{2/(r2^r+2)}\ge N^{2\log\log x/\log x}\ge\exp(6x/\log x).$$

Since $6>\log 4$, we have that the contribution to (6) from terms with $f>1$ is small compared to the main term given by (7), so that

$$S_{A,N}=(1+o(1))\frac{N}{4e^\gamma\log x}.$$

Together with (5), we now have

$$\#(\overline{\mathcal{S}}_x\cap(A,A+N])=(1+o(1))\frac{N}{2^{\pi(x)+1}e^\gamma\log x}.$$

Since the number of squares in the interval $(A,A+N]$ is at most $N^{1/2}$, we obtain

$$\#\left(\mathcal{S}_x\cap(A,A+N]\right)=(1+o(1))\frac{N}{2^{\pi(x)+1}e^\gamma\log x}.$$

Taking $A=0$ and $N=M(x)$ we derive (2) and conclude the proof of Theorem 1.

We remark that by being a little more careful with the estimates, we can prove the theorem with "3" replaced with any fixed number larger than $\log 8$.

3 Distribution of pseudopowers

3.1 Proof of Theorem 3

Let g be a given integer with $|g| \geq 2$ which we assume to be fixed. Let $p_g(x)$ be the least positive integer which is not a power of g yet is a power of g modulo every prime $p \leq x$ with $p \nmid g$. It is easy to see that

$$q_g(x) \leq g p_g(x). \tag{18}$$

Indeed, the integer $gp_g(x)$ is not a power of g, it is a power of g modulo every prime $p \leq x$ with $p \nmid g$, and it is zero modulo p for every prime $p \mid g$, and so is a power of g modulo these primes too.

For every prime $p \nmid g$ let $l_g(p)$ be the multiplicative order of g modulo p, and let $i_g(p) = (p-1)/l_g(p)$, the index of the subgroup of powers of g in the multiplicative group modulo p. Let

$$M_g(x) = \prod_{\substack{p \leq x \\ p \nmid g}} p, \quad I_g(x) = \prod_{p \mid M_g(x)} i_g(p).$$

It follows from [10, Theorem 1] that $I_g(x) \leq \exp(0.42x)$ for all sufficiently large x. We conditionally improve this result.

Lemma 6. *Assume the GRH. There is a number c_g such that for $x \geq 3$,*

$$I_g(x) \leq \exp(c_g x \log\log x / \log x)$$

Proof. In Kurlberg and Pomerance [11, Theorem 23], following ideas of Hooley [8] and Pappalardi [13], it is shown conditionally on the GRH that

$$\sum_{\substack{p \mid M_g(x) \\ l_g(p) \leq p/y}} 1 \ll_g \frac{\pi(x)}{y} + \frac{x \log\log x}{(\log x)^2}$$

for $1 \leq y \leq \log x$. Applying this result with $y = \log x$, we have

$$\sum_{\substack{p \mid M_g(x) \\ i_g(p) \geq \log x}} 1 \ll_g \frac{x \log\log x}{(\log x)^2}.$$

Indeed, $i_g(p) \geq y$ implies that $l_g(p) \leq (p-1)/y < p/y$. Since we trivially have $i_g(p) \leq x$ for each prime $p \mid M_g(x)$ with $p \nmid g$, we thus have

$$I_g(x) = \prod_{\substack{p|M_g(x) \\ i_g(p)<\log x}} i_g(p) \prod_{\substack{p|M_g(x) \\ i_g(p)\geq \log x}} i_g(p) \leq (\log x)^{\pi(x)} x^{O_g(x \log\log x/(\log x)^2)}.$$

The lemma follows. □

For each prime $p \nmid g$, let χ_p be a character modulo p of order $i_g(p)$. Then

$$\sum_{j=1}^{i_g(p)} \chi_p^j(n) = \begin{cases} i_g(p), & \text{if } n \text{ is a power of } g \text{ modulo } p, \\ 0, & \text{else.} \end{cases}$$

Thus,

$$\begin{aligned} &\prod_{p|M_g(x)} \sum_{j=1}^{i_g(p)} \chi_p^j(n) \\ &\qquad = \begin{cases} I_g(x), & \text{if } n \text{ is a power of } g \text{ modulo every } p \mid M_g(x), \\ 0, & \text{else.} \end{cases} \end{aligned} \tag{19}$$

Let $\Lambda(n)$ denote the von Mangoldt function. From the definition of $p_g(x)$ we deduce that

$$S_g := \sum_{n<p_g(x)} \Lambda(n) \prod_{p|M_g(x)} \sum_{j=1}^{i_g(p)} \chi_p^j(n) = I_g(x) \sum_{\substack{n<p_g(x) \\ n \text{ is a power of } g}} \Lambda(n).$$

The last sum is 0 if g is not a prime or prime power, and in any event is always at most $\log p_g(x) \ll x$. Thus,

$$S_g \ll I_g(x)x. \tag{20}$$

We now multiply out the product in (19); it is seen as a sum of $I_g(x)$ characters modulo $M_g(x)$. The contribution to S_g from the principal character $\prod_p \chi_p^{i_g(p)}$ is $\psi(p_g(x)) + O(x)$. We may assume that $p_g(x) \geq e^{\pi(x)}$ since otherwise the theorem follows immediately from (18), so that the contribution to S_g from the principal character is $(1+o(1))p_g(x)$, by the prime number theorem.

The contribution to S_g from each nonprincipal character χ is

$$\sum_{n<p_g(x)} \chi(n)\Lambda(n) \ll p_g(x)^{1/2}\left((\log M_g(x))^2 + (\log p_g(x))^2\right) \ll p_g(x)^{1/2}x^2$$

assuming the GRH. Hence, the contribution to S_g from nonprincipal characters is $O(I_g(x)p_g(x)^{1/2}x^2)$. Thus,

$$S_g = (1+o(1))p_g(x) + O(I_g(x)p_g(x)^{1/2}x^2),$$

so that from (20) we deduce that

$$p_g(x) \ll I_g(x)^2x^4.$$

Theorem 3 now follows immediately from (18) and Lemma 6.

We remark that an alternate way to handle primes dividing g is to eschew (18) and instead multiply the product in (19) by $\sum_{\chi \bmod g}\chi(n)$. This sum is $\varphi(g)$ when $n \equiv 1 \pmod g$ and is 0 otherwise. Note that a number that is 1 mod p is always a power of g modulo p. Although this is somewhat more complicated, it does lead to a proof that there is a *prime* number below the bound $\exp(a_g x \log\log x/\log x)$ that is an x-pseudopower base g.

3.2 Proof of Theorem 4

We use the method of proof of Theorem 1. Accordingly we only outline some new elements and suppress the details.

For a nonzero integer n, let $\mathrm{rad}(n)$, the *radical* of n, be the largest squarefree divisor of n. That is, $\mathrm{rad}(n)$ is the product of the distinct prime factors of n. Also, let $\omega(n)$ denote the number of distinct prime factors of n. Let $\overline{\mathcal{P}}_x$ denote the set of positive integers which are either an x-pseudopower base g or a true power of g. Then a positive integer $n \in \overline{\mathcal{P}}_x$ if and only if both

(i) n is in the subgroup $\langle g\rangle$ of $(\mathbb{Z}/p\mathbb{Z})^*$ when $p \le x$ and $p \nmid g$;

(ii) $n \equiv 0$ or $1 \pmod p$ when $p \le x$ and $p \mid g$.

Assuming then that $x \ge |g|$, the cardinality of $\overline{\mathcal{P}}_x \cap (0, M(x)]$ is

$$2^{\omega(g)}\prod_{p\mid M_g(x)} l_g(p) = 2^{\omega(g)}\prod_{p\mid M_g(x)}\frac{p-1}{i_g(p)} = \frac{2^{\omega(g)}\varphi(M_g(x))}{I_g(x)}$$
$$\sim \frac{2^{\omega(g)}M(x)}{e^\gamma\varphi(\mathrm{rad}(g))I_g(x)\log x},$$

by the formula of Mertens.

It is easy to see that this expression is exponentially large, either from the observation that $l_g(p) \geq 2$ whenever $\left(\frac{g}{p}\right) = -1$, so that $\#(\overline{\mathcal{P}}_x \cap (0, M(x)])) \geq 2^{(1/2+o(1))\pi(x)}$, or using $I_g(x) \leq e^{0.42x}$ from [10]. Further, the number of true powers of g in $(0, M(x)]$ is small; it is $O(x)$. Thus,

$$\#\left(\mathcal{P}_x \cap (0, M(x)]\right) = (1+o(1))\frac{2^{\omega(g)}M(x)}{e^{\gamma}\varphi(\mathrm{rad}(g))I_g(x)\log x}, \qquad x \to \infty. \quad (21)$$

To prove Theorem 4 we again use Lemma 6, which is GRH-conditional. But the framework of the proof follows the argument of Theorem 1, and in particular it uses the unconditional Lemma 5. Notice that the proof of Theorem 3 used Riemann Hypotheses a second time, namely in the estimation of the weighted character sums. Now we use unweighted character sums and so are able to use Lemma 5. The set-up is as follows. Let

$$P_{A,N} = \sum_{ab=\mathrm{rad}(g)} \sum_{\substack{A<n\leq A+N \\ n\equiv 0 \,(\mathrm{mod}\ a) \\ n\equiv 1 \,(\mathrm{mod}\ b)}} \prod_{p \mid M_g(x)} \sum_{j=1}^{i_g(p)} \chi_p^j(n). \quad (22)$$

This expression counts integers $n \in (A, A+N]$ that are 0 or 1 (mod p) for each prime $p \mid g$ and in the subgroup $\langle g \rangle$ of $(\mathbb{Z}/p\mathbb{Z})^*$ for each prime $p \leq x$ with $p \nmid g$. Namely, it counts members of $\overline{\mathcal{P}}_x$, and does so with the weight $I_g(x)$.

To prove Theorem 4 one then expands the product in (22). As usual, the contribution from the principal character is easily estimated: it is the number of integers $n \in (A, A+N]$ which are 0 or 1 (mod p) for each prime $p \mid g$ and are coprime to $M_g(x)$. Thus, the principal character gives the contribution

$$(1+o(1))\frac{2^{\omega(g)}}{\mathrm{rad}(g)} \cdot \frac{\varphi(M_g(x))}{M_g(x)} N = (1+o(1))\frac{2^{\omega(g)}N}{e^{\gamma}\varphi(\mathrm{rad}(g))\log x},$$

which when divided by the weight $I_g(x)$ gives the main term for our count.

The nonprincipal characters have conductors corresponding to those divisors f of $M_g(x)$ with $f > 1$ and $i_g(p) > 1$ for each prime $p \mid f$. For such integers f, the characters that occur with conductor f are induced by characters in the set

$$X_f = \Big\{ \prod_{p \mid f} \chi_p^{j_p} \ : \ 1 \leq j_p \leq i_g(p) - 1 \text{ for } p \mid f \Big\}.$$

Thus, the contribution of the nonprincipal characters to $P_{A,N}$ is

$$P^*_{A,N} := \sum_{ab=\mathrm{rad}(g)} \sum_{\substack{f \mid M_g(x) \\ f>1}} \sum_{\chi \in X_f} \sum_{\substack{A<n\le A+N \\ n\equiv 0 \pmod a \\ n\equiv 1 \pmod b \\ (n, M_g(x)/f)=1}} \chi(n),$$

where X_f is empty if $i_g(p) = 1$ for some prime $p \mid f$. The inner sum is

$$\sum_{d \mid M_g(x)/f} \mu(d) \sum_{\substack{A<n\le A+N \\ n\equiv 0 \pmod{ad} \\ n\equiv 1 \pmod b}} \chi(n).$$

As before we estimate the character sum here trivially if d is large, we use the Pólya–Vinogradov inequality if f is small, and we use Lemma 5 in the remaining cases. However, we modify slightly the choice of r in the proof of Theorem 1 and take it now as the largest integer with

$$r2^r + 2 \le \frac{\log x}{(\log\log x)^2}.$$

Then we still have (14) and thus the conditions (15) and (16) are still satisfied so that Lemma 5 may be used. Since each $|X_f| < I_g(x)$, we obtain

$$|P^*_{A,N}| \le 4^{(1+o(1))\pi(x)} I_g(x) N^{1-2/(r2^r+2)}.$$

This leads us to the asymptotic formula

$$P_{A,N} = (1+o(1))\frac{2^{\omega(g)}N}{e^\gamma \varphi(\mathrm{rad}(g))\log x} + O\left(I_g(x) 4^{(1+o(1))\pi(x)} N^{1-2/(r2^r+2)}\right).$$

For $N \ge \exp(b_g x/\log\log x)$ we have

$$N^{2/(r2^r+2)} \ge N^{2(\log\log x)^2/\log x} > \exp\left(2b_g x \log\log x/\log x\right).$$

Using Lemma 6 and taking $b_g = c_g$, we conclude the proof of Theorem 4.

Acknowledgments

The first author was supported in part by NSF grant DMS-0703850. The second author was supported in part by ARC grant DP0556431.

References

[1] E. Bach, R. Lukes, J. Shallit and H. C. Williams, 'Results and estimates on pseudopowers', *Math. Comp.*, **65** (1996), 1737–1747.

[2] R. C. Baker and G. Harman, 'The Brun-Titchmarsh theorem on average', *Proc. Conf. in Honor of Heini Halberstam (Allerton Park, IL, 1995)*, Progr. Math., vol. 138, Birkhäuser, Boston, 1996, 39–103.

[3] R. C. Baker and G. Harman, 'Shifted primes without large prime factors', *Acta Arith.*, **83** (1998), 331–361.

[4] D. A. Burgess, 'On character sums and L-series. II', *Proc. London Math. Soc.*, **13** (1963), 524–536.

[5] S. W. Graham and C. J. Ringrose, 'Lower bounds for least quadratic nonresidues', *Analytic Number Theory, Allerton Park 1989*, Progress in Mathematics, vol. 85, Birkhäuser, Basel, 1990, 269–309.

[6] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London, 1974.

[7] D. R. Heath-Brown and S. V. Konyagin, 'New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum', *Ouart. J. Math.*, **51** (2000), 221–235.

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

[9] H. Iwaniec and E. Kowalski, *Analytic number theory*, Colloquium Pubs., Vol. 53, Amer. Math. Soc., Providence, RI, 2004.

[10] S. Konyagin, C. Pomerance, and I. E. Shparlinski, 'On the distribution of pseudopowers', to appear.

[11] P. Kurlberg and C. Pomerance, 'On the period of the linear congruential and power generators', *Acta Arith.*, **119** (2005), 149–169.

[12] D. H. Lehmer, 'A sieve problem on "pseudo-squares"', *Math. Tables and Other Aids to Computation*, **8** (1954), 241–242.

[13] F. Pappalardi, 'On the order of finitely generated subgroups of $\mathbb{Q}^*$ (mod p) and divisors of $p-1$', *J. Number Theory*, **57** (1996), 207–222.

[14] A. Schinzel, 'On the congruence $a^x \equiv b \pmod{p}$', *Bull. Acad. Polon. Sci., Sér. Sci. Math. Astronom. Phys.*, **8** (1960), 307–309.

[15] A. Schinzel, 'A refinement of a theorem of Gerst on power residues', *Acta Arith.*, **17** (1970), 161–168.

[16] A. Schinzel, 'On pseudosquares', *New trends in probability and statistics, Palonga, 1996*, Vol. 4, 213–220, VSP, Utrecht, 1997.

[17] H. C. Williams, 'Primality testing on a computer', *Ars Combinatoria*, **5** (1978), 127–185.