MATHEMATICS OF COMPUTATION
Volume 65, Number 216
October 1996, Pages 1737–1747

# RESULTS AND ESTIMATES ON PSEUDOPOWERS

ERIC BACH, RICHARD LUKES, JEFFREY SHALLIT, AND H. C. WILLIAMS

ABSTRACT. Let $n$ be a positive integer. We say $n$ *looks like a power of* 2 modulo a prime $p$ if there exists an integer $e_p \geq 0$ such that $n \equiv 2^{e_p} \pmod{p}$. First, we provide a simple proof of the fact that a positive integer which looks like a power of 2 modulo all but finitely many primes is in fact a power of 2.

Next, we define an *$x$-pseudopower of the base* 2 to be a positive integer $n$ that is not a power of 2, but looks like a power of 2 modulo all primes $p \leq x$. Let $P_2(x)$ denote the least such $n$. We give an unconditional upper bound on $P_2(x)$, a conditional result (on ERH) that gives a lower bound, and a heuristic argument suggesting that $P_2(x)$ is about $\exp(c_2 x/\log x)$ for a certain constant $c_2$. We compare our heuristic model with numerical data obtained by a sieve. Some results for bases other than 2 are also given.

## 1. INTRODUCTION

It is a general, though hardly universal, principle in number theory that if an equation is solvable modulo all but finitely many primes $p$, then it is solvable over $\mathbb{Z}$, the integers. For example, let $a$ be a positive integer. Then it is well known that if $a$ looks like a square mod $p$ (i.e., there exists $x$ such that $x^2 \equiv a \pmod{p}$) for all but finitely many primes $p$, then $a$ is in fact the square of an integer. For a proof, see [6, p. 62].

Trost [23] generalized this theorem to higher powers. He proved that if $x^n \equiv a \pmod{p}$ has a solution for all but finitely many primes $p$, then either (i) there exists an integer $b$ with $a = b^n$, or (ii) $8 \mid n$ and $a = 2^{n/8} b^n$. Also see [1, 7].

Let $n$ be a positive integer. If $n$ is a nonsquare that looks like an odd square modulo all primes $\leq x$ (i.e., $n \equiv 1 \pmod{8}$, and $\left(\frac{n}{p}\right) = 1$ for all primes $p \leq x$), then $n$ is said to be an *$x$-pseudosquare*. Pseudosquares were first studied by Lehmer, Lehmer, and Shanks [10]. Williams et al. [12, 21] have computed the least $x$-pseudosquare for all $x \leq 271$. It is possible to show, assuming the Extended Riemann Hypothesis (ERH), that the least $x$-pseudosquare is $> e^{\sqrt{x/2}}$ [25].

In this paper, we consider the analogues of these questions for powers of 2 instead of squares.

Received by the editor February 27, 1995 and, in revised form, September 11, 1995.
1991 *Mathematics Subject Classification.* Primary 11Y70; Secondary 11Y55, 11A15.
*Key words and phrases.* Pseudopowers.
The research of the first and third authors was supported in part by NSF Grant DCR 92-08639. The research of the first author was also supported by a Foreign Researcher Award from NSERC. The research of the third author was also supported by a grant from NSERC and the Wisconsin Alumni Research Foundation. The research of the second and fourth authors was supported in part by NSERC Grant A7649.

We introduce some notation that will be used in this paper. If $p$ is a prime, then by $\nu_p(n)$ we mean the exponent of the highest power of $p$ that divides $n$. We will use the familiar convention that sums over indices $p$ and $q$, such as $\sum_{p\le x} f(p)$, are taken over primes only. Also, we define $\vartheta(x) = \sum_{p\le x} \log p$, and $\psi(x) = \sum_{p^k \le x} \log p$, where this last sum is over all nontrivial prime powers $\le x$. Finally, if $g$ is a unit mod $p$, we define $\langle g\rangle_p$ to be the multiplicative subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ generated by $g$.

## 2. Numbers that look like powers of 2

In this section, we prove the following theorem:

**Theorem 1.** *Let $n$ be a positive integer. Suppose that for all but finitely many primes $p$ there exists an integer $e_p \ge 0$ such that $n \equiv 2^{e_p} \pmod{p}$. Then $n$ is a power of 2.*

As Armand Brumer kindly pointed out to us (personal communication), this theorem is a special case of a more general theorem of Schinzel [17]. (See also [18, Thm. 2]; [19, Thm. 2].) Since our proof seems to be simpler than Schinzel's, we give it here.

*Proof.* We prove the contrapositive. Assume $n$ is not a power of 2. Let $q$ be the least prime for which $n$ is not a $q$th power. Let $\zeta$ be a primitive $q$th root of unity, and consider the number field $K = \mathbb{Q}(\zeta)$. Since $n$ is not a power of 2, it has at least one odd prime factor, and the extension field $L = K(\sqrt[q]{2}, \sqrt[q]{n})$ has degree $q^2$ over $K$. By the Chebotarev density theorem (e.g., see [9, p. 169]), there are infinitely many degree-1 primes $P$ in $K$'s ring of integers such that

$$X^q - 2 \text{ splits completely } \pmod{P}$$

whereas

$$X^q - n \text{ is irreducible } \pmod{P}\ .$$

Each such $P$ lies over an ordinary prime $p$ for which $2 \in ((\mathbb{Z}/p\mathbb{Z})^*)^q$ but $n \notin ((\mathbb{Z}/p\mathbb{Z})^*)^q$. Thus, $n$ is not a power of 2 modulo infinitely many primes. □

## 3. Bounds on pseudopowers of 2

As mentioned in §1, we define an integer $n$ to be an *$x$-pseudopower of the base* 2 if $n$ is not a power of 2, but looks like a power of 2 modulo all primes $\le x$, i.e., if for all primes $p \le x$ there exists an integer $e_p \ge 0$ such that $n \equiv 2^{e_p} \pmod{p}$. We denote the least such $x$-pseudopower as $P_2(x)$. In this section we obtain upper and lower bounds on the size of $P_2(x)$.

**Theorem 2.** *For $x \ge 3$ we have $P_2(x) < e^{1.000081x}$.*

*Proof.* Suppose $n$ is the smallest $x$-pseudopower of the base 2. Then $n$ is odd, for if not, $n/2$ would also be an $x$-pseudopower. Hence, if $p_1 = 2, p_2, \ldots, p_k$ are the primes $\le x$, we know that $n$ is the least non-unit solution in the interval

$[1, p_1 p_2 \cdots p_k]$ of the following system of congruences:

$$
\begin{aligned}
n &\equiv 1 \pmod 2, \\
n &\equiv 1 \text{ or } 2 \pmod 3, \\
n &\equiv 1, 2, 3, \text{or } 4 \pmod 5, \\
n &\equiv 1, 2, \text{or } 4 \pmod 7, \\
&\vdots \\
n &\in \langle 2 \rangle_{p_k} \pmod{p_k}.
\end{aligned} \tag{1}
$$

Now if $x \geq 3$ (i.e., $k \geq 2$), then this system clearly has at least one non-unit solution, which cannot be a power of 2, since $n$ is odd. Hence we find $P_2(x) \leq p_1 p_2 \cdots p_k$. The prime number theorem tells us that

$$P_2(x) \leq \prod_{p \leq x} p = e^{\vartheta(x)} = e^{x(1+o(1))}.$$

Furthermore, a result announced by Schoenfeld [20] provides the more explicit upper bound $e^{1.000081x}$. □

We can obtain a lower bound on $P_2(x)$ if we assume the ERH:

**Theorem 3.** *If the Riemann hypothesis holds for Dedekind zeta functions, then there is a constant $A > 0$ such that $P_2(x) \geq \exp(A\sqrt{x}/(\log x)^3)$.*

*Proof.* Let $n = P_2(x)$, and consider the proof of Theorem 1. There, $q$ was defined to be the least prime such that $n$ is not a $q$th power. Considering the exponents in $n$'s prime factorization, we have

$$n \geq 2^{\prod_{p<q} p} = 2^{e^{\theta(q-1)}}.$$

From the prime number theorem, we know $\theta(x) \sim x$, and it follows that $q = O(\log \log n)$. Let $\Delta$ be the discriminant of $L = K(\sqrt[q]{2}, \sqrt[q]{n})$. Using formulas for the discriminants of towers [5, Satz 39] and composed fields [22], we have

$$\log |\Delta| \leq 4q^3 \log q + q^3 \log(2n) = O((\log n)(\log \log n)^3).$$

If the ERH holds, there is a degree-1 prime $P$ of $K$ modulo which $X^q - 2$ splits completely and $X^q - n$ is irreducible, of norm $O((\log |\Delta|)^2)$. (See [8].) Taking $p$ to be the norm of $P$, we find as before that $n \notin \langle 2 \rangle$ mod $p$. Necessarily, $p > x$, so we have $x = O((\log n)^2 (\log \log n)^6)$. Recalling that $n = P_2(x)$, we obtain the result. □

The estimate of Theorem 3 could be made explicit by using a strong form of the generalized Linnik theorem; see [2].

## 4. A heuristic estimate for $P_2(x)$

Theorem 1 implies that $P_2(x) \to \infty$. The theorems of the last two sections give us bounds of the form

$$Ax^{1/2-\epsilon} \leq \log P_2(x) \leq Bx,$$

in which $A$ and $B$ are certain positive constants. (The lower bound relies on the ERH.) In this section, we argue that the growth rate of $\log P_2(x)$ is close to $c_2 x / \log x$, for a certain constant $c_2$.

We consider a probabilistic model. The fraction of integers $n$ satisfying the system of congruences (1) for $p \le x$ is

$$\frac{1}{2} \prod_{3 \le p \le x} \frac{|\langle 2 \rangle_p|}{p}.$$

If we choose integers at random, the expected number of draws until we find one meeting the conditions is

$$2 \prod_{3 \le p \le x} \frac{p}{|\langle 2 \rangle_p|} = \left( \prod_{2 \le p \le x} \frac{p}{p-1} \right) \left( \prod_{3 \le p \le x} \frac{p-1}{|\langle 2 \rangle_p|} \right).$$

We therefore expect the least number satisfying the conditions to be about this large.

By Mertens' theorem, the first factor is asymptotic to $e^\gamma \log x$, where $\gamma$ is Euler's constant. To estimate the second factor, we will have to resort to a heuristic argument. We have

$$\prod_{3 \le p \le x} \frac{p-1}{|\langle 2 \rangle_p|} = \exp \left( \sum_{3 \le p \le x} \log \frac{p-1}{|\langle 2 \rangle_p|} \right).$$

We observe that $\sum_{3 \le p \le x} \log \frac{p-1}{|\langle 2 \rangle_p|}$ is $\pi(x) - 1$ times the average value of $\log \frac{p-1}{|\langle 2 \rangle_p|}$, for odd primes $p \le x$. It is reasonable to believe that this average has a limit $c_2$ as $x \to \infty$, and we give two different arguments for this below. Assuming the existence of this limit, the expected number of draws is

$$e^\gamma (\log x)(e^{\pi(x)-1})^{c_2 + o(1)} = \exp((c_2 + o(1)) \frac{x}{\log x}). \tag{2}$$

This suggests an "expected value" for $P_2(x)$, but we must also consider possible fluctuations about this mean. Let $Z_k$ be the number of random samples from $\{1, \ldots, p_1 p_2 \cdots p_k\}$ needed to satisfy (1). We recall the Borel-Cantelli lemma, which states that if $E_1, E_2, \ldots$ are events for which $\sum_k \Pr[E_k]$ converges, then almost surely only finitely many $E_k$ occur. Let $\epsilon > 0$ be arbitrary, and let $E_k$ be the event that $Z_k > (1+\epsilon) E[Z_k] \log k$. Observing that $(1 - 1/E[Z_k])^{E[Z_k]} \le e^{-1}$, we have

$$\sum_{k \ge 1} \Pr[E_k] \le \sum_{k \ge 1} \left( \frac{1}{e} \right)^{(1+\epsilon) \log k} < \infty.$$

We can replace $\log k$ by $\log p_k$ in this argument and get the same result (the two are asymptotic to each other). Therefore, the following inequality holds with probability 1:

$$Z_k \le e^\gamma (\log x)^{1+\epsilon} (e^{\pi(x)-1})^{c_2 + o(1)} = \exp((c_2 + o(1)) \frac{x}{\log x}).$$

(Here we are again assuming the existence of $c_2$, and putting $x = p_k$.) Based on this result, and the fact that $E(\log Z_k) = \log E(Z_k) + O(1)$, a consequence of the geometric distribution of $Z_k$, we conjecture that

$$\log P_2(x) \sim \frac{c_2 x}{\log x}. \tag{3}$$

We now consider the problem of computing $c_2$. The simplest idea is that 2 acts like a randomly chosen element $g$ of $(\mathbb{Z}/p\mathbb{Z})^*$. As we will see, this is not quite correct, but it gives a place to start. Let the prime factorization of $p-1$ be $q_1^{e_1} \dots q_r^{e_r}$. Then

$$\log \frac{p-1}{|\langle g \rangle_p|} = \sum_{1 \le i \le r} \log \frac{q^{e_i}}{|\langle g \rangle_{p,q_i}|},$$

where $\langle g \rangle_{p,q}$ denotes the group generated by $g$'s image in the $q$-Sylow subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. (This is the group generated by $g^{(p-1)/q}$.)

Let $q$ be one of the prime divisors of $p-1$, with $q^e \,||\, p-1$. Then the $q$-Sylow subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ has a chain decomposition into cyclic groups of the form

$$1 \subset C_q \subset C_{q^2} \subset \cdots \subset C_{q^e}.$$

The location of $g$ in this chain determines its order in the $q$-Sylow group, and if $g$ is chosen at random, we find that

$$\begin{aligned} E[\log \frac{q^e}{\langle g \rangle_{p,q}}] &= \frac{q-1}{q}\left(\log 1 + \frac{\log q}{q} + \frac{\log q^2}{q^2} + \cdots + \frac{\log q^{e-1}}{q^{e-1}}\right) + \frac{\log q^e}{q^e} \\ &= \left(\frac{q-1}{q} \sum_{1 \le i \le e-1} \frac{i \log q}{q^i}\right) + \frac{e \log q}{q^e}. \end{aligned}$$

So far, we have given a rigorous argument valid for one prime $p$. Now, we fix $q$ and consider all the primes $p$ having $q$ as a prime divisor of $p-1$. If $e \ge 1$, by considering the possible residue classes for $p-1 \bmod q^{e+1}$, we find that the density of primes $p$ for which $q^e \,||\, p-1$ (relative to all primes) is $1/q^e$. Taking this to be the "probability" that $q^e \,||\, p-1$, we compute

$$\begin{aligned} c &= \sum_{q \ge 2} \sum_{e \ge 1} \left( \left(\frac{q-1}{q} \sum_{1 \le i \le e-1} \frac{i \log q}{q^i}\right) + \frac{e \log q}{q^e}\right) \Pr[q^e \,||\, p-1] \\ &= \sum_{q \ge 2} \frac{q \log q}{(q-1)^2(q+1)} \end{aligned}$$

as the "expected value" of $\log \frac{p-1}{|\langle g \rangle_p|}$.

We can compute an accurate value for $c$ in the following way. We first note that

$$\frac{q}{(q-1)^2(q+1)} = \sum_{n \ge 2} \frac{\lfloor n/2 \rfloor}{q^n}.$$

This reduces the computation of $c$ to the evaluation of $\sum_q (\log q)/q^n$ for various $n$. Using Möbius inversion, these sums can be rewritten in terms of the logarithmic derivative of the zeta function (see (5.1) of [16]). Doing all this, we find that

$$c = -\sum_{m \ge 1} \mu(m) \sum_{n \ge 2} \left\lfloor \frac{n}{2} \right\rfloor \frac{\zeta'}{\zeta}(mn).$$

Integer values of the zeta function and its derivative are easy to obtain by Euler-Maclaurin summation [4]. Numerically, we have

$$c \doteq 0.89846489937400140618.$$

This argument assumed a randomly chosen base. We now consider the specific base 2. The actual average value of $\log \frac{p-1}{|\langle 2 \rangle_p|}$, for odd primes $p \le 10^6$, is 0.923465. On the other hand, the corresponding averages for bases 3,5,6 are all close to $c$. (They are 0.896144, 0.894457, and 0.895721, respectively.)

The discrepancy for the base 2 is due to the effect of the quadratic reciprocity law, or more precisely, to the quadratic character of 2. (Thanks to Carl Pomerance for suggesting this.) We have $\left(\frac{2}{p}\right) = +1$ if and only if $p \equiv \pm 1 \pmod 8$, which means that 2 cannot mimic a random element of the 2-Sylow subgroup. If $\nu_2(p-1) = 1$, there is no problem, but if $\nu_2(p-1) = 2$, then $p \equiv 5 \pmod 8$, so $\left(\frac{2}{p}\right) = -1$, and the image of 2 generates the 2-Sylow subgroup. Similarly, for $\nu_2(p-1) \geq 3$, the image of 2 never generates the 2-Sylow subgroup. If we assume that the order of 2 is constrained only by these requirements, we see that the contribution for 2 should be

$$\frac{\log 2}{2} \cdot \frac{1}{2} + \sum_{e \geq 3} \left( \left( \sum_{1 \leq i \leq e-1} \frac{i \log 2}{2^{i+1}} \right) + \frac{e \log 2}{2^{e-1}} \right) \frac{1}{2^e}.$$

(Note that there is no contribution for $e = 2$.) The upshot is that we must add $(\log 2)/24$ to the value of $c$ for the base 2. The resulting constant is

$$c_2 \doteq 0.9273460318973324607,$$

which is more in line with our observations.

We close this section with another argument that $\log \frac{p-1}{|\langle 2 \rangle_p|}$, averaged over odd primes $\leq x$, has a limiting value. For any given $x$, we can express the average as

$$\sum_{t \geq 1} A(2, t; x) \log t, \tag{4}$$

where $A(2, t; x)$ denotes the fraction of odd $p \leq x$ with the index of $\langle 2 \rangle \bmod p$ equal to $t$. (Note that this sum is finite.) Lenstra [11] has shown that for every $t$, the limit

$$A(2, t) = \lim_{x \to \infty} A(2, t; x) \tag{5}$$

exists, assuming the ERH. Thus, it is plausible that the sum in (4) has a limit as $x \to \infty$, and that the limit is

$$c_2' = \sum_{t \geq 1} A(2, t) \log t. \tag{6}$$

(Murata [14] gives an estimate for the rate of convergence in (5), but it does not seem sharp enough to prove this.)

We can compute $c_2'$ using results of Wagstaff [24], who expressed $A(2, t)$ as a rational number times Artin's constant. For our purposes it is convenient to use the following formulas. Let

$$g(t) = \frac{1}{t^2} \prod_{q \mid t} \frac{q^2 - 1}{q^2 - q - 1},$$

and let

$$A = \prod_{q \geq 2} (1 - \frac{1}{q(q-1)}) \doteq 0.373955813619202$$

be Artin's constant. Then we have

$$A(2, t) = \begin{cases} Ag(t), & \text{if } 4 \nmid t; \\ 2/3Ag(t), & \text{if } 4 \,\|\, t; \\ 2Ag(t), & \text{if } 8 \mid t. \end{cases}$$

By comparison with the Euler $\varphi$-function, it can be shown that

$$g(t) = O((\log\log t)/t^2),$$

so that $\sum_{t\geq 1} A(2,t)\log t$ converges.

Using a segmented version of the Sieve of Eratosthenes [3, 15] we were able to compute $g(t)$ for $t < 10^9$, and obtain the approximation

$$c_2' \doteq 0.927346$$

(correct to six figures). Within the limits of this calculation, we have $c_2' \doteq c_2$. We conjecture that this is actually an equality.

## 5. Pseudopowers of the base 2 and numerical evidence for the heuristic model

Table 1 gives, for $1 \leq k \leq 55$, the least positive odd number $n > 1$ for which $n$ looks like a power of 2 modulo the primes $p_1 = 2, p_2, \ldots, p_k$. The data is only provided for the "record-setting" values of $k$, that is, those $k$ for which $P_2(p_k) \neq P_2(p_{k-1})$. For values of $k < 55$ that are not listed, $P_2(p_k)$ is the last preceding value; thus, for example, $P_2(p_6) = 23$.

TABLE 1

| $k$ | $p_k$ | $P_2(p_k)$ | $c_2^{(k)}$ | $R_2^{(k)}$ |
|---|---|---|---|---|
| 1 | 2 | 3 | 0.000000 | 0.192 |
| 2 | 3 | 5 | 0.000000 | 0.417 |
| 3 | 5 | 7 | 0.000000 | 0.541 |
| 4 | 7 | 11 | 0.231049 | 0.807 |
| 5 | 11 | 23 | 0.173287 | 0.684 |
| 7 | 17 | 43 | 0.231049 | 0.799 |
| 9 | 23 | 127 | 0.259930 | 0.784 |
| 11 | 31 | 1087 | 0.387120 | 0.813 |
| 14 | 43 | 2209 | 0.435612 | 0.982 |
| 15 | 47 | 2837 | 0.454008 | 1.042 |
| 20 | 71 | 7603 | 0.371013 | 1.016 |
| 21 | 73 | 115669 | 0.456435 | 0.957 |
| 24 | 89 | 1062839 | 0.517447 | 1.007 |
| 25 | 97 | 4007837 | 0.524768 | 0.966 |
| 30 | 113 | 38863631 | 0.543879 | 1.024 |
| 31 | 127 | 101665279 | 0.622095 | 1.129 |
| 33 | 137 | 234556697 | 0.604875 | 1.117 |
| 36 | 151 | 1848054121 | 0.618817 | 1.118 |
| 48 | 223 | 3131990286049 | 0.581310 | 1.028 |
| 50 | 229 | 41398091214971 | 0.580003 | 0.979 |
| 51 | 233 | 335444151885977 | 0.609992 | 0.980 |
| 52 | 239 | 663176716985449 | 0.611623 | 0.981 |
| 53 | 241 | 10600009924847711 | 0.644141 | 0.970 |
| 54 | 251 | 28185732773917153 | 0.662354 | 0.987 |
| 55 | 257 | 306313044048233909 | 0.701433 | 0.998 |

These values were obtained using the Manitoba Scalable Sieve Unit (MSSU), a sieve machine designed and built by the fourth author and his colleagues. This machine searches for the least integer satisfying a set of congruence conditions, such as (1), and is described in detail elsewhere [12, 13].

It will be noted that (2) is not a very good predictor of $P_2(p_k)$ within the range of this table. For example, if we take $k = 55$, so that $p_k = 257$, then $e^\gamma \log p_k \; e^{(k-1)c_2} \approx 6 \times 10^{22}$, whereas $P_2(p_k) \approx 3 \times 10^{17}$. We believe that the discrepancy is mainly caused by slow convergence of the mean values of $\log \frac{p-1}{|\langle 2\rangle_p|}$ to $c_2$. As an example of this, for odd primes $\leq 257$, the true mean value is 0.701433, rather less than the presumed asymptotic value of 0.927346. Of course, this error is exacerbated by the exponentiation in (2).

We can check our heuristic assumption that the solutions to (1) behave randomly by replacing $c_2$ by $c_2^{(k)}$, the true mean value of $\log \frac{p-1}{|\langle 2\rangle_p|}$ over odd primes $\leq p_k$, in (2). These values are also listed in Table 1, together with the ratio

$$R_2^{(k)} = \frac{\gamma + \log\log(p_k) + c_2^{(k)}(k-1)}{\log P_2(k)}.$$

It seems that $R_2^{(k)} \to 1$, which is consistent with (2).

## 6. Pseudopowers for other bases

One can replace the base 2 by any other number. In this section, we briefly discuss how our results extend to other bases, and present empirical data for the bases 3 and 5.

For simplicity we assume that $b$ is prime. As before, we define $P_b(x)$ to be the least $n > 1$ that is not a power of $b$, but appears to be such a power modulo the primes $\leq x$. Analogously to (1), we see that $P_b(p_k)$ is the least number greater than 1 satisfying $n \in \langle b\rangle \pmod{p_i}$ for $i \leq k$, $p_i \neq b$, and $n \equiv 1 \pmod{b}$ (if $b \leq p_k$).

Therefore, the analog of Theorem 2 holds for $x > b$. The analogs of Theorems 1 and 3 remain true (and are proved the same way), with the modification that the constant $A$ now depends on $b$. Using the same heuristic argument as before, we expect that

$$P_b(x) = (b-1)e^\gamma (\log x)(e^{\pi(x)-1})^{c_b + o(1)},$$

where $c_b$ is the asymptotic average value of $\log \frac{p-1}{|\langle b\rangle|}$.

Tables 2 and 3 give pseudopowers of 3 and 5, found using the MSSU. As before, we only list the record-breaking values of $P_3$ and $P_5$. To compare the data with our heuristic predictions, we also tabulated $c_b^{(k)}$, the average value of $\log \frac{p-1}{|\langle b\rangle|}$ over the primes different from $b$ and $\leq p_k$, and the ratio

$$R_b^{(k)} = \frac{\gamma + \log(b-1) + \log\log p_k + c_b^{(k)}(k-1)}{\log P_b(k)}$$

for $b = 3, 5$.

We close with some remarks about the likely values of $c_3$ and $c_5$. Wagstaff's formula for $A(2,t)$ is a special case of a more general one for $A(b,t)$, the asymptotic fraction of primes $p$ for which $\langle b\rangle$ has index $t$ mod $p$. (This is also a rational multiple of Artin's constant.) Let

$$c'_b = \sum_{t \geq 1} A(b,t) \log t.$$

TABLE 2

| $k$ | $p_k$ | $P_3(p_k)$ | $c_3^{(k)}$ | $R_3^{(k)}$ |
|---|---|---|---|---|
| 1 | 2 | 5 | 0.000000 | 0.562 |
| 2 | 3 | 7 | 0.000000 | 0.701 |
| 4 | 7 | 13 | 0.000000 | 0.755 |
| 5 | 11 | 31 | 0.173287 | 0.826 |
| 6 | 13 | 157 | 0.415888 | 0.849 |
| 9 | 23 | 841 | 0.346574 | 0.770 |
| 10 | 29 | 859 | 0.308065 | 0.778 |
| 12 | 37 | 1543 | 0.315067 | 0.820 |
| 13 | 41 | 6241 | 0.422931 | 0.876 |
| 18 | 61 | 36481 | 0.485484 | 1.041 |
| 19 | 67 | 170041 | 0.519547 | 1.001 |
| 20 | 71 | 241081 | 0.528684 | 1.030 |
| 21 | 73 | 1515361 | 0.591837 | 1.023 |
| 27 | 103 | 16226731 | 0.550833 | 1.032 |
| 28 | 107 | 32913169 | 0.556104 | 1.030 |
| 29 | 109 | 52078027 | 0.585753 | 1.082 |
| 36 | 151 | 872200213 | 0.519796 | 1.024 |
| 41 | 179 | 1327190419 | 0.506807 | 1.104 |
| 42 | 181 | 8479278889 | 0.528258 | 1.075 |
| 44 | 193 | 89400402001 | 0.577596 | 1.101 |
| 58 | 271 | 384810485528569 | 0.559402 | 1.039 |
| 63 | 307 | 2346816388490401 | 0.572087 | 1.087 |
| 65 | 313 | 150139363999760521 | 0.597531 | 1.043 |

TABLE 3

| $k$ | $p_k$ | $P_5(p_k)$ | $c_5^{(k)}$ | $R_5^{(k)}$ |
|---|---|---|---|---|
| 1 | 2 | 3 | 0.000000 | 1.454 |
| 2 | 3 | 7 | 0.000000 | 1.057 |
| 3 | 5 | 11 | 0.000000 | 1.017 |
| 5 | 11 | 31 | 0.173287 | 1.028 |
| 8 | 19 | 311 | 0.354987 | 0.963 |
| 10 | 29 | 961 | 0.353117 | 0.925 |
| 11 | 31 | 3931 | 0.548064 | 1.048 |
| 17 | 59 | 32761 | 0.429183 | 0.985 |
| 19 | 67 | 96721 | 0.481038 | 1.050 |
| 20 | 71 | 2048071 | 0.594618 | 1.012 |
| 22 | 79 | 3962941 | 0.570995 | 1.016 |
| 24 | 89 | 15942061 | 0.551480 | 0.974 |
| 34 | 139 | 1049824801 | 0.543683 | 1.035 |
| 42 | 181 | 537343041691 | 0.592626 | 1.033 |
| 43 | 191 | 6791126548441 | 0.633339 | 1.023 |
| 53 | 241 | 28764591571409101 | 0.641573 | 0.977 |
| 54 | 251 | 88428973201069961 | 0.672913 | 1.008 |

By summing over $t < 10^9$, we found that

$$c_3', c_5' \doteq 0.898465,$$

which is, as far as we know, the same as the constant $c$ defined in § 4. We conjecture that $c_3 = c_3'$, $c_5 = c_5'$, and that both of these equal $c$.

## Acknowledgments

Part of this work was done while the third author was on sabbatical at the University of Wisconsin in the fall of 1993, and while the first author visited the University of Waterloo in the winter of 1995. We thank the referee for a careful reading of this paper. We also thank Anil Goel for assistance with LaTeX.

## References

N. C. Ankeny and C. A. Rogers. A conjecture of Chowla. *Ann. Math.* **53** (1951), 541–550. MR **12:**804h

2. E. Bach and J. Sorenson. Explicit bounds for primes in residue classes. In Walter Gautschi, ed., *Mathematics of Computation 1943–1993: A Half-Century of Computational Mathematics, Proc. Symp. Appl. Math.* **48** (1994), 535–539. Full version submitted to *Math. Comp.* CMP 95:07
3. C. Bays and R. H. Hudson. The segmented sieve of Eratosthenes and primes in arithmetic progressions to $10^{12}$. *BIT* **17** (1977), 121–127. MR **56:**5405
4. H. M. Edwards. *Riemann's Zeta Function.* Academic Press, New York, 1974. MR **57:**5922
5. D. Hilbert. Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **4** (1897), 175–546. Reprinted in *Gesammelte Abhandlungen,* Vol. I, pp. 63–363.
6. K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, 2nd edition, 1990. MR **92e:**11001

J. Kraft and M. Rosen. Eisenstein reciprocity and $n$th power residues. *Amer. Math. Monthly* **88** (1981), 269–270. MR **82g:**10008

8. J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Inventiones Math.* **54** (1979), 271–296. MR **81b:**12013
9. S. Lang. *Algebraic Number Theory.* Addison-Wesley, 1970. MR **44:**181
10. D. H. Lehmer, E. Lehmer, and D. Shanks. Integer sequences having prescribed quadratic character. *Math. Comp.* **24** (1970), 433–451. MR **42:**5889
11. H. W. Lenstra, Jr. On Artin's conjecture and Euclid's algorithm in global fields. *Inventiones Math.* **42** (1977), 201–224. MR **58:**576
12. R. F. Lukes, C. D. Patterson, and H. C. Williams. Some results on pseudosquares. *Math. Comp.* **65** (1996), 361–372. CMP 96:03
13. R. F. Lukes, C. D. Patterson, and H. C. Williams. Numerical sieving devices: their history and some applications. *Nieuw Arch. Wisk.* (4) **13** (1995), 113–139. CMP 95:14
14. L. Murata. A problem analogous to Artin's conjecture for primitive roots and its applications. *Arch. Math.* **57** (1991), 555–565. MR **93c:**11071
15. P. Pritchard. Fast compact prime number sieves (among others). *J. Algorithms* **4** (1983), 332–344. MR **85h:**11080
16. J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Ill. J. Math.* **6** (1962), 64–94. MR **25:**1139
17. A. Schinzel. On the congruence $a^x \equiv b \pmod{p}$. *Bull. Acad. Polon. Sci.* **8** (1960), 307–309. MR **23:**A2377
18. A. Schinzel. A refinement of a theorem of Gerst on power residues. *Acta Arith.* **17** (1970), 161–168. MR **44:**1644
19. A. Schinzel. On power residues and exponential congruences. *Acta Arith.* **27** (1975), 397–420. MR **52:**337
20. L. Schoenfeld. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. *Math. Comp.* **30** (1976), 337–360. Corrigenda in *Math. Comp.* **30** (1976), 900. MR **56:**15581b; MR **56:**15581c

21. A. J. Stephens and H. C. Williams. An open architecture number sieve. In J. H. Loxton, editor, *Number Theory and Cryptography*, Vol. 154 of *London Mathematical Society Lecture Note Series*, pages 38–75. Cambridge University Press, 1990. CMP 90:13
22. H. Tôyama. A note on the different of the composed field. *Kodai Math. Sem. Report* **7** (1955), 43–44. MR **17**:714
23. E. Trost. Zur Theorie der Potenzreste. *Nieuw Arch. Wiskunde* **18** (1934), 58–61.
24. S. S. Wagstaff, Jr. Pseudoprimes and a generalization of Artin's conjecture. *Acta Arith.* **41** (1982), 141–150. MR **83m**:10004
25. H. C. Williams and J. O. Shallit. Factoring integers before computers. In Walter Gautschi, ed., *Mathematics of Computation 1943–1993: A Half-Century of Computational Mathematics*, *Proc. Symp. Appl. Math.* **48** (1994), 481–531. CMP 95:07

COMPUTER SCIENCES DEPARTMENT, UNIVERSITY OF WISCONSIN, 1210 W. DAYTON, MADISON, WISCONSIN 53706
*E-mail address*: `bach@cs.wisc.edu`

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MANITOBA, WINNIPEG, MANITOBA R3T 2N2, CANADA
*E-mail address*: `rflukes@cs.umanitoba.ca`

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO N2L 3G1, CANADA
*E-mail address*: `shallit@graceland.uwaterloo.ca`

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MANITOBA, WINNIPEG, MANITOBA R3T 2N2, CANADA
*E-mail address*: `hugh_williams@csmail.cs.umanitoba.ca`