MATHEMATICS OF COMPUTATION
Volume 66, Number 220, October 1997, Pages 1719–1727
S 0025-5718(97)00890-9

COMMENTS ON SEARCH PROCEDURES FOR PRIMITIVE ROOTS

ERIC BACH

ABSTRACT. Let p be an odd prime. Assuming the Extended Riemann Hypothesis, we show how to construct $O((\log p)^4(\log\log p)^{-3})$ residues modulo p, one of which must be a primitive root, in deterministic polynomial time. Granting some well-known character sum bounds, the proof is elementary, leading to an explicit algorithm.

1. INTRODUCTION

Shoup [17] has recently shown that if the Extended Riemann Hypothesis (ERH) holds, the least primitive root mod p is $O(\log p)^6$. The exponent of 6 improved a similar result of Wang [19]. A result of this type immediately gives an efficient search procedure for primitive roots; that is, it shows how to construct a small set S, one of whose elements must generate the multiplicative group mod p.

The purpose of this paper is to give another search procedure for primitive roots. Our set S is asymptotically smaller than Shoup's – it has size $O((\log p)^4/(\log\log p)^3)$ – and can also be constructed in polynomial time, assuming ERH. This result may be of use in situations when the size of the search set is a bottleneck. In addition, both Shoup and Wang relied on intricate sieve estimates. The proofs below rely on much simpler techniques, allowing us to give an explicit algorithm. On the other hand, our procedure uses slightly more computation and yields a set composed of larger elements.

The basic idea of our construction is the following. Let p be a prime. We partially factor $p-1 = q_1^{e_1}\cdots q_r^{e_r}Q$, by removing all prime factors q_i less than a parameter B. In this factorization, Q will be relatively prime to the q_i's, so the multiplicative group modulo p is the direct product of a cyclic group of order $q_1^{e_1}\cdots q_r^{e_r}$ and a cyclic group of order Q. We choose B small enough that the q_i's can be obtained quickly, but large enough to guarantee (under ERH) that some small b has order a multiple of Q. The ERH guarantees small q_i-th power nonresidues, which we combine to obtain a generator a for the first group. Then we combine a with each potential b, to obtain a small set S of residues, one of which must be a generator.

As motivation for such a search procedure, we can argue that the deterministic complexity of primitive root construction is within a polynomial factor of the time to find a discrete logarithm. (The best deterministic method for discrete logs [16] uses $p^{1/2+o(1)}$ steps, although there are randomized algorithms that do better [13].)

Received by the editor April 13, 1994 and, in revised form, September 13, 1994 and July 12, 1996.

1991 *Mathematics Subject Classification.* Primary 11Y16; Secondary 11A07, 11M26.

Key words and phrases. Primes, generators, extended Riemann hypothesis.

Assuming ERH, the primes less than $O(\log p)^2$ generate $(\mathbf{Z}/p\mathbf{Z})^*$, so to construct a generator, it suffices to find some $g \in S$ for which $g^x = q$ can be solved for every prime $q = O(\log p)^2$.

The best unconditional estimate on the least primitive root is due to Wang [19], who showed it is bounded by $p^{1/4+o(1)}$. (See Murata [12] for a review of this problem.) Shparlinski [18] showed that in any finite field with q elements, a primitive root can be found using $q^{1/4+o(1)}$ operations. No rigorous search procedure with smaller complexity seems to be known.

The rest of this paper is organized as follows. In §2, we prove some necessary analytic results. In §3, we give our search procedure (in explicit form), and discuss some related algorithms. Finally, in §4 we present some conjectures and data related to small primitive roots.

2. Analytic results

In this section we provide some estimates from analytic number theory, on which our search procedure relies. Since our goal is to get an explicit algorithm we will give these in concrete form.

In the sequel, p, q, and ℓ will stand for primes, with the convention that q divides $p-1$. We let $\Lambda(n)$ denote *von Mangoldt's function*, which is $\log p$ when n is a prime power p^k, and zero otherwise.

We let χ denote a *Dirichlet character* mod p. This is a mapping from $\mathbf{Z}$ to $\mathbf{C}$ with period p that is zero on multiples of p, and otherwise induces a homomorphism from $(\mathbf{Z}/p\mathbf{Z})^*$ to $\mathbf{C}^*$. From this it follows that $\chi(n)$ is either zero or a root of unity. We let χ_0 denote the *principal character*, which is 0 on multiples of p and 1 otherwise.

The *Extended Riemann Hypothesis* (ERH) asserts that all Dirichlet L-functions, which are defined by $L(s,\chi) = \sum_{n\geq 1} \chi(n)n^{-s}$ when the real part of s exceeds 1 and analytic continuation otherwise, are zero-free to the right of $\mathrm{Re}(s) = 1/2$. This includes the ordinary Riemann hypothesis (for the zeta function) as a special case.

Finally, we let $\omega(m)$ denote the number of distinct prime divisors of m.

Lemma 2.1 [ERH]. *There is a constant $A > 0$ with the following property. For $N \geq 1$, we have*

$$\left| \sum_{n<N} \Lambda(n)\chi_0(n)(1-n/N) - N/2 \right| \leq A\sqrt{N},$$

and if $\chi \neq \chi_0$,

$$\left| \sum_{n<N} \Lambda(n)\chi(n)(1-n/N) \right| \leq A\sqrt{N}\log p.$$

If $p \geq 10^6$ and $N > 26000$ we may take $A = 7/9$.

Proof. We have

$$\sum_{n<N} \Lambda(n)\chi_0(n)(1-n/N) = \sum_{n<N} \Lambda(n)(\chi_0(n)-1)(1-n/N) + \sum_{n<N} \Lambda(n)(1-n/N).$$

The first term is bounded in absolute value by $\sum_{p^k<N} \log p \leq \log N$. We estimate the second via the explicit formula for $\sum_{n<N} \Lambda(n)(N-n)$ [8, p. 73], which implies

for $N \geq 1$

$$|\sum_{n<N} \Lambda(n)(1-n/N) - N/2| \leq \sqrt{N} \sum_{\substack{\zeta(\rho)=0 \\ \mathrm{Re}(\rho)=1/2}} |\frac{1}{\rho(\rho+1)}| + 3 \leq \sqrt{N}/20 + 3.$$

(To get the last estimate, observe that $\sum_\rho |\rho(\rho+1)|^{-1} \leq \sum_\rho (\rho^{-1} + \bar{\rho}^{-1}) = \gamma + 2 - \log(4\pi) < 1/20$.)

Similarly, for nonprincipal χ and $N \geq 1$ we have

$$|\sum_{n<N} \Lambda(n)\chi(n)(1-n/N)| \leq (\sqrt{N} + 2 + 3/N) \sum_{\substack{L(\rho,\chi)=0 \\ \mathrm{Re}(\rho)=1/2}} |\frac{1}{\rho(\rho+1)}| + \log N + 2$$

(as follows from [2], p. 292), and

$$\sum_\rho |\frac{1}{\rho(\rho+1)}| \leq \frac{4}{3} \sum_\rho \frac{1}{|3/2-\rho|^2} = \frac{2}{3} \sum_\rho (\frac{1}{3/2-\rho} + \frac{1}{3/2-\bar{\rho}}) \leq \frac{2}{3}(\log p + 5/3).$$

(The last estimate derives from Lemma 6 of [3].) The numerical bound can be readily verified from these results. □

Aside from our determination of A (which we need later), this result is well known. (See, e.g. Montgomery [11] or Lemma 9.3 of [5].) It is easy to prove, by direct verification for $N < 30$ and analytic computation otherwise, that $A = 4$ suffices for all cases.

Lemma 2.2 [ERH]. *Let T be a nonempty set of prime divisors of $p-1$. Let $f(n)$ be 1 if n is a q-th power nonresidue for each $q \in T$, and 0 otherwise. Then*

$$\sum_{n<N} f(n)\Lambda(n)(1-n/N) \geq (1 - \sum_{q \in T} 1/q)N/2 - A|T|\sqrt{N}\log p,$$

where A is the constant in Lemma 2.1.

Proof. Summing over the characters of order q, we have

$$\frac{1}{q}\sum_\chi \chi(n) = \begin{cases} 1, & \text{if } n \text{ is a } q\text{-th power in } (\mathbf{Z}/p\mathbf{Z})^*; \\ 0, & \text{otherwise.} \end{cases}$$

By inclusion-exclusion, we have

$$\begin{aligned} \sum_{n<N} f(n)\Lambda(n)(1-n/N) &\geq \sum_{n<N} \Lambda(n)\chi_0(n)(1-n/N) \\ &\quad - \sum_{q \in T} \sum_{\substack{n<N \\ n \in ((\mathbf{Z}/p\mathbf{Z})^*)^q}} \Lambda(n)(1-n/N) \\ &= \sum_{n<N} \Lambda(n)\chi_0(n)(1-n/N) - \sum_{q \in T} \frac{1}{q} \sum_\chi \sum_{n<N} \Lambda(n)\chi(n)(1-n/N). \end{aligned}$$

The result follows by extracting the contribution of $\chi = \chi_0$ and grouping it with the first sum, and using Lemma 2.1. □

The next result defines the factor bound B implicitly. To see that this is legitimate, observe that for $y > 0$, the equation $y = x \log x$ has two solutions, the larger of which is greater than 1 and asymptotic to $y/\log y$.

Lemma 2.3. *Let p be a prime and $C > 1$. If $B \log B = C \log p$ and $B \geq 1$, then*

$$\sum_{\substack{q \mid p-1 \\ q > B}} \frac{1}{q} < \frac{1}{C}.$$

We have $B \sim C(\log p)/(\log\log p)$ and $\pi(B) \sim C(\log p)/(\log\log p)^2$.

Proof. The sum is less than $(\log_B p)/B = 1/C$. We leave the rest to the reader. □

Lemma 2.4 [ERH]. *Let B and C be as in Lemma 2.3, and denote the set of prime divisors of $p-1$ exceeding B by T. If T is nonempty, there is some b that is a q-th power nonresidue for each $q \in T$, satisfying*

$$b \leq \frac{4A^2}{(1 - C^{-1})^2} (\omega(p-1) \log p)^2$$

where A is defined in Lemma 2.1. Indeed, we can take b prime. For $p \geq 10^6$ and $C = 30$, we have the explicit bound

$$b \leq 5 \frac{(\log p)^2}{(\log\log p)^4}.$$

Proof. Suppose there are no such b below N. Because T cannot contain more than $\omega(p-1)$ primes, Lemmas 2.1–2.3 imply that

$$\frac{N}{2} \left(1 - \frac{1}{C}\right) \leq A\sqrt{N} (\log p) \omega(p-1).$$

Dividing by $\sqrt{N}$ and rearranging, we obtain a bound for N, which implies the estimate for b.

By the definition of Λ, we can take b to be a prime power ℓ^k. However, if ℓ^k is relatively prime to p and outside several subgroups of $(\mathbf{Z}/p\mathbf{Z})^*$, the same must be true of ℓ.

We obtain the numerical bound as follows. First, we may as well assume that $p \geq 10^6$, for if not, p has a prime primitive root b obeying the bound. (This can be verified by computation. See Table 1 below.) We can also assume $N \geq 5(\log p)^4/(\log\log p)^2$ (if not, the result is true), so $N \geq 26000$. The result now follows from the explicit estimate in Lemma 2.1, together with Robin's bound [14]

$$\omega(m) \leq 1.3841 \frac{\log m}{\log\log m}. \qquad \square$$

Lemma 2.5 [ERH]. *If $q \mid p-1$, the least q-th power nonresidue mod p is prime and $\leq 2(\log p)^2$.*

Proof. See [3]. □

In big-O form, this theorem was first proved by Ankeny [1].

3. A polynomial time search procedure

In this section, we present an explicit search procedure, and briefly discuss some related algorithms.

Algorithm 3.1.

Find $B \geq 1$ so that $B \log B = 30 \log p$.

Factor $p-1 = q_1^{e_1} \dots q_r^{e_r} Q$, where $q_i < B$ and Q is free of primes $< B$.

For each $i = 1, \dots, r$:

Choose a prime $b_i \leq 2(\log p)^2$ so that $b_i^{(p-1)/q_i} \not\equiv 1$.

Let $a_i = b_i^{(p-1)/q_i^{e_i}} \bmod p$.

Let $a = \prod_{i=1}^{r} a_i$.

Let $S = \{ab^{(p-1)/Q} \bmod p : b \text{ is prime and } b \leq 5\frac{(\log p)^4}{(\log\log p)^2}\}$.

Theorem 3.2 [ERH]. *If p is an odd prime, then Algorithm 3.1 computes a set S of residues mod p such that: 1) S contains a primitive root mod p, and 2) $|S| = O(\frac{(\log p)^4}{(\log\log p)^3})$.*

Proof. We first prove 1). By Lemma 2.5, b_i is a q_i-th power nonresidue, so that a_i has order $q_i^{e_i}$ mod p. Therefore a, the product of the a_i's, has order $(p-1)/Q$. It is possible that $Q = 1$, in which case a is already a primitive root. If not, Lemma 2.4 implies that one of the residues $b^{(p-1)/Q}$ will have order Q, making $ab^{(p-1)/Q}$ a primitive root. The truth of 2) is clear from the algorithm and the prime number theorem. □

It will be noted that there is some freedom in the coefficient C used to define B. Our particular choice, $C = 30$, arose from observing that the running time is relatively insensitive to the cost of the factorization step but depends severely on the size of S. Thus it is worthwhile to make the former large so as to reduce the latter. We remark that a more complicated proof, in which C grows with p and the character sum in [3] is employed, would allow us to replace the constant 5 in the definition of S by $1 + o(1)$.

We now analyze the running time of Algorithm 3.1. The most expensive steps are the construction of a and the formation of the numbers comprising S. By Lemma 2.3, $r = O((\log p)/(\log\log p)^2)$, so a can be found using $O((\log p)^4/(\log\log p)^3)$ multiplications mod p. Similarly, by Theorem 3.2, once we have a, we can form S using $O((\log p)^5/(\log\log p)^3)$ multiplications mod p. (All of the other steps can be seen to take much less time than this.) We thus obtain the following time bounds for Algorithm 3.1: $O((\log p)^7/(\log\log p)^3)$ bit operations, using ordinary arithmetic,

and $O((\log p)^6/(\log\log p)^{2+o(1)})$ bit operations asymptotically. (For the last result, one must specify a machine model, for example, the multitape Turing machine.)

As an example, we construct a primitive root for $p = 3821$. We have $p - 1 = 2^2 \cdot 5 \cdot 191$. For this example, we choose $B = 8$, so that $q_1 = 2$ and $q_2 = 5$. The least quadratic nonresidue is 2, and the least 5-th power nonresidue is 3, so $a = 2^{3820/2^2} \cdot 3^{3820/5} \equiv 1916$ generates the group of order 20. We now consider $b \geq 2$; the first try works, and $2^{20} \cdot 1916 \equiv 1279$ is a primitive root.

We now make some remarks related to our search procedure.

1. As an alternative to the ERH in Algorithm 3.1, one could use randomization as follows. For $i = 1, \ldots, r$, test b_i's at random until a q_i-th power nonresidue is found. Also replace the search through $b = 2, 3, 5, \ldots$ by a random choice of b. It is not difficult to see that the chance of finding a primitive root is $\geq 1/2$, and the expected number of multiplications mod p is $O((\log p)/(\log\log p))^2$. With naive arithmetic, this uses $O((\log p)^4/(\log\log p)^2)$ bit operations; its asymptotic complexity is $O((\log p)^3/(\log\log p)^{2+o(1)})$. Compared to a naive guess, this procedure has a higher chance of obtaining a primitive root, since the density of primitive roots is $\Omega((\log\log p)^{-1})$, but requires more work.

2. Because the Jacobi symbol algorithm is more efficient than Euler's criterion [15], it should be used in the search for a quadratic nonresidue.

3. Using results about additive functions on shifted primes (e.g. [6]), it can be shown that $\sum_{q|p-1} 1/q$ has a limiting distribution, whose mean value is

$$\sum_{q|p-1} (q(q-1))^{-1} \doteq 0.773156.$$

This suggests that for many primes, we can take $B = 1$ in Algorithm 3.1 and skip the first part of the construction. For example, 74% of the primes less than 10^6 have $\sum_{q|p-1} 1/q < 0.9$.

4. On probabilistic grounds, one expects at least half of the elements of S to be primitive roots. (The precise fraction depends on B and the factorization of $p-1$.) A probabilistic argument similar to the one given in the next section suggests that it should be sufficient to take $b = O(\log p \log\log p)$ in Algorithm 3.1.

5. The algorithm of Itoh [9] is similar to ours in its reliance on a partial factorization of $p-1$. This algorithm takes as input $g \in (\mathbf{Z}/p\mathbf{Z})^*$, and tries to decide if g is a primitive root. Although some inputs cause an incorrect decision, the result is correct with high probability when g is a random choice from $(\mathbf{Z}/p\mathbf{Z})^*$. For another use of partial factorization, see Cunningham [7].

4. How large is the least primitive root?

In this section we speculate, using ideas from [4], about the growth rate of the least primitive root mod p. This is evidently related to the cost of searching for a primitive root.

Let $\hat{g}(p)$ be the least prime primitive root mod p. If we choose $r(p)$ so that

$$\sum_p \left(1 - \frac{\varphi(p-1)}{p-1}\right)^{r(p)} < \infty,$$

then $\hat{g}(p)$ should exceed the $r(p)$-th prime only finitely often. (This comes from assuming that the small primes $2, 3, 5, \ldots$ act like random samples from $(\mathbf{Z}/p\mathbf{Z})^*$, and applying the Borel-Cantelli lemma.) By Landau's lower bound [10] for the Euler φ-function, we can take $r(p) = (e^\gamma + o(1)) \log p \log\log p$.

On the other hand, no value of $r(p)$ smaller than this will make the sum converge, assuming ERH. This can be proved as follows. Choose a positive $\alpha < e^\gamma$ and let $r(p) = \alpha \log p \log\log p$. Further choose $\epsilon > 0$ so that $\alpha e^{-\gamma} + \epsilon < 1$, and define $Q_x = \prod_{q \le \epsilon \log x} q$. (In this product q is prime.) Then for any $x > 0$, we have

$$\sum_p \left(1 - \frac{\varphi(p-1)}{p-1}\right)^{r(p)} \ge \sum_{\substack{x/2 < p \le x \\ p \equiv 1 \bmod Q_x}} \left(1 - \frac{\varphi(p-1)}{p-1}\right)^{r(p)}.$$

For such p, we have

$$\varphi(p-1)/(p-1) \le \prod_{q \le \epsilon \log x} (1 - 1/q),$$

which is $(e^{-\gamma} + o(1))/\log\log p$ by Mertens's theorem. (Note that $\log\log x \sim \log\log p$.) Therefore the sum is bounded below by

$$\sum_{\substack{x/2 < p \le x \\ p \equiv 1 \bmod Q_x}} \left(1 - \frac{e^{-\gamma} + o(1)}{\log\log p}\right)^{r(p)} = \sum_{\substack{x/2 < p \le x \\ p \equiv 1 \bmod Q_x}} p^{-\alpha(e^{-\gamma} + o(1))}.$$

Assuming ERH, there is a uniform bound for the number of primes $\le x$ and congruent to 1 mod n: $\pi(x, n, 1) = \frac{\mathrm{li}(x)}{\varphi(n)} + O(\sqrt{x}(\log x + \log n))$. Applying this with $n = Q_x$, estimating $\varphi(Q_x)$ by the prime number theorem, and bounding the sum above in a simple fashion (as the number of terms times the smallest term), we find that the original sum is $\Omega(x^{1 - \epsilon - \alpha e^{-\gamma} + o(1)})$. Since x is arbitrary the sum cannot converge.

Thus, the probabilistic model of [4] leads to the conjecture that

$$\limsup_{p \to \infty} \frac{\hat{g}(p)}{\log p (\log\log p)^2} = e^\gamma.$$

This is in rough agreement with empirical data, as Table 1 shows. (Values for $p \le 2 \times 10^6$ appear in Western and Miller [20, p. xlvi]; the others were computed by Scott Lindhurst.)

We do not have a comparable conjecture concerning extremal values of $g(p)$, the least primitive root mod p. Certainly, $g(p) \le \hat{g}(p)$ so it is plausible that $g(p) = O(\log p (\log\log p)^2)$. (But this may not be sharp, since the least primitive root is not necessarily prime.) On the other hand, the ERH implies that $g(p)$ is infinitely often $\Omega(\log p \log\log p)$, as this is true of the least quadratic nonresidue [11]. Since the data of [20] do not clearly favor either growth rate, it would be interesting to extend the model of [4] to take composite numbers into account. We will not explore this matter further here.

TABLE 1. Record Values of $\hat{g}(p)$ for $p < 2^{31}$.

p	$\hat{g}(p)$	$\frac{\hat{g}(p)}{e^{\gamma}\log p(\log\log p)^2}$
3	2	115.559706
7	3	1.953084
23	5	0.685570
41	7	0.614838
109	11	0.551000
191	19	0.738260
271	43	1.451413
2791	53	0.874297
11971	79	0.941673
31771	107	1.059694
190321	149	1.102962
2080597	151	0.812905
3545281	163	0.824196
4022911	211	1.051558
73189117	223	0.824189
137568061	263	0.917462
443571241	277	0.873004
565822531	307	0.948147
1160260711	347	1.011101
1622723341	349	0.990421

ACKNOWLEDGEMENTS

Preparation of this paper was supported in part by the National Science Foundation, via grants DCR-9208639 and CCR-9510244. I would also like to thank the referees for helpful comments on an earlier version.

REFERENCES

1. N. C. Ankeny, *The least quadratic non residue*, Ann. Math. **55** (1952), 65–72. MR **13:**538c
2. E. Bach, *Fast algorithms under the extended Riemann hypothesis: a concrete estimate*, Proc. 14th Ann. ACM Symp. Theor. Comput., ACM, New York, 1982, pp. 290–295.
3. E. Bach, *Analytic Methods in the Analysis and Design of Number-theoretic Algorithms*, MIT Press, Cambridge, 1985. MR **87i:**11185
4. E. Bach and L. Huelsbergen, *Statistical evidence for small generating sets*, Math. Comp. **61** (1993), 69–82. MR **93k:**11089
5. E. Bach, *Improved approximations for Euler products*, in Number Theory: Fourth Conference of the Canadian Number Theory Association (K. Dichler, ed.), AMS, 1995, pp. 13–28. MR **96i:**11124
6. M. B. Barban, A. I. Vinogradov, and B. V. Levin, *Limit laws for functions of the class H of I. P. Kubilius which are defined on a set of "shifted" primes*, Litovskii Mat. Sb. **5** (1965), 5–8. (Russian) MR **34:**5974
7. A. Cunningham, *Solution to problem 14327*, Math. Questions Educ. Times **73** (1900), 45–47.
8. A. E. Ingham, *The Distribution of Prime Numbers*, Cambridge Univ. Press, 1932. MR **91f:**11064
9. T. Itoh, *How to recognize a primitive root modulo a prime*, unpublished manuscript, 1989.
10. E. Landau, *Über den Verlauf der zahlentheoretischen Funktion* $\varphi(x)$, Arch. Math. Phys. **5** (1903), 92–103.

11. H. L. Montgomery, *Topics in Multiplicative Number Theory*, Springer-Verlag, New York, 1971. MR **49:**2616
12. L. Murata, *On the magnitude of the least primitive root*, J. Number Theory **37** (1991), 47-66. MR **91j:**11082
13. C. Pomerance, *Fast, rigorous factorization and discrete logarithm algorithms*, in Discrete Algorithms and Complexity (D. S. Johnson, et al., eds.), Academic Press, 1987, pp. 119-143. MR **88m:**11109
14. G. Robin, *Estimation de la fonction de Tchebychef* Θ *sur le* k*-ième nombre premier et grandes valeurs de la fonction* $\omega(n)$*, nombre de diviseurs de* n, Acta Arith **42** (1983), 367–389. MR **85j:**11109
15. J. O. Shallit, *On the worst case of three algorithms for computing the Jacobi symbol*, J. Symbol. Comput. **10** (1990), 593–610. MR **91m:**11112
16. D. Shanks, *Class number, a theory of factorization, and genera.*, Proc. Symposia Pure Math. **20** (1971), 415–440. MR **47:**4932
17. V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp. **58** (1992), 369–380. MR **92e:**11140
18. I. Shparlinski, *On finding primitive roots in finite fields*, Theoret. Comput. Sci. **157** (1996), 273–275. MR **97a:**11203
19. Y. Wang, *On the least primitive root of a prime*, Acta Math. Sinica **9** (1959), 432–441 (Chinese), English translation in Sci. Sinica **10** (1961), 1-14. MR **22:**4659; MR **24:**A702
20. A. E. Western and J. C. P. Miller, *Tables of Indices and Primitive Roots*, Cambridge University Press, 1968 (Royal Society Math. Tables vol. 9). MR **39:**7792

Computer Sciences Department, University of Wisconsin, 1210 W. Dayton St., Madison, Wisconsin 53706

E-mail address: bach@cs.wisc.edu