Journal of Number Theory **88**, 49–58 (2001)
doi:10.1006/jnth.2000.2604, available online at http://www.idealibrary.com on IDEAL®

On the Distribution of Small Powers of a Primitive Root

C. I. Cobeli

Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, 70700 Bucharest, Romania
E-mail: ccobeli@stoilow.roimar.imar.ro

S. M. Gonek[1]

Department of Mathematics, University of Rochester, Rochester, New York 14627
E-mail: gonek@math.rochester.edu

and

Department of Mathematics and Statistics, McGill University, Burnside Hall, 805 Sherbrooke Street West, Montreal, Quebec, Canada, H3A-2K6; and Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, 70700 Bucharest, Romania
E-mail: zaharescu@math.mcgill.ca

Communicated by D. Goss

Received June 7, 1999

Let $\mathcal{N}_g = \{g^n : 1 \leqslant n \leqslant N\}$, where g is a primitive root modulo an odd prime p, and let $f_g(m, H)$ denote the number of elements of $\mathcal{N}_g$ that lie in the interval $(m, m+H]$, where $1 \leqslant m \leqslant p$. H. Montgomery calculated the asymptotic size of the second moment of $f_g(m, H)$ about its mean for a certain range of the parameters N and H and asked to what extent this range could be increased if one were to average over all the primitive roots (mod p). We address this question as well as the related one of averaging over the prime p. © 2001 Academic Press

1. INTRODUCTION AND STATEMENT OF RESULTS

Let g be a primitive root modulo an odd prime p and let

$$\mathcal{N}_g = \{g^n : 1 \leqslant n \leqslant N\},$$

[1] Research of the second author was supported in part by a grant from the National Science Foundation.

0022-314X/01 $35.00

where $N \leqslant p$. A number of authors (see, for example, [2–6]) have investigated the degree to which the elements of $\mathcal{N}_g$ are well-distributed among the numbers 1, ..., p. Such questions are of interest not only in number theory, but increasingly in computer science as well. In fact, Montgomery's paper [4], which motivated the present article, arose in response to a question about the running time of the Quicksort algorithm. To study the distribution of the elements of $\mathcal{N}_g$ in short intervals, Montgomery defined the function

$$f(m, H) = f_g(m, H) = |\{n \in (m, m+H] : n \equiv n' \ (\mathrm{mod}\ p),\, n' \in \mathcal{N}_g\}|$$

and computed the second moment of $f_g(m, H)$ about its mean. Since each element of $\mathcal{N}_g$ is counted in exactly H of the intervals $(m, m+H]$ as H varies from 1 to p, this mean is

$$\frac{1}{p} \sum_{m=1}^{p} f_g(m, H) = NH/p.$$

Montgomery showed that

$$\sum_{m=1}^{p} (f_g(m, H) - NH/p)^2 \sim NH, \tag{1}$$

uniformly for $NH \approx p$ and $p^{5/7+\varepsilon} \leqslant N = o(p)$, and from this he easily deduced (for the same range of the parameters N and H) that a positive proportion of the intervals $(m, m+H]$ contain an element of $\mathcal{N}_g$. Montgomery noted that if the Generalized Lindelöf Hypothesis holds, then the exponent 5/7 can be reduced to 2/3, and that this is almost certainly the limit of his method. He also remarked that it would be interesting to know how much the range of N might be enlarged if one were to average over the choice of primitive root. In this direction Konyagin and Shparlinski [2] recently proved that

$$\frac{1}{\phi(p-1)} \sum_{g \in \mathcal{G}_p} \left| \sum_{m=1}^{p} (f_g(m, H) - NH/p)^2 - NH \right| \ll NH^2 p^{-1} + N^3 H p^{-1/2+\varepsilon},$$

where $\mathcal{G}_p$ denotes the set of all $\phi(p-1)$ primitive roots (mod p). From this one sees that

$$\frac{1}{\phi(p-1)} \sum_{g \in \mathcal{G}_p} \sum_{m=1}^{p} (f_g(m, H) - NH/p)^2 \sim NH, \tag{2}$$

uniformly for $NH \approx p$ and $p^{\varepsilon} \leqslant N \leqslant p^{1/4-\varepsilon}$. Of course from (1) it follows that this also holds in the range $p^{5/7+\varepsilon} \leqslant N = o(p)$, and Konyagin and Shparlinski pose the problem of narrowing the gap in N. Our first theorem allows us to do this.

THEOREM 1. *Let p be an odd prime, H and N positive integers $\leqslant p$, and let $f_g(m, H)$ be as above. Then we have*

$$\frac{1}{\phi(p-1)} \sum_{g \in \mathcal{G}_p} \left| \sum_{m=1}^{p} (f_g(m, H) - NH/p)^2 - NH \right| \\ \ll NH(N+H)\, p^{-1} + H^{3/2} p^{1/2} (\log p)^3.$$

On taking $NH \approx p$ in Theorem 1, we easily deduce that (2) holds for $p^{2/3+\varepsilon} \leqslant N \leqslant p^{1-\varepsilon}$. Another deduction is that in this same range (1) holds for almost all primitive roots (mod p).

COROLLARY 1. *Let $\varepsilon > 0$ and let H and N be positive integers with $HN \approx p$ and $p^{2/3+\varepsilon} \leqslant N \leqslant p^{1-\varepsilon}$. Then, with the possible exception of at most $p^{1-\varepsilon/2}$ primitive roots g* (mod p), *we have*

$$\sum_{m=1}^{p} (f_g(m, H) - NH/p)^2 \sim NH.$$

Our next result is easily deduced from Corollary 1 in the same way that Montgomery [4] deduces the corollary to his Theorem 2. We therefore do not include the argument here.

COROLLARY 2. *Let $HN \approx p$, and $p^{2/3+\varepsilon} \leqslant N \leqslant p^{1-\varepsilon}$. Then with the possible exception of at most $p^{1-\varepsilon/2}$ primitive roots g* (mod p), *a positive proportion of the intervals $(m, m+H]$, $1 \leqslant m \leqslant p$, contain a member of $\mathcal{N}_g$.*

In the last section of the paper we take up a related question, namely, what can be said about the variance of $f_g(m, H)$ if for each prime p we take the "worst" primitive root and then average over the primes in a fixed interval $(P, 2P]$. Because of the dependence on p we now write $f_{p,g}(m, H)$ for $f_g(m, H)$ and $\mathcal{N}_{p,g}$ for $\mathcal{N}_g$. Our result is

THEOREM 2. *Let $\varepsilon > 0$ and let N, H, and P be positive integers with $NH \approx P$. Then for any positive integer k we have*

$$\sum_{\substack{p \in (P, 2P] \\ p \text{ prime}}} \max_{g \in \mathcal{G}_p} \left| \sum_{m=1}^{p} (f_{p,g}(m, H) - NH/p)^2 - NH \right| \\ \ll_k P(N+H) \log P^{-1} + (PH)^{3/2 - 1/2k + \varepsilon} (H^{1/2} + P^{1/k}). \tag{3}$$

If we choose k optimally with respect to N (or H) we obtain the following analogue of Corollary 1.

COROLLARY 3. *Let $\varepsilon > 0$ and let N, H, and P be positive integers with $NH \approx P$ and $P^{19/27+\varepsilon} \leqslant N \leqslant P^{1-\varepsilon}$. Then with the possible exception of at most $O(P^{1-\varepsilon/2})$ primes $p \in (P, 2P]$, we have for every primitive root g* (mod p)

$$\sum_{m=1}^{p} (f_{p,g}(m, H) - NH/p)^2 \sim NH.$$

Our final result follows from Corollary 3 in the same way that Corollary 2 follows from Corollary 1.

COROLLARY 4. *Assume the same hypotheses as in Corollary 3. With the possible exception of at most $P^{1-\varepsilon/2}$ primes $p \in (P, 2P]$, for every primitive root g (mod p) a positive proportion of the intervals $(m, m+H]$, $1 \leqslant m \leqslant p$, contain a member of $\mathcal{N}_{g,p}$.*

2. PROOF OF THEOREM 1

For h relatively prime to p we write $\chi_g(h) = e(\mathrm{ind}_g(h)/(p-1))$, where $e(x) = e^{2\pi i x}$ and $\mathrm{ind}_g(h)$ denotes the index of h with respect to the primitive root g (mod p). We also write

$$S(\chi) = \sum_{|h| \leqslant H} \left(1 - \frac{|h|}{H}\right) \chi(h)$$

for any Dirichlet character χ. We begin with the formula

$$\sum_{m=1}^{p} (f_g(m, H) - NH/p)^2 = NH(1 - H/p)(1 - N/p) + O\left(p^{-3/2} H \sum_{s=1}^{(p-1)/2} c_s \, |S(\chi_g^s)|\right), \tag{4}$$

which follows from (6.1), (6.5), (6.6), (2.3), and the estimate above (6.7) in Montgomery [4]. Here c_s is defined by

$$c_s = \begin{cases} pN & \text{if } \; 1 \leqslant s \leqslant p/N, \\ p^2 s^{-1} \log(2Ns/p) & \text{if } \; p/N \leqslant s \leqslant (p-1)/2. \end{cases} \tag{5}$$

Note that if $s \leqslant p/N$, then $c_s = pN \leqslant p^2/s$, so we may replace c_s in (4) by $(p^2 \log p)/s$ throughout the range $1 \leqslant s \leqslant (p-1)/2$. Doing this and averaging the result over all the primitive roots (mod p), we find that

$$\begin{aligned}
\frac{1}{\phi(p-1)} \sum_{g \in \mathscr{G}_p} \left| \sum_{m=1}^{p} (f_g(m, H) - NH/p)^2 - NH \right| \\
&\ll NH(N+H)\, p^{-1} + Hp^{-1/2} (\log p)^2 \sum_{s=1}^{(p-1)/2} s^{-1} \left(\sum_{g \in \mathscr{G}_p} |S(\chi_g^s)| \right) \\
&= NH(N+H)\, p^{-1} + Hp^{-1/2} (\log p)^2\, \mathscr{E}, \qquad (6)
\end{aligned}$$

say. We now fix an arbitrary primitive root g. Since every other primitive root is of the form g^m, with $1 \leqslant m < p-1$ and $(m, p-1) = 1$, we see that

$$\mathscr{E} = \sum_{s=1}^{(p-1)/2} s^{-1} \left(\sum_{\substack{m=1 \\ (m,\, p-1)=1}}^{p-1} |S(\chi_{g^m}^s)| \right).$$

Now for every h relatively prime to p, there is a unique r with $1 \leqslant r \leqslant p-1$, such that $h \equiv (g^m)^r \pmod p$. Hence we have

$$\begin{aligned}
\chi_{g^m}^{ml}(h) &= e\left(\frac{ml \operatorname{ind}_{g^m}(h)}{p-1} \right) = e\left(\frac{mlr}{p-1} \right) \\
&= e\left(\frac{l \operatorname{ind}_g(h)}{p-1} \right) = \chi_g^l(h).
\end{aligned}$$

If we write $ml = s$, so that $l \equiv s\bar{m} \pmod{p-1}$ with $\bar{m}$ the multiplicative inverse of m mod $p-1$, this becomes

$$\chi_{g^m}^s(h) = \chi_g^{s\bar{m}}(h).$$

Thus we see that

$$\begin{aligned}
\mathscr{E} &= \sum_{s=1}^{(p-1)/2} s^{-1} \left(\sum_{\substack{m=1 \\ (m,\, p-1)=1}}^{p-1} |S(\chi_g^{s\bar{m}})| \right) \\
&= \sum_{n=1}^{p-1} |S(\chi_g^n)| \left(\sum_{\substack{s=1 \\ (s\bar{n},\, p-1)=1}}^{(p-1)/2} s^{-1} \right) \\
&\ll \log p \sum_{n=1}^{p-1} |S(\chi_g^n)|.
\end{aligned}$$

As n varies from 1 to $p-1$ in the last sum, χ_g^n runs over all the characters (mod p), hence

$$\mathscr{E} \ll \log p \sum_{\chi (\mathrm{mod}\ p)} |S(\chi)|.$$

By the Cauchy–Schwarz inequality this is

$$\ll p^{1/2} \log p \left(\sum_{\chi (\mathrm{mod}\ p)} |S(\chi)|^2 \right)^{1/2}$$
$$= p^{1/2} \log p \left(\sum_{|h_1|,\, |h_2| \leqslant H} \ \sum_{\chi (\mathrm{mod}\ p)} (1-|h_1|/H)(1-|h_2|/H)\, \chi(h_1)\, \bar{\chi}(h_2) \right)^{1/2}.$$

The sum over χ equals 0 unless $h_1 \equiv h_2 (\mathrm{mod}\ p)$, in which case it equals $p-1$. Since $H \leqslant p$, the latter case occurs at most $O(1)$ times for each h_1, so we see that

$$\mathscr{E} \ll H^{1/2} p \log p.$$

Combining this with (6), we obtain Theorem 1.

3. PROOF OF COROLLARY 1

Let $\mathscr{G}_p^*$ be the subset of $\mathscr{G}_p$ consisting of those primitive roots g for which

$$\left| \sum_{m=1}^{p} \left(f_g(m, H) - \frac{NH}{p} \right)^2 - NH \right| \gg p^{1-\varepsilon/2}.$$

Then we have

$$|\mathscr{G}_p^*|\, p^{1-\varepsilon/2} \ll \sum_{g \in \mathscr{G}_p^*} \left| \sum_{m=1}^{p} \left(f_g(m, H) - \frac{NH}{p} \right)^2 - NH \right|$$
$$\ll \sum_{g \in \mathscr{G}_p} \left| \sum_{m=1}^{p} \left(f_g(m, H) - \frac{NH}{p} \right)^2 - NH \right|.$$

On the other hand, by our hypotheses and Theorem 1 this is

$$\ll \phi(p-1)(N + (p/N)^{3/2}\, p^{1/2} \log^3 p)$$
$$\ll p(p^{1-\varepsilon} + (p^{1/3-\varepsilon})^{3/2}\, p^{1/2} \log^3 p)$$
$$\ll p^{2-\varepsilon}.$$

It follows that

$$|\mathscr{G}_p^*| \ll p^{1-\varepsilon/2}.$$

4. PROOF OF THEOREM 2

Given N, H, and P with $NH \approx P$, for each $p \in (P, 2P]$ we let g_p denote any primitive root (mod p) for which the maximum

$$\max_{g \in \mathscr{G}_p} \left| \sum_{m=1}^{p} (f_{p,g}(m, H) - NH/p)^2 - NH \right|$$

is attained. Then we must show that

$$\sum_{\substack{p \in (P, 2P] \\ p \text{ prime}}} \left| \sum_{m=1}^{p} (f_{g_p}(m, H) - NH/p)^2 - NH \right|$$
$$\ll_k (N+H)\, P(\log P)^{-1} + (PH)^{3/2 - 1/2k + \varepsilon} (H^{1/2} + P^{1/k}).$$

Replacing g in (4) by g_p and summing over $p \in (P, 2P]$, we obtain

$$\begin{aligned} &\sum_{\substack{p \in (P, 2P] \\ P \text{ prime}}} \left| \sum_{m=1}^{p} (f_{g_p}(m, H) - NH/p)^2 - NH \right| \\ &\quad \ll (N+H)\, P(\log P)^{-1} + HP^{-3/2} \sum_{\substack{p \in (P, 2P] \\ p \text{ prime}}} \sum_{s=1}^{(p-1)/2} c_s\, |S(\chi_{g_p}^s)| \\ &\quad = (N+H)\, P(\log P)^{-1} + \mathscr{E}', \end{aligned} \tag{7}$$

say, where

$$\chi_{g_p}(h) = e(\operatorname{ind}_{g_p}(h)/(p-1)).$$

We estimate $\mathscr{E}'$ by splitting the sum over s into the blocks

$$\begin{aligned} I_0 &= [1, p/N], \\ I_1 &= [p/N, 2p/N], \ldots, I_j = [2^{j-1}p/N, 2^j p/N], \ldots, \\ I_{J-1} &= [2^{J-2}p/N, 2^{J-1}p/N], \\ I_J &= [2^{J-1}p/N, (p-1)/2], \end{aligned}$$

where $J=[\log((1-1/p)\,N)/\log 2] \ll \log P$. Assuming that the j_0^{th} block makes the largest contribution to $\mathscr{E}'$, we see that

$$\mathscr{E}' \ll HP^{-3/2}\log P \sum_{\substack{p\in(P,2P]\\ p\ prime}} \sum_{s\in I_{j_0}} c_s\,|S(\chi_{g_p}^s)|.$$

Now by (5),

$$c_s \ll P^2 \log P/(2^{j_0}H)$$

uniformly for $s\in I_{j_0}$. Hence

$$\mathscr{E}' \ll 2^{-j_0}P^{1/2}(\log P)^2 \sum_{\substack{p\in(P,2P]\\ p\ prime}} \sum_{s\in I_{j_0}} |S(\chi_{g_p}^s)|.$$

We apply Holder's inequality to the double sum on the right and obtain

$$\mathscr{E}' \ll 2^{-j_0}P^{1/2}(\log P)^2\,(P(\log P)^{-1}\,|I_{j_0}|)^{1-1/2k}\Bigg(\sum_{\substack{p\in(P,2P]\\ p\ prime}} \sum_{s\in I_{j_0}} |S(\chi_{g_p}^s)|^{2k}\Bigg)^{1/2k},$$

where k is a positive integer. Then, since

$$|I_{j_0}| \approx 2^{j_0}P/N \approx 2^{j_0}H,$$

we have

$$\mathscr{E}' \ll P^{3/2-1/2k+\varepsilon}H^{1-1/2k}\Bigg(\sum_{\substack{p\in(P,2P]\\ p\ prime}} \sum_{s\in I_{j_0}} |S(\chi_{g_p}^s)|^{2k}\Bigg)^{1/2k}.$$

We next write

$$\begin{aligned}(S(\chi_{g_p}^s))^k &= \Bigg(\sum_{|h|\leqslant H}\left(1-\frac{|h|}{H}\right)\chi_{g_p}^s(h)\Bigg)^k\\ &= \sum_{|h|\leqslant H^k} a(h)\,\chi_{g_p}^s(h),\end{aligned}$$

where

$$a(h) \ll d_k(h), \tag{8}$$

d_k being the kth divisor function. We may then write

$$\mathscr{E}' \ll P^{3/2-1/2k+\varepsilon} H^{1-1/2k} \Bigg(\sum_{\substack{p \in (P, 2P] \\ p \text{ prime}}} \sum_{s \in I_{j_0}} \Bigg| \sum_{|h| \leqslant H^k} a(h) \, \chi_{g_p}^s(h) \Bigg|^2 \Bigg)^{1/2k}.$$

The characters $\chi_{g_p}^s$ are all primitive, so we can apply Gallagher's form of the large sieve inequality for character sums [1] to estimate the expression in parentheses. Using (8) as well, we find that

$$\mathscr{E}' \ll P^{3/2-1/2k+\varepsilon} H^{1-1/2k} \Bigg((H^k + P^2) \sum_{|h| \leqslant H^k} |d_k(h)|^2 \Bigg)^{1/2k}.$$

Since $\sum_{h \leqslant x} d_k^2(h) \ll_k x (\log x)^{k^2-1}$, this is

$$\ll_k P^{3/2-1/2k+\varepsilon} H^{3/2-1/2k+\varepsilon} (H^{1/2} + P^{1k}).$$

Finally, we insert this estimate for $\mathscr{E}'$ into (7) and obtain (3).

5. PROOF OF COROLLARY 3

If for some range of the parameters H and N the right-hand side of (3) is $\ll P^{2-\varepsilon}$, then Corollary 3 will follow (for these values of H and N) by the same argument used to deduce Corollary 1. Suppose, to begin with, that $P^\varepsilon \ll N \ll P^{1-\varepsilon}$, that $NH \approx P$, and that $k < 100$, say. The right-hand side of (3) is then

$$\ll P^{2-\varepsilon} + (PH)^{3/2-1/2k+\varepsilon} \, (H^{1/2} + P^{1/k}),$$

and we require that

$$(PH)^{3/2-1/2k+\varepsilon} \, (H^{1/2} + P^{1/k}) \ll P^{2-\varepsilon}.$$

This means that H must satisfy the two inequalities

$$P^{3/2-1/2k+\varepsilon} H^{2-1/2k+\varepsilon} \ll P^{2-\varepsilon} \qquad \text{and} \qquad P^{3/2+1/2k+\varepsilon} H^{3/2-1/2k+\varepsilon} \ll P^{2-\varepsilon}.$$

These are equivalent to

$$H^{(4k-1)/2k+\varepsilon} \ll P^{(k+1)/2k-2\varepsilon} \qquad \text{and} \qquad H^{(3k-1)/2k+\varepsilon} \ll P^{(k-1)/2k-2\varepsilon},$$

or

$$H \ll P^{\min\{(k+1)/(4k-1),\,(k-1)/(3k-1)\}-3\varepsilon}.$$

As we are free to choose the positive integer k, we do this in such a way that it allows for the maximal possible size of H. Now the function $f_1(x)=\frac{x+1}{4x-1}$ is decreasing on $[1, \infty)$, while the function $f_2(x)=\frac{x-1}{3x-1}$ is increasing on $[1, \infty)$. Thus $f(x)=\min\{\frac{x+1}{4x-1}, \frac{x-1}{3x-1}\}$ has a global maximum when $f_1(x)=f_2(x)$, and this occurs at $x=(7+\sqrt{41})/2\approx 6.7$. The optimal k is therefore either 6 or 7. We have $f(6)=f_2(6)=5/17$ and $f(7)=f_1(7)=8/27$. The larger of these two is 8/27, so (9) holds with $H\ll P^{8/27-\varepsilon}$. In terms of N, since $NH\approx P$ and $P^{\varepsilon}\ll N\ll P^{1-\varepsilon}$, we find that (9) holds provided that $P^{19/27+\varepsilon}\ll N\ll P^{1-\varepsilon}$. This completes the proof of Corollary 3.

REFERENCES

1. H. Davenport, "Multiplicative Number Theory," 2nd ed., revised by H. L. Montgomery, Springer-Verlag, New York, 1980.
2. S. Konyagin and I. Shparlinski, "Exponential Sums with Finitely Generated Groups and Their Applications," Cambridge Univ. Press, Cambridge, UK, 1999.
3. N. M. Korobov, On the distribution of digits in periodic fractions, *Math. USSR Sb.* **18** (1972), 654–670.
4. H. L. Montgomery, Distribution of small powers of a primitive root, *in* "Advances in Number Theory, Kingston, ON, 1991," pp. 137–149, Oxford Univ. Press, New York, 1993.
5. H. Niederreiter, Quasi-Monte Carlo methods and pseudo-random numbers, *Bull. Amer. Math. Soc.* **84** (1978), 957–1041.
6. I. E. Shparlinski, "Computational Problems in Finite Fields," Kluwer Academic, North-Holland, 1992.