PORTUGALIAE MATHEMATICA
Vol. 59 Fasc. 2 – 2002
Nova Série

ON THE SET $a\,x + b\,g^x \pmod{p}$

Cristian Cobeli, Marian Vâjâitu and Alexandru Zaharescu

Abstract: Given nonzero integers a, b we prove an asymptotic result for the distribution function of the set $a\,x + b\,g^x \pmod{p}$, as p goes to infinity and g is a primitive root mod p.

1 – Introduction

Various aspects of the distribution of powers of a primitive root g modulo a large prime number p have been investigated by a number of authors (see for example [2], [3], [4], [6], [7], [8]). In this paper we fix nonzero integers a, b and study the distribution function of the set $a\,x + b\,g^x \pmod{p}$, as p goes to infinity and g is a primitive root mod p. In particular we are interested in the distance between x and g^x as x runs over the set $\{1, 2, ..., p-1\}$. Throughout this paper g^x means the least positive residue of g^x mod p. We also consider a short interval version of the problem, more precisely we fix two intervals $\mathcal{I}$, $\mathcal{J}$ and work only with those integers $x \in \mathcal{I}$ for which $g^x \pmod{p}$ belongs to $\mathcal{J}$. In the following we let $\mathcal{I} = \{0, 1, ..., M-1\}$, $\mathcal{J} = \{0, 1, ..., N-1\}$ with M, N positive integers $\leq p$ and denote $\mathcal{M} = \{x \in \mathcal{I}\colon\ g^x \in \mathcal{J},\ a\,x + b\,g^x < t\}$. The distribution function is given by $D(t) = D(a, b, p, g, \mathcal{I}, \mathcal{J}, t) = \#\mathcal{M}$. Replacing if necessary a, b and t by $-a, -b$ and $-t$ respectively, we may assume in the following that $b > 0$. We now introduce a function $G(t, a, b, M, N)$ which will appear in the estimation of $D(t)$.

Received: November 15, 2000; *Revised*: April 27, 2001.
AMS Subject Classification: 11A07.

If $a > 0$ we set

$$G(t,a,b,M,N) = \begin{cases} 0, & \text{if } t < 0, \\ \dfrac{t^2}{2\,a\,b}, & \text{if } 0 \le t < U, \\ \dfrac{U^2}{2\,a\,b} + \dfrac{U(t-U)}{a\,b}, & \text{if } U \le t < V, \\ MN - \dfrac{(a\,M + b\,N - t)^2}{2\,a\,b}, & \text{if } V \le t < aM + bN, \\ MN, & \text{if } aM + bN \le t\ , \end{cases}$$

where $U = \min\{aM, bN\}$ and $V = \max\{aM, bN\}$. If $a < 0$ then we let

$$G(t,a,b,M,N) = \begin{cases} 0, & \text{if } t < aM, \\ -\dfrac{(t-a\,M)^2}{2\,a\,b}, & \text{if } aM \le t \le W, \\ \left(MN + \dfrac{(W-aM)^2}{a\,b}\right)\dfrac{t-W}{Z-W} - \dfrac{(W-aM)^2}{2\,a\,b}, & \text{if } W < t < Z, \\ MN + \dfrac{(t-b\,N)^2}{2\,a\,b}, & \text{if } Z \le t < bN, \\ MN, & \text{if } bN \le t\ , \end{cases}$$

where $W = \min\{0,\, bN + aM\}$ and $Z = \max\{0,\, bN + aM\}$. We will prove the following

Theorem 1. *For any a, b, p, g, $\mathcal{I}$, $\mathcal{J}$, t as above one has*

$$D(a,b,p,g,\mathcal{I},\mathcal{J},t) = \frac{G(t,a,b,M,N)}{p} + O_{a,b}(p^{1/2} \log^3 p)\ .$$

It is well established that the discrete exponential map $x \mapsto g^x \bmod p$ is a "random" map, and this is used by random number generators which use the linear congruential method [1]. There are various ways to check this randomness. For instance, if we count those $x \in \{1, 2, ..., p-1\}$ for which $g^x < x$, respectively those x for which $g^x > x$ there should be no bias towards any one of these inequalities, in other words one would expect that about half of the x's are larger than g^x and half of the x's are smaller than g^x. We can actually prove this statement by using Theorem 1.

Corollary 1. *One has*

$$\left| \#\Big\{0 \le x \le p-1 \colon\ x > g^x\Big\} - \frac{p}{2} \right| \le 7\,p^{1/2}(1+\log p)^3 \ .$$

As another application of Theorem 1 we have the following asymptotic result for all even moments of the distance between x and g^x.

Corollary 2. *Let k be a positive integer. Then we have*

$$M(p,g,2\,k) := \sum_{x=0}^{p-1} (g^x - x)^{2k} \ = \ \frac{p^{2k+1}}{(k+1)\,(2\,k+1)} + O_k(p^{2k+1/2}\ \log^3 p) \ .$$

In particular, for $k=1$ one has

$$M(p,g,2) \ = \ \frac{p^3}{6} + O(p^{5/2}\ \log^3 p) \ .$$

This says that in quadratic average $|g^x - x|$ is $\sim \frac{p}{\sqrt{6}}$.

2 – Setting the problem

We will need a bound for the exponential sum

$$S(m,n,g,p) \ = \ \sum_{z=0}^{p-1} e_p(m\,z + n\,g^z) \ ,$$

where m,n are integers and $e_p(t) = e^{\frac{2\pi i t}{p}}$. This problem was handled by Mordell [5].

Lemma 1 (Mordell)**.** *Let p be a prime, g a primitive root mod p and m,n integers, not both multiples of p. Then*

$$|S(m,n,g,p)| \ < \ 2\,p^{1/2}(1+\log p) \ . \ \blacksquare$$

The next lemma allows us to compute quite general sums involving x and g^x.

Lemma 2. *Let $\mathcal{U}$, $\mathcal{V}$ be subsets of $\{0,1,...,p-1\}$, let f be a complex valued function defined on $\mathcal{U}\times\mathcal{V}$ and consider the transform*

$$\check{f}(m,n) \;=\; \sum_{(x,y)\in\mathcal{U}\times\mathcal{V}} f(x,y)\, e_p(m\,x+n\,y)\;.$$

Then

$$\sum_{\substack{(x,y)\,\in\mathcal{U}\times\mathcal{V}\\ y\,\equiv\, g^x \pmod p}} f(x,y) \;=\; \frac{1}{p^2}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1}\check{f}(m,n)\; S(-m,-n,g,p)\;.$$

Proof: Using the definition, the right hand side can be written as

$$\begin{aligned}
\frac{1}{p^2}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1}\check{f}(m,n)\,S(-m,-n,g,p) \;=\\
&= \frac{1}{p^2}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1}\sum_{(x,y)\in\mathcal{U}\times\mathcal{V}} f(x,y)\,e_p(mx+ny)\sum_{z=0}^{p-1} e_p(-m\,z-n\,g^z)\\
&= \frac{1}{p^2}\sum_{(x,y)\in\mathcal{U}\times\mathcal{V}} f(x,y)\sum_{z=0}^{p-1}\sum_{m=0}^{p-1} e_p(m(x-z))\sum_{n=0}^{p-1} e_p(n(y-g^z))\;.
\end{aligned}$$

Here the sum over n is zero unless $y\equiv g^z \pmod p$ when it equals p. Similarly, since $0<x,z\le p-1$ the sum over m is zero unless $x=z$ when it equals p. Thus the sum over z is zero if $y\not\equiv g^x \pmod p$ and it equals p^2 if $y\equiv g^x \pmod p$, which proves the statement of the lemma. ∎

We will apply Lemma 2 with $\mathcal{U}=\mathcal{I}$, $\mathcal{V}=\mathcal{J}$ and

$$f(x,y) \;=\; f(t,x,y,a,b) \;=\; \begin{cases} 1, & \text{if } \; a\,x+b\,y<t,\\ 0, & \text{if } \; a\,x+b\,y\ge t\;. \end{cases} \tag{1}$$

Then the distribution function is given by

$$D(t) \;=\; \sum_{\substack{(x,y)\in\mathcal{I}\times\mathcal{J}\\ y\equiv g^x \pmod p}} f(x,y) \tag{2}$$

and this is a sum as in Lemma 2. The coefficients $\check{f}(m,n)$ can be estimated accurately, as we will see in the next section.

3 – Proof of Theorem 1

In what follows we assume that $0 \le m, n \le p-1$. We find an upper bound for $\check{f}(m,n) = \check{f}(t,m,n,a,b)$ which is independent of t and then calculate explicitly $\check{f}(0,0)$, which gives the main term of $D(t)$. There are four cases.

I. $m=0$, $n \ne 0$. We have

$$\check{f}(t,0,n,a,b) \;=\; \sum_{(x,y)\in \mathcal{I}\times\mathcal{J}} f(x,y)\; e_p(n\,y)\;.$$

By the definition of $f(x,y)$ it follows that for each $x \in \mathcal{I}$ we have a sum of $e_p(ny)$ with y running in a subinterval of $\mathcal{J}$, that is a sum of a geometric progression with ratio $e_p(n)$. The absolute value of such a sum is $\le \frac{2}{|e_p(n)-1|}$ and consequently

$$|\check{f}(t,0,n,a,b)| \;\le\; |\mathcal{I}|\,\frac{2}{|e_p(n)-1|} \;=\; \frac{M}{\sin\frac{n\,\pi}{p}} \;\le\; \frac{M}{2\left\|\frac{n}{p}\right\|}\,, \tag{3}$$

where $\|\cdot\|$ denotes the distance to the nearest integer.

II. $m \ne 0$, $n=0$. Similarly, as in case **I**, we have

$$|\check{f}(t,m,0,a,b)| \;\le\; \frac{N}{2\left\|\frac{m}{p}\right\|}\;. \tag{4}$$

III. $m \ne 0$, $n \ne 0$. We need the following lemma.

Lemma 3. *Let $h, k \not\equiv 0 \pmod p$, L, T and $u \ge 0$ be integers. Let $S = \sum_{x=0}^{L}\sum_{y=0}^{ux+T} e_p(hx)\, e_p(ky)$. Then one has*

$$|S| \;\le\; \frac{1}{4\left\|\frac{k}{p}\right\|}\,\min\left\{L,\,\frac{1}{2\left\|\frac{h+u\,k}{p}\right\|}\right\} + \frac{1}{4\left\|\frac{k}{p}\right\|}\cdot\frac{1}{2\left\|\frac{h}{p}\right\|}\;. \;\blacksquare$$

The proof is left to the reader. We now return to the estimation of $\check{f}(m,n)$. Writing

$$\check{f}(m,n) \;=\; \sum_{\substack{(x,y)\in\mathcal{I}\times\mathcal{J}\\ ax+by\,<\,t}} e_p(m\,x+n\,y)$$

as a sum of b sums according to the residue of x modulo b, one arrives at sums as in Lemma 3, with $h = m\,b$, $k = n$, $u = -a$. It follows that

$$|\check{f}(t,m,n,a,b)| \ll_{a,b} \frac{1}{2\left\|\frac{n}{p}\right\|} \min\left\{M, \frac{1}{2\left\|\frac{m\,b-a\,n}{p}\right\|}\right\} + \frac{1}{2\left\|\frac{n}{p}\right\|} \cdot \frac{1}{2\left\|\frac{mb}{p}\right\|} \ . \tag{5}$$

IV. $m,n = 0$. By definition, we have

$$\check{f}(t,0,0,a,b) = \sum_{(x,y)\in\mathcal{I}\times\mathcal{J}} f(t,x,y,a,b) \ .$$

Let $\mathcal{D}$ be the set of real points from the rectangle $[0,M)\times[0,N)$ which lie below the line $a\,x + b\,y = t$. Then $\check{f}(t,0,0,a,b)$ equals the number of integer points from $\mathcal{D}$. Therefore

$$\check{f}(t,0,0,a,b) = \text{Area}(\mathcal{D}) + O(\text{length}(\partial\mathcal{D})) \ .$$

An easy computation shows that Area$(\mathcal{D})$ equals the expression $G(t,a,b,M,N)$ defined in the Introduction, while the length of the boundary $\partial\mathcal{D}$ is $\le 2\,M + 2\,N \le 4\,p$. Hence

$$\check{f}(t,0,0,a,b) = G(t,a,b,M,N) + O(p) \ .$$

By (2) and Lemma 2 we know that

$$\left| D(t) - \frac{1}{p^2}\,\check{f}(0,0)\,S(0,0,g,p)\right| \le D_1 + D_2 + D_3 \ ,$$

where

$$D_1 = \frac{1}{p^2}\sum_{m=1}^{p-1} |\check{f}(m,0)|\;|S(m,0,g,p)|\,, \qquad D_2 = \frac{1}{p^2}\sum_{n=1}^{p-1} |\check{f}(0,n)|\;|S(0,n,g,p)|$$

and

$$D_3 = \frac{1}{p^2}\sum_{m=1}^{p-1}\sum_{n=1}^{p-1} |\check{f}(m,n)|\;|S(m,n,g,p)| \ .$$

One has

$$\frac{1}{p^2}\,\check{f}(0,0)\,S(0,0,g,p) = \frac{\check{f}(0,0)}{p} = \frac{G(t,a,b,M,N)}{p} + O(1) \ .$$

Next, since $S(m,0,g,p) = \sum_{x=0}^{p-1} e_p(mx) = 0$ for $1 \le m \le p-1$, it follows that $D_1 = 0$. By (3) and Lemma 1 we have

$$\begin{aligned} D_2 \ &\le \ \frac{1}{p^2}\sum_{n=1}^{p-1} \frac{M}{\left\|\frac{n}{p}\right\|}\, p^{1/2}(1+\log p) \ = \ 2\,M\,p^{-3/2}(1+\log p)\sum_{n=1}^{\frac{p-1}{2}} \frac{p}{n} \\ &\le \ 2\,p^{1/2}(1+\log p)^2 \ . \end{aligned}$$

In order to estimate D_3 we first use Lemma 1 and (5) to obtain

$$(6)\quad D_3 \ll_{a,b} \frac{\log p}{p^{3/2}} \sum_{m=1}^{p-1}\sum_{n=1}^{p-1} \frac{1}{\left\|\frac{n}{p}\right\|} \min\left\{M, \frac{1}{\left\|\frac{mb-an}{p}\right\|}\right\} + \frac{\log p}{p^{3/2}} \sum_{m=1}^{p-1}\sum_{n=1}^{p-1} \frac{1}{\left\|\frac{n}{p}\right\|} \cdot \frac{1}{\left\|\frac{mb}{p}\right\|} .$$

The first double sum in (6) is

$$\sum_{m=1}^{p-1}\sum_{n=1}^{p-1} \frac{1}{\left\|\frac{n}{p}\right\|} \min\left\{M, \frac{1}{\left\|\frac{mb-an}{p}\right\|}\right\} \le$$

$$\le \sum_{n=1}^{p-1} \frac{1}{\left\|\frac{n}{p}\right\|} \sum_{\substack{m=1\\ mb-an\equiv 0 \pmod p}}^{p-1} p + \sum_{n=1}^{p-1} \frac{1}{\left\|\frac{n}{p}\right\|} \sum_{\substack{m=1\\ mb-an\not\equiv 0 \pmod p}}^{p-1} \frac{1}{\left\|\frac{mb-an}{p}\right\|}$$

$$\le p \sum_{n=1}^{\frac{p-1}{2}} \frac{p}{n} + \sum_{n=1}^{p-1} \frac{1}{\left\|\frac{n}{p}\right\|} \sum_{m'=1}^{p-1} \frac{1}{\left\|\frac{m'}{p}\right\|} \le p^2(1+\log p) + 4p^2(1+\log p)^2 ,$$

while the second double sum is

$$\sum_{m=1}^{p-1}\sum_{n=1}^{p-1} \frac{1}{\left\|\frac{n}{p}\right\|} \cdot \frac{1}{\left\|\frac{mb}{p}\right\|} = 4 \sum_{m=1}^{\frac{p-1}{2}} \frac{p}{m} \sum_{n=1}^{\frac{p-1}{2}} \frac{p}{n} \le 4p^2(1+\log p)^2 .$$

Hence $D_3 \ll_{a,b} p^{1/2} \log^3 p$. Putting all these together, Theorem 1 follows. ∎

4 – Proof of the Corollaries

For the proof of the first Corollary, let us notice that

$$\#\left\{0 \le x \le p-1 \colon\ x > g^x\right\} = D(a{=}-1,\, b{=}1,\, p, g, \mathcal{I}, \mathcal{J}, t=0)$$

with $\mathcal{I} = \mathcal{J} = \{0, 1, ..., p-1\}$. Here $M = N = p$, $W = Z = 0$ and so

$$G(t{=}0,\, a{=}-1,\, b{=}1,\, M{=}p,\, N{=}p) = -\frac{(a\,M-t)^2}{2\,a\,b} = \frac{p^2}{2} .$$

Thus

$$\#\left\{0 \le x \le p-1 \colon\ x > g^x\right\} = \frac{p}{2} + O(p^{\frac{1}{2}} \log^3 p) .$$

One obtains the more precise upper bound $7p^{\frac{1}{2}} \log^3 p$ for the error term by following the proof of Theorem 1 in this particular case.

To prove Corollary 2 note that

$$\begin{aligned} M(p,g,2k) &= \sum_{x=0}^{p-1}(g^x - x)^{2k} \\ &= \sum_{-p<t<p} t^{2k} \ \#\Big\{0 \le x,\ y \le p{-}1 :\ y \equiv g^x \ (\mathrm{mod}\, p),\ \ y - x = t\Big\}\ . \end{aligned}$$

This equals

$$\sum_{-p<t<p} t^{2k}\Big(D(t+1) - D(t)\Big) \ = \ D(p)\,(p-1)^{2k} \ + \sum_{-p<t<p} D(t)\,\Big((t-1)^{2k} - t^{2k}\Big)$$

where $D(t) = D(a{=}-1,\ b{=}1,\ p, g, \mathcal{I}, \mathcal{J}, t)$ with $\mathcal{I} = \mathcal{J} = \{0,1,...,p{-}1\}$. From Theorem 1 it follows that

$$\begin{aligned} M(p,g,2k) \ = \ & p^{2k-1}\, G(p,-1,1,p,p) \ + \ \frac{1}{p} \sum_{-p<t<p} G(t,-1,1,p,p)\,\Big((t-1)^{2k} - t^{2k}\Big) \\ & + \ O_k\Big(p^{2k+\frac12}\ \log^3 p\Big) \ + \ O\Big(p^{1/2}\ \log^3 p \sum_{-p<t<p} \Big|(t-1)^{2k} - t^{2k}\Big|\Big)\ . \end{aligned}$$

Since $(t-1)^{2k} - t^{2k} = -2\,k\,t^{2k-1} + O_k(p^{2k-2})$ and $0 \le G(t,-1,1,p,p) \le p^2$ we derive

$$\begin{aligned} M(p,g,2k) \ = \ & p^{2k-1}\, G(p,-1,1,p,p) \\ & - \ \frac{2\,k}{p} \sum_{-p<t<p} t^{2k-1}\, G(t,-1,1,p,p) \ + \ O_k\Big(p^{2k+\frac12}\ \log^3 p\Big)\ . \end{aligned}$$

From the definition of G we see that

$$G(t,-1,1,p,p) \ = \ \begin{cases} 0, & \text{if } \ t < -p, \\ \dfrac{(p+t)^2}{2}, & \text{if } \ -p \le t \le 0, \\ p^2 - \dfrac{(p-t)^2}{2}, & \text{if } \ 0 < t < p, \\ p^2, & \text{if } \ p \le t\ . \end{cases}$$

Using the fact that for any positive integer r one has $\sum_{-p<t<p} t^r = \frac{2\,p^{r+1}}{r+1} + O_r(p^r)$ if r is even and $\sum_{-p<t<p} t^r = 0$ if r is odd, the statement of Corollary 2 follows after a straightforward computation. ∎

ACKNOWLEDGEMENTS – We acknowledge the valuable discussions with S.M. Gonek on the subject.

REFERENCES

[1] Knuth, D. – *The Art of Computer Programming*, 2nd edition, Addison–Wesley, Reading, Mass, 1973.

[2] Konyagin, S. and Shparlinski, I. – *Character Sums With Exponential Functions and Their Applications*, Cambridge Tracts in Mathematics, 136, Cambridge University Press, Cambridge, 1999.

[3] Korobov, N.M. – On the distribution of digits in periodic fractions, *Math. USSR Sbornik,* 18(4) (1972), 654–670.

[4] Montgomery, H.L. – *Distribution of small powers of a primitive root*, in "Advances in Number Theory" (Kingston, ON, 1991), Oxford Sci. Publ., Oxford Univ. Press, New York, 1993, pp. 137–149. *Amer. Math. Soc.,* 111(2) (1991), 523–531.

[5] Mordell, L.J. – On the exponential sum $\sum_{x=1}^{X} \exp\bigl(2\pi i\,(a\,x + b\,g^x)/p\bigr)$, *Mathematika,* 19 (1972), 84–87.

[6] Niederreiter, H. – Quasi-Monte Carlo methods and pseudo-random numbers, *Bull. Amer. Math. Soc.,* 84 (1978), 957–1041.

[7] Rudnick, Z. and Zaharescu, A. – The distribution of spacings between small powers of a primitive root, *Israel J. Math.,* 120(A) (2000), 271–287.

[8] Shparlinski, I.E. – *Computational Problems in Finite Fields*, Kluwer Acad. Publ. North–Holland, 1992.

Cristian Cobeli, Marian Vâjâitu and Alexandru Zaharescu,
Institute of Mathematics of the Romanian Academy,
P.O. Box 1-764, 70 700 Bucharest – ROMANIA

E-mail: ccobeli@stoilow.imar.ro
mvajaitu@stoilow.imar.ro