ACTA ARITHMETICA
LXXXVII.3 (1999)

On characters of order p (mod p^2)

by

Leo Murata (Yokohama)

1. Statement of results. Let p be an odd prime number, and a be a natural number which is not divisible by p. We put, for $\nu \geq 1$,

$$r(a, p^\nu) = [(\mathbb{Z}/p^\nu\mathbb{Z})^\times : \langle a \bmod p^\nu \rangle],$$

where $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ denotes the multiplicative group of all irreducible residue classes modulo p^ν, $\langle a \bmod p^\nu \rangle$ the cyclic subgroup generated by the class $a \pmod{p^\nu}$, and [:] the index of the subgroup. This number $r(a, p^\nu)$ is called the *residual index of a modulo p^ν*. When $r(a, p^\nu) = 1$, we say that a is a *primitive root mod p^ν*.

In the present article, we shall make some observations about the distribution of primitive roots with respect to the moduli p and p^2. Since the distribution of primitive roots is closely related to other number-theoretical topics, such as the value distribution of Dirichlet characters, and the equidistribution property of the arguments of Gauss sums, we have some applications in these topics.

In this section we explain our results; the proofs are found in the second section.

The author expresses his sincere gratitude to his colleagues, S. Egami, P. Elliott, Y. Motohashi, G. Tenenbaum, for their kind suggestions.

First, we notice that $r(a, p^\nu)$ and $r(a, p^{\nu+1})$ are not independent. A residue class $a \pmod{p^\nu}$ splits into p residue classes modulo $p^{\nu+1}$:

$$\{a + kp^\nu \pmod{p^{\nu+1}} : k = 0, 1, \ldots, p-1\}.$$

Then we have the following relations.

Lemma. *Let $r(a, p^\nu) = R$ and $N = \frac{1}{R}(p-1)p^{\nu-1}$. Then*

1. *For any k, $r(a + kp^\nu, p^{\nu+1}) = R$ or Rp.*

1991 *Mathematics Subject Classification*: 11L05, 11L40, 11N25.

2. *If* $N \equiv 0 \pmod p$, *then for any* k, $r(a+kp^\nu, p^{\nu+1}) = R$. *If* $N \not\equiv 0 \pmod p$, *then there exists one and only one* $K = K(a,p^\nu)$, $0 \le K \le p-1$, *such that*

$$r(a+kp^\nu, p^{\nu+1}) = \begin{cases} Rp & \text{if } k = K, \\ R & \text{if } k \ne K. \end{cases}$$

From this lemma we see that, when a is a primitive root mod p, i.e. $\nu = 1$, $R = 1$ and $N = p-1$, then according to whether $K(a,p) \ne 0$ or $= 0$, a is a primitive root mod p^2 or a pth power residue mod p^2. Moreover, if a is a primitive root mod p^2, i.e. $\nu = 2$, $R = 1$ and $N = p(p-1)$, then the lemma shows again that, for any k, $r(a+kp^2, p^3) = 1$. In particular, by the same argument, we see that a primitive root mod p^2 is automatically a primitive root mod p^ν, $\nu \ge 2$.

Let $g(p^\nu)$ be the least primitive root mod p^ν. Then the above well known observation yields the following.

THEOREM 1. *For any* $\varepsilon > 0$ *and any* $\nu \ge 1$, *we have*

$$g(p^\nu) \ll p^{1/4+\varepsilon}.$$

For the case $\nu = 1$, this was proved by Burgess [2] using his famous estimate of character sums. For the case $\nu = 2$, it was proved by Cohen–Odoni–Stothers [3].

In the above theorem, the condition $K(a,p) = 0$ plays an important role. We are interested in the distribution property of the set

$$\{K(a,p) : 1 \le a \le p-1\}.$$

In order to consider this set, we introduce here a distribution function. For $\theta \in \mathbb{R}$, define

$$f_p(\theta) = \frac{1}{p-1} |\{1 \le a \le p-1 : K(a,p) \le \theta(p-1)\}|.$$

This is a non-decreasing function, $f_p(\theta) = 0$ for $\theta < 0$ and $f_p(\theta) = 1$ for $\theta > 1$. Moreover we can prove

THEOREM 2. *For* $0 \le \theta \le 1$, *we have*

$$f_p(\theta) = \theta + O(p^{-1/12} \log p).$$

This theorem shows that the set $\{K(a,p)\}_{a=1}^{p-1}$ distributes in the interval $[1, p-1]$ almost *uniformly*.

Here we note an interesting property of $K(a,p)$. Let $\mathbb{Z}_p$ denote the ring of p-adic integers. Then the polynomial $X^{p-1} - 1$ decomposes into $p-1$ components in $\mathbb{Z}_p[X]$:

$$X^{p-1} = (X-\omega_1)(X-\omega_2)\dots(X-\omega_{p-1}), \qquad \omega_i \in \mathbb{Z}_p.$$

Fermat's little theorem implies that, for any a with $1 \le a \le p-1$, there exists one and only one $(p-1)$th root of unity whose first Hensel coefficient

is equal to a. So we can set

$$\omega_a = a + c_{a,2}p^1 + \ldots + c_{a,m}p^{m-1} + \ldots, \quad a = 1, \ldots, p-1;\ 0 \le c_{a,m} \le p-1.$$

In other terms, ω_a is the value of the Teichmüller character at $a \pmod p$.

It follows from the lemma that

$$K(a,p) = c_{a,2} = \frac{\omega(a) - a}{p}.$$

The distribution of primitive roots mod p^2 is controlled by the p-adic coefficients of the $(p-1)$th roots of unity in $\mathbb{Z}_p$, and also by the values of the Teichmüller character.

For the next topic we need some new notation.

Let χ_0 be the principal Dirichlet character mod p^2, and put

$$D = \{\chi : \text{a non-principal Dirichlet character mod } p^2 \text{ such that } \chi^p = \chi_0\},$$
$$\overline{D} = D \cup \{\chi_0\}.$$

Note that $|D| = p-1$ and every element in D is primitive.

For a non-principal Dirichlet character ψ mod q, and for integers M, N, define the *character sum of* ψ by

$$S(\psi; M, N) = \sum_{n=M+1}^{M+N} \psi(n),$$

and the *Gauss sum of* ψ by

$$G(\psi) = \sum_{n=1}^{q} \psi(n) \exp\left(\frac{2\pi i n}{q}\right).$$

It is known that, for a primitive character ψ, $|G(\psi)| = \sqrt{q}$, so $G(\psi)q^{-1/2}$ lies on the unit circle in the complex plane.

For these two quantities—character sums and Gaussian sums—we can prove the following results:

THEOREM 3. *For any $M, N \in \mathbb{N}$, we have*

$$\frac{1}{p-1} \sum_{\chi \in D} S(\chi; M, N) \ll p^{11/12} \log p, \qquad \textit{uniformly in } M, N.$$

THEOREM 4. *For any natural number k, we have*

$$\frac{1}{p-1} \sum_{\chi \in D} \left(\frac{G(\chi)}{p}\right)^k \ll p^{-1/12}, \qquad \textit{uniformly in } k.$$

An application of the Pólya–Vinogradov inequality yields the estimate

$$\frac{1}{p-1} \sum_{\chi \in D} S(\chi; M, N) \ll p \log p,$$

and Burgess' bound gives the estimate, for any $\varepsilon > 0$,

$$\frac{1}{p-1}\sum_{\chi\in D} S(\chi; M, N) \ll N^{1/2}p^{3/8+\varepsilon}.$$

We also have the bound $\ll p\log\log p$ under G.R.H. ([5], see also [7]). Theorem 3 means that, if we take an average of $S(\chi; M, N)$ over the set D, then we are able to prove a little better estimate than the Pólya–Vinogradov bound.

As we remarked in the above, for $\chi \in D$, $G(\chi)p^{-1}$ lies on the unit circle in the complex plane, so we can define the *argument of Gauss sum* $a(\chi)$ by

$$\frac{G(\chi)}{p} = e^{2\pi i a(\chi)}, \quad 0 \le a(\chi) < 1.$$

We see from Theorem 4, by Weyl's criterion, that the set $\{a(\chi) : \chi \in D\}$ is *approximately uniformly distributed* in the interval $[0, 1)$. Moreover, we can prove the following quantitative result.

THEOREM 5. *Let $I = [a, b]$ be an interval of length $b - a < 1$. Then*

$$\left|\frac{1}{p-1}\sum_{a(\chi)\in I} 1 - (b-a)\right| \ll p^{-1/12}\log p.$$

In fact, this is a direct consequence of the Erdős–Turán inequality (cf. for example [1], Theorem 2.1).

2. Proofs

Proof of the Lemma. 1. It is obvious that $(a + kp^\nu)^{pN} \equiv 1 \pmod{p^{\nu+1}}$. This means that the order of the class $a + kp^\nu$ in the group $(\mathbb{Z}/p^{\nu+1}\mathbb{Z})^\times$ is a divisor of pN. From our assumption, this order must be equal to N or pN, therefore $r(a + kp^\nu, p^{\nu+1}) = Rp$ or R, respectively.

2. We define x by

$$a^N \equiv 1 + xp^\nu \pmod{p^{\nu+1}}, \quad 0 \le x \le p-1.$$

First we show that, if $N \equiv 0 \pmod{p}$, then $x \neq 0$. Let s be N/p and assume $x = 0$, i.e.

$$a^N \equiv 1 \pmod{p^{\nu+1}}.$$

Then we can take two numbers j and y which satisfy the relations

$$a^s \equiv 1 + yp^j \pmod{p^{j+1}}, \quad y \neq 0,\ j < \nu.$$

We have

$$a^N - 1 = (a^s - 1)(a^{s(p-1)} + \ldots + a^s + 1)$$

and

$$\sum_{k=0}^{p-1} a^{sk} = \sum_{k=0}^{p-1}(1+kyp^j) + T(p^{j+1}) = p + T(p^{j+1}), \tag{1}$$

where the terms in $T(\ )$ are multiples of p^{j+1}. Combining (1) with $a^N = 1+T(p^{\nu+1})$, we have $a^s \equiv 1 \pmod{p^\nu}$, which means $r(a,p^\nu) = Rp$ and this contradicts our assumption. Thus we get $x \neq 0$.

Now it is clear that $r(a+Kp^\nu, p^{\nu+1}) = pR$ happens if and only if

$$(a+Kp^\nu)^N \equiv 1 \pmod{p^{\nu+1}}. \tag{2}$$

Since $(a+Kp^\nu)^N - 1 = xp^\nu + a^{N-1}NKp^\nu + T(p^{\nu+1})$, (2) holds if and only if K satisfies the relation

$$ax + NK \equiv 0 \pmod{p}.$$

If $N \equiv 0 \pmod{p}$, then, as proved above, $x \not\equiv 0 \pmod{p}$, and there exists no K which satisfies the above relation. This proves the first part of assertion 2.

If $N \not\equiv 0 \pmod{p}$, then we can determine only one K by

$$K \equiv -axN^{-1} \pmod{p}, \qquad 0 \le K \le p-1.$$

For this value of K, $r(a+Kp^\nu, p^{\nu+1}) = Rp$ and for $k \neq K$, $r(a+kp^\nu, p^{\nu+1}) = R$. ∎

Proof of Theorem 2. Let ω be the Teichmüller character that maps $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\mathbb{Q}_p$. Let $1 \le a \le p-1$, and put

$$\omega(a) = a + c_{a,2}p^1 + \ldots + c_{a,m}p^{m-1} + \ldots$$

Then the above lemma implies that $c_{a,2} = K(a,p)$, and thus

$$a^p - a \equiv K(a,p)p \pmod{p^2}. \tag{3}$$

Now we show that, for any c not divisible by p,

$$\sum_{a=1}^{p} e\left(\frac{c(a^p-a)}{p^2}\right) \ll p^{11/12}\left(1 + \frac{|c|}{p}\log p\right), \tag{4}$$

where $e(x)$ means, as usual, $\exp(2\pi i x)$. In fact the left hand side is equal to

$$\sum_{a=1}^{p} e\left(\frac{ca^p}{p^2}\right) + \sum_{a=1}^{p} e\left(\frac{ca^p}{p^2}\right)\left\{e\left(\frac{-ca}{p^2}\right) - 1\right\}. \tag{5}$$

Here we refer to Heath-Brown's recent results on Heilbronn's exponential sum ([4]): For any integer c not divisible by p, and for any positive integers M and N, we have

$$\sum_{a=1}^{p} e\left(\frac{ca^p}{p^2}\right) \ll p^{11/12} \tag{6}$$

as well as

$$\sum_{a=M+1}^{M+N} e\left(\frac{ca^p}{p^2}\right) \ll p^{11/12}\log p \tag{7}$$

uniformly in c, M, N. Now the first term in (5) is bounded by (6), and to the second term in (5) we apply partial summation and the estimate (7), getting the claim (4).

We now define, for any $t \in \mathbb{R}$,

$$\psi_\theta(t) = \begin{cases} 1 & \text{if } t \le \theta(p-1), \\ 0 & \text{if } \theta(p-1) < t, \end{cases}$$

and write its Fourier expansion as

$$\psi_\theta(t) = \sum_{k=0}^{p-1} c(k,\theta) e\left(\frac{kt}{p}\right),$$

where

$$c(k,\theta) = \begin{cases} \dfrac{1}{p}\displaystyle\sum_{m=0}^{p-1} \psi_\theta(m) e\left(\frac{-km}{p}\right) & \text{if } k \ne 0, \\ \dfrac{1}{p}[\theta(p-1)] & \text{if } k = 0. \end{cases}$$

We easily get, for $k \ne 0$,

$$|c(k,\theta)| \le \frac{1}{p}\left|\sum_{m=0}^{[\theta(p-1)]} e\left(\frac{-km}{p}\right)\right| \ll \frac{1}{k}. \tag{8}$$

Then we have

$$\begin{aligned} f_p(\theta) &= \frac{1}{p-1}\sum_{a=1}^{p-1}\psi_\theta(K(a,p)) = \frac{1}{p-1}\sum_{k=0}^{p-1} c(k,\theta)\sum_{a=1}^{p-1} e\left(\frac{kK(a,p)}{p}\right) \\ &= c(0,\theta) + \frac{1}{p-1}\sum_{k=1}^{p-1} c(k,\theta)\sum_{a=1}^{p-1} e\left(\frac{k(a^p-a)}{p^2}\right), \end{aligned}$$

where we have used the relation (3). Now, with the estimate (8), we have

$$\begin{aligned} f_p(\theta) &= \theta + O\left(\frac{1}{p}\right) + \frac{1}{p-1} O\left(p^{11/12}\sum_{k=1}^{p-1}\frac{1}{k}\left(1+\frac{k}{p}\log p\right)\right) \\ &= \theta + O(p^{-1/12}\log p). \ \blacksquare \end{aligned}$$

Proof of Theorem 3. For simplicity, we assume $M = 0$. We prepare the character sum which singles out pth power residue classes mod p^2:

$$\frac{1}{p}\sum_{\chi \in \overline{D}} \chi(a+kp) = \begin{cases} 1 & \text{if } r(a+kp,p^2) \equiv 0 \pmod p, \\ 0 & \text{otherwise.} \end{cases}$$

Let N be a natural number $\le p^2$, and let

$$\theta = \frac{N}{p^2} \quad \text{and} \quad \theta' = \left[\frac{N}{p}\right].$$

From our lemma again, the conditions $r(a+kp, p^2) \equiv 0 \pmod p$ and $K(a,p) = k$ are equivalent. Hence

$$\sum_{t=0}^{\theta'} \left(\frac{1}{p} \sum_{\chi \in \overline{D}} \chi(a+tp) \right) = \begin{cases} 1 & \text{if } K(a,p) \le \theta(p-1), \\ 0 & \text{if } K(a,p) > \theta(p-1). \end{cases}$$

So we can express $f_p(\theta)$ by character sums:

$$\begin{aligned} f_p(\theta) &= \frac{1}{p-1} \sum_{t=0}^{\theta'} |\{1 \le a \le p-1 : K(a,p) = t\}| \\ &= \frac{1}{p(p-1)} \sum_{\chi \in \overline{D}} \sum_{t=0}^{\theta'} \sum_{a=1}^{p-1} \chi(a+tp). \end{aligned}$$

Then, with Burgess' bound,

$$\begin{aligned} \frac{1}{p-1} \sum_{\chi \in D} S(\chi; 0, N) &= \frac{1}{p-1} \sum_{\chi \in D} S(\chi; 0, (\theta'+1)p) + O(p^{7/8+\varepsilon}) \\ &= p f_p(\theta) - \frac{1}{p-1} \sum_{n < (\theta'+1)p} 1 + O(p^{7/8+\varepsilon}), \end{aligned}$$

for any $\varepsilon > 0$. The second term is $p\theta + O(1)$ as $p \to \infty$, and we can estimate the first term by Theorem 2. ∎

Proof of Theorem 4. First we shall prove that, for any a not divisible by p,

$$\sum_{\chi \in D} G(\chi)\chi(a) \ll p \cdot p^{11/12}, \tag{9}$$

uniformly in a. In fact,

$$\begin{aligned} \sum_{\chi \in D} G(\chi)\chi(a) &= \sum_{n=1}^{p^2} e\left(\frac{n}{p^2}\right) \sum_{\chi \in D} \chi(an) \\ &= \sum_{\substack{n=1 \\ an \equiv y^p \,(\mathrm{mod}\, p^2)}}^{p^2} (p-1) e\left(\frac{n}{p^2}\right) - \sum_{\substack{n=1 \\ an \not\equiv y^p \,(\mathrm{mod}\, p^2)}}^{p^2} e\left(\frac{n}{p^2}\right) \\ &= p \sum_{y=1}^{p} e\left(\frac{y^p \overline{a}}{p^2}\right), \end{aligned}$$

where $\overline{a}$ denotes the inverse residue class of $a \pmod{p^2}$. Then the Heath-Brown's estimate (6) yields the desired bound.

In order to prove Theorem 4, it is sufficient to show

$$\sum_{\chi \in D} \left(\frac{G(\chi)}{p} \right)^k \ll p^{11/12}, \quad \text{uniformly in } k < p^2. \tag{10}$$

For k not divisible by p, Odoni [6] proves that, if we choose a *normal* character $\chi \in D$ which has the property $\chi(1+p) = e(-1/p)$, then any character $\psi \in D$ can be written in the form $\psi = \chi^t$, $1 \le t \le p-1$, and

$$G(\psi) = G(\chi^t) = \chi^t(t) p e\left(\frac{t}{p^2} \right). \tag{11}$$

We now choose a *new normal* character $\tau \in D$ which has the property $\tau(1+p) = e(-k/p)$, i.e. $\tau = \chi^k$. Then by Odoni's argument, we can prove

$$G(\tau) = p\tau(k) e\left(\frac{k}{p^2} \right)$$

as well as

$$G(\tau^t) = p\tau^t(kt) e\left(\frac{kt}{p^2} \right) \quad \text{for } 1 \le t \le p-1. \tag{12}$$

Then we have, by (11) and (12),

$$\begin{aligned} \sum_{\psi \in D} \left(\frac{G(\psi)}{p} \right)^k &= \sum_{t=1}^{p-1} \left\{ \chi^t(t) e\left(\frac{t}{p^2} \right) \right\}^k = \sum_{t=1}^{p-1} \tau^t(t) e\left(\frac{kt}{p^2} \right) \\ &= \sum_{t=1}^{p-1} \frac{G(\tau^t)}{p} \tau^t(\overline{k}) = \frac{1}{p} \sum_{\psi \in D} G(\psi)\psi(\overline{k}), \end{aligned}$$

and (10) is proved by (9).

When $k = sp$ with $1 \le s < p$, then by (11) again, we have

$$\sum_{\psi \in D} \left(\frac{G(\psi)}{p} \right)^{sp} = -1.$$

The uniformity in k is now clear, and this ends the proof of Theorem 4. ∎

References

[1] R. C. Baker, *Diophantine Inequalities*, Clarendon Press, Oxford, 1986.

[2] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (2) 12 (1962), 179–192.

[3] S. D. Cohen, R. W. K. Odoni and W. W. Stothers, *On the least primitive root modulo p^2*, Bull. London Math. Soc. 6 (1974), 42–46.

[4] D. R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, in: Analytic Number Theory, Progr. Math. 136, Birkhäuser, 1996, 451–463.
[5] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math. 43 (1977), 69–82.
[6] R. Odoni, *On Gauss sums* (*mod* p^n), $n \geq 2$, Bull. London Math. Soc. 5 (1973), 325–327.
[7] R. E. A. C. Paley, *A theorem on characters*, J. London Math. Soc. 7 (1932), 28–32.

Department of Mathematics
Meiji-Gakuin University
1518 Kamikurata
Totsuka, Yokohama, 244 Japan
E-mail: leo@gen.meijigakuin.ac.jp

Received on 22.12.1997 (3316)