ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

557

ON kth POWER COSET REPRESENTATIVES MOD p

BY

RITVA METSÄNKYLÄ

HELSINKI 1973
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1973.557

ISSN 0066-1953
ISBN 951-41-0136-7

Communicated 8 October 1973 by K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1973

On kth power coset representatives mod p

1. Introduction. Let p be an odd prime, k a positive integer and d the greatest common divisor of k and $p-1$. Let $C(p)$ denote the multiplicative group consisting of the residue classes mod p which are relatively prime to p. The group $C(p)$ has a multiplicative subgroup, $C_k(p)$, consisting of the kth power residues. It is easily seen that $[C(p) : C_k(p)] = d$. In the following we shall assume that $d > 1$.

We denote by $H_0 (= C_k(p))$, $H_1, \ldots, H_{d-1}$ the cosets of $C_k(p)$ in $C(p)$. Let $g_m(p, k)$ be the smallest positive representative of H_m. We may assume that

$$1 = g_0(p, k) < g_1(p, k) < \ldots < g_{d-1}(p, k).$$

It is the purpose of this note to find an upper bound for $g_m(p, k)$ in terms of m, p, and k.

In [1] K. K. Norton derived estimates for the numbers $g_m(n, k)$, where n is an arbitrary integer. It follows from Theorem (7.16) in [1] that

$$g_m(p, k) \leqq 1 + \{dm/(d-m)\}^{\frac{1}{2}} p^{\frac{1}{2}} \log p.$$

We now show that

$$g_m(p, k) < 2\{dm/(d-m)\}^{\frac{1}{2}} p^{\frac{1}{2}}, \tag{1}$$

and, furthermore, that if -1 is a kth power residue mod p, then

$$g_m(p, k) < \{dm/(d-m)\}^{\frac{1}{2}} p^{\frac{1}{2}}. \tag{2}$$

An estimate slightly weaker than (2) has been proved in the unpublished work [3] of the author. The method used below, as well as in [3], resembles that of [4].

It should be noted that for the numbers $g_1(p, k)$ and $g_{d-1}(p, k)$ there exist better estimates than (1) and (2) (see e.g. [1], p. 162, and [2], p. 87).

2. Preliminary results. If $1 \leqq m \leqq d-1$, we write

$$L = L_{d-m} = \{0\} \cup H_m \cup H_{m+1} \cup \ldots \cup H_{d-1}.$$

Then $g_m(p, k)$ is the smallest positive representative of L. For the number $|L|$ of elements in L, we have the equation

(3) $$|L| = 1 + (d-m)(p-1)/d\,.$$

Put

(4) $$e(x) = e^{2\pi i x/p}\,,\quad S(a) = \sum_{x \in L} e(ax)$$

(as usual, we have identified residues and residue classes). As in [4] we obtain

(5) $$\sum_{a=0}^{p-1} |S(a)|^2 = \sum_{x \in L} \sum_{y \in L} \sum_{a=0}^{p-1} e(a(x-y)) = p|L|\,.$$

On the other hand, if a and b belong to the same coset of $C_k(p)$, then $S(a) = S(b)$ and so

(6) $$\sum_{a=0}^{p-1} |S(a)|^2 = |S(0)|^2 + ((p-1)/d) \sum_a^* |S(a)|^2\,,$$

where in $\sum_a^*$ a runs through the representatives of the cosets of $C_k(p)$ in $C(p)$. By (4), $S(0) = |L|$. Combining (3), (5), and (6) we thus have

$$\sum_a^* |S(a)|^2 = m(d-m)p/d + m^2/d\,.$$

Consequently, if $a \not\equiv 0 \pmod{p}$, then

(7) $$\begin{aligned} |S(a)| &\leqq \{m(d-m)p/d + m^2/d\}^{\frac{1}{2}} \\ &< \{m(d-m)p/d\}^{\frac{1}{2}} + m^{3/2}/\{d(d-m)p\}^{\frac{1}{2}}\,. \end{aligned}$$

For simplicity, we write

(8) $$s = \{m(d-m)p/d\}^{\frac{1}{2}} + m^{3/2}/\{d(d-m)p\}^{\frac{1}{2}}\,.$$

We shall also need the sum

(9) $$T(a) = \sum_{b=0}^{u} e(ab)\,,$$

where u is an integer, $0 \leqq u \leqq p-1$. Now $T(0) = u + 1$, and in the same way as in (5) we can show that

(10) $$\sum_{a=1}^{p-1} |T(a)|^2 = (u+1)(p-u-1)\,.$$

3. Proof of the inequality (1). In order to prove (1) we choose an integer u such that

(11) $$\{dm/(d-m)\}^{\frac{1}{2}} p^{\frac{1}{2}} - 1 \leqq u < \{dm/(d-m)\}^{\frac{1}{2}} p^{\frac{1}{2}}\,.$$

We may assume that $u \leqq (p-1)/2$, because otherwise (1) would be trivial. We set $U = \{0, 1, \ldots, u\}$.

Consider the congruence

(12) $$x - y - z \equiv 0 \pmod p,$$

where $x \in L$, $y \in U$, $z \in U$, and so $0 \leqq y + z \leqq 2u$. Let N be the number of solutions (x, y, z) of (12). If $N > 1$, then there exists an element x in L such that $0 < x \leqq 2u$ and hence the estimate (1) is valid. Using (4) and (9) we get

$$\begin{aligned} pN &= \sum_{x\in L} \sum_{y=0}^{u} \sum_{z=0}^{u} \sum_{t=0}^{p-1} e(t(x-y-z)) \\ &= \sum_{t=0}^{p-1} S(t)T(-t)^2 \\ &= |L|\,(u+1)^2 + \sum_{t=1}^{p-1} S(t)T(-t)^2 . \end{aligned}$$

Furthermore, by (3), (7), (8), (10), and (11) we see that

$$\begin{aligned} pN &> (u+1)^2 \{(d-m)p/d + m/d\} - s \sum_{t=1}^{p-1} |T(-t)|^2 \\ &= (u+1)^2 \{(d-m)p/d + m/d - s(p/(u+1) - 1)\} \\ &> (u+1)^2 \{m(d-m)p/d\}^{\frac{1}{2}} \\ &\geqq (u+1)mp . \end{aligned}$$

From this it follows that $N > 1$.

4. Proof of the inequality (2). Now let -1 be a kth power residue mod p. Let u be defined as in (11). Instead of (12) we now consider the congruence

(13) $$x - y + z \equiv 0 \pmod p,$$

where $x \in L$, $y \in U$, $z \in U$, so that $-u \leqq y - z \leqq u$. In this case we get for the number N of solutions of (13) the expression

$$N = p^{-1} \sum_{t=0}^{p-1} S(t)\, |T(t)|^2 .$$

Hence N has the same lower bound as above. Since now $N > u + 1$, there exists an element x in L such that $-u \leqq x \leqq u$ and $x \neq 0$. By assumption, x and $-x$ belong to the same coset of $C_k(p)$ and thus (2) has been proved.

University of Turku
Turku, Finland

References

[1] Norton, K. K.: Upper bounds for kth power coset representatives modulo n. - Acta Arith. 15 (1969), 161 – 179.

[2] —»— Numbers with small prime factors, and the least kth power non-residue. - Mem. Amer. Math. Soc. 106 (1971), 106 pp.

[3] Taipalus, R. (now Metsänkylä, R.): On the non-trivial solvability of the congruence $a_1x_1^k + \ldots + a_sx_s^k \equiv 0 \pmod{p}$, M. Sc. Thesis, University of Turku (1969). (Finnish).

[4] Tietäväinen, A.: On the trace of a polynomial over a finite field. - Ann. Univ. Turku. Ser. A I 87 (1966), 7 pp.

Printed October 1973