COLLOQUIUM MATHEMATICUM

VOL. 102 2005 NO. 1

ON SETS WHICH CONTAIN A qTH POWER RESIDUE FOR ALMOST ALL PRIME MODULES

BY

MARIUSZ SKAŁBA (Warszawa)

Abstract. A classical theorem of M. Fried [2] asserts that if non-zero integers $\beta_1, \ldots, \beta_l$ have the property that for each prime number p there exists a quadratic residue β_j mod p then a certain product of an odd number of them is a square. We provide generalizations for power residues of degree n in two cases: 1) n is a prime, 2) n is a power of an odd prime. The proofs involve some combinatorial properties of finite Abelian groups and arithmetic results of [3].

Our starting point is the following theorem of M. Fried [2] (rediscovered much later by other writers [1], [3]).

THEOREM. *Let $\beta_1, \ldots, \beta_l$ be rational integers. The following two conditions are equivalent*:

(L) *for each sufficiently large prime number p there exists j such that the congruence*

$$x^2 \equiv \beta_j \pmod{p}$$

is solvable,

(G) *there exists $J \subseteq \{1, \ldots, l\}$ of odd cardinality such that*

$$\prod_{j \in J} \beta_j = \gamma^2 \quad \text{for some } \gamma \in \mathbb{Z}.$$

The generalization of the above theorem to power residues of degree n, where n is any fixed exponent, is provided in [3]. But the counterpart of the above condition (G) has a quite complex combinatorial structure (condition (ii) of Lemma 3). The aim of this paper is to replace it by a condition which resembles the above condition (G) for $n = 2$. We succeed in two special cases: $n = q$ is a prime (Theorem 1) and $n = q^m$, $q \neq 2$ (Theorem 2).

THEOREM 1. *Let K be an algebraic number field, $\beta_1, \ldots, \beta_l \in K^*$ and q a rational prime. The following two conditions are equivalent*:

2000 *Mathematics Subject Classification*: 11R20, 11A15.

Key words and phrases: power residue, finite Abelian group.

(L) *for almost all prime ideals* $\mathfrak{p}$ *of* K *at least one of the congruences*

$$x^q \equiv \beta_j \pmod{\mathfrak{p}}$$

is solvable,

(G) *for each sequence of integers* (c_j), $j = 1, \ldots, l$, *there exists a sequence of integers* (f_j), $j = 1, \ldots, l$, *satisfying*

$$\sum_{j=1}^{l} f_j \not\equiv 0 \pmod{q} \quad \textit{and} \quad \prod_{j=1}^{l} \beta_j^{c_j f_j} = \gamma^q$$

with some $\gamma \in K^*$.

For the case of q^mth power residues, but only for $q \neq 2$, we have

THEOREM 2. *Let* K *be an algebraic number field*, $\beta_1, \ldots, \beta_l \in K^*$, $n = q^m$ *where* q *is an odd prime. The following two conditions are equivalent*:

(L) *for almost all prime ideals* $\mathfrak{p}$ *of* K *at least one of the congruences*

$$x^n \equiv \beta_j \pmod{\mathfrak{p}}$$

is solvable,

(G) *for each sequence of integers* (c_j), $j = 1, \ldots, l$, *there exist two subsets* A, B *of* $\{1, \ldots, l\}$ *satisfying*

$$|A| \not\equiv |B| \pmod{q} \quad \textit{and} \quad \prod_{j\in A} \beta_j^{c_j} = \gamma^n \prod_{j\in B} \beta_j^{c_j}$$

with some $\gamma \in K^*$.

LEMMA 1. *Let* q *be a natural number and consider a system of* $q-1$ *integers* $c^{(1)}, \ldots, c^{(q-1)}$. *If for each non-empty subset* $C \subseteq \{1, \ldots, q-1\}$ *we have* $\sum_{i\in C} c^{(i)} \not\equiv 0 \pmod{q}$ *then there exists an integer* c *such that*

$$c^{(1)} \equiv c^{(2)} \equiv \cdots \equiv c^{(q-1)} \equiv c \pmod{q}.$$

Proof. Without any claim for priority we prove the lemma for completeness of presentation. For any permutation τ of $\{1, \ldots, q-1\}$ the sequence

$$c^{(\tau(1))}, c^{(\tau(1))} + c^{(\tau(2))}, \ldots, c^{(\tau(1))} + \ldots + c^{(\tau(q-1))}$$

gives all non-zero residue classes mod q . This observation implies

$$\sum_{j=1}^{q-2} c^{(\tau(j))} \equiv \sum_{j=1}^{q-3} c^{(\tau(j))} + c^{(\tau(q-1))} \pmod{q},$$

hence $c^{(\tau(q-2))} \equiv c^{(\tau(q-1))} \pmod{q}$, which finishes the proof.

LEMMA 2. *Let* G *be a finite Abelian group*, $\widehat{G}$ *its group of characters and* $g_j \in G$ $(1 \leq j \leq l)$. *The following conditions are equivalent*:

(C1) *for each* $\chi \in \widehat{G}$ *there exists* j *such that* $\chi(g_j) = 1$,

(C2) *there exists an involution* σ *of the family* $\mathcal{F}$ *of all subsets of* $\{1, \ldots, l\}$ *such that for each* $A \in \mathcal{F}$,

$$|\sigma(A)| \not\equiv |A| \pmod 2 \quad \textit{and} \quad \prod_{j \in \sigma(A)} g_j = \prod_{j \in A} g_j.$$

If we assume additionally that G *is a* q*-group*, *where* q *is a prime*, *then both conditions are equivalent to*

(C3) *for each sequence of integers* (c_j), $j = 1, \ldots, l$, *there exist subsets* $A, B \in \mathcal{F}$ *satisfying*

$$|A| \not\equiv |B| \pmod q \quad \textit{and} \quad \prod_{j \in A} g_j^{c_j} = \prod_{j \in B} g_j^{c_j}. \tag{1}$$

If additionally G *is an elementary* q*-group then these conditions are equivalent to*

(C4) *for each sequence of integers* (c_j), $j = 1, \ldots, l$, *there exists a sequence of integers* (f_j), $j = 1, \ldots, l$, *satisfying*

$$\sum_{j=1}^{l} f_j \not\equiv 0 \pmod q \quad \textit{and} \quad \prod_{j=1}^{l} g_j^{c_j f_j} = 1.$$

Proof. The equivalence of (C1) and (C2) is proved in [3]. We will show first that (C1) *and* (C2) imply (C3). Let $c_1, \ldots, c_l$ be arbitrary integers. Obviously the system $(g_j^{c_j})$ of elements of G satisfies (C1), hence (C2) as well. Therefore there exists an involution σ of the family $\mathcal{F}$ such that for each $A \in \mathcal{F}$,

$$|\sigma(A)| \equiv |A| + 1 \pmod 2 \quad \text{and} \quad \prod_{j \in \sigma(A)} g_j^{c_j} = \prod_{j \in A} g_j^{c_j}.$$

Now let $\zeta_q = \exp(2\pi i/q) \in \mathbb{C}$. Then

$$(1 - \zeta_q)^l = \sum_{A \in \mathcal{F}} (-1)^{|A|} \zeta_q^{|A|} = \sum_{A \in \mathcal{F},\, |A| \text{ even}} \{\zeta_q^{|A|} - \zeta_q^{|\sigma(A)|}\}$$

and since the left hand side is not 0 there must exist $A \in \mathcal{F}$ such that

$$|\sigma(A)| \not\equiv |A| \pmod q.$$

So we can put $B = \sigma(A)$.

We owe to A. Schinzel the proof that (C3) implies (C1). Assume to the contrary that there exists $\chi \in \widehat{G}$ such that for each $1 \le j \le l$ we have

$$\chi(g_j) \neq 1.$$

Denoting by e the exponent of the group G we can write

$$\chi(g_j) = \zeta_e^{d_j}, \quad \text{where} \quad d_j \not\equiv 0 \pmod e.$$

Now we define the sequence $c_1, \ldots, c_l$ by the conditions

$$c_j d_j \equiv e/q \pmod{e}, \qquad j = 1, \ldots, l.$$

By (C3) there exist $A, B \in \mathcal{F}$ such that (1) is satisfied. Hence we obtain

$$\prod_{j\in A} \chi(g_j)^{c_j} = \prod_{j\in B} \chi(g_j)^{c_j}$$

and further

$$\prod_{j\in A} \zeta_e^{d_j c_j} = \prod_{j\in B} \zeta_e^{d_j c_j},$$

which gives $\zeta_e^{(e/q)|A|} = \zeta_e^{(e/q)|B|}$ and finally $(e/q)|A| \equiv (e/q)|B| \pmod{e}$, hence $|A| \equiv |B| \pmod{q}$, a contradiction. Hence for each $\chi \in \widehat{G}$ there exists $1 \le j \le l$ such that $\chi(g_j) = 1$ and we have shown (C1).

Now we show that (C3) implies (C4). By (C3) for each sequence of integers (c_j), $j = 1, \ldots, l$, there exist disjoint subsets $A, B \in \mathcal{F}$ satisfying (1). We put $f_j = 1$ for $j \in A$, $f_j = -1$ for $j \in B$, and $f_j = 0$ for $j \notin A \cup B$.

Now we will close the circle of implications by showing that (C4) implies (C1). It is obvious that it is sufficient to prove (C1) for the following system of elements:

$$\underbrace{g_1, \ldots, g_1}_{q-1 \text{ times}}, \underbrace{g_2, \ldots, g_2}_{q-1 \text{ times}}, \cdots \underbrace{g_l, \ldots, g_l}_{q-1 \text{ times}}. \tag{2}$$

We will now verify that the system (2) satisfies (C3). Take an arbitrary sequence of integers

$$c_1^{(1)}, \ldots, c_1^{(q-1)}, c_2^{(1)}, \ldots, c_2^{(q-1)}, \ldots, c_l^{(1)}, \ldots, c_l^{(q-1)}.$$

Two cases can occur.

(1) *There exists $j \in \{1, \ldots, l\}$ and a non-empty subset $C \subseteq \{1, \ldots, q-1\}$ such that* $\sum_{i\in C} c_j^{(i)} \equiv 0 \pmod{q}$. Then we put simply $A = C$ and $B = \emptyset$.

(2) *For each $j \in \{1, \ldots, l\}$ and each non-empty subset $C \subseteq \{1, \ldots, q-1\}$ we have* $\sum_{i\in C} c_j^{(i)} \not\equiv 0 \pmod{q}$. By Lemma 1, for each $j \in \{1, \ldots, l\}$ there exists c_j such that

$$c_j^{(1)} \equiv c_j^{(2)} \equiv \cdots \equiv c_j^{(q-1)} \equiv c_j \pmod{q}.$$

By (C4) there exist integers $f_1, \ldots, f_l$ such that

$$\prod_{j=1}^{l} (g_j^{c_j})^{f_j} = 1 \tag{3}$$

and we can assume that $0 \le f_j \le q-1$ for $j = 1, \ldots, l$. We put

$$A = \bigcup_{j=1}^{l} ((j-1)(q-1), (j-1)(q-1) + f_j], \qquad B = \emptyset.$$

By (3) condition (C3) holds for the system (2) and the exponents $(c_j^{(i)})$.

LEMMA 3. *Let $w_n(K)$ be the number of nth roots of unity contained in a number field K and assume that*

$$(w_n(K), \mathrm{l.c.m.}[K(\zeta_q):K]) = 1, \tag{4}$$

where the least common multiple is over all prime divisors q of n and additionally $q=4$ if $4\,|\,n$. Let $\beta_1,\ldots,\beta_l \in K^*$. Then the following two conditions are equivalent:

(i) *for almost all prime ideals $\mathfrak{p}$ of K there exists $1 \le j \le l$ such that the congruence*
$$x^n \equiv \beta_j \pmod{\mathfrak{p}}$$
is solvable in K,

(ii) *there exists an involution σ of the family of all subsets of $\{1,\ldots,l\}$ such that for each $A \subset \{1,\ldots,l\}$*,
$$|\sigma(A)| \equiv |A| + 1 \pmod 2$$
and
$$\prod_{j\in\sigma(A)} \beta_j = \gamma_A^n \prod_{j\in A} \beta_j, \tag{5}$$
where $\gamma_A \in K^*$.

Proof. This is a special case of Corollary 1 of [3], for $k=0$.

Proof of Theorems 1 and 2. The equivalence of both conditions (L) and (G) follows immediately from Lemmas 3 and 2.

REFERENCES

[1] M. Filaseta and D. R. Richman, *Sets which contain a quadratic residue mod p for almost all p*, Math. J. Okayama Univ. 31 (1989), 1–8.

[2] M. Fried, *Arithmetical properties of value sets of polynomials*, Acta Arith. 15 (1969), 91–115.

[3] A. Schinzel and M. Skałba, *On power residues*, ibid. 108 (2003), 77–94.

Institute of Mathematics
Polish Academy of Sciences
P.O. Box 21
00-956 Warszawa, Poland
E-mail: skalba@impan.gov.pl

Received 1 September 2004;
revised 25 October 2004 (4491)