Canad. Math. Bull.Vol. **36** (2), 1993 pp. 144–146

ON MAXIMAL RESIDUE DIFFERENCE SETS MODULO p

J. FABRYKOWSKI

ABSTRACT. A residue difference set modulo p is a set $\mathcal{A} = \{a_1, a_2, \ldots, a_k\}$ of integers $1 \leq a_i \leq p-1$ such that $(\frac{a_i}{p}) = 1$ and $(\frac{a_i - a_j}{p}) = 1$ for all i and j with $i \neq j$, where $(\frac{a}{p})$ is the Legendre symbol. We give a lower and an upper bound for m_p—the maximal cardinality of such set $\mathcal{A}$ in the case of $p \equiv 1 \pmod 4$.

1. **Introduction.** Throughout this paper p denotes a prime $\equiv 1 \pmod 4$ and $(\frac{a}{p})$ the Legendre symbol modulo p. A set $\mathcal{A} = \{a_1, a_2, \ldots, a_k\}$ of integers $1 \leq a_i \leq p-1$, $1 \leq i \leq k$ satisfying the conditions:

(i) $(\frac{a_i}{p}) = 1$ for $1 \leq i \leq k$

(ii) $(\frac{a_i - a_j}{p}) = 1$ for $1 \leq i, j \leq k$, $i \neq j$

is called a *residue difference set modulo p*.

For a fixed prime p, let m_p denote the maximal value of k. The size of m_p has been investigated by Buell and Williams [1]. They proved that

$$\frac{1}{2} \log p < m_p < p^{1/2} \log p \text{ for all primes } p, \text{ and} \tag{1}$$

$$m_p < (1+\epsilon) p^{1/2} \log p / 4 \log 2 \text{ for all sufficiently large primes } p > C = C(\epsilon). \tag{2}$$

They have also mentioned that extensive numerical computations suggest $m_p \sim c \log p$ for some constant c with $1 \leq c \leq 2$.

In this paper we shall prove the following:

THEOREM.

$$m_p > \frac{1-\epsilon}{2 \log 2} \log p \textit{ for all } p > p_0(\epsilon), \tag{3}$$

$$m_p \leq p^{1/2} \textit{ for all primes } p. \tag{4}$$

To prove the theorem we require the following Lemma which was proved in [1]:

LEMMA. *For any integer $k \geq 1$, let $a_0, a_1, \ldots, a_{k-1}$ be k integers such that $a_0 = 0$, $a_1 = 1$, $1 < a_i < p$, $2 \leq i \leq k-1$, $a_i \neq a_j$ for $i \neq j$. If*

$$S(a_0, a_1, \ldots, a_{k-1}) = \sum_{\substack{x=0 \\ x \neq a_0, a_1, \ldots, a_{k-1}}}^{p-1} \left\{ \prod_{j=1}^{k-1} \left(1 + \left(\frac{x - a_j}{p} \right) \right) \right\}$$

Received by the editors January 28, 1992.

AMS subject classification: Primary: 11A07; secondary: 11B75.

© Canadian Mathematical Society 1993.

https://doi.org/10.4153/CMB-1993-021-7 Published online by Cambridge University Press

then

$$|S(a_0, a_1, \ldots, a_{k-1}) - p| \leq p^{1/2}\{(k-2)2^{k-1} + 1\} + k2^{k-1}.$$

2. **Proof of the theorem.** Buell and Williams proved their upper bounds for m_p by developing a procedure that generates a residue difference set. We modify this procedure to obtain a simple proof of (3).

The set A_1 of possible values of a_1 such that $(\frac{a_1}{p}) = 1$ consists of all quadratic residues modulo p. Let us choose the smallest possible element from this set, that is $a_1 = 1$. The set A_2 of possible values of b such that $\{1, b\}$ is a residue difference set is

$$A_2 = \Big\{b \,;\, \Big(\frac{b}{p}\Big) = \Big(\frac{b-1}{p}\Big) = 1\Big\}.$$

Again, as before let us choose the smallest possible element from A_2 and call it a_2.

The set A_3 of possible values of c such that $\{1, a_2, c\}$ is a residue set is

$$A_3 = \Big\{c \,;\, \Big(\frac{c}{p}\Big) = \Big(\frac{c-1}{p}\Big) = \Big(\frac{c-a_2}{p}\Big) = 1\Big\}.$$

Let us choose, the smallest possible such c and call it a_3.

Proceeding in this way we generate a residue difference set $\mathcal{A} = \{1, a_2, \ldots, a_{k-1}\}$ and a set A_k of possible values a_k so that $\{1, a_2, \ldots, a_{k-1}, a_k\}$ is also a residue difference set. We can continue our procedure as long as $|A_k| > 0$. By the principle of the procedure:

$$\begin{aligned}|A_k| &= \frac{1}{2^k} \sum_{a_{k-1} < a_k < p} \Big\{1 + \Big(\frac{a_k}{p}\Big)\Big\}\Big\{1 + \Big(\frac{a_k - 1}{p}\Big)\Big\} \\ &\qquad \Big\{1 + \Big(\frac{a_k - a_2}{p}\Big)\Big\} \cdot \cdots \cdot \Big\{1 + \Big(\frac{a_k - a_{k-1}}{p}\Big)\Big\} \\ &= \frac{1}{2^k} \sum_{\substack{x=0 \\ x \neq a_0, a_1, a_2, \ldots, a_{k-1}}}^{p-1} \prod_{j=0}^{k-1} \Big\{1 + \Big(\frac{x - a_j}{p}\Big)\Big\} = \frac{1}{2^k} S(a_0, \ldots, a_{k-1}).\end{aligned}$$

Thus by the Lemma:

$$|A_k| \geq \frac{p}{2^k} - p^{1/2}\Big(\frac{k-2}{2} + \frac{1}{2^k}\Big) - \frac{k}{2}. \tag{5}$$

The choice $k = [\frac{1-\epsilon}{2} \log_2 p] + 1$, $(\epsilon > 0)$ makes the right hand side of (5) positive provided $p > p_0(\epsilon)$; thus (3) follows.

In order to prove (4) we recall the value of the Gauss' sum:

$$G_p(x) = \sum_{j=0}^{p-1} e\Big(\frac{j^2 x}{p}\Big) = \Big(\frac{x}{p}\Big)\sqrt{p}, \text{ for } p \not| \, x. \tag{6}$$

Let $N_p = \{n \,;\, 1 \leq n \leq p-1, (\frac{n}{p}) = -1\}$, so $|N_p| = \frac{p-1}{2}$. From (6) it follows:

$$\sum_{n \in N_p} e\Big(\frac{nx}{p}\Big) = -\frac{1}{2} - \frac{1}{2}\Big(\frac{x}{p}\Big)\sqrt{p} \text{ for } p \not| \, x. \tag{7}$$

https://doi.org/10.4153/CMB-1993-021-7 Published online by Cambridge University Press

Let now $\mathcal{A} = \{a_1, \ldots, a_k\}$ be any residue difference set modulo p and set

$$g_p(x) = \sum_{a \in \mathcal{A}} e\left(\frac{ax}{p}\right).$$

We have:

$$\begin{aligned} 0 &\le \sum_{n \in N_p} |g_p(n)|^2 \\ &= \sum_{n \in N_p} \sum\sum_{a,a' \in \mathcal{A}} e\left(\frac{(a-a')n}{p}\right) \\ &= \sum_{n \in N_p} |A| + \sum\sum_{\substack{a,a' \in \mathcal{A} \\ a \neq a'}} \sum_{n \in N_p} e\left(\frac{(a-a')n}{p}\right) \\ &= |\mathcal{A}| \frac{p-1}{2} + (|\mathcal{A}|^2 - |\mathcal{A}|)\left(-\frac{1}{2} - \frac{1}{2}\sqrt{p}\right) \end{aligned} \tag{8}$$

using (7) and the fact that $(\frac{a-a'}{p}) = 1$.

Solving, the inequality (8) for $|\mathcal{A}|$ we obtain $|\mathcal{A}| \le \sqrt{p}$ which proves (4).

REFERENCES

1. D. A. Buell and K. S. Williams, *Maximal Residue Difference Sets Modulo p*, Proc. Amer. Math. Soc. **69**(1978), 205–209.

Department of Mathematics and Astronomy
University of Manitoba
Winnipeg, Manitoba
R3T 2N2

https://doi.org/10.4153/CMB-1993-021-7 Published online by Cambridge University Press