ACTA ARITHMETICA
118.4 (2005)

On sums and products of residues modulo p

by

A. SÁRKÖZY (Budapest)

1. Introduction. Throughout the paper we use the notation $e(\alpha)=e^{2\pi i\alpha}$.

Our goal is to show that if A, B, C, D are "large" subsets of $\mathbb{Z}_p$, then the equation

$$a+b=cd, \quad a\in A,\ b\in B,\ c\in C,\ d\in D, \tag{1}$$

can be solved.

THEOREM. *If p is a prime, $A, B, C, D \subset \mathbb{Z}_p$, and the number of solutions of* (1) *is denoted by N, then*

$$\left|N-\frac{|A|\,|B|\,|C|\,|D|}{p}\right| \le (|A|\,|B|\,|C|\,|D|)^{1/2}p^{1/2}. \tag{2}$$

COROLLARY 1. *If p is a prime, $A, B, C, D \subset \mathbb{Z}_p$ and*

$$|A|\,|B|\,|C|\,|D| > p^3, \tag{3}$$

then (1) *can be solved.*

Note that Corollary 1 and thus also the Theorem is the best possible apart from the constant factor in (2), resp. (3). Indeed, taking $A=B=\{n: 1\le n<p/2\}$ (here and in what follows we do not distinguish between integers and residue classes represented by them), $C=\{1,\dots,p\}$ and $D=\{0\}$, we have

$$|A|\,|B|\,|C|\,|D| = \left(\frac{1}{4}+o(1)\right)p^3,$$

however, (1) has no solution.

Moreover, we remark that these results cannot be extended from prime moduli to composite moduli, i.e., from $\mathbb{Z}_p$ to $\mathbb{Z}_m$. Indeed, let $m=2k$ be an even positive integer, and let $A=C=\{2,4,\dots,2k\}\subset\mathbb{Z}_m$, $B=\{1,3,\dots,2k-1\}$ and $D=\mathbb{Z}_m$. Then we have

---

2000 *Mathematics Subject Classification*: 11Bxx, 11Txx.

Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. T043623.

$$|A|\,|B|\,|C|\,|D| = \tfrac{1}{8}m^4$$

so that much more holds than the m-analogue of (3), however, clearly (1) has no solution. One might like to study the question that in what rings R (including infinite ones) is it true that if A, B, C, D are "dense" subsets of R, then (1) must be solvable.

First, in Section 2 we will show that the Theorem and Corollary 1 generalize several earlier theorems, and the proofs of the Theorem and Corollary 1 will be presented in Section 3.

2. Consequences

Corollary 2. *If p is a prime number, χ is a (multiplicative) character modulo p of order d, $n \in \mathbb{Z}$, $A, B \subset \mathbb{Z}_p$ and*

$$|A|\,|B| > d^2\left(1-\frac{1}{p}\right)^{-2} p \tag{4}$$

then there are $a \in A$, $b \in B$ with

$$\chi(a+b) = e\left(\frac{n}{d}\right). \tag{5}$$

Proof. Writing $C = \{u : u \in \mathbb{Z}_p,\ \chi(u) = 1\}$ and $D = \bigl\{v : v \in \mathbb{Z}_p,\ \chi(v) = e\bigl(\frac{n}{d}\bigr)\bigr\}$, we have

$$|C| = |D| = \frac{p-1}{d},$$

so that, by (4),

$$|A|\,|B|\,|C|\,|D| > d^2\,\frac{p^3}{(p-1)^2}\,\frac{(p-1)^2}{d^2} = p^3.$$

Thus by Corollary 1, (1) can be solved. If a, b, c, d satisfy (1) then we have

$$\chi(a+b) = \chi(cd) = \chi(c)\chi(d) = 1 \cdot e\left(\frac{n}{d}\right) = e\left(\frac{n}{d}\right)$$

so that (5) holds and this completes the proof of Corollary 2.

In particular, if $\chi(n) = \bigl(\frac{n}{p}\bigr)$ (for $(n,p) = 1$) is the Legendre symbol in Corollary 2 so that $d = 2$, then we have the following consequence:

Corollary 3. *If p is an odd prime, $A, B \subset \mathbb{Z}_p$ and*

$$|A|\,|B| > 4\left(1-\frac{1}{p}\right)^{-2} p,$$

then there are $a, a' \in A$, $b, b' \in B$ with

$$\left(\frac{a+b}{p}\right) = 1, \qquad \left(\frac{a'+b'}{p}\right) = -1.$$

This sharpens and generalizes a result of Erdős and Sárközy [1]; see also [2] and [3].

COROLLARY 4. *If p is a prime, $k \in \mathbb{N}$, $(p-1,k) > 1$, $A, B \subset \mathbb{Z}_p$ and for all $a \in A$, $b \in B$, $a+b$ is a kth power in $\mathbb{Z}_p$, i.e., writing $E = \{x^k : x \in \mathbb{Z}_p\}$ we have $A+B \subset E$, then*

$$|A|\,|B| \le 9\left(1-\frac{1}{p}\right)^{-2} p. \tag{6}$$

Note that apart from the constant factor in the upper bound in (6), this is Gyarmati's Theorem 8(b) in [5].

Proof of Corollary 4. We have to show that if $A, B \subset \mathbb{Z}_p$ and

$$|A|\,|B| > 9\left(1-\frac{1}{p}\right)^{-2} p, \tag{7}$$

then there are $a \in A, b \in B$ with

$$a+b \notin E. \tag{8}$$

Write $D = (p-1,k)$ (so that $D > 1$), let $r(n,D)$ denote the least non-negative residue of n modulo D, let g be a primitive root modulo p, and define C, D by $C = \{g^u : 0 \le r(u,D) < D/2\}$, $D = \{g^v : 0 < r(v,D) \le D/2\}$ so that, by $D > 1$,

$$\min\{|C|,|D|\} \ge \left[\frac{D}{2}\right]\frac{p-1}{D} \ge \frac{p-1}{3}. \tag{9}$$

By (7) and (9) we have

$$|A|\,|B|\,|C|\,|D| > 9\left(1-\frac{1}{p}\right)^{-2} p\left(\frac{p-1}{3}\right)^{2} = p^3$$

so that, by Corollary 1, (1) can be solved. If a, b, c, d satisfy (1) then $a+b$ can be written in form

$$a+b = cd = g^u \cdot g^v = g^{u+v}$$

with $0 < r(u+v,D) < D$ so that $D \nmid (u+v)$. Thus D does not divide the (base g) index of $a+b$ modulo p whence (8) follows.

COROLLARY 5. *If p is a prime, $k \in \mathbb{N}$, $A, B \subset \mathbb{Z}_p$ and, writing $D = (k, p-1)$, we have*

$$|A|\,|B| > D^2\left(1-\frac{1}{p}\right)^{-2} p, \tag{10}$$

then the equation

$$a+b = x^k, \qquad a \in A,\ b \in B,\ x \in \mathbb{Z}_p,\ x \ne 0, \tag{11}$$

can be solved.

This is a variant of a special case of Gyarmati's Theorem 10(b) in [5]. Note that it follows from this corollary that if $m, n, k \in \mathbb{N}$ are fixed and p is a prime large enough then the congruence

$$x^m + y^n \equiv z^k \pmod{p},$$

and in particular the Fermat congruence

$$x^n + y^n \equiv z^n \pmod{p}$$

has non-trivial solution x, y, z; the latter is Schur's theorem [7].

Proof of Corollary 5. Writing $F = \{x^k : x \in \mathbb{Z}_p,\ x \neq 0\}$, we clearly have

$$|F| = \frac{p-1}{D}.$$

Thus taking $C = D = F$, by (10) we have

$$|A|\,|B|\,|C|\,|D| = |A|\,|B| \left(\frac{p-1}{D}\right)^2 > p^3$$

so that by Corollary 1 (1) can be solved. For a, b, c, d satisfying (1) we have

$$a + b = cd \in CD = F \cdot F = F$$

which proves the solvability of (11).

Corollary 6. *If p is a prime, S, T are integers with $1 \leq T \leq p$, $C, D \subset \mathbb{Z}_p$ and*

$$|C|\,|D| > \frac{4}{T^2}\, p^3, \tag{12}$$

then

$$cd \equiv n \pmod{p}, \qquad c \in C,\ d \in D,\ S < n \leq S + T, \tag{13}$$

can be solved.

This is a slight sharpening of the Corollary in [6]; the connection with the problem of the least quadratic non-residue was analyzed there. See also [4].

Proof of Corollary 6. Define A, B by $A = \{a : S \leq a \leq S + [T/2]\}$, $B = \{b : 0 < b \leq T - [T/2]\}$ so that

$$\min\{|A|, |B|\} \geq T - \left[\frac{T}{2}\right] \geq \frac{T}{2}. \tag{14}$$

It follows from (12) and (14) that

$$|A|\,|B|\,|C|\,|D| > \left(\frac{T}{2}\right)^2 \frac{4}{T^2}\, p^3 = p^3$$

so that, by Corollary 1, there are a, b, c, d satisfying (1):

$$a + b = cd. \tag{15}$$

By the definition of A and B, here we have

$$S < a + b \le S + T \tag{16}$$

and (13) follows from (15) and (16).

3. The proofs

Proof of the Theorem. For every $a, b, c, d \in \mathbb{Z}_p$ we have

$$\frac{1}{p}\sum_{k=0}^{p-1} e\biggl((a+b-cd)\,\frac{k}{p}\biggr) = \begin{cases} 1 & \text{if } a+b = cd, \\ 0 & \text{if } a+b \ne cd, \end{cases}$$

so that

$$N = \frac{1}{p}\sum_{a\in A}\sum_{b\in B}\sum_{c\in C}\sum_{d\in D}\sum_{k=0}^{p-1} e\biggl((a+b-cd)\,\frac{k}{p}\biggr).$$

Separating the term with $k = 0$ we obtain

$$N = \frac{|A|\,|B|\,|C|\,|D|}{p} + \frac{1}{p}\sum_{k=1}^{p-1}\sum_{a\in A}\sum_{b\in B}\sum_{c\in C}\sum_{d\in D} e\biggl((a+b-cd)\,\frac{k}{p}\biggr)$$

$$= \frac{|A|\,|B|\,|C|\,|D|}{p} + \frac{1}{p}\sum_{k=1}^{p-1}\biggl(\sum_{a\in A} e\biggl(a\,\frac{k}{p}\biggr)\biggr)\biggl(\sum_{b\in B} e\biggl(b\,\frac{k}{p}\biggr)\biggr)\biggl(\sum_{c\in C}\sum_{d\in D} e\biggl(-cd\,\frac{k}{p}\biggr)\biggr)$$

whence, writing $F(\alpha) = \sum_{a\in A} e(a\alpha)$ and $G(\alpha) = \sum_{b\in B} e(b\beta)$,

$$\biggl|\,|N| - \frac{|A|\,|B|\,|C|\,|D|}{p}\biggr| \tag{17}$$

$$= \frac{1}{p}\biggl|\sum_{k=1}^{p-1} F\biggl(\frac{k}{p}\biggr) G\biggl(\frac{k}{p}\biggr)\biggl(\sum_{c\in C}\sum_{d\in D} e\biggl(-cd\,\frac{k}{p}\biggr)\biggr)\biggr|$$

$$\le \frac{1}{p}\sum_{k=1}^{p-1}\biggl|F\biggl(\frac{k}{p}\biggr)\biggr|\,\biggl|G\biggl(\frac{k}{p}\biggr)\biggr|\,\biggl|\sum_{c\in C}\sum_{d\in D} e\biggl(-cd\,\frac{k}{p}\biggr)\biggr|.$$

Now we need Vinogradov's lemma [8, p. 29]:

LEMMA 7. *Let* $(a, q) = 1$, $q > 1$. *Let*

$$S = \sum_{x=0}^{q-1}\sum_{y=0}^{q-1} \zeta(x)\eta(y) e\biggl(xy\,\frac{a}{q}\biggr)$$

and suppose that

$$\sum_{x=0}^{q-1} |\zeta(x)|^2 = X_0, \qquad \sum_{y=0}^{q-1} |\eta(y)|^2 = Y_0.$$

Then

$$|S| \le (X_0 Y_0 q)^{1/2}.$$

We use this lemma with $a = -k$, $q = p$,

$$\zeta(x) = \begin{cases} 1 & \text{if } x \in C, \\ 0 & \text{if } x \notin C, \end{cases} \qquad \eta(x) = \begin{cases} 1 & \text{if } d \in D, \\ 0 & \text{if } d \notin D, \end{cases}$$

so that $X_0 = |C|$ and $Y_0 = |D|$. We obtain

$$\left| \sum_{c \in C} \sum_{d \in D} e\left(-cd \, \frac{k}{p} \right) \right| \le (|C|\,|D|p)^{1/2} \quad \text{for } (k,p) = 1. \tag{18}$$

By using Cauchy's inequality and a Parseval formula type identity, it follows from (17) and (18) that

$$\begin{aligned} \left| N - \frac{|A|\,|B|\,|C|\,|D|}{p} \right| &\le \frac{1}{p} \sum_{k=1}^{p-1} \left| F\left(\frac{k}{p}\right) \right| \left| G\left(\frac{k}{p}\right) \right| (|C|\,|D|p)^{1/2} \\ &\le \frac{(|C|\,|D|)^{1/2}}{p^{1/2}} \sum_{k=0}^{p-1} \left| F\left(\frac{k}{p}\right) \right| \left| G\left(\frac{k}{p}\right) \right| \\ &\le \left(\frac{|C|\,|D|}{p} \right)^{1/2} \left(\sum_{k=0}^{p-1} \left| F\left(\frac{k}{p}\right) \right|^2 \right)^{1/2} \left(\sum_{k=0}^{p-1} \left| G\left(\frac{k}{p}\right) \right|^2 \right)^{1/2} \\ &= \left(\frac{|C|\,|D|}{p} \right)^{1/2} (|A|p)^{1/2} (|B|p)^{1/2} \\ &= (|A|\,|B|\,|C|\,|D|)^{1/2} p^{1/2} \end{aligned}$$

which completes the proof of the Theorem.

Proof of Corollary 1. By our Theorem, it follows from (3) that

$$\begin{aligned} N &\ge \frac{|A|\,|B|\,|C|\,|D|}{p} - (|A|\,|B|\,|C|\,|D|)^{1/2} p^{1/2} \\ &= \frac{|A|\,|B|\,|C|\,|D|^{1/2}}{p} \left((|A|\,|B|\,|C|\,|D|)^{1/2} - p^{3/2} \right) > 0. \end{aligned}$$

References

[1] P. Erdős and A. Sárközy, *On differences and sums of integers, I*, J. Number Theory 10 (1978), 430–450.

[2] P. Erdős and N. H. Shapiro, *On the least primitive root of a prime*, Pacific J. Math. 7 (1957), 861–865.

[3] J. Friedlander and H. Iwaniec, *Estimates for character sums*, Proc. Amer. Math. Soc. 119 (1993), 365–372.

[4] M. Z. Garaev and F. Luca, *On a theorem of A. Sárközy and applications*, J. Théor. Nombres Bordeaux, to appear.

[5] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97 (2001), 53–65.
[6] A. Sárközy, *On the distribution of residues of products of integers*, Acta Math. Hungar. 49 (1987), 397–401.
[7] I. Schur, *Über die Kongruenz* $x^m + y^m \equiv z^m \pmod{p}$, Jahresber. Deutschen Math. Verein. 25 (1916), 114–117.
[8] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, Interscience, London 1954 (translated from the Russian, the Russian original appeared in 1947).

Department of Algebra and Number Theory
Eötvös Loránd University
Pázmány Péter sétány 1/c
H-1117 Budapest, Hungary
E-mail: sarkozy@cs.elte.hu

Received on 7.3.2005 (4953)