ACTA ARITHMETICA
XCVII.1 (2001)

On a problem of Diophantus

by

KATALIN GYARMATI (Budapest)

1. Introduction. The Greek mathematician Diophantus of Alexandria noted that the rational numbers $\frac{1}{16}$, $\frac{33}{16}$, $\frac{17}{4}$, and $\frac{105}{16}$ have the following property: the product of any two of them increased by 1 is a square of a rational number. Later Fermat found a set of four positive integers with the above property: $\{1, 3, 8, 120\}$ (see [3]). Recently Phil Gibbs has found a set of six rational numbers having this property: $\left\{\frac{11}{192}, \frac{32}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$ (unpublished yet). A set of positive integers $\{a_1, \ldots, a_m\}$ is said to have the *property of Diophantus* if $a_i a_j + 1$ is a perfect square for all $1 \le i < j \le m$. Such a set is called a *Diophantine m-tuple*. It is a well known open question whether there exist Diophantine quintuples.

Dujella and Pethő [4] proved that the pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple. Recently Dujella has proved that there are no Diophantine ninetuples (unpublished yet).

Euler (see [3]) showed that every Diophantine pair can be extended to a quadruple. Arkin, Hoggatt and Straus [1] proved that this also holds for Diophantine triples.

Erdős [5] and Moser (see [16]) asked the additive analog of the problem, i.e., whether for all k there are integers $a_1 < \ldots < a_k$ such that $a_i + a_j$ is a perfect square for all $1 \le i < j \le k$. Lagrange [11] and Nicolas [12] found a set of six integers such that the sum of any two of them is a perfect square. Rivat, Sárközy and Stewart [13] proved that if $\mathcal{A} \subseteq \{1, \ldots, N\}$ and $a + a'$ is a perfect square for all $a, a' \in \mathcal{A}, a \ne a'$, then $|\mathcal{A}| \ll \log N$.

In this paper our goal is to extend the problems and results described above in various directions. One of the theorems to be proved will also generalize the following result of Schur (see [7]): for all positive integers n there exists a real number M such that the Fermat congruence $x^n + y^n \equiv z^n \pmod{p}$ has a non-trivial solution if p is a prime and $p \ge M$. Another proof for this result can be found in [10, pp. 97–98].

2000 *Mathematics Subject Classification*: Primary 11B99; Secondary 11L40, 11N36.

2. The results

Theorem 1. *If $\mathcal{A}, \mathcal{B} \subseteq \{1, \dots, N\}$ and $ab+1$ is a kth power for all $a \in \mathcal{A}$, $b \in \mathcal{B}$ then*

$$\text{(a)} \qquad \min(|\mathcal{A}|, |\mathcal{B}|) \le \frac{1}{\log 2} \log N \qquad \textit{for } k = 2,$$

$$\text{(b)} \qquad \min(|\mathcal{A}|, |\mathcal{B}|) \le \frac{1}{\log(k-1)} \log\log N + 1 \qquad \textit{for } k \ge 3.$$

Probably for $k = 2$, $|\mathcal{A}| \ge 2$ we have $|\mathcal{B}| \ll \log N$. We have been able to prove this only under a further condition:

Theorem 2. *Let $\mathcal{A}, \mathcal{B} \subseteq \{1, \dots, N\}$, $a_1, a_2 \in \mathcal{A}$, $a_1 \le a_2 \le 2a_1$. If $ab+1$ is a perfect square for all $a \in \mathcal{A}$, $b \in \mathcal{B}$ then*

$$|\mathcal{B}| \le \frac{1}{\log 2} \log N.$$

Conversely, we can give a set $\mathcal{B}$ where $\log N \ll |\mathcal{B}|$.

Theorem 3. *There exists $\mathcal{B} \subseteq \{1, \dots, N\}$ such that if $\mathcal{A} = \{1, 2\}$ then $ab+1$ is a perfect square for all $a \in \mathcal{A}$, $b \in \mathcal{B}$ and $|\mathcal{B}| \ge \left[\frac{1}{\log 36} \log N\right]$.*

Next we study the modular analog of the problem. It turns out that unlike the problem of Diophantus, here arbitrarily large "good" sets exist.

Theorem 4. *There is a constant p_0 such that if p is a prime of the form $4k+1$ and $p > p_0$ then there exists $\mathcal{A} \subseteq \mathbb{Z}_p$ so that $|\mathcal{A}| \ge \frac{1}{6 \log 3} \log p$ and $aa' + 1$ is a square (i.e., quadratic residue or 0) mod p for all $a, a' \in \mathcal{A}$, $a \ne a'$.*

Next we will give an upper bound for $|\mathcal{A}|\,|\mathcal{B}|$ for sets $\mathcal{A}$, $\mathcal{B}$ with the property that $ab+1$ is a square mod p for all $a \in \mathcal{A}$, $b \in \mathcal{B}$. The proof will be based on the following theorem of Vinogradov:

Theorem 5. *If $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$ and*

$$S = \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \left(\frac{ab+1}{p} \right)$$

then $|S| \le \sqrt{2p|\mathcal{A}|\,|\mathcal{B}|}$.

From this it is easy to deduce:

Theorem 6. *If p is a prime, $\mathcal{A}, \mathcal{B} \subseteq \{1, \dots, p-1\}$ and for all $a \in \mathcal{A}$, $b \in \mathcal{B}$ the number $ab+1$ is quadratic residue or 0 (mod p) then $|\mathcal{A}|\,|\mathcal{B}| \le (\sqrt{2p}+1)^2$.*

In order to see that the same holds in the general case where $ab+1$ is a kth power for all $a \in \mathcal{A}$, $b \in \mathcal{B}$ or $a+b$ is a kth power for all $a \in \mathcal{A}$, $b \in \mathcal{B}$ we have to use multiplicative characters. χ_0 will denote the principal character.

Part (a) of the next theorem generalizes Vinogradov's Theorem 5, while part (b) is due to Erdős and Shapiro:

THEOREM 7. *Let $\mathcal{A}$, $\mathcal{B} \subseteq \{1, \dots, p\}$ and $\chi \neq \chi_0$ be a multiplicative character mod p. Then*

$$\text{(a)} \qquad \Big|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(ab+1)\Big| \le \sqrt{p|\mathcal{A}|\,|\mathcal{B}|},$$

$$\text{(b)} \qquad \Big|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(a+b)\Big| \le \sqrt{p|\mathcal{A}|\,|\mathcal{B}|}.$$

Using this theorem we will get

THEOREM 8. *Let $k \in \mathbb{N}$. If p is a prime, $(p-1,k) \neq 1$, $\mathcal{A}, \mathcal{B} \subseteq \{1, \dots \dots, p-1\}$ and*

(a) *for all $a \in \mathcal{A}$, $b \in \mathcal{B}$, there exists an integer x such that $ab + 1 \equiv x^k \pmod{p}$ or*

(b) *for all $a \in \mathcal{A}$, $b \in \mathcal{B}$, there exists an integer x such that $a + b \equiv x^k \pmod{p}$*

then $|\mathcal{A}|\,|\mathcal{B}| \le (\sqrt{p}+2)^2$.

The importance of the condition $(p-1,k) \neq 1$ lies in the fact that if $(p-1,k) = 1$ then the congruence $x^k \equiv a \pmod{p}$ has precisely one solution for all $a \in \mathbb{N}$ and thus there is no non-trivial upper bound for $|\mathcal{A}|\,|\mathcal{B}|$.

Next we extend the additive analog of the problem of Diophantus to the case of two different sequences and $k \ge 2$. The proof is like that in the case of a single set $\mathcal{A}$ and $k = 2$ (see [13]). The interesting feature of these results is that the proofs are based on a sieve result.

THEOREM 9. *For any integer $k > 1$, there is a real number N_0 such that if $N \ge N_0$, $\mathcal{A}, \mathcal{B} \subseteq \{1, \dots, N\}$ and $a + b$ is a kth power for all $a \in \mathcal{A}$, $b \in \mathcal{B}$ then $\min(|\mathcal{A}|, |\mathcal{B}|) \le 4k \log N$.*

Finally we will generalize the problems further by replacing x^k by a polynomial $h(x)$.

THEOREM 10. *Let $h(x) \in F_p[x]$ where the degree of $h(x)$ is $n > 1$. Let p be a prime and $p > n$, $\mathcal{A}, \mathcal{B} \subseteq \{1, \dots, p-1\}$ and*

$$|\mathcal{A}|\,|\mathcal{B}| \ge p\left(\frac{p-1}{p-n}\right)^2 (n-1)^2.$$

(a) *If for all $d > 1$, $d \,|\, p-1$, the polynomial $h(x)$ is not the constant multiple of a dth power of a polynomial mod p then there exist $a \in \mathcal{A}$, $b \in \mathcal{B}$ such that the congruence $ab \equiv h(x) \pmod{p}$ is solvable and, indeed, denoting the number of solutions of the congruence in $a \in \mathcal{A}$, $b \in \mathcal{B}$, $x \in F_p$ by N, we* *have*

$$|N-|\mathcal{A}|\,|\mathcal{B}||<\frac{n}{p-1}|\mathcal{A}|\,|\mathcal{B}|+(n-1)\sqrt{p|\mathcal{A}|\,|\mathcal{B}|}.$$

(b) *There exist* $a\in\mathcal{A}$, $b\in\mathcal{B}$ *such that the congruence* $a+b\equiv h(x)$ $(\operatorname{mod} p)$ *is solvable, and denoting the number of solutions of the congruence* (*in* a, b, x) *by* M, *we have*

$$|M-|\mathcal{A}|\,|\mathcal{B}||<(n-1)\sqrt{p|\mathcal{A}|\,|\mathcal{B}|}.$$

The starting point in our proof will be Weil's Theorem. Is the condition that for all $d\,|\,p-1$, $h(x)$ is not the constant multiple of a dth power necessary? Suppose that there are constants c, d and $h'(x)\in F_p[x]$ such that $d\,|\,p-1$ and $h(x)=c(h'[x])^d$. Let m be a number which is not a dth power mod p and $\mathcal{A}=\{x^d : x\in F_p,\ x\neq 0\}$, $\mathcal{B}=\{cmx^d : x\in F_p,\ x\neq 0\}$. Then for all $a\in\mathcal{A}$, $b\in\mathcal{B}$ there are no $x\in F_p$ such that $ab=cx^d$; therefore the congruence $ab\equiv h(x)$ $(\operatorname{mod} p)$ is not solvable in F_p. Specializing this theorem we obtain a generalization of the Fermat congruence.

Corollary. *Let* $n\in\mathbb{N}$ *and let* $f(x),g(x),h(x)\in F_p[x]$ *have degree* $\leq n$ *each. Let* p *be a prime and* $p>n^4$.

(a) *Suppose that, for all* $d>1$, $d\,|\,p-1$, *neither of* $f(x)$, $g(x)$, $h(x)$ *is the constant multiple of a dth power of a polynomial mod p. Then the congruence* $f(x)g(y)\equiv h(z)$ $(\operatorname{mod} p)$ *is solvable.*

(b) *The congruence* $f(x)+g(y)\equiv h(z)$ $(\operatorname{mod} p)$ *is solvable.*

This result is not new (see [10, pp. 97–98]); the point is that it is obtained here as a very special case of a general result involving general sequences.

3. Proofs

Proof of Theorem 1. Let $x,y\in\mathcal{A}$, $x<y$ and $c,d\in\mathcal{B}$, $c<d$. Then $(y-x)(d-c)>0$. From this,

$$(xc+1)(yd+1)>(xd+1)(yc+1).$$

Now $(xc+1)(yd+1)$ is a kth power and $\sqrt[k]{(xd+1)(yc+1)}$ is an integer, thus

$$xycd+xc+yd+1\geq(\sqrt[k]{(xd+1)(yc+1)}+1)^k.$$

So

$$xycd+xc+yd+1\geq xycd+xd+yc+1+k(xycd)^{(k-1)/k}.$$

Using $xd+yc>xc$ we get $yd>k^k(xc)^{k-1}$.

Let $\mathcal{A}=\{a_1,\dots,a_m\}$, $\mathcal{B}=\{b_1,\dots,b_n\}$ where $a_1<\dots<a_m$ and $b_1<\dots<b_n$. For simplicity we assume that $m\leq n$. In the case $k=2$ we get $a_1b_1\geq 4$ or $a_2b_2\geq 16$ because a_ib_j+1 is a perfect square for all

$1 \le i \le j \le 2$. From this,

$$N^2 \ge a_m b_m > 4a_{m-1}b_{m-1} > \ldots > 4^m.$$

So $m \le \frac{1}{\log 2} \log N$.

A similar result holds in the case $k > 2$. Then we have $a_{t+1}b_{t+1} > (a_t b_t)^{k-1}$ for $1 \le t \le m$. Using the fact that $a_1 b_1 > 2^{k-1}$ we get

$$N^2 \ge a_m b_m > (a_{m-1}b_{m-1})^{k-1} > \ldots > 2^{(k-1)^m}.$$

Then

$$m \le \frac{1}{\log(k-1)} \log\log N + 1,$$

which completes the proof of Theorem 1.

Proof of Theorem 2. Let $\mathcal{B} = \{b_1, \ldots, b_n\}$ where $b_1 < \ldots < b_n$. We have proved that $a_2 b_{t+1} > 4a_1 b_t$ for $1 \le t \le n-1$. As $2a_1 \ge a_2$, we have $b_{t+1} > 2b_t$. Therefore $N \ge 2^m$, whence the statement of the theorem follows.

Proof of Theorem 3. Let $x_1 = 5$, $x_2 = 29$ and $x_n = 6x_{n-1} - x_{n-2}$ for $n \ge 3$. Then $x_n \le 6x_{n-1}$. From this we have $x_n < 6^n$. Let $\mathcal{B} = \{x_i^2 - 1 : x_i < \sqrt{N}\}$.

It remains to prove that $|\mathcal{B}| \ge \left[\frac{1}{\log 36} \log N\right]$ and for all $a \in \mathcal{A}, b \in \mathcal{B}$ the number $ab + 1$ is a perfect square. If $6^i \le \sqrt{N}$ then $x_i^2 - 1 \in \mathcal{B}$. So $|\mathcal{B}| \ge \left[\frac{1}{\log 36} \log N\right]$. We write

$$y_n = \tfrac{1}{2}x_{n+1} - \tfrac{3}{2}x_n.$$

Then

$$y_{n+1} = \tfrac{1}{2}(6x_{n+1} - x_n) - \tfrac{3}{2}x_{n+1} = 4x_n + 3\left(\tfrac{1}{2}x_{n+1} - \tfrac{3}{2}x_n\right) = 4x_n + 3y_n.$$

So we have

$$y_{n+1} = 3y_n + 4x_n, \qquad x_{n+1} = 2y_n + 3x_n.$$

Therefore the numbers y_n, x_n satisfy the Pell equation $y^2 - 2x^2 = -1$ since the numbers 3, 2 form the smallest solution of the Pell equation $y^2 - 2x^2 = 1$. Therefore both $(x_i^2 - 1) + 1 = x_i^2$ and $2(x_i^2 - 1) + 1 = y_i^2$ are perfect squares. This completes the proof of Theorem 3.

Theorem 4 will follow from the following Ramsey type result:

Lemma 1. *If s_1, s_2, s_3 are non-negative integers then there exists an integer r with the following property: If G is a complete graph, $|G| \ge r$ and C is any 3-colouring of the edges of G with colours c_1, c_2, c_3, then for some $1 \le i \le 3$ the graph G has a subgraph G' which is monochromatic with colour c_i and $|G'| \ge s_i$. Furthermore, denoting the least integer r with this property by $R(s_1, s_2, s_3)$ we have*

$$R(s_1, s_2, s_3) \le \frac{(s_1 + s_2 + s_3)!}{s_1! s_2! s_3!}.$$

Proof. If any of the numbers $s_1,\ s_2,\ s_3$ is 0 then the lemma is trivial because $R(s_1, s_2, s_3) = 0$. We may assume that $s_1, s_2, s_3 > 0$. The following inequality is well known [9, p. 75]:

$$R(s_1, s_2, s_3) \le R(s_1 - 1, s_2, s_3) + R(s_1, s_2 - 1, s_3) + R(s_1, s_2, s_3 - 1)$$

for $s_1, s_2, s_3 > 0$. Using induction we get the assertion.

Proof of Theorem 4. Consider the graph whose vertices are the residue classes modulo p. Since p is a prime of the form $4k+1$ there exists an integer i such that $i^2 \equiv -1 \pmod p$.

Let the edge e join the classes a and b. We colour e with c_1 if $\left(\frac{ab+1}{p}\right) = 1$ or 0. Furthermore we colour e with c_2 if $\left(\frac{-ab+1}{p}\right) = 1$ or 0 and $\left(\frac{ab+1}{p}\right) = -1$. Finally we colour e with c_3 if $\left(\frac{-a^2b^2+1}{p}\right) = 1$ or 0 and $\left(\frac{ab+1}{p}\right) = \left(\frac{-ab+1}{p}\right) = -1$ (we set $\left(\frac{0}{p}\right) = 0$). We colour all edges because otherwise

$$\left(\frac{ab+1}{p}\right) = \left(\frac{-ab+1}{p}\right) = \left(\frac{-a^2b^2+1}{p}\right) = -1.$$

So

$$-1 = \left(\frac{(ab+1)(-ab+1)(-a^2b^2+1)}{p}\right) = \left(\frac{(a^2b^2-1)^2}{p}\right).$$

But this contradicts the obvious fact that $\left(\frac{(a^2b^2-1)^2}{p}\right) = 1$ or 0.

Take $c = \left[\frac{1}{3\log 3}\log p\right] + 1$. Applying Lemma 1 we obtain

$$R(c, c, c) \le \frac{(3c)!}{c!c!c!}.$$

By the Stirling formula, as $c \to \infty$ we have

$$\frac{(3c)!}{c!c!c!} \le (1 + o(1)) \frac{\left(\frac{3c}{e}\right)^{3c}\sqrt{2\pi 3c}}{\left(\left(\frac{c}{e}\right)^{c}\sqrt{2\pi c}\right)^3} \le 3^{3c-3} \le p.$$

Thus if p is large enough then $R(c, c, c) \le p$. Therefore the graph has a subgraph X which is monochromatic with colour c_j for some $1 \le j \le 3$ and $|X| \ge c$.

Let $\mathcal{A}$ be X if we coloured the edges of X with c_1, let it be $\{ix : x \in X\}$ if we coloured the edges of X with c_2, and $\{ix^2 : x \in X\}$ if we coloured the edges of X with c_3.

Now $|\mathcal{A}| \ge \frac{1}{2}|X|$. Using the definition of colouring, we conclude that the product of any two elements of $\mathcal{A}$ increased by 1 is a quadratic residue or 0 mod p.

Proof of Theorem 5. See [17, Chap. 5, Problem 8].

Proof of Theorem 6. We may assume that $|\mathcal{A}| \le |\mathcal{B}|$. Using the assumption that for all $a \in \mathcal{A}$, $b \in \mathcal{B}$ we have $\left(\frac{ab+1}{p}\right) = 1$ or 0, it follows from

Theorem 5 that

$$|\mathcal{A}|\,|\mathcal{B}| - \sqrt{|\mathcal{A}|\,|\mathcal{B}|} \le |\mathcal{A}|(|\mathcal{B}|-1) \le \sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+1}{p}\right) \le \sqrt{2p|\mathcal{A}|\,|\mathcal{B}|}.$$

But this is equivalent to the assertion.

Proof of Theorem 7. Erdős and Shapiro proved Theorem 7(b) in [6]. Later Friedlander and Iwaniec [8] studied similar questions. They proved that if $\mathcal{A} \subseteq (M, M+A)$, $\mathcal{B} \subseteq (M, M+B)$, $AB \le p$ and $B \le A$ then for any integer $r \ge 1$ and $\varepsilon > 0$, we have

$$\Big|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(a+b)\Big| \ll A^{1/2}|\mathcal{A}|^{1/2}|\mathcal{B}|\left(\frac{(A+p^{1/(2r)}B)B}{A^2|\mathcal{B}|^2}\right)^{1/(4r)} p^{1/(8r)+\varepsilon} + |\mathcal{A}|^{1/2}|\mathcal{B}|^{1/2}(A+p^{1/(2r)}B)^{1/2},$$

the implied constant depending on r and ε.

In order to prove Theorem 7(a), we will use Gaussian sums. Let

$$\tau(\chi) = \sum_{m=1}^{n}\chi(m)e\left(\frac{m}{q}\right),$$

where χ is a primitive character. Then $|\tau(\chi)| = \sqrt{p}$; the proof can be found in [2, p. 66]. We shall need the following lemmas.

Lemma 2. *If χ is a primitive character mod p then*

$$\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{h=1}^{p}\overline{\chi}(h)e\left(\frac{hn}{p}\right).$$

Proof. See [2, p. 68].

The following lemma is well known and very simple.

Lemma 3. *If $T(\alpha) = \sum_{n=1}^{p} c_n e(n\alpha)$ then*

$$\sum_{h=1}^{p}\left|T\left(\frac{h}{p}\right)\right|^2 = p\sum_{n=1}^{p}|c_n|^2.$$

By Lemma 2 we get

$$S = \Big|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(ab+1)\Big| = \left|\frac{1}{\tau(\overline{\chi})}\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{h=1}^{p}\overline{\chi}(h)e\left(\frac{(ab+1)h}{p}\right)\right|.$$

We replace $h = lb^{-1}$ and use the fact that $|\tau(\overline{\chi})| = \sqrt{p}$:

$$S = \frac{1}{\sqrt{p}}\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{l=1}^{p}\overline{\chi}(lb^{-1})e\left(\frac{al+lb^{-1}}{p}\right)\right|.$$

Let $\mathcal{B}' = \{b^{-1} : b \in \mathcal{B}\}$. It is trivial that $|\mathcal{B}'| = |\mathcal{B}|$. Furthermore,

$$\begin{aligned} S &= \frac{1}{\sqrt{p}} \left| \sum_{l=1}^{p} \overline{\chi}(l) \sum_{a\in\mathcal{A}} e\Big(\frac{al}{p}\Big) \sum_{b\in\mathcal{B}'} \overline{\chi}(b) e\Big(\frac{bl}{p}\Big) \right| \\ &\le \frac{1}{\sqrt{p}} \sum_{l=1}^{p} \left| \sum_{a\in\mathcal{A}} e\Big(\frac{al}{p}\Big) \right| \left| \sum_{b\in\mathcal{B}'} \overline{\chi}(b) e\Big(\frac{bl}{p}\Big) \right|. \end{aligned}$$

Using the Cauchy–Schwarz inequality we get

$$S \le \frac{1}{\sqrt{p}} \sqrt{ \sum_{l=1}^{p} \left| \sum_{a\in\mathcal{A}} e\Big(\frac{al}{p}\Big) \right|^2 \sum_{l=1}^{p} \left| \sum_{b\in\mathcal{B}'} \overline{\chi}(b) e\Big(\frac{bl}{p}\Big) \right|^2 }.$$

Applying Lemma 3 with $c_n = 0$ if $n \notin \mathcal{A}$ and $c_n = 1$ if $n \in \mathcal{A}$ we get

$$\sum_{l=1}^{p} \left| \sum_{a\in\mathcal{A}} e\Big(\frac{al}{p}\Big) \right|^2 = p|\mathcal{A}|.$$

Similarly, writing $c_n = 0$ if $n \notin \mathcal{B}'$ and $c_n = \overline{\chi}(n)$ if $n \in \mathcal{B}'$, by Lemma 3 we get

$$\sum_{l=1}^{p} \left| \sum_{b\in\mathcal{B}'} \overline{\chi}(b) e\Big(\frac{bl}{p}\Big) \right|^2 = p|\mathcal{B}|.$$

Therefore $S \le \sqrt{p}\sqrt{|\mathcal{A}|\,|\mathcal{B}|}$.

Proof of Theorem 8. Let $f(a,b)$ be $ab+1$ in case (a) and $a+b$ in case (b). It will be sufficient to prove that Theorem 8 holds when k is a prime. Indeed, in the general case we know that $(k, p-1) \ne 1$, thus k has a k_0 prime divisor which divides $p-1$. Then $f(a,b)$ is a perfect k_0th power mod p for all $a \in \mathcal{A}$, $b \in \mathcal{B}$.

So consider the case when k is a prime and thus $k \mid p-1$. Without loss of generality we may assume that $|\mathcal{A}| \le |\mathcal{B}|$. We will using the following simple statement: for $(x,p) = 1$ we have

$$\sum_{\chi:\, \chi^k = \chi_0} \chi(x) = \begin{cases} k & \text{if } x \text{ is a } k\text{th power mod } p \text{ and } x \not\equiv 0 \text{ mod } p, \\ 0 & \text{if } x \text{ is not a } k\text{th power mod } p \text{ or } x \equiv 0 \text{ mod } p. \end{cases}$$

Now for $|\mathcal{A}| \le |\mathcal{B}|$ Theorem 7 shows that

$$\begin{aligned} k(|\mathcal{A}|\,|\mathcal{B}| - \sqrt{|\mathcal{A}|\,|\mathcal{B}|}) \le k|\mathcal{A}|(|\mathcal{B}|-1) &\le \sum_{a\in\mathcal{A}} \sum_{\substack{b\in\mathcal{B} \\ f(a,b)\ne 0}} \sum_{\chi:\, \chi^k=\chi_0} \chi(f(a,b)) \\ &\le |\mathcal{A}|\,|\mathcal{B}| + \sum_{\substack{\chi:\, \chi^k=\chi_0 \\ \chi\ne\chi_0}} \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \chi(f(a,b)) \\ &\le |\mathcal{A}|\,|\mathcal{B}| + (k-1)\sqrt{p}\sqrt{|\mathcal{A}|\,|\mathcal{B}|}. \end{aligned}$$

It follows that

$$|\mathcal{A}|\,|\mathcal{B}| \le \left(\sqrt{p} + \frac{k}{k-1}\right)^2.$$

In order to prove Theorem 9, we shall need the following lemma.

LEMMA 4 (Gallagher). *Let X be a set of integers in the interval $[M+1, M+N]$. For each prime p let $\nu_X(p)$ denote the number of residue classes modulo p that contain an element of X. Then for any finite set $\mathcal{P}$ of primes we have*

$$|X| \le \frac{\sum_{p\in\mathcal{P}} \log p - \log N}{\sum_{p\in\mathcal{P}} (\log p)/\nu_X(p) - \log N}$$

provided that the denominator is positive.

Proof. This is Gallagher's "larger sieve" (see [13]).

Proof of Theorem 9. Let $\mathcal{A}'$ and $\mathcal{B}'$ denote the sets of integers r such that $r \in \{1,\dots,p-1\}$ and there is at least one $a \in \mathcal{A}$ resp. $b \in \mathcal{B}$ congruent to r modulo p. Then using Theorem 8 with $\mathcal{A}'$ and $\mathcal{B}'$, respectively, we get

$$\min\{\nu_{\mathcal{A}}(p), \nu_{\mathcal{B}}(p)\} \le \sqrt{p} + 3.$$

Let $\mathcal{P} = \{p : p \text{ is a prime}, p \equiv 1 \pmod k, p \le 4(\varphi(k)\log N)^2\}$. Divide the set $\mathcal{P}$ into two parts:

$$\mathcal{P}_{\mathcal{A}} = \{p \in \mathcal{P} : \min\{\nu_{\mathcal{A}}(p), \nu_{\mathcal{B}}(p)\} = \nu_{\mathcal{A}}(p)\},$$
$$\mathcal{P}_{\mathcal{B}} = \{p \in \mathcal{P} : \min\{\nu_{\mathcal{A}}(p), \nu_{\mathcal{B}}(p)\} \ne \nu_{\mathcal{A}}(p)\}.$$

It follows from Lemma 4 that either of the following inequalities is true if its denominator is positive:

$$|\mathcal{A}| \le \frac{\sum_{p\in\mathcal{P}_{\mathcal{A}}} \log p - \log N}{\sum_{p\in\mathcal{P}_{\mathcal{A}}} (\log p)/\nu_{\mathcal{A}}(p) - \log N}, \quad |\mathcal{B}| \le \frac{\sum_{p\in\mathcal{P}_{\mathcal{B}}} \log p - \log N}{\sum_{p\in\mathcal{P}_{\mathcal{B}}} (\log p)/\nu_{\mathcal{B}}(p) - \log N}.$$

We may assume that

$$\sum_{p\in\mathcal{P}_{\mathcal{A}}} \frac{\log p}{\nu_{\mathcal{A}}(p)} - \log N \ge \sum_{p\in\mathcal{P}_{\mathcal{B}}} \frac{\log p}{\nu_{\mathcal{B}}(p)} - \log N.$$

Then by Mertens's theorem and the prime number theorem for arithmetic progressions of small moduli we have

$$\begin{aligned} W &= 2\biggl(\sum_{p\in\mathcal{P}_{\mathcal{A}}} \frac{\log p}{\nu_{\mathcal{A}}(p)} - \log N\biggr) \ge \sum_{p\in\mathcal{P}_{\mathcal{A}}} \frac{\log p}{\nu_{\mathcal{A}}(p)} - \log N + \sum_{p\in\mathcal{P}_{\mathcal{B}}} \frac{\log p}{\nu_{\mathcal{B}}(p)} - \log N \\ &= \sum_{p\in\mathcal{P}} \frac{\log p}{\min(\nu_{\mathcal{A}}(p), \nu_{\mathcal{B}}(p))} - 2\log N \ge \sum_{p\in\mathcal{P}} \frac{\log p}{\sqrt{p}+3} - 2\log N \\ &= (2+o(1))\log N, \end{aligned}$$

whence

$$|\mathcal{A}| \leq \frac{\sum_{p\in\mathcal{P}} \log p - \log N}{(1+o(1))\log N} \leq 4k \log N.$$

This completes the proof of Theorem 9.

Proof of Theorem 10. (a) We shall need the following lemmas:

Lemma 5. *We have*

$$\sum_{\chi} \Big|\sum_{n=1}^{p-1} c_n \chi(n)\Big|^2 = (p-1)\sum_{n=1}^{p-1} c_n^2.$$

This lemma is well known and easy to prove.

Lemma 6. *Suppose χ is a modulo p character of order $d>1$. Suppose $f(x)\in F_p[x]$ has m distinct roots over the algebraic closure of F_p, and it is not the constant multiple of the dth power of a polynomial over F_p. Then*

$$\Big|\sum_{x\in F_p} \chi(f(x))\Big| \leq (m-1)\sqrt{p}.$$

Proof. This lemma was proved by A. Weil (see [15, p. 43]).

If $ab \equiv h(x) \pmod p$ then $\sum_\chi \chi(a^{-1}b^{-1}h(x)) = p-1$, otherwise $\sum_\chi \chi(a^{-1}b^{-1}h(x)) = 0$. It is clear that there exist $a\in\mathcal{A}$, $b\in\mathcal{B}$ such that the congruence $ab\equiv h(x) \pmod p$ is solvable if and only if

$$0<(p-1)N = \sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{\chi}\chi(a^{-1}b^{-1}h(x)).$$

Let H denote the number of distinct zeros of $h(x)$. Then

$$|(p-H)|\mathcal{A}|\,|\mathcal{B}| - (p-1)N| = \Big|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{\chi\neq\chi_0}\chi(a^{-1}b^{-1}h(x))\Big|.$$

Using the Cauchy–Schwarz inequality and Lemmas 5 and 6 we have

$$\begin{aligned}
&\Big|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{\chi\neq\chi_0}\chi(a^{-1}b^{-1}h(x))\Big| \\
&\qquad\leq \sum_{\chi\neq\chi_0}\Big|\sum_{a\in\mathcal{A}}\chi(a^{-1})\sum_{b\in\mathcal{B}}\chi(b^{-1})\Big|\Big|\sum_{x=0}^{p-1}\chi(h(x))\Big| \\
&\qquad\leq \sqrt{\sum_{\chi\neq\chi_0}\Big|\sum_{a\in\mathcal{A}}\chi(a^{-1})\Big|^2}\sqrt{\sum_{\chi\neq\chi_0}\Big|\sum_{b\in\mathcal{B}}\chi(b^{-1})\Big|^2}(H-1)\sqrt{p} \\
&\qquad\leq (H-1)(p-1)\sqrt{p|\mathcal{A}|\,|\mathcal{B}|}.
\end{aligned}$$

If

$$|\mathcal{A}|\,|\mathcal{B}| \ge p\left(\frac{p-1}{p-H}\right)^2 (n-1)^2$$

then

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{\chi}\chi(a^{-1}b^{-1}h(x)) > 0.$$

Furthermore,

$$(H-1)\sqrt{p|\mathcal{A}|\,|\mathcal{B}|} > \left|N - \frac{p-H}{p-1}|\mathcal{A}|\,|\mathcal{B}|\right| \ge |N - |\mathcal{A}|\,|\mathcal{B}|| - \frac{H}{p-1}|\mathcal{A}|\,|\mathcal{B}|.$$

Thus Theorem 10(a) is proved.

(b) We will use the following lemma:

LEMMA 7. *Suppose p is a prime. Suppose $g(x) = a_nx^n + \ldots + a_0$ is a polynomial with integer coefficients*, $0 < n < p$ *and* $p\nmid a_n$. *Then*

$$\left|\sum_{x=0}^{p-1} e\left(\frac{g(x)}{p}\right)\right| \le (n-1)\sqrt{p}.$$

Proof. This lemma was proved by A. Weil (see [15, p. 45]).

If $a + b \equiv h(x) \pmod{p}$ then

$$\sum_{k=0}^{p-1} e\left(\frac{k(h(x)-a-b)}{p}\right) = p,$$

otherwise

$$\sum_{k=0}^{p-1} e\left(\frac{k(h(x)-a-b)}{p}\right) = 0.$$

It is clear that there exist $a \in \mathcal{A}$, $b \in \mathcal{B}$ such that the congruence $a+b \equiv h(x) \pmod{p}$ is solvable if and only if

$$0 < pN = \sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{k=0}^{p-1} e\left(\frac{k(h(x)-a-b)}{p}\right).$$

Then

$$|p|\mathcal{A}|\,|\mathcal{B}| - pN| = \left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{k=1}^{p-1} e\left(\frac{k(h(x)-a-b)}{p}\right)\right|.$$

Using the Cauchy–Schwarz inequality and Lemmas 3 and 7 we have

$$\begin{aligned}
\Bigl|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{k=1}^{p-1} e\Bigl(\frac{k(h(x)-a-b)}{p}\Bigr)\Bigr| \\
&= \sum_{k=1}^{p-1}\Bigl|\sum_{a\in\mathcal{A}} e\Bigl(-\frac{ka}{p}\Bigr)\sum_{b\in\mathcal{B}} e\Bigl(-\frac{kb}{p}\Bigr)\Bigr|\Bigl|\sum_{x=0}^{p-1} e\Bigl(\frac{kh(x)}{p}\Bigr)\Bigr| \\
&\le \sqrt{\sum_{k=1}^{p-1}\Bigl|\sum_{a\in\mathcal{A}} e\Bigl(-\frac{ka}{p}\Bigr)\Bigr|^2}\sqrt{\sum_{k=1}^{p-1}\Bigl|\sum_{b\in\mathcal{B}} e\Bigl(-\frac{kb}{p}\Bigr)\Bigr|^2}(n-1)\sqrt{p} \\
&\le (n-1)p\sqrt{p|\mathcal{A}|\,|\mathcal{B}|}.
\end{aligned}$$

If $|\mathcal{A}|\,|\mathcal{B}| > p(n-1)^2$ then

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{k=1}^{p-1} e\Bigl(\frac{k(h(x)-a-b)}{p}\Bigr) > 0.$$

Thus Theorem 10 is proved.

Proof of Corollary. In part (a) it will be sufficient to prove that the statement holds in the case when for all $d\,|\,p-1$, $h(x)$ is not the constant multiple of a dth power. Let $\mathcal{A}=\{f(x): x\in F_p\}$, $\mathcal{B}=\{g(y): y\in F_p\}$. Then $|\mathcal{A}|, |\mathcal{B}| \ge (p-1)/n$ because the congruences $f(x)\equiv a \pmod{p}$, $g(y)\equiv a \pmod{p}$ have at most n solutions. So

$$|\mathcal{A}|\,|\mathcal{B}| > p\Bigl(\frac{p-1}{p-n}\Bigr)^2(n-1)^2.$$

Using Theorem 10 we get the statement of Corollary.

I would like to thank Professor András Sárközy for the valuable advice.

References

[1] J. Arkin, V. E. Hogatt and E. G. Straus, *On Euler's solution of a problem of Diophantus*, Fibonacci Quart. 17 (1979), 333–339.

[2] H. Davenport, *Multiplicative Number Theory*, Markham, Chicago, 1967.

[3] A. Dujella, *On Diophantine quintuples*, Acta Arith. 81 (1997), 69–79.

[4] A. Dujella and A. Pethő, *Generalization of a theorem of Baker and Davenport*, Quart J. Math. Oxford Ser. (2) 49 (1998), 291–306.

[5] P. Erdős, *Quelques problèmes de la théorie des nombres*, in: Monograph. Enseign. Math. 6, Geneva, 1963, 81–135.

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

[7] P. Erdős and J. Surányi, *Selected Topics in Number Theory*, Polygon, 1996 (in Hungarian; English version in preparation).

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

[9] R. L. Graham, B. L. Rothschild and J. H. Spencer, *Ramsey Theory*, Wiley, 1980.

[10] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1980.

[11] J. Lagrange, *Six entiers dont les sommes deux à deux sont des carrés*, Acta Arith. 40 (1981), 91–96.

[12] J.-L. Nicolas, *Six nombres*, *dont les sommes deux à deux sont des carrés*, Bull. Soc. Math. France 49–50 (1977), 141–143.

[13] J. Rivat, A. Sárközy and C. L. Stewart, *Two problems on sum sets*, Illinois J. Math., to appear.

[14] A. Sárközy, *On difference sets of sequences of integers*, *II*, Ann. Univ. Sci. Budapest Eötvös Sect. Math. 21 (1978), 45–53.

[15] W. M. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Math. 536, Springer, 1976.

[16] W. Sierpiński, *A Selection of Problems in the Theory of Numbers*, Pergamon Press, 1964.

[17] I. M. Vinogradov, *Elements of Number Theory*, Dover, 1954.

Department of Algebra and Number Theory
Eötvös University
Kecskemeti u. 10-12
H-1053 Budapest, Hungary
E-mail: gykati@cs.elte.hu

Received on 27.7.1999
and in revised form on 26.5.2000 (3661)