ACTA ARITHMETICA
135.1 (2008)

Subset sums avoiding quadratic nonresidues

by

Péter Csikvári (Budapest)

1. Introduction. It is a well-known problem to estimate the largest clique of the Paley graph, i.e., to estimate $|A|$ for $A \subset F_p$ ($p \equiv 1 \pmod 4$) such that $A-A = \{a-a' \mid a, a' \in A\}$ avoids the set of quadratic nonresidues. In this paper we study a much simpler problem, namely with $A-A$ replaced by the set

$$\mathrm{FS}(A) = \Big\{ \sum \varepsilon_a a \mid \varepsilon_a = 0 \text{ or } 1 \text{ and } \sum \varepsilon_a > 0 \Big\}.$$

In other words, we will estimate the maximal cardinality of $A \subset F_p$ such that $\mathrm{FS}(A)$ avoids the set of quadratic nonresidues. We show that this problem is strongly related to the problem of estimating the least quadratic nonresidue $n(p)$, since the set $\{1, 2, \dots, [n(p)^{1/2}]\}$ satisfies the above condition. We prove that the maximal value of $|A|$ is $\Omega(\log\log p)$. On the other hand, we show that $|A| = O(n(p)\log^3 p)$. The proof is based on the fact that if t is a quadratic nonresidue then $\mathrm{FS}(A) \cap t \cdot \mathrm{FS}(A) = \emptyset$ or $\{0\}$ where by definition $t \cdot B = \{tb \mid b \in B\}$. We show that if t is small then $|\mathrm{FS}(A)|$ is much greater than $|A|$.

In the next section we study the case when $t = n(p) = 2$. In Section 3 we prove the upper bound $|A| = O(n(p)\log^3 p)$. In the last section we show that the maximal value of $|A|$ is $\Omega(\log\log p)$.

2. The case $n(p) = 2$. In the case $n(p) = 2$ we have $\mathrm{FS}(A) \cap 2 \cdot \mathrm{FS}(A) = \emptyset$ or $\{0\}$. First we consider the case $\mathrm{FS}(A) \cap 2 \cdot \mathrm{FS}(A) = \emptyset$.

Theorem 2.1. *If* $\mathrm{FS}(A) \cap 2 \cdot \mathrm{FS}(A) = \emptyset$ *then* $|\mathrm{FS}(A)| = 2^{|A|}$.

Proof. We have to show that if $\mathrm{FS}(A) \cap 2 \cdot \mathrm{FS}(A) = \emptyset$ then all the subset sums are different. Indeed, if two different sums had the same value then omitting the intersection we would get $s = a_{i_1} + \cdots + a_{i_l} = a_{j_1} + \cdots + a_{j_m}$

2000 *Mathematics Subject Classification*: Primary 11B75.
Key words and phrases: subset sums, quadratic residues.

$(i_u \neq j_v)$. In this case s and $2s = a_{i_1} + \cdots + a_{i_l} + a_{j_1} + \cdots + a_{j_m}$ would be in $\mathrm{FS}(A)$, which contradicts the assumption. ∎

A trivial consequence of Theorem 2.1 is

COROLLARY 2.2. *If* $n(p) = 2$ (*i.e.* $\left(\frac{2}{p}\right) = -1$) *and every element of* $\mathrm{FS}(A)$ *is a quadratic residue then* $|A| \leq (\log p)/\log 2$.

THEOREM 2.3. *Assume that* $0 \notin A$. *If* $\mathrm{FS}(A) \cap 2 \cdot \mathrm{FS}(A) = \emptyset$ *or* $\{0\}$ *then* $|A| \leq (2 \log p)/\log 2$.

REMARK 1. $0 \notin A$ is just a simplifying condition: if we leave out the 0 from A then $\mathrm{FS}(A)$ will not change and the cardinality of A will only decrease by 1.

Proof of Theorem 2.3. We will say that $\sum_{i \in I} a_i = a$ is an *irreducible a-sum* if there is no $\emptyset \neq J \subset I$ for which $\sum_{i \in J} a_i = 0$. Two irreducible a-sums are disjoint, because if $\sum_{i \in I_1} a_i = \sum_{j \in I_2} a_j$ then $\sum_{i \in I_1 \setminus I_2} a_i = \sum_{i \in I_2 \setminus I_1} a_i = s \neq 0$ and $s, 2s \in \mathrm{FS}(A)$ contradicts the assumption. On the other hand, in case $a \neq 0$ there cannot be two disjoint irreducible a-sums. Thus we only get an a-sum as the sum of "the" irreducible a-sum and a 0-sum. Each 0-sum is a sum of irreducible 0-sums so the number of 0-sums is at most $2^{|A|/2}$ since every irreducible 0-sum has at least two elements (here we have used the simplifying condition that $0 \notin A$). Hence $p \cdot 2^{|A|/2} \geq 2^{|A|}$, which yields the conclusion. ∎

COROLLARY 2.4. *If* $n(p) = 2$ *and every element of* $\mathrm{FS}(A)$ *is a square mod* p *then* $|A| \leq (2 \log p)/\log 2$.

COROLLARY 2.5. *If* $A \subset \{1, \ldots, N\}$ *and every element of* $\mathrm{FS}(A)$ *is a perfect square then* $|A| = O(\log \log N)$.

Proof. We will use Gallagher's larger sieve [4]. Let $y = 40 \log N \log \log N$ and let $S = \{p \leq y \mid p \text{ prime}, \ p \equiv 3 \text{ or } 5 \pmod 8\}$. By Corollary 2.4, $\nu(p) \leq (2 \log p)/\log 2$ for these primes p. By the larger sieve

$$|A| \leq \frac{\sum_{p \in S} \Lambda(p) - \log N}{\sum_{p \in S} \frac{\Lambda(p)}{\nu(p)} - \log N}$$

if the denominator is positive. We have

$$\log y \leq 2 \log \log N$$

if N is large enough. Furthermore

$$\sum_{p \in S} \Lambda(p) = \frac{1}{2}\, y + o(y)$$

and

$$\sum_{p\in S}\frac{\Lambda(p)}{\nu(p)} \ge \frac{(\log 2)y}{4\log y} + o\Big(\frac{y}{\log y}\Big) \ge \frac{y}{10\log y}$$

if y, thus also N, is large enough. Hence for large N,

$$\sum_{p\in S}\frac{\Lambda(p)}{\nu(p)} \ge \frac{40\log N\log\log N}{20\log\log N} = 2\log N.$$

Thus $|A| \le 40\log\log N$. ∎

3. Upper bound. First we will prove a theorem on Abelian groups from which the upper bound follows.

THEOREM 3.1. *Let $A \subset G$ where G is a finite Abelian group. Assume that $|A| \ge 2000t\log^3|G|$. Then there exists a $d \ne 0$ for which $\{d, 2d, \dots, td\} \subset \mathrm{FS}(A)$.*

Proof. We argue by contradiction. Assume that there exists a set A for which $|A| = n > 2000t\log^3|G|$ such that $\mathrm{FS}(A)$ does not contain any set $\{d, 2d, \dots, td\}$ where $d \ne 0$. We can also assume that $0 \notin A$. Let r be a fixed positive integer which we will choose later. We will use the Erdős–Rado theorem on Δ-systems.

LEMMA 3.2 (Erdős–Rado). *Assume that $A_1, \dots, A_m$ are subsets of a given set such that $m \ge r!(t-1)^r$ and $|A_i| = r$. Then they contain a Δ-system with t elements, i.e., $A_{i_1}, \dots, A_{i_t}$, $i_1 < \dots < i_t$, such that $A_{i_k} \cap A_{i_l} = \bigcap_{j=1}^{t} A_{t_j}$ for all $1 \le k < l \le t$.*

Again we first give an upper bound for the number of irreducible sums. (We recall that $\sum_{a\in I} a$ is irreducible if there is no $J \ne \emptyset$ with $J \subset I$ such that $\sum_{a\in J} a = 0$, and we call a sum an irreducible a-sum if it is irreducible and its value is a.) We estimate the number of r-term irreducible a-sums. If $a \ne 0$ then there exist at most $r!(t-1)^r$ r-term irreducible a-sums. Indeed, otherwise these sums as a set contain a Δ-system with t elements by the lemma. If we leave out the intersection of the sums of sets we get t disjoint sums having the same nonzero value since the sums were irreducible. Let d be the value of these sums. Then adding together some of these disjoint sums we find that $\{d, 2d, \dots, td\} \subset \mathrm{FS}(A)$ contradicting the assumption. This argument cannot be applied for $a = 0$ immediately since it may occur that t disjoint irreducible r-term sums form a Δ-system. Although we can easily solve this problem, now we can say that there are at most $n(r-1)!(t-1)^{r-1}$ irreducible 0-sums since if there are more then there is an $a \in A$ appearing in more than $(r-1)!(t-1)^{r-1}$ irreducible sums as a summand. Omitting a from these sums we get the previous case with $(r-1)$-term sums instead

of r, since these new sums have value $-a$ which is not 0 as $0 \notin A$, and are irreducible since a subsum of an irreducible sum is still irreducible.

Now we give an upper bound for the number of r-term a-sums. Every a-sum is a sum of an irreducible a-sum and some irreducible 0-sums (this decomposition is, of course, not unique, but this is not a problem since we only give an upper bound). Let us consider those representations where the irreducible r-term a-sum has k_1 terms and the irreducible 0-sums have $k_2, \dots, k_m$ terms, respectively. According to the previous argument the number of these sums is at most

$$\begin{aligned} k_1!(t-1)^{k_1} n(k_2-1)!(t-1)^{k_2-1} \cdots n(k_m-1)!(t-1)^{k_m-1} \\ \le \prod_{i=1}^{m} (n(k_i-1)!(t-1)^{k_i-1}) = n^m \Big(\prod_{i=1}^{m} (k_i-1)! \Big) (t-1)^{r-m}, \end{aligned}$$

since $\sum_{i=1}^{m} k_i = r$ and we will choose r later so that $k_1(t-1) \le r(t-1) \le n$. We now show that

$$n^m \Big(\prod_{i=1}^{m} (k_i-1)! \Big) (t-1)^{r-m} \le r^{r/2} n^{r/2+1} (t-1)^{r/2}.$$

Indeed, since every irreducible 0-sum has at least two elements (as $0 \notin A$), we have $m - 1 \le r/2$ and $n^{r/2+1-m} \ge (r(t-1))^{r/2+1-m}$. Hence

$$\begin{aligned} r^{r/2} n^{r/2+1} (t-1)^{r/2} &\ge r^{r/2} n^m (r(t-1))^{r/2+1-m} (t-1)^{r/2} \\ &\ge n^m r^{r-m} (t-1)^{r-m} \ge n^m \Big(\prod_{i=1}^{m} (k_i-1)! \Big) (t-1)^{r-m}, \end{aligned}$$

since $\prod_{i=1}^{m} (k_i-1)! \le (r-m)! \le r^{r-m}$. Let $p(r)$ denote the number of partitions of r. Then every $a \in G$ can be represented as a sum of r elements of A in at most $p(r) r^{r/2} n^{r/2+1} (t-1)^{r/2}$ ways. Since there are $\binom{n}{r}$ r-term sums we have

$$\binom{n}{r} \le |G| \cdot p(r) r^{r/2} n^{r/2+1} (t-1)^{r/2}.$$

We will choose r so that

$$\frac{\binom{n}{r}}{p(r) r^{r/2} n^{r/2+1} (t-1)^{r/2}}$$

is nearly maximal. For two consecutive r's consider the fraction

$$\begin{aligned} \frac{\binom{n}{r}}{p(r) r^{r/2} n^{r/2+1} (t-1)^{r/2}} : \frac{\binom{n}{r+1}}{p(r+1)(r+1)^{(r+1)/2} n^{(r+1)/2+1} (t-1)^{(r+1)/2}} \\ = \frac{r+1}{n-r} \frac{p(r+1)}{p(r)} \left(1 + \frac{1}{r}\right)^{r/2} (n(r+1)(t-1))^{1/2}. \end{aligned}$$

For the best choice of r this must be approximately 1. Let us choose $r =$

$[n^{1/3} : e(t-1)^{1/3}]$; up to a constant factor this is the best choice. Now we can use the elementary estimates $m(m/e)^m > m! > (m/e)^m$ for $m \geq 6$ to obtain

$$\begin{aligned}|G| &\geq \frac{\binom{n}{r}}{p(r)r^{r/2}n^{r/2+1}(t-1)^{r/2}} \\ &\geq \frac{\left(\frac{n}{e}\right)^n}{r(n-r)\left(\frac{r}{e}\right)^r\left(\frac{n-r}{e}\right)^{n-r}p(r)r^{r/2}n^{r/2+1}(t-1)^{r/2}} \\ &= \frac{1}{nr(n-r)p(r)}\left(\frac{n}{n-r}\right)^{n-r}\left(\frac{n^{1/2}}{r^{3/2}(t-1)^{1/2}}\right)^r \geq \frac{1}{|G|^3p(r)}\,(e^{3/2})^r.\end{aligned}$$

In the latter inequality we have used the fact that $|G| \geq \max\{n, r, n-r\}$. Now we use the classical estimate

$$p(r) < \exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{r}\right) < \exp\left(\frac{1}{2}\,r\right).$$

It follows that $|G|^4 > e^r$ so $4\log|G| \geq r$. Thus $4^3\log^3|G| \geq r^3 > n/30(t-1)$, whence $2000(t-1)\log^3|G| > n$, contrary to assumption. ∎

Remark 2. The basic idea of this proof comes from an article of Erdős and Sárközy [3], who study what can be said about the length of an arithmetic progression contained in the set of subset sums of a subset of $\{1, \ldots, N\}$.

The statement of Theorem 3.1 is nearly sharp since for the set

$$A = \{t, t+1, \ldots, [\sqrt{2}\,t]\} \subset Z_n$$

with $t^3 < n$ no two elements of $\mathrm{FS}(A)$ have quotient t, and $|A| = \Omega(t)$. On the other hand, a basis of Z_3^n shows that the set of subset sums does not contain two elements with quotient 2, and we have $|A| = \Omega(\log|Z_3|^n)$. Other much trickier examples can be found in the above mentioned article.

Corollary 3.3. *Let $A \subset F_p$. Assume that $\mathrm{FS}(A)$ avoids the quadratic nonresidues. Then $|A| = O(n(p)\log^3 p)$, where $n(p)$ denotes the least quadratic nonresidue.*

Proof. Otherwise one can apply Theorem 3.1 with $t = n(p)$ to deduce that there exists a $d \neq 0$ for which d and $n(p)d$ are both quadratic residues, which is a contradiction. ∎

Remark 3. If we also assume that $0 \notin \mathrm{FS}(A)$, i.e., every element of $\mathrm{FS}(A)$ is a quadratic residue, then $|A| = O(n(p)\log^2 p)$, so that we can win a factor $\log p$ since we do not need to estimate the number of irreducible sums, and we can apply the Erdős–Rado theorem immediately. On the other hand, obviously one can replace the set of quadratic nonresidues by the set of quadratic residues, since one can multiply each element of A with the same quadratic nonresidue and by construction no subset sum of the new set is a quadratic residue.

Remark 4. Since $n(p) = O_\varepsilon(p^{1/4\sqrt{e}+\varepsilon})$ [1], we get this upper bound also for the maximal value of $|A|$. According to a result of Burgess and Elliott [2], if $g(p)$ denotes the least primitive root modulo p then

$$\frac{1}{\pi(x)}\sum_{p\le x} g(p) \le C\log^2 x \log\log^4 x.$$

Since $n(p) \le g(p)$ this shows that on average the maximal value of $|A|$ cannot be greater than $\log^6 p$.

4. Lower bound. In this section we will show that the maximal value of $|A|$ is at least $\Omega(\log\log p)$. The proof is based on Weil's estimation of character sums.

Theorem 4.1. *There exists an $A \subset F_p$ such that $|A| = \Omega(\log\log p)$ and* $\mathrm{FS}(A)$ *avoids the set of quadratic nonresidues.*

First we prove a lemma.

Lemma 4.2. *Let Q be the set of quadratic residues. Assume that for some set B we have $Q + B = F_p$. Then $|B| \ge \frac{1}{4}\log p$.*

Proof. Let $B = \{b_1, \dots, b_k\}$ and $Q_i = Q + b_i$. Then

$$\Big|F_p - \bigcup_{i=1}^{k} Q_i\Big| = |F_p| - \sum |Q_i| + \sum |Q_i \cap Q_j| - \cdots$$

by the inclusion-exclusion formula. Now,

$$|Q_{i_1}\cap\cdots\cap Q_{i_l}| = \sum_{a\in F_p}\frac{1}{2^l}\left(1+\left(\frac{a-b_{i_1}}{p}\right)\right)\cdots\left(1+\left(\frac{a-b_{i_l}}{p}\right)\right)+m(i_1,\dots,i_l)$$

where $|m(i_1,\dots,i_l)| \le l/2$, since it may occur that $a - b_{i_j} = 0$. By Weil's theorem [5],

$$\left|\sum_{n=1}^{p}\left(\frac{f(n)}{p}\right)\right| \le (t-1)\sqrt{p}$$

where $f(x) = \prod_{i=1}^{t}(x - a_i)$ and $a_1, \dots, a_t$ are distinct elements of F_p. Multiplying out the product we see that

$$\left(1+\left(\frac{a-b_{i_1}}{p}\right)\right)\dots\left(1+\left(\frac{a-b_{i_l}}{p}\right)\right) = 1 + \sum\left(\frac{f(a)}{p}\right)$$

where f runs through the $2^l - 1$ polynomials of the type considered above. Hence

$$|Q_{i_1}\cap\cdots\cap Q_{i_l}| = p/2^l + m'(i_1,\dots,i_l)$$

where $|m'(i_1,\dots,i_l)| \le 2^{-l}(2^l-1)(l-1)\sqrt{p} + l/2$. We can assume that $l \le k \le \sqrt{p}$ (if $k \ge \sqrt{p}$ we are done). Thus $|m'(i_1,\dots,i_l)| \le k\sqrt{p}$. It follows

that

$$0 = \Big|F_p - \bigcup_{i=1}^{k} Q_i\Big| = p - \sum_{i=1}^{k}\left(\frac{p}{2} + m'(i)\right) + \sum\left(\frac{p}{4} + m'(i,j)\right) - \cdots$$
$$= p(1-1/2)^k + M$$

where $|M| \le 2^k k\sqrt{p}$. Hence $p/2^k = |M| \le 2^k k\sqrt{p}$, thus $\sqrt{p} < k4^k < e^{2k}$ so that $k \ge \frac{1}{4}\log p$. ∎

REMARK 5. Clearly the same statement holds for the set R of quadratic nonresidues.

Proof of Theorem 4.1. Let A be a maximal set for which $\mathrm{FS}(A)$ avoids the quadratic nonresidues. We will show that

$$|A| \ge \frac{1}{\log 2}\log\log p - 2.$$

Suppose otherwise. Then $|\mathrm{FS}(A)| \le 2^{|A|} \le \frac{1}{4}\log p$, thus $R - \mathrm{FS}(A) \ne F_p$ so there exists an $s \in F_p$ for which $s \notin R-(a_{i_1}+\cdots+a_{i_l})$ for any $a_{i_1},\dots,a_{i_l} \in A$. Hence one can add s to A, which contradicts the maximality of A. ∎

REMARK 6. There exists a set B for which $|B| = [10\log p]$ and $Q + B = F_p$. Let us choose the elements of B independently at random with probability $P(b \in B) = (c\log p)/p$. Then

$$P(x \notin Q+B) = \prod_{i=1}^{(p-1)/2} P(x - i^2 \notin B) = \left(1 - \frac{c\log p}{p}\right)^{(p-1)/2}$$

since we have chosen the elements independently. Hence

$$P(Q + B \ne F_p) \le \sum_{x=0}^{p-1} P(x \notin Q+B) = p\left(1 - \frac{c\log p}{p}\right)^{(p-1)/2} \le pe^{-\frac{1}{3}c\log p}.$$

On the other hand, by the Chernoff inequality [6] we have

$$P(|\,|B| - c\log p| \ge \lambda\sigma) \le 2\max(e^{-\lambda^2/4}, e^{-\lambda\sigma/2})$$

where

$$\frac{1}{2}\,c\log p \le \sigma^2 = p\,\frac{c\log p}{p}\left(1 - \frac{c\log p}{p}\right) \le c\log p.$$

Choosing $c = 4$ and $\lambda = \sqrt{8\log p}$ we get

$$P(|\,|B| - 4\log p| \ge 4\sqrt{2}\log p) \le 2e^{-2\log p} = 2/p^2.$$

We have $pe^{-\frac{4}{3}\log p} = p^{-1/3}$. Since $2/p^2 + 1/p^{1/3} < 1$ for $p \ge 3$, with positive probability we have $|B| \le 10\log p$ and $Q + B = F_p$.

We have shown that in the case $\left(\frac{2}{p}\right) = -1$ we have $|\mathrm{FS}(A)| = 2^{|A|}$. Thus in general probably one cannot get an estimate better than $\Omega(\log\log p)$,

since after the selection of $|A|-1$ elements the set of subset sums has $2^{|A|-1}$ elements and it cannot be the additive complement of $-R$, while sets with more than $10\log p$ elements are such complements with high probability.

Acknowledgements. I profited much from discussions with A. Sárközy and K. Gyarmati.

References

[1] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 (1957), 106–112.
[2] D. A. Burgess and P. D. T. A. Elliott, *The average of the least primitive root*, ibid. 15 (1968), 39–50.
[3] P. Erdős and A. Sárközy, *Arithmetic progressions in subset sums*, Discrete Math. 102 (1992), 249–264.
[4] P. X. Gallagher, *A larger sieve*, Acta Arith. 18 (1971), 77–81.
[5] W. E. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Springer, Berlin, 1975.
[6] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math. 105, Cambridge Univ. Press, Cambridge, 2006 (p. 24).

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

Received on 25.10.2007
and in revised form on 29.6.2008 (5558)