ACTA ARITHMETICA
XLV (1985)

Regular coverings of the integers by arithmetic progressions

by

R. J. SIMPSON (Adelaide, Australia)

1. Introduction. We write $\langle a, d\rangle$ for the arithmetic progression, henceforth AP, consisting of all integers congruent to a modulo d.

DEFINITION 1. A collection $\mathscr{A} = \{\langle a_i, d_i\rangle : i = 1, \ldots, t\}$ of AP's is called a *regular covering* if every integer belongs to at least one AP in $\mathscr{A}$, and no subcollection has this property. We write $|\mathscr{A}|$ for the number of AP's in $\mathscr{A}$.

DEFINITION 2. A *disjoint covering* is a regular covering in which each integer belongs to exactly one AP.

We will also need the following function. If the canonical prime factorization of n is

$$n = \prod_{i=1}^{t} p_i^{\alpha_i},$$

then

$$f(n) = \sum_{i=1}^{t} \alpha_i (p_i - 1).$$

We note that $f(n)$ is a completely additive function.

In [4] Š. Znám conjectured that if $\mathscr{A}$ is a disjoint covering and P is the least common multiple of the moduli of the AP's in $\mathscr{A}$, then

$$|\mathscr{A}| \geqslant f(P) + 1. \tag{1.1}$$

In [2] and [3] Znám proved some results in this direction and in [1] Korec proved the conjecture.

In [5] Znám conjectured that $\mathscr{A}$ need only be regular for (1.1) to hold. In Theorem 2 of the present paper we prove a result slightly stronger than this, the conjecture itself being proved in the first corollary to that theorem.

In Section 2 we prove some straightforward lemmata and in Section 3 we prove Theorem 1 which gives a general property of regular coverings. The corollary to this theorem is used in the proof of Theorem 2.

2. Some lemmata.

LEMMA 1. (i) *$\langle a, d\rangle$ intersects $\langle A, D\rangle$ if and only if*

$$a \equiv A\big(\mathrm{mod}\,(d, D)\big)$$

where (d, D) is the greatest common divisor of d and D.

(ii) *If $\langle a, d\rangle$ intersects both $\langle A_1, D_1\rangle$ and $\langle A_2, D_2\rangle$ then*

$$A_1 \equiv A_2\big(\mathrm{mod}\,(d, D_1, D_2)\big).$$

Proof. (i) The intersection of $\langle a, d\rangle$ and $\langle A, D\rangle$ consists of those integers x satisfying

$$x \equiv a(\mathrm{mod}\ d), \quad x \equiv A(\mathrm{mod}\ D).$$

By the Chinese Remainder Theorem these congruences are simultaneously solvable if and only if $a \equiv A\big(\mathrm{mod}\,(d, D)\big)$.

(ii) By (i) we have

$$a \equiv A_1\big(\mathrm{mod}\,(d, D_1)\big) \quad \text{and} \quad a \equiv A_2\big(\mathrm{mod}\,(d, D_2)\big)$$

which imply the result. ■

LEMMA 2. *Suppose $\mathscr{A} = \{\langle a_i, d_i\rangle: i = 1, \ldots, t\}$ is a regular covering and p divides d_j for some j where p is a prime. Then the set*

$$\{a_i:\ p|d_i\}$$

contains a complete set of residues modulo p. Here $p|d_i$ means p divides d_i.

Proof. Suppose there is a residue class r mod p such that $\mathscr{A}$ contains no AP for which p divides d_i and a_i is congruent to r mod p. Then the integers congruent to r mod p must be covered by AP's in the collection

$$\mathscr{B} = \{\langle a_i, d_i\rangle \in \mathscr{A}:\ p\nmid d\}.$$

By the regularity of $\mathscr{A}$ there is some integer x_0 which is not an element of any AP in $\mathscr{B}$. Let P be the least common multiple of the moduli of AP's occurring in $\mathscr{B}$ and choose x so that

$$x \equiv x_0(\mathrm{mod}\ P) \quad \text{and} \quad x \equiv r(\mathrm{mod}\ p).$$

Then x does not belong to any AP in $\mathscr{A}$. This contradiction proves the lemma. ■

LEMMA 3 (Reduction of a collection of AP's). (i) *Suppose $\{\langle a_i, d_i\rangle: i = 1, \ldots, t\}$ is a minimal covering of the AP $\langle a, d\rangle$ and*

$$\delta_i = (d, d_i) \quad \textit{for} \quad i = 1, \ldots, t.$$

If we construct another collection of AP's

$$\mathscr{A}^* = \{\langle a_i^*, d_i^*\rangle:\ i = 1, \ldots, t\}$$

where

$$d_i^* = d_i/\delta_i \quad \textit{and} \quad a_i^*\, d/\delta_i \equiv (a_i - a)/\delta_i\ (\mathrm{mod}\ d_i^*),$$

then $\mathscr{A}^*$ is a regular covering.

(ii) *In particular, if d divides d_i*

$$d_i^* = d_i/d, \quad a_i^* \equiv \frac{a_i - a}{d}(\mathrm{mod}\ d_i^*).$$

Proof. (i) Note that δ_i divides $a_i - a$ by (i) of Lemma 1. Let m be any integer. We claim that m belongs to $\langle a_i^*, d_i^*\rangle$ if and only if $a+md$ belongs to $\langle a_i, d_i\rangle$. For,

$$a + md \in \langle a_i, d_i\rangle \Leftrightarrow md/\delta_i \equiv (a_i - a)/\delta_i\ (\mathrm{mod}\ d_i^*)$$
$$\Leftrightarrow m \in \langle a_i^*, d_i^*\rangle.$$

Thus $\mathscr{A}^*$ covers the integers, and if any proper subset of $\mathscr{A}^*$ covers the integers then a proper subset of $\mathscr{A}$ would cover $\langle a, d\rangle$, contradicting the minimality of $\mathscr{A}$. Thus $\mathscr{A}^*$ is regular.

(ii) If d divides d_i then δ_i equals d and the result follows. ■

When using the construction described in this lemma we will say $\mathscr{A}^*$ is the *reduction of $\mathscr{A}$ via $\langle a, d\rangle$*.

3. The first theorem.

THEOREM 1. *Suppose $\mathscr{A}$ is regular, $\langle a, d\rangle \in \mathscr{A}$ and p^α is the highest power of a prime p which divides d. Then*

(i) *for $1 \leqslant k \leqslant \alpha$, $\mathscr{A}$ has a subcollection $\mathscr{A}_k$ where*

$$\mathscr{A}_k = \{\langle a_i^{(k)}, d_i^{(k)}\rangle:\ 1 \leqslant i \leqslant p-1\}$$

such that for each i satisfying $1 \leqslant i \leqslant p-1$,

$$p_i^k | d_i^{(k)},$$
$$a_i^{(k)} \equiv a(\mathrm{mod}\ p^{k-1}),$$
$$\frac{a_i^{(k)} - a}{p^{k-1}} \equiv i(\mathrm{mod}\ p).$$

(ii) *The $\alpha(p-1)$ AP's $\langle a_i^{(k)}, d_i^{(k)}\rangle$ are pairwise disjoint, and each is disjoint from $\langle a, d\rangle$.*

Proof. (i) We prove the result for an arbitrary value of k.

Let $\mathscr{C}$ be a minimal subcollection of $\mathscr{A}$ such that $\mathscr{C}$ covers $\langle a, p^{k-1}\rangle$ and let $\mathscr{C}^*$ be the reduction of $\mathscr{C}$ via $\langle a, p^{k-1}\rangle$. Now $\langle a, d\rangle$ is a subset of $\langle a, p^{k-1}\rangle$ so the regularity of $\mathscr{A}$ implies that $\langle a, d\rangle$ belongs to $\mathscr{C}$. By (ii) of Lemma 3 $\langle 0, d/p^{k-1}\rangle$ belongs to $\mathscr{C}^*$. Since p divides d/p^{k-1} Lemma 2 implies that $\mathscr{C}^*$ contains a further $p-1$ AP's $\langle a_1^*, d_1^*\rangle, \ldots, \langle a_{p-1}^*, d_{p-1}^*\rangle$ such that

$\{0, a_1^*, \ldots, a_{p-1}^*\}$ is a complete residue system modulo p and that each d_i^* is divisible by p.

For each i, let $\langle a_i^{(k)}, d_i^{(k)}\rangle$ be the AP of which $\langle a_i^*, d_i^*\rangle$ is the reduction. Then by Lemma 3,

$$d_i^* = \frac{d_i^{(k)}}{(p^{k-1}, d_i^{(k)})}.$$

Since p divides d_i^* this implies that p^k divides $d_i^{(k)}$. Now $\langle a_i^{(k)}, d_i^{(k)}\rangle$ intersects $\langle a, p^{k-1}\rangle$ so by (i) of Lemma 1,

$$a_i^{(k)} \equiv a \pmod{p^{k-1}}$$

and by (ii) of Lemma 3,

$$a_i^* \equiv \frac{a_i^{(k)}-a}{p^{k-1}} \pmod{p}.$$

Since a_i^* runs through a reduced residue system modulo p we can, by appropriate ordering, ensure that,

$$\frac{a_i^{(k)}-a}{p^{k-1}} \equiv i \pmod{p}.$$

(ii) We prove this part by contradiction. Suppose $\langle a_i^{(k)}, d_i^{(k)}\rangle$ intersects $\langle a_{i'}^{(k')}, d_{i'}^{(k')}\rangle$ where $k' \geqslant k$ so that p^k divides $(d_i^{(k)}, d_{i'}^{(k')})$. Then by (i) of Lemma 1,

$$a_i^{(k)} \equiv a_{i'}^{(k')} \pmod{p^k},$$

and so

$$\frac{a_i^{(k)}-a}{p^{k-1}} \equiv \frac{a_{i'}^{(k')}-a}{p^{k-1}} \pmod{p}.$$

The left-hand side here is congruent to i and the right to 0 if k' exceeds k and to i' if k' equals k. The first alternative is impossible since i belongs to the reduced residue system modulo p, and the second implies that the two AP's are identical.

Similarly $\langle a_i^{(k)}, d_i^{(k)}\rangle$ intersecting $\langle a, d\rangle$ would imply

$$a_i^{(k)} \equiv a \pmod{p^k}$$

and thus

$$\frac{a_i^{(k)}-a}{p^{k-1}} \equiv 0 \pmod{p}.$$

This is a contradiction since the left is congruent to i modulo p. ∎

Corollary 1. *With $\mathscr{A}$ as in the theorem, let n and β be integers satisfying*

$$0 \leqslant n \leqslant p^\alpha, \quad 0 < \beta \leqslant \alpha$$

and

$$\mathscr{B} = \bigcup_{s=1}^{n} \langle b_s, p^\alpha\rangle$$

where the numbers b_s are distinct modulo p^α. Then

$$|\{\langle a, d\rangle \in \mathscr{A}:\ p^\beta | d,\ \langle a, d\rangle \cap \mathscr{B} = \emptyset\}| \geqslant (\alpha-\beta+1)(p-1)+1-n.$$

Proof. By the theorem, $\mathscr{A}$ contains the $(p-1)(\alpha-\beta+1)+1$ AP's

$$\langle a_i^{(k)}, d_i^{(k)}\rangle \quad \text{for} \quad k = \beta, \ldots, \alpha,\ i = 1, \ldots, p-1$$

and

$$\langle a, d\rangle.$$

Each of these has modulus divisible by p^β. Now suppose both $\langle a_i^{(k)}, d_i^{(k)}\rangle$ and $\langle a_{i'}^{(k')}, d_{i'}^{(k')}\rangle$ intersect $\langle b_s, p^\alpha\rangle$ and that $k' \geqslant k$. Then by (ii) of Lemma 1,

$$a_i^{(k)} \equiv a_{i'}^{(k')} \pmod{p^k},$$

which leads to a contradiction as in part (ii) of the theorem. Similarly no $\langle a_i^{(k)}, d_i^{(k)}\rangle$ will intersect $\langle a, p^\alpha\rangle$, which contains $\langle a, d\rangle$. Thus at most n of our AP's will intersect AP's in $\mathscr{B}$ leaving at least $(\alpha-\beta+1)(p-1)+1-n$ non-intersecting AP's. ∎

4. The second theorem.

Theorem 2. *If $\mathscr{A}$ is regular, P is the least common multiple of the moduli of the AP's in $\mathscr{A}$, D divides P and D does not equal P, then*

$$|\{\langle a, d\rangle \in \mathscr{A}:\ d \nmid D\}| \geqslant 1+f\left(\frac{P}{D}\right).$$

Proof. We prove the theorem by induction on $\nu(P)$, the number of distinct prime divisors of P.

If $\nu(P)$ equals 1 then

$$P = p^\alpha, \quad D = p^\beta, \quad 0 \leqslant \beta < \alpha,$$

where p is a prime. We then have

$$|\{\langle a, d\rangle \in \mathscr{A}:\ d \nmid p^\beta\}| = |\{\langle a, d\rangle \in \mathscr{A}:\ p^{\beta+1} | d\}|.$$

By Corollary 1 this is not less than

$$(\alpha-(\beta+1)+1)(p-1)+1 = f(p^\alpha/p^\beta)+1.$$

This shows that the theorem holds when $\nu(P)$ equals 1.

To continue the induction suppose that the theorem holds for $\nu(P)$ not exceeding n. Let $\mathscr{A}$ be regular and let the least common multiple of the moduli of the AP's in $\mathscr{A}$ be $p^\alpha P$, where p is a prime not dividing P and $\nu(P)$

equals n, so that $\nu(p^\alpha P) = n+1$. We will write the AP's in $\mathscr{A}$ in the form $\langle a, p^\gamma d\rangle$ where p does not divide d. We must find a lower bound for

$$|\{\langle a, p^\gamma d\rangle \in \mathscr{A}:\ p^\gamma d \nmid p^\beta D\}|$$

where p does not divide D.

We now introduce some notation. For each residue class s modulo p^α let $\mathscr{A}_s$ be a minimal subcollection of $\mathscr{A}$ that covers $\langle s, p^\alpha\rangle$. It is clear that such a subcollection exists. We then set

$P_s = \operatorname{lcm}\{d:\ \langle a, p^\gamma d\rangle \in \mathscr{A}_s\}$,
$R_0 = D$,
$R_s = \operatorname{lcm}\{R_{s-1}, P_s\}$,
$D_s = (R_{s-1}, P_s)$,
$Q_s = \{\langle a, p^\gamma d\rangle \in \mathscr{A}_s:\ d \nmid D_s\}$, for $s = 1, \ldots, p^\alpha$.

We remark that:

$$\frac{P_s}{D_s} = \frac{R_s}{R_{s-1}} \quad \text{for} \quad s = 1, \ldots, p^\alpha, \tag{4.1}$$

$$R_{p^\alpha} = P, \tag{4.2}$$

$$Q_s \text{ is empty if } D_s = P_s, \tag{4.3}$$

$$Q_s = \{\langle a, p^\gamma d\rangle \in \mathscr{A}_s:\ d \mid R_s,\ d \nmid R_{s-1}\}. \tag{4.4}$$

It is clear from the last remark and from the definition of R_s that the collections Q_s are pairwise disjoint.

CLAIM. *If D_s does not equal P_s,*

$$|Q_s| \geqslant f\left(\frac{P_s}{D_s}\right)+1. \tag{4.5}$$

Proof of Claim. Since $\mathscr{A}_s$ is a minimal covering of $\langle s, p^\alpha\rangle$ we may reduce it to get a regular covering $\mathscr{A}_s^*$. Any AP $\langle a, p^\gamma d\rangle$ in $\mathscr{A}_s$ will be reduced, according to Lemma 3, to an AP of the form $\langle a^*, d\rangle$. Since $D_s | P_s$ and $\nu(P_s)$ is at most n, it follows from the induction hypothesis that if D_s does not equal P_s,

$$|Q_s| = |\{\langle a^*, d\rangle \in \mathscr{A}_s^*:\ d \nmid D_s\}| \geqslant f\left(\frac{P_s}{D_s}\right)+1. \ \blacksquare$$

We now obtain a lower bound for the cardinality of the set $\{\langle a, p^\gamma d\rangle \in \mathscr{A}:\ p^\gamma d \nmid p^\beta D\}$. We note that,

$$p^\gamma d \nmid p^\beta D \Rightarrow p^{\beta+1} | p^\gamma \text{ or } d \nmid D \quad \text{and} \quad \bigcup_{s=1}^{p^\alpha} \mathscr{A}_s = \mathscr{A}.$$

Therefore the cardinality equals

$$\Big|\Big(\bigcup_{s=1}^{p^\alpha} \{\langle a, p^\gamma d\rangle \in \mathscr{A}_s:\ d \nmid D\}\Big) \cup \{\langle a, p^\gamma d\rangle \in \mathscr{A}:\ p^{\beta+1} | p^\gamma\}\Big|.$$

Each collection in the first union contains a subcollection

$$\{\langle a, p^\gamma d\rangle \in \mathscr{A}_s:\ d \nmid D_s\} = Q_s,$$

so the required cardinality is at least

$$\Big|\Big(\bigcup_{s=1}^{p^\alpha} Q_s\Big) \cup \{\langle a, p^\gamma d\rangle \in \mathscr{A}:\ p^{\beta+1} | p^\gamma\}\Big| \geqslant \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} |Q_s| + \Big|\Big\{\langle a, p^\gamma d\rangle \in \mathscr{A} \setminus \bigcup_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} \mathscr{A}_s:\ p^{\beta+1} | p^\gamma\Big\}\Big|. \tag{4.6}$$

By (4.1) to (4.5) and the additivity of f,

$$\sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} |Q_s| \geqslant \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} f\left(\frac{P_s}{D_s}\right) + \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1 = \sum_{s=1}^{p^\alpha} f\left(\frac{R_s}{R_{s-1}}\right) + \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1 = f\left(\frac{P}{D}\right) + \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1. \tag{4.7}$$

We now consider the second term in (4.6). We put

$$B = \bigcup_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} \langle s, p^\alpha\rangle$$

and note that if the intersection of $\langle a, p^\gamma d\rangle$ and $\langle s, p^\alpha\rangle$ is empty then $\langle a, p^\gamma d\rangle$ does not belong to $\mathscr{A}_s$, so the second term in (4.6) is at least

$$|\{\langle a, p^\gamma d\rangle \in \mathscr{A}:\ \langle a, p^\gamma d\rangle \cap B = \emptyset,\ p^{\beta+1} | p^\gamma\}|.$$

By Corollary 1 this is at least

$$(\alpha-(\beta+1)+1)(p-1)+1-\sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1 = f\left(\frac{p^\alpha}{p^\beta}\right)+1-\sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1. \tag{4.8}$$

On adding the right-hand sides of (4.7) and (4.8) we obtain the required lower bound. That is,

$$|\{\langle a, p^\gamma d\rangle \in \mathscr{A}:\ p^\gamma d \nmid p^\beta D\}| \geqslant f\left(\frac{P}{D}\right) + \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1 + f\left(\frac{p^\alpha}{p^\beta}\right) + 1 - \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1 = f\left(\frac{p^\alpha P}{p^\beta D}\right)+1.$$

Thus the theorem holds when the least common multiple of the moduli has $n+1$ distinct prime factors and the theorem is proven by induction. $\blacksquare$

COROLLARY 2. *If $\mathscr{A}$ is regular, P the least common multiple of the moduli of the AP's in $\mathscr{A}$ then*

$$|\mathscr{A}| \geqslant f(P)+1.$$

Proof. If P does not equal 1 the result is immediate on putting D equal 1 in the theorem. If P equals 1 then $\mathscr{A}$ must be $\{\langle 0, 1\rangle\}$ and the result still holds. ∎

Now let $\mathscr{A}$ be a collection of AP's, not necessarily regular, which covers the integers. Znám ([5]) defines an AP $\langle a_0, d_0\rangle$ in $\mathscr{A}$ as *essential* if $\mathscr{A}\setminus\langle a_0, d_0\rangle$ does not cover the integers. The following result extends Theorem 1 of [5].

Corollary 3. *If $\mathscr{A}$ covers the integers, $\langle a_0, d_0\rangle$ is essential in $\mathscr{A}$, then*

$$|\{\langle a, d\rangle \in \mathscr{A}: (d, d_0) > 1\}| \geqslant f(d_0)+1.$$

Proof. Let $\mathscr{A}^*$ be a regular subcollection of $\mathscr{A}$, and P the least common multiple of the moduli of the AP's in it. It is clear that $\langle a_0, d_0\rangle$ belongs to $\mathscr{A}^*$ and hence that d_0 divides P. Then

$$|\{\langle a, d\rangle \in \mathscr{A}: (d, d_0) > 1\}| \geqslant \left|\left\{\langle a, d\rangle \in \mathscr{A}^*: d \nmid \frac{P}{d_0}\right\}\right| \geqslant f(d_0)+1. \quad ∎$$

Acknowledgement. The author wishes to thank Dr. J. Pitman for her unrelenting assistance in the preparation of this paper.

References

[1] I. Korec, *On a generalization of Mycielski's and Znám's conjectures about coset decomposition of Abelian groups*, Fund. Math. 85 (1974), pp. 41–48.

[2] Š. Znám, *On Mycielski's problem on systems of arithmetic sequences*, Colloq. Math. 15 (1966), pp. 201–204.

[3] — *A remark to a problem of J. Mycielski on arithmetic sequences*, ibid. 20 (1969), pp. 69–70.

[4] — *On exactly covering systems of arithmetic sequences*, Colloquia Math. Soc. János Bolyai, 2. Number Theory, Debrecen 1968.

[5] — *On properties of systems of arithmetic sequences*, Acta Arith. 26 (1975), pp. 279–283.

THE UNIVERSITY OF ADELAIDE
G.P.O. Box 498, Adelaide
S. A. 5001, Australia

Received on 5.10.1983
and in revised form on 20.3.1984 (1375)

ACTA ARITHMETICA
XLV (1985)

Verzichtbare und unverzichtbare Elemente bei der Darstellung als Summe und als Differenz von Quadraten

von

Erhard Deinert, Erich Härtter und Joachim Zöllner (Mainz)

Wir bezeichnen die Menge der Quadrate der ganzen Zahlen mit Q_0. Nach einem bekannten Satz von Lagrange ist jede natürliche Zahl als Summe von vier Elementen aus Q_0 darstellbar. In [3] wurde gezeigt, daß es unendliche Mengen $S \subset Q_0$ gibt, so daß jede natürliche Zahl auch noch als Summe von vier Quadraten aus $Q_0 \setminus S$ darstellbar ist. Erdös und Nathanson [2] haben darüber hinaus die Existenz von Mengen S mit dieser Eigenschaft und $|(Q_0\setminus S)\cap[0, x]| \leqslant Cx^{3/8+\varepsilon}$ für beliebiges $\varepsilon > 0$ nachgewiesen, wobei $C > 0$ nur von ε abhängt(¹). In der vorliegenden Arbeit werden genau die Quadrate bestimmt, die in jedem Fall in $Q_0\setminus S$ noch enthalten sein müssen. Solche Quadrate nennen wir unverzichtbar.

Sei Q die Menge der Quadrate der natürlichen Zahlen. Genau die von 1 und 4 verschiedenen natürlichen Zahlen, die $\not\equiv 2 \pmod 4$ sind, lassen sich als Differenz zweier Quadrate aus Q darstellen. In [3] wurde gezeigt, daß dies auch noch mit den Quadraten aus $Q\setminus T$ möglich ist, wobei $T \subset Q$ eine geeignete unendliche Menge von Quadraten ist. Auch in diesem Fall werden die unverzichtbaren Quadrate charakterisiert.

1. Zunächst führen wir einige Bezeichnungen ein(²):

Sei $E(n^2)$ die Menge aller $z \in N_0$, für die gilt: Aus $z = a_1^2+a_2^2+a_3^2+a_4^2$ mit $a_i \in N_0$ $(i = 1, 2, 3, 4)$ folgt $a_i^2 = n^2$ für mindestens ein i.

Sei weiter $U := \{n^2|\ E(n^2) \neq \emptyset\}$ und $\bar{U} := \{n^2|\ |E(n^2)| = \infty\}$.

Sei analog $E^-(n^2)$ die Menge aller $z \in N$, für die gilt: Aus $z = a_1^2 - a_2^2$ mit $a_i \in N$ $(i = 1, 2)$ folgt $a_i^2 = n^2$ für $i = 1$ oder für $i = 2$.

Entsprechend wie oben sei dann $U^- := \{n^2|\ E^-(n^2) \neq \emptyset\}$ und $\bar{U}^- := \{n^2|\ |E^-(n^2)| = \infty\}$.

(¹) Nathanson [5] zeigte, daß sogar $|(Q_0\setminus S)\cap[0, x]| \leqslant Cx^{1/3+\varepsilon}$ gilt.

(²) N ist die Menge der natürlichen Zahlen; $N_0 = N \cup \{0\}$ die Menge der nichtnegativen ganzen Zahlen.