Atti Accademia Nazionale Lincei Classe Scienze Fisiche Matematiche Naturali

Rendiconti Lincei
Matematica e Applicazioni

Enrico Bombieri, Umberto Zannier

A Note on squares in arithmetic progressions, II

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Serie 9, Vol. **13** (2002), n.2, p. 69–75.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLIN_2002_9_13_2_69_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Accademia Nazionale dei Lincei, 2002.

Rend. Mat. Acc. Lincei
s. 9, v. 13:69-75 (2002)

Teoria dei numeri. — *A* Note *on squares in arithmetic progressions, II.* Nota di Enrico Bombieri e Umberto Zannier, presentata (*) dal Socio E. Bombieri.

Abstract. — We show that the number of squares in an arithmetic progression of length N is at most $c_1 N^{3/5}(\log N)^{c_2}$, for certain absolute positive constants c_1, c_2. This improves the previous result of Bombieri, Granville and Pintz [1], where one had the exponent $\frac{2}{3}$ in place of our $\frac{3}{5}$. The proof uses the same ideas as in [1], but introduces a substantial simplification by working only with elliptic curves rather than curves of genus 5 as in [1].

Key words: Diophantine equations; Elliptic curves; Arithmetic progressions.

Riassunto. — *Una* Nota *sul numero di quadrati in una progressione aritmetica, II.* Si dimostra che il numero di quadrati in una progressione aritmetica di lunghezza N non supera $c_1 N^{3/5}(\log N)^{c_2}$, per due costanti positive assolute c_1, c_2. Questo teorema migliora il precedente risultato di Bombieri, Granville e Pintz [1], dove si aveva l'esponente $\frac{2}{3}$ al posto del nuovo esponente $\frac{3}{5}$. La dimostrazione si basa sulle idee introdotte in [1], con una importante semplificazione ottenuta lavorando con curve ellittiche invece che con curve di genere 5 come in [1].

1. The main result

Let $Q(N; q, a)$ denote the number of squares in the arithmetic progression $qn + a$, $n = 1, 2, \ldots, N$, and let $Q(N)$ be the maximum of $Q(N; q, a)$ over all non-trivial arithmetic progressions $qn + a$. Rudin conjectured that $Q(N) = O(\sqrt{N})$, and it is quite likely that $Q(N) \sim \sqrt{\frac{8}{3}N}$ as N tends to ∞. The most optimistic conjecture is that $Q(N) = Q(N; 24, -23)$ for every sufficiently large N. We refer to [1] for a discussion of Rudin's conjecture and evidence for these bounds.

The bound $Q(N) = o(N)$ follows, as observed by Szemerédi [2], from Szemerédi's theorem on arithmetic progressions (in this case, length 4 suffices) and Euler's result, already stated by Fermat in 1640, that no four squares can form an arithmetic progression. The main result of [1] states that $Q(N) \le cN^{2/3}(\log N)^{c'}$ for two positive absolute, and computable, constants c, c' and represents a substantial improvement over the qualitative bound obtained through the use of Szemerédi's theorem.

In this paper we prove

Theorem 1. *We have* $Q(N) \le c_1 N^{3/5}(\log N)^{c_2}$ *for two positive absolute, and computable, constants* c_1, c_2.

(*) Nella seduta dell'8 febbraio 2002.

2. First reductions and lemmas

We begin by stating certain elementary reductions which restrict the ranges to be considered for q and a, referring to [1] for the easy proofs.

First of all, there is no loss of generality in assuming that q and a are coprime [1, p. 371], and moreover we need only consider the case in which q is rather large with respect to N, namely

$$q > e^{\sqrt{N}}\,, \tag{1}$$

as shown in [1, p. 371], using a large sieve argument. Indeed, the large sieve proves that $Q(N; q, a) \ll \sqrt{N}\log N$ uniformly in q, unless q is divisible by at least half of the primes up to $3\sqrt{N}$. Therefore, the crux of the matter consists in dealing with very large values of q with many small prime factors.

As in [1], we consider first two solutions $qn_i + a = m_i^2$, $i = 0, 1$ and $1 \le n_i \le N$, for two squares in the progression $qn + a$. Then n_0 and n_1 are uniquely determined by the rational point on $\mathbb{P}^1$ with homogenous coordinates $(m_0 : m_1)$, as long as $q > 2N$ and $GCD(q, a) = 1$ (see [1, p. 372]). This remark establishes a one-to-one correspondence, once q and a are fixed, between certain rational points $(m_0 : m_1)$ and pairs (n_0, n_1) of solutions.

Next, consider a third solution $qn_2 + a = m_2^2$. By eliminating a we obtain

$$(n_1 - n_2)m_0^2 + (n_2 - n_0)m_1^2 + (n_0 - n_1)m_2^2 = 0\,, \tag{2}$$

which is the equation of a conic in the projective plane $\mathbb{P}^2$, with a rational point with projective coordinates $(m_0 : m_1 : m_2)$. By the previous remark, the rational point $(m_0 : m_1 : m_2)$ determines uniquely n_0, n_1 and n_2.

There are too many rational points on a conic for this result to be directly useful, hence we consider a fourth solution $qn_3 + a = m_3^2$, yielding as before an equation

$$(n_2 - n_3)m_1^2 + (n_3 - n_1)m_2^2 + (n_1 - n_2)m_3^2 = 0. \tag{3}$$

Now we interpret the system of equations (2) and (3) as the intersection of two quadrics in projective space $\mathbb{P}^3$, giving an elliptic curve C with a rational point $(m_0 : m_1 : m_2 : m_3)$ in homogeneous coordinates. Again, such a rational point determines uniquely $n_0, \ldots, n_3$. We have $(m_i + m_j)(m_i - m_j) = m_i^2 - m_j^2 = q(n_i - n_j)$, from which it follows

$$|m_i| < qN \tag{4}$$

for every i.

From (2) and (3) we deduce

$$\left((n_2 - n_1)m_0 m_3\right)^2 = \left((n_2 - n_0)m_1^2 + (n_0 - n_1)m_2^2\right)\left((n_2 - n_3)m_1^2 + (n_3 - n_1)m_2^2\right)\,,$$

which, after multiplying both sides by $(n_2 - n_0)^2(n_2 - n_3)^2 m_1^2 m_2^{-6}$, becomes

$$Y^2 = X(X + A)(X + B) \tag{5}$$

with

$$(6) \quad X = (n_2 - n_0)(n_2 - n_3)\left(\frac{m_1}{m_2}\right)^2, \qquad Y = (n_2 - n_0)(n_2 - n_1)(n_2 - n_3)\frac{m_0 m_1 m_3}{m_2^3}$$

and

$$(7) \qquad A = (n_0 - n_1)(n_2 - n_3), \quad B = (n_1 - n_3)(n_0 - n_2).$$

Note that $B - A = (n_1 - n_2)(n_0 - n_3)$.

Equation (5) gives us an elliptic curve E with integer coefficients, of discriminant

$$(8) \qquad \Delta = 16 \prod_{i<j} (n_i - n_j)^2.$$

The associated morphism $C \to E$ has degree 4.

Up to now, we have followed the arguments in [1]. The new observation is that, since $m_i^2 \equiv a \pmod q$, the rational point (X, Y) on the elliptic curve E satisfies the additional constraint

$$(9) \qquad X \equiv (n_2 - n_0)(n_2 - n_3) \pmod q.$$

Moreover, an easy estimate using (4) shows that

$$(10) \qquad h(1 : X : Y) \le 3 \log q + 6 \log N.$$

The key step in the proof will be a uniform bound for the number of rational points of E satisfying (9) and (10).

We may also work with the Néron-Tate height $\widehat{h}(P) = \lim 4^{-n} h(2^n P)$ rather than the absolute logarithmic height $h(P)$ of a point P. Explicit bounds for the difference of the two heights have been obtained by Zimmer in [3], for curves given in Weierstrass model $y^2 = 4x^3 - g_2 x - g_3$. There is no problem in adapting Zimmer's bound to curves as in (5), and for our curve E and any rational point $P = (1 : X : Y)$ on E we obtain

$$(11) \qquad |h(P) - \widehat{h}(P)| \le c_3 \log N$$

for an explicitly computable (and not too large) absolute constant c_3. Since we assume $\log q > \sqrt{N}$, these corrections by an amount proportional to $\log N$ are negligible compared to $\log q$ as soon as N is sufficiently large. Therefore, given $\varepsilon > 0$ and assuming $N \ge N_1(\varepsilon)$ sufficiently large as a function of ε alone, we need only compute the number of rational points $P = (1 : X : Y)$ of E satisfying (9) and

$$(12) \qquad \widehat{h}(P) \le (3 + \varepsilon) \log q.$$

The key lemma is

LEMMA 1. *Let $\mathcal{X}$ be the set of rational points of E satisfying the congruence* (9) *and let $\varepsilon > 0$. We assume $N \ge N_1(\varepsilon)$, $q > e^{\sqrt{N}}$, where $N_1(\varepsilon)$ is a certain computable function of ε.*

Let $P_1, P_2, P_3 \in \mathcal{X}$ be three distinct points such that $P_i + P_j \ne O$ for every $i \ne j$. Then we have

$$\max_{ij} \widehat{h}(P_i - P_j) > (1 - \varepsilon) \log q.$$

PROOF. By (11), since $q > e^{\sqrt{N}}$ and $N \geq N_1(\varepsilon)$ it suffices to prove the statement with the absolute logarithmic height h in place of the canonical height $\widehat{h}$.

We write $X(P)$, $Y(P)$ for the (X, Y)-coordinates of a point P of E, not equal to the origin O at ∞. Let $i, j \in \{1, 2, 3\}$, $i \neq j$. By the addition formula on E, we have

$$X(P_i - P_j) = \left(\frac{Y(P_i) + Y(P_j)}{X(P_i) - X(P_j)}\right)^2 - X(P_i) - X(P_j) - A - B; \tag{13}$$

note that $X(P_i) - X(P_j) \neq 0$ because $P_i \neq \pm P_j$ by hypothesis. The congruence (9) shows that

$$X(P_i) - X(P_j) \equiv 0 \pmod{q}. \tag{14}$$

Moreover, since $(n_2 - n_0)(n_2 - n_3)$ is an integer, the congruence (9) shows that for any $P \in \mathcal{X}$ the denominator of $X(P)$ is coprime with q, hence the same holds for the other coordinate $Y(P)$.

Let (1)

$$q_{ij} := GCD(Y(P_i) + Y(P_j), q);$$

then by (13) and (14) we see that the denominator of $X(P_i - P_j)$ is divisible by $(q/q_{ij})^2$. Therefore, the denominator of $Y(P_i - P_j)$ is divisible by $(q/q_{ij})^3$ and *a fortiori*

$$h(P_i - P_j) \geq 3 \log(q/q_{ij}). \tag{15}$$

If the lemma were false, (15) would imply $q_{ij} \geq q^{\frac{2}{3}+\frac{\varepsilon}{3}}$ and, since each q_{ij} divides q, we would get

$$q_0 := GCD(q_{12}, q_{23}, q_{31}) \geq q^{3(\frac{2}{3}+\frac{\varepsilon}{3})-2} = q^{\varepsilon}. \tag{16}$$

Now q_0 divides the numerator of each $Y(P_i) + Y(P_j)$ and summing over distinct pairs ij we see that q_0 divides the numerator of $2(Y(P_1) + Y(P_2) + Y(P_3))$. Hence q_0 divides the numerator of each fraction $2Y(P_i)$, $i = 1, 2, 3$.

On the other hand, by (9) we see that for $P \in \mathcal{X}$ we have

$$4Y(P)^2 = 4X(P)(X(P) + A)(X(P) + B) \equiv 4(n_2 - n_0)^2(n_2 - n_1)^2(n_2 - n_3)^2 \pmod{q}.$$

Since q_0 divides both q and $2Y(P_i)$, we conclude that q_0 divides $4(n_2 - n_0)^2(n_2 - n_1)^2(n_2 - n_3)^2$, hence $q_0 < 4N^6$. Since $q > e^{\sqrt{N}}$, this contradicts (16) for N sufficiently large as a function of ε, completing the proof. $\square$

Let $r = \mathrm{rank}_{\mathbb{Q}} E(\mathbb{Q})$. As usual, the real vector space $\mathbb{R}^r = \mathbb{R} \otimes E(\mathbb{Q})$ can be equipped with the euclidean norm $|\mathbf{x}|$ defined by $|\mathbf{x}| = \sqrt{\widehat{h}(P)}$ if $\mathbf{x}$ is the class of $P \in E(\mathbb{Q})$ modulo torsion and extending it by continuity and linearity to all of $\mathbb{R}^r$.

(1) If u/v is a rational fraction in lowest terms with $GCD(v, q) = 1$, we define $GCD(u/v, q) = GCD(u, q)$.

LEMMA 2. *Suppose $N \geq N_1(\varepsilon)$. Then the number of points of $\mathcal{X}$ whose image in $\mathbb{R} \otimes E(\mathbb{Q})$ lies in any given ball of radius $\rho := \frac{1}{2}(1-\varepsilon)^{1/2}\sqrt{\log q}$ is at most* 4.

PROOF. If we had five points of $\mathcal{X}$ with image in such a ball, three of them, say P_1, P_2, P_3, would satisfy $P_i + P_j \neq O$ for every $i \neq j$. By Lemma 1, there would be such a pair i, j with $\sqrt{\widehat{h}(P_i - P_j)} > (1-\varepsilon)^{1/2}\sqrt{\log q} = 2\rho$. This contradicts the triangle inequality, proving what we want. □

COROLLARY. *Let $\varepsilon = \frac{1}{100}$ and $N \geq N_1(\frac{1}{100})$. Let δ be the GCD of the differences $n_i - n_j$ for $0 \leq i < j \leq 3$.*

Then the number of points of $\mathcal{X}$ with $\widehat{h}(P) \leq (3+\varepsilon)\log q$ does not exceed (2) $4 \times 8^{\sum_{i<j}\omega((n_j - n_i)/\delta)}$.

PROOF. Since δ^2 divides both $A = (n_0 - n_1)(n_2 - n_3)$ and $B = (n_1 - n_3)(n_0 - n_2)$ in (5), the change of variables $X = \delta^2 X'$, $Y = \delta^3 Y'$ shows that the curve E is isomorphic over $\mathbb{Q}$ to the elliptic curve E' obtained by replacing A, B by A/δ^2 and B/δ^2. By [1, Lemma 5], the $\mathbb{Q}$-rank r of E, which is the same as the rank of E', does not exceed

$$r \leq \omega(A/\delta^2) + \omega(B/\delta^2) + \omega((B-A)/\delta^2) \leq \sum_{i<j}\omega((n_j - n_i)/\delta).$$

Let us abbreviate $R := (3+\varepsilon)^{1/2}\sqrt{\log q}$. By a well-known covering argument (3), the ball of radius R can be covered with not more than $\lfloor (1 + 2R/\rho)^r \rfloor$ balls of radius ρ. With $\varepsilon = \frac{1}{100}$ we have $1 + 2R/\rho < 8$, and the result follows from Lemma 2. □

3. PROOF OF THEOREM 1

We conclude the proof of Theorem 1 using the same combinatorial argument as in [1]. Let us fix q and a, coprime with $q > 2N$. Let $\mathcal{Z}$ be a set of Z integers in the interval $[1, N]$ such that $qn + a$ is a square. For $d \geq 1$ let us define

$$\mathcal{Z}(d, l) := \{n \in \mathcal{Z} : n \equiv l \pmod{d}\};$$

$Z(d, l)$ is the number of elements of $\mathcal{Z}(d, l)$.

Let $\mathbf{n} := (n_0, \ldots, n_3)$ be a quadruple of distinct points of $\mathcal{Z}(d, l)$. Then $\mathbf{n}$ determines a point $\mathbf{m}$ on the elliptic curve intersection of the two quadrics (2) and (3). Note that each $n_{ij} := n_i - n_j$ is divisible by d; therefore, the homogeneous vector with coordinates n_{ij}, $0 \leq i < j \leq 3$, has an integral representative $\mathbf{k}$ with coordinates $k_{ij} = n_{ij}/d$, hence with $|k_{ij}| < N/d$. Conversely, let $\mathbf{k}$ be a homogeneous vector of integers k_{ij} with $k_{ij} + k_{ji} = 0$, $k_{ij} + k_{jl} + k_{li} = 0$ for every i, j, l and $k_{ij} \neq 0$ if $i \neq j$. Then $\mathbf{k}$ determines two quadrics as in (2), (3) and, by the remark immediately preceding (2), given a point

(2) Here $\omega(l)$ is the number of distinct prime factors of l.

(3) It suffices to take a maximal set of disjoint balls of radius $\rho/2$ in the ball of radius $R + \rho/2$; doubling the radius of these balls we obtain a covering.

$(m_0 : m_1 : m_2 : m_3)$ on the resulting elliptic curve $C(\mathbf{k})$ there is at most one point $\mathbf{n}$ with integer coordinates such that $qn_i + a = (cm_i)^2$ with rational c and k_{ij} proportional to $n_i - n_j$.

Any such elliptic curve $C(\mathbf{k})$ determines another elliptic curve $E(\mathbf{k})$ as in (5) and, as remarked before, a morphism $C(\mathbf{k}) \to E(\mathbf{k})$ of degree 4 and a set $\mathcal{X}(\mathbf{k})$. Therefore, the number of rational points $\mathbf{m}$ on $C(\mathbf{k})$ we are concerned with is not more than 4 times the number of points counted in the Corollary to Lemma 2, namely $16 \times 8^{\sum_{i<j} \omega(k_{ij})}$.

Let $D \geq 1$ to be chosen later. As in [1, Lemma 6], we obtain this time

$$\sum_{D<d\leq 2D} \sum_{l=1}^{d} \binom{Z(d,l)}{4} \leq \sum_{\mathbf{k}\leq N/D} 16 \times 8^{\sum_{i<j} \omega(k_{ij})}.$$

Since k_{01}, k_{02}, k_{03} determine every other k_{ij}, using the inequality between arithmetic and geometric means

$$8^{\sum_{i<j} \omega(k_{ij})} \leq \frac{1}{6} \sum_{i<j} 8^{6\omega(k_{ij})}$$

and the elementary bound

$$\sum_{m\leq x} u^{\omega(m)} \ll x(\log x)^{u-1},$$

we get

$$\sum_{\mathbf{k}\leq N/D} 16 \times 8^{\sum_{i<j} \omega(k_{ij})} \ll \left(\frac{N}{D}\right)^3 (\log N)^{8^6-1}.$$

This gives

$$\sum_{D<d\leq 2D} \sum_{l=1}^{d} \binom{Z(d,l)}{4} \ll \left(\frac{N}{D}\right)^3 (\log N)^{8^6-1}.$$

The contribution to $Z = \sum_l Z(d,l)$ from terms with $Z(d,l) \leq 4$ is not more than $4d$, while

$$\binom{Z(d,l)}{4} \geq Z(d,l)$$

whenever $Z(d,l) \geq 5$. Hence

$$DZ \leq \sum_{D<d\leq 2D} \left(4d + \sum_{l=1}^{d} \binom{Z(d,l)}{4}\right) \ll D^2 + \left(\frac{N}{D}\right)^3 (\log N)^{8^6-1}.$$

The theorem, with $c_2 = 8^6 - 1$, follows by choosing $D = N^{3/5}$. □

ACKNOWLEDGEMENTS

The second author supported in part for a visit to the Institute for Advanced Study, Princeton, N.J.

References

[1] E. Bombieri - A. Granville - J. Pintz, *Squares in arithmetic progressions*. Duke Math. J., 66, 1992, 369-385.
[2] E. Szemerédi, *The number of squares in arithmetic progressions*. Stud. Sci. Math. Hungar., 9, 1974, 417.
[3] H.G. Zimmer, *On the difference of the Weil height and the Néron-Tate height*. Math. Z., 147, 1976, 35-51.

Pervenuta l'8 dicembre 2001,
in forma definitiva il 14 gennaio 2002.

E. Bombieri:
Institute for Advanced Study
School of Mathematics
Princeton, NJ 08540 (U.S.A.)
eb@math.ias.edu

U. Zannier:
IUAV DCA
Santa Croce, 191 - 30135 Venezia
zannier@iuav.it