# Squares in Arithmetic Progressions

Enrico Bombieri, Andrew Granville and János Pintz

I. Let $Q(N; q, a)$ denote the number of squares in the arithmetic progression $qn+a$, $n = 1, 2, \cdots, N$; and let $Q(N)$ be the maximum of $Q(N; q, a)$ over all non-trivial arithmetic progressions $qn + a$.

It seems to be remarkably difficult to obtain non-trivial upper bounds for $Q(N)$. There are currently two proofs known of the weak bound $Q(N) = o(N)$ (which is an old conjecture of Erdös) and both are far from trivial. The first proof, found by Szemerédi [S] in 1974, has for its main tool Szemerédi's celebrated theorem that, for fixed $\delta$ and positive $k$, a subset of $1, \cdots, N$ with cardinality at least $\delta N$ must contain a $k$-term arithmetic progression, as soon as $N$ is sufficiently large (the value of $k$ used here is $k = 4$). The second proof, which appears to be new, uses instead Faltings's celebrated theorem that the number of rational points on a curve of genus $g \geqq 2$ is finite (the value of $g$ is now $g = 5$). We shall describe both these proofs later in this section.

In this paper we improve the above upper bound, though we are still far from proving Rudin's conjecture that $Q(N) \asymp \sqrt{N}$ (see Erdös and Graham [EG], p. 17, for a history of this and related problems). In fact the most optimistic conjecture is $Q(N) = \sqrt{\frac{8}{3}N} + O(1)$, and even $Q(N) = Q(N; 24, -23)$ for all large $N$, possibly $N \geqq 8$.

Theorem. *There are at most $c_1 N^{2/3} (\log N)^{c_2}$ squares in any arithmetic progression $a + q$, $a + 2q, \cdots, a + Nq$ with $q \neq 0$. The constants $c_1$, $c_2$ are absolute and effectively computable.*

A possible value for $c_2$ is $(7^{30} - 1)/6$, although this is clearly unimportant.

Let $Q_k(N)$ be the maximum number of $k$-th powers which can appear in an arithmetic progression of length $N$. Much of the same arguments which go into proving our Theorem can be adapted to deal with $Q_k(N)$, and we expect that they should lead to $Q_3(N) \ll N^{3/5+\epsilon}$, and $Q_k(N) \ll N^{1/2+\epsilon}$ for $k \geqq 4$. However there are further complications in the study of the Mordell-Weil group of the Jacobians of the associated curves, and we shall limit ourselves to some comments at the end of this paper about this point.

We now present an outline of our proof and describe its origins: In a letter written to Frenicle in 1640, Fermat proposed the problem of proving that there are no four squares in arithmetic progression. Fermat may well have been able to prove this, but the first published proof appeared in 1780, due to Euler.

Now let $\mathcal{Z} = \{n \ : \ 1 \leqq n \leqq N, \ qn + a \text{ is a square}\}$. Szemerédi [S] noted that $\mathcal{Z}$ must then contain $o(N)$ elements, for if $|\mathcal{Z}| > \delta N$ then $\mathcal{Z}$ would contain a four term arithmetic progression (by Szemerédi's theorem), and thus there would be four squares in arithmetic progression, contradicting Euler's Theorem.

We could use this proof to improve the bound $Q(N) = o(N)$, by employing quantitative versions of Szemerédi's theorem. However, an old result of Behrend states that there are subsets of $1, \cdots, N$ of size $N/\exp(c\sqrt{\log N})$, which are free of three term arithmetic progressions, and so Szemerédi's argument cannot be used directly to save even a small power of $N$ in the upper bound for $Q(N)$.

To get such an improved upper bound for $Q(N)$, we might first try to generalize Euler's Theorem, by showing that for certain triples $1 \leqq k_1 < k_2 < k_3$ of integers, there are few pairs $(b,d)$ of coprime integers for which $b$, $b+k_1d$, $b+k_2d$, $b+k_3d$ are all squares. We shall see in section III that such pairs $(b,d)$ give rise to rational points (of infinite order) of a certain elliptic curve, and thus if the rank of this elliptic curve is 0 we deduce that there are no quadruples of integers $n_0, n_1, n_2, n_3$ in $\mathcal{Z}$ for which $n_1 - n_0 : n_2 - n_1 : n_3 - n_2 = k_1 : k_2 : k_3$. If we could collect enough restrictions of this kind then we might be able to prove a better upper bound for $Q(N)$; however we have been unable to prove that very many of these elliptic curves have rank 0. Moreover, it appears to be a difficult combinatorial problem to show that a set avoiding certain gaps is thin, and variations on this argument, allowing for example elliptic curves of rank 1, do not seem to avoid the combinatorial difficulties mentioned before.

The new idea in this paper is that one might employ five squares in the argument above, instead of four. As we shall see in the next section, we now generate a non–singular curve of genus 5 (instead of an elliptic curve), and may use Faltings's theorem: Thus, for any quadruple $1 \leqq k_1 < k_2 < k_3 < k_4$ of integers, we know that there are only finitely many quintuples of squares $b$, $b+k_1d$, $b+k_2d$, $b+k_3d$, $b+k_4d$. From here it is easy to again prove that $Q(N) = o(N)$: Pick an integer $M$ arbitrarily large, and consider each of the intervals $[0,M), [M,2M), \cdots, [rM,(r+1)M)$, where $r = [N/M]$. If any such interval contains five elements of $\mathcal{Z}$, then this represents a quintuple of squares $b, b+k_1d, b+k_2d, b+k_3d, b+k_4d$ with $1 \leqq k_1 < k_2 < k_3 < k_4 < M$. By Faltings's Theorem there are only finitely many such quintuples, and so the total number of elements of $\mathcal{Z}$ is $\leqq 4r + O_M(1)$; the result follows from letting $M \to \infty$. Even easier arguments along the same lines prove the corresponding theorem for $k$-th powers.

In order to prove our Theorem we shall appeal to an explicit version of Faltings's Theorem, contained in Lemma 5. Together with lemmas 2 and 3, it will allow us to show that, for any fixed $\epsilon > 0$, and any given $1 \leqq k_1 < k_2 < k_3 < k_4 < N$, there are $\ll_\epsilon N^\epsilon$ quintuples of squares $b$, $b+k_1d$, $b+k_2d$, $b+k_3d$, $b+k_4d$, with $d$ greater than a constant depending only on $N$ and $\epsilon$. Thus, using the argument in the paragraph above with $M = N^{1/5-\epsilon}$, we obtain the bound $Q(N;q,a) \ll N^{4/5+\epsilon}$ provided $q$ is sufficiently large. In section V we use more sophisticated combinatorics to replace the exponent '4/5' with '2/3', and we replace the $N^\epsilon$ with a power of $\log N$ by taking more care with our explicit upper bound from Faltings's theorem. We see no compelling reason why the exponent '2/3' in the Theorem could not be improved by a better combinatorial argument.

In the paragraph above we noted that our method only takes effect when $q$ is sufficiently large. The value of this 'sufficiently large' is given explicitly in the text, and for smaller values of $q$ the following argument, using the large sieve, gives a much better bound than the Theorem: If $p$ is a prime that does not divide $q$, and $b$ is not a quadratic residue modulo $p$ then $n \notin \mathcal{Z}$ whenever $n \equiv (b-a)/q \pmod{p}$; thus there are $(p-1)/2$ residue classes (mod $p$) that cannot contain elements of $\mathcal{Z}$. The large sieve (see for example the top equation on p.18 of [B]) then tells us that, for any integer $Z$,

$$Q(N;q,a) \leqq (N+Z^2) \Big/ \sum_{p\le Z,\ (p,q)=1} \frac{p-1}{2p}.$$

We take $Z=[3\sqrt{N}]$ and deduce the bound $Q(N;q,a) \ll \sqrt{N}\log N$, unless $q$ were divisible by at least half of the primes $\leqq Z$, in which case we would certainly have $q \geqq e^{\sqrt{N}}$ for large $N$. This estimate will be used later in the proof.

To lend more credence to the conjecture $Q(N) \sim \sqrt{\frac{8}{3}N}$, one may also try to count directly the number of solutions of the congruence $m^2 \equiv a \pmod{q}$ for $m$ in an appropriate interval. It is then easy to see that $Q(N;q,a) \leqq \sqrt{\frac{8}{3}N} + o(\sqrt{N})$ provided $q \ll \exp(c\log N \log\log N)$ for any fixed $c < \frac{1}{2\log 2}$, the maximum being attained only for the progression $24n-23$, provided $N$ is sufficiently large.

We finally make the straightforward observation that we may assume $q$ and $a$ to be coprime. For, if we first divide out any square that may divide $\gcd(q,a)$, we can then replace the interval $1,\cdots,N$ by a suitable arithmetic progression modulo $\gcd(q,a)$ and then we can divide out the factor $\gcd(q,a)^2$.

Acknowledgement. We wish to thank Pierre Deligne, Noam Elkies, Paul Erdös, Gerd Faltings, Hendrik W. Lenstra and Carl Pomerance for some useful discussions and suggestions. In particular, we owe to Faltings the remark that in our case one can avoid the use of his deep theorem, replacing it by a gap theorem of Mumford which has a relatively easy proof; this may be of importance in other situations. However we have decided to base our proof on Faltings's Theorem, because it is more elegant and easier to state, if not to prove.

II. Let $qn_0 + a = m_0^2$ and $qn_1 + a = m_1^2$ be two distinct solutions. Then we may view the pair $(m_0, m_1)$ as a rational point on the projective line $\mathbf{P}^1$ with homogeneous co-ordinates $(x_0, x_1)$. Conversely, suppose that $\gcd(q, a) = 1$ and $q > 2N$ and that $qn_i + a = m_i^2$, $qn_i' + a = {m_i'}^2$, $i = 1, 2$ are two pairs of distinct solutions with $(m_1, m_2)$ proportional to $(m_1', m_2')$. Then $n_1' = n_1$ and $n_2' = n_2$. In fact, we obtain

$$\frac{qn_1' + a}{qn_1 + a} = \frac{qn_2' + a}{qn_2 + a}$$

and clearing denominators we get $q(n_1 n_2' - n_1' n_2) + a(n_1 + n_2' - n_1' - n_2) = 0$. Now $q$ and $a$ are coprime, therefore $q \mid n_1 + n_2' - n_1' - n_2$ and since $q > 2N$ we get $n_1 + n_2' - n_1' - n_2 = 0$. This in turn implies that $n_1 n_2' - n_1' n_2 = 0$, and our assertion follows.

Next, let $qn_i + a = m_i^2$, $i = 0, 1, 2$ be three distinct terms in our progression. By eliminating $q, a$ we get

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

which we interpret as giving a rational point $(m_0, m_1, m_2)$ on the conic $C_1$ defined by

$$(n_1 - n_2)x_0^2 + (n_2 - n_0)x_1^2 + (n_0 - n_1)x_2^2 = 0$$

in the projective plane $\mathbf{P}^2$ with homogeneous co-ordinates $(x_0, x_1, x_2)$. More generally, let us consider vectors of $l + 2$ points $\mathbf{n} = (n_0, \cdots, n_{l+1})$ such that $qn_i + a = m_i^2$ is a square for each $i$ and let us denote by $\mathbf{k}$ the vector of gaps $k_{ij} = n_j - n_i$. Then $\mathbf{n}$ determines a rational point $(m_0, \cdots, m_{l+1})$ on the algebraic projective curve $C_l(\mathbf{k})$ defined by

$$(n_i - n_{i+1})x_{i-1}^2 + (n_{i+1} - n_{i-1})x_i^2 + (n_{i-1} - n_i)x_{i+1}^2 = 0$$

for $i = 1, \cdots, l$. It is easily verified that the curve $C_l$ is non-singular of degree $2^l$ in $\mathbf{P}^{l+1}$, by applying the Jacobian criterion and Bézout's Theorem.

The genus of the curve $C_l$ is $(l - 2)2^{l-1} + 1$; this follows from the well-known fact (see e.g. [H], Appendix One, p. 159, (1)) that the total Chern class of a non-singular complete intersection $X$ of $r$ hypersurfaces of degrees $d_1, \cdots, d_r$ in $\mathbf{P}^{n+r}$ is

$$c(X) = (1 + h)^{n+r+1}(1 + d_1 h)^{-1} \cdots (1 + d_r h)^{-1}$$

where $h$ is the class of a hyperplane section of $X$. Alternatively, one can proceed by induction on $l$ by considering the double cover $C_{l+1} \to C_l$ induced by the projection $(x_0, \cdots, x_l, x_{l+1}) \to (x_0, \cdots, x_l)$, checking that it is ramified at exactly $2\deg(C_l)$ points and applying Hurwitz's genus formula. In particular, every curve $C_2$ is an elliptic curve.

In the special case in which $l = 3$ the genus is 5 and we have five projections

$$\pi_i : C_3(\mathbf{k}) \to C_2(\mathbf{k}^{(i)})$$

for $i = 0, \cdots, 4$ from $C_3(\mathbf{k})$ to the curve $C_2(\mathbf{k}^{(i)})$ of genus 1 associated to the vector $\mathbf{n}^{(i)}$ obtained from $\mathbf{n}$ by omitting the component $n_i$. We denote by $J(C_3(\mathbf{k}))$ the Jacobian variety of $C_3(\mathbf{k})$, and similarly $J(C_2(\mathbf{k}^{(i)}))$ will be the Jacobian of the curve $C_2(\mathbf{k}^{(i)})$. The curve $C_2(\mathbf{k}^{(i)})$ has a rational point, for example $(1,1,1,1)$, and therefore it may be identified with its own Jacobian.

The following lemma reduces the study of the Jacobian of $C_3(\mathbf{k})$ to the study of the elliptic curves $C_2(\mathbf{k}^{(i)})$, and this allows us to do the Fermat descent on $J(C_3(\mathbf{k}))$ in a simple and elementary fashion. A thorough discussion of curves of genus 5 which are intersection of three non-singular quadrics can be found in [ACGH], Ch. VI, Ex. F-G, pp. 271-276.

Lemma 1. *The product map*

$$f : C_3(\mathbf{k}) \to \prod_{i=0}^{4} C_2(\mathbf{k}^{(i)})$$

*with* $f = (\pi_0, \cdots, \pi_4)$ *induces an isogeny*

$$f_* : J(C_3(\mathbf{k})) \to \prod_{i=0}^{4} J(C_2(\mathbf{k}^{(i)}))$$

*with kernel a subgroup of the group of 2-division points of* $J(C_3(\mathbf{k}))$.

Proof. We denote by $cl$ the homomorphism from divisors of degree 0 on a curve $C$ to its Jacobian $J(C)$. Hence let $\sum a_\nu P_\nu$ be a divisor of degree 0 on $C_3(\mathbf{k})$ and let $cl(\sum a_\nu P_\nu) = \delta$. Clearly it suffices to prove that $cl(\pi_i(\sum a_\nu P_\nu)) = 0$ for $i = 0, \cdots, 4$ implies $2\delta = 0$ on $J(C_3(\mathbf{k}))$.

We verify this fact as follows. Let $G$ be the group of automorphisms of $C_3(\mathbf{k})$ of type

$$\gamma(x_0, x_1, x_2, x_4) = (\epsilon_0 x_0, \epsilon_1 x_1, \epsilon_2 x_2, \epsilon_3 x_3, \epsilon_4 x_4)$$

with $\epsilon_i = \pm 1$, and let $\gamma_i$ be the element with $\epsilon_i = -1$ and $\epsilon_j = 1$ for $j \neq i$. Then $\pi_i^{-1} \circ \pi_i(P) = P + \gamma_i(P)$, thus the pull-back by $\pi_i$ of $cl(\pi_i(\sum a_\nu P_\nu)) = 0$ yields $cl(\sum a_\nu \gamma_i(P_\nu)) = -\delta$ for every $i$. This gives $\gamma_0\gamma_1\gamma_2\gamma_3\gamma_4(\delta) = -\delta$. On the other hand, $\gamma_0\gamma_1\gamma_2\gamma_3\gamma_4$ is the identity in $G$ and we conclude that $\delta = -\delta$, as we wanted.

Corollary. *Let* $r(\mathbf{k})$ *be the rank the Mordell-Weil group of rational points of the Jacobian of* $C_3(\mathbf{k})$, *and similarly let* $r(\mathbf{k}^{(i)})$ *denote the rank of the Mordell-Weil group of rational points of the elliptic curve* $C_2(\mathbf{k}^{(i)})$. *Then*

$$r(\mathbf{k}) = \sum_{i=0}^{4} r(\mathbf{k}^{(i)})\,.$$

III. We need estimates for the rank of the elliptic curves $C_2(\mathbf{k}^{(i)})$. This can be done by performing a 2-descent, which is done most easily as follows.

Let us consider for example the curve $C_2(\mathbf{k}^{(4)})$, which is the complete intersection of the two quadrics

$$\begin{aligned}(n_1-n_2)x_0^2+(n_2-n_0)x_1^2+(n_0-n_1)x_2^2=0\\ (n_2-n_3)x_1^2+(n_3-n_1)x_2^2+(n_1-n_2)x_3^2=0\,.\end{aligned}$$

This is equivalent to saying that there exist $q$ and $a$ such that $qy_0+a=x_0^2$, $qy_1+a=x_1^2$, $qy_2+a=x_2^2$, $qy_3+a=x_3^2$ and $y_1-y_0=n_1-n_0$, $y_2-y_1=n_2-n_1$, $y_3-y_2=n_3-n_2$. In particular, we see that $q=(x_1^2-x_0^2)/(n_1-n_0)$. If we write $z=y_0+a/q$ and multiply together the first four equations we get

$$z(z+(n_1-n_0))(z+(n_2-n_0))(z+(n_3-n_0))=(x_0x_1x_2x_3/q^2)^2\,.$$

We set in succession $z=1/u$, $x_0x_1x_2x_3/q^2=v/u^2$, $(n_1-n_0)(n_2-n_0)(n_3-n_0)u=w$, $(n_1-n_0)(n_2-n_0)(n_3-n_0)v=t$ and $w=s-(n_1-n_0)(n_2-n_0)$ and find

$$t^2=s(s+(n_1-n_0)(n_3-n_2))(s+(n_2-n_0)(n_3-n_1))$$

with

$$\begin{aligned}s&=(n_3-n_0)((n_2-n_0)x_1^2-(n_2-n_1)x_0^2)/x_0^2\\ t&=(n_1-n_0)(n_2-n_0)(n_3-n_0)x_1x_2x_3/x_0^3\,.\end{aligned}$$

This is the equation of a cubic elliptic curve $E(\mathbf{k}^{(4)})$ with rational 2-division points, namely the points $(0,0)$, $(-(n_1-n_0)(n_3-n_2),0)$, $(-(n_2-n_0)(n_3-n_1),0)$ and the point at $\infty$ of the elliptic curve. The discriminant of the curve is

$$\Delta^{(4)}=16\prod_{0\le i<j\le 3}(n_j-n_i)^2\,.$$

The map $C_2(\mathbf{k}^{(4)})\to E(\mathbf{k}^{(4)})$ we have constructed is an isogeny of degree 4, therefore these two curves have the same rank. The same considerations of course apply to every $C_2(\mathbf{k}^{(i)})$.

Lemma 2. *Let $E$ be the cubic elliptic curve*

$$t^2=(s-e_1)(s-e_2)(s-e_3)$$

*with rational integers $e_i$ and let $\Delta=16(e_1-e_2)^2(e_2-e_3)^2(e_3-e_1)^2$ be its discriminant. Let $E(\mathbf{Q})$ be the Mordell-Weil group of rational points of $E$. Then*

$$|E(\mathbf{Q})/2E(\mathbf{Q})|\leqq 2^{2+\sum_{i<j}\omega(e_j-e_i)}$$

*where $\omega(n)$ denotes the number of distinct prime factors of $n$. In particular, we have*

$$\operatorname{rank}(E(\mathbf{Q}))\leqq\omega(e_2-e_1)+\omega(e_3-e_2)+\omega(e_3-e_1)\,.$$

Proof. The following elegant and explicit treatment of the Fermat descent, apart from some minor changes, can be found in Lang [L], Ch. V, Theorem 1.1; see also the survey article of Cassels [C], p. 268. We include it here for completeness.

Let $(s, t)$ ba a rational point other than a 2-division point $(e_1, 0)$, $(e_2, 0)$, $(e_3, 0)$, $\infty$, and let us write $s - e_i = a_i u_i^2$ with $u_i \in \mathbf{Q}^*$ and $a_i$ a non-zero square-free integer. Note that $a_i$ is coprime to the denominator of $s$, which is a perfect square. Since $(s-e_1)(s-e_2)(s-e_3)$ is a square, $a_1 a_2 a_3$ is a square too and since the $a_i$'s are square-free we have $a_1 = b_2 b_3$, $a_2 = b_3 b_1$, $a_3 = b_1 b_2$ for a suitable triple $(b_1, b_2, b_3)$ of coprime square-free integers; the triple $(b_1, b_2, b_3)$ is uniquely determined up to sign. Taking differences we deduce that

$$b_i \mid e_j - e_k$$

for every permutation $(i, j, k)$ of $(1, 2, 3)$.

We define a map $\alpha_i : E(\mathbf{Q}) \to \mathbf{Q}^*/(\mathbf{Q}^*)^2$ by

$$\begin{aligned} \alpha_i(\infty) &= 1 \\ \alpha_i((e_i, 0)) &= (e_j - e_i)(e_k - e_i) \bmod (\mathbf{Q}^*)^2 \\ \alpha_i((s, t)) &= s - e_i \bmod (\mathbf{Q}^*)^2 \quad \text{otherwise} \end{aligned}$$

and define $\alpha : E(\mathbf{Q}) \to (\mathbf{Q}^*/(\mathbf{Q}^*)^2)^3$ by $\alpha = (\alpha_1, \alpha_2, \alpha_3)$.

We claim that each $\alpha_i$ is a group homomorphism. This is the same as saying that if $P_i = (s_i, t_i)$, $i = 1$, 2, 3 are three collinear points on $E$ then

$$\alpha_i(P_1)\alpha_i(P_2)\alpha_i(P_3) = 1 \,.$$

Suppose first that no $P_i$ is a 2-division point nor $\infty$. Let $t = \lambda s + \mu$ be the line through $P_1$, $P_2$ and $P_3$; then $s_1$, $s_2$, $s_3$ are the roots of the monic cubic polynomial $(s - e_1)(s - e_2)(s - e_3) - (\lambda s + \mu)^2$. If we make a translation by $e_i$ and look at the constant term of the polynomial we obtain, by symmetric functions:

$$(s_1 - e_i)(s_2 - e_i)(s_3 - e_i) = (\lambda e_i + \mu)^2$$

which is a square, whence $\alpha_i(P_1)\alpha_i(P_2)\alpha_i(P_3) = 1$, as claimed. The case in which one of the points $P_i$ is a 2-division point or $\infty$ can be handled in a similar fashion, by looking at the coefficient of the linear term in the cubic polynomial, rather than the constant term; this is the only modification of any substance needed in the proof.

Next, we claim that $\ker(\alpha) = 2E(\mathbf{Q})$. Let $P_1 = (s_1, t_1)$ be a rational point on $E$, let $t = \lambda s + \mu$ be the tangent line at $P_1$ and let $(s_2, t_2) = -2P_1$ be the third intersection point. Then $s_1, s_1, s_2$ are the roots of $(s - e_1)(s - e_2)(s - e_3) - (\lambda s + \mu)^2$ and the same argument as before shows that

$$s_2 - e_i = (\frac{\lambda e_i + \mu}{s_1 - e_i})^2$$

is a square, for $i = 1$, 2, 3. This shows that $2E(\mathbf{Q}) \subset \ker(\alpha)$. Conversely, suppose that $\alpha((s, t)) = 1$ and $P = (s, t)$ is not a 2-division point. Then $s - e_i = u_i^2$ is a square for

$i = 1, 2, 3$, with $u_i$ determined only up to sign. Hence let us solve, for any choice of the signs ±, the system of equations

$$\frac{\lambda e_i + \mu}{s_1 - e_i} = \pm u_i$$

for $i = 1, 2, 3$, in the unknowns $\lambda$, $\mu$, $s_1$. This is a linear system with non-zero determinant. To see this last point, we substitute $e_i = s - u_i^2$ and obtain a Vandermonde determinant which is easily seen to vanish only if $u_i^2 = u_j^2$ for some $i \neq j$; this cannot occur because $u_i^2 = s - e_i$ and $e_i \neq e_j$. Solving the system by Cramer's rule shows that $\lambda$, $\mu$, $s_1$ are rational numbers and $s_1$ and $t_1 = \lambda s_1 + \mu$ give the 8 points $P_1 = (s_1, t_1)$ for which $2P_1 = \pm P = (s, \pm t)$. A rather similar analysis holds if $(s, t)$ is a 2-division point, proving that $\ker(\alpha) = 2E(\mathbf{Q})$.

The proof of Lemma 2 is completed by noting that the image of $\alpha$ admits for representatives a subset of the triples $(b_2 b_3, b_3 b_1, b_1 b_2)$, with square-free, coprime $b_i$'s with $b_i \,|\, e_j - e_k$, and counting the number of triples $(b_1, b_2, b_3)$ up to a multiplier $\pm 1$. Since $E(\mathbf{Q})$ has rational 2-torsion we also have

$$|E(\mathbf{Q})/2E(\mathbf{Q})| \geqq 4 \cdot 2^{\mathrm{rank}(E(\mathbf{Q}))}$$

and the last clause of Lemma 2 follows from the fact that $E(\mathbf{Q})$ is finitely generated.

An immediate consequence of Lemma 1 and Lemma 2 is

Lemma 3. *We have*

$$r(\mathbf{k}) \leqq 3 \sum_{0 \leq i < j \leq 4} \omega(n_j - n_i)\,.$$

IV. We have already remarked that in estimating $Q(N)$ we may suppose that $q > e^{\sqrt{N}}$ and that $q$, $a$ are coprime. The following simple lemma shows that in this case the rational points we obtain on the curves $C_3(\mathbf{k})$ are quite large and well localized.

Lemma 4. *Suppose that* $\gcd(q,a)=1$ *and* $q > e^{\sqrt{N}}$. *Let* $qn_i + a = m_i^2$, $i = 0, \cdots, 4$ *be five distinct squares with* $1 \leqq n_i \leqq N$. *Then* $\mathbf{m} = (m_0, \cdots, m_4)$ *is a rational point on the curve* $C_3(\mathbf{k})$ *with height*

$$\frac{\sqrt{N}}{2} \leqq \frac{1}{2}\log q \leqq h(\mathbf{m}) \leqq \log q + \log N\,.$$

Proof. In fact, $\gcd(m_j, m_i)^2$ divides $m_j^2 - m_i^2 = q(n_j - n_i)$, while on the other hand $\gcd(m_i, q) = 1$ because otherwise $q$ and $a$ would have a common factor. This proves that $\gcd(m_j, m_i)^2$ divides $n_j - n_i$ and *a fortiori* we get

$$\gcd(m_0, \cdots, m_4)^2 \leqq \min_{i \neq j}\ |n_j - n_i|\,.$$

We write $m_i^* = m_i/\gcd(m_0, \cdots, m_4)$ and conclude that $|m_j^{*2} - m_i^{*2}| \geqq q$ for $j \neq i$ and in particular $\max m_j^{*2} \geqq q$. This proves the left hand side inequality of Lemma 4 because $h(\mathbf{m}) = \max \log |m_j^*|$. For the right-hand side inequality we simply note that $q(n_j - n_i) = m_j^2 - m_i^2 \geqq |m_j| + |m_i|$.

Lemma 5. *With the same hypotheses as in Lemma 4, the curve* $C_3(\mathbf{k})$ *has at most*

$$28 \cdot 7^{r(\mathbf{k})}$$

*rational points* $\mathbf{x}$ *of height* $h(\mathbf{x}) > c_1 \log N$. *Here* $c_1$ *is an absolute constant.*

Remark. As observed by Faltings, Lemma 4 restricts the height of the rational points of $C_3(\mathbf{k})$ which are of interest to us to an interval of type $[H, cH]$ for some constant $H$, and then one could use the easier Mumford's Theorem in place of Faltings's Theorem.

Proof. Lemma 5 is a consequence of the simplified proof of Faltings's Theorem in [B2]. However we cannot apply directly Theorem 2 of [B2] because we need to know how the various constants appearing there depend on the height of a defining set of equations for the curve $C$. A future paper [B3] will contain a more precise version of Theorem 2 of [B2] explicit in all constants, which includes Lemma 5 as a special case.

Thus in what follows we briefly indicate how to proceed to a reading of [B2] so to control constants in terms of the height of a set of defining equations of a non-singular projective model of $C$, leaving however much of the details to the forthcoming paper [B3]. In our discussion we will be consistent with the notation of [B2], except for the fact that the quantity $N$ introduced in section 3 of [B2] will be called here $\overline{N}$ in order to avoid a conflict with the meaning of $N$ elsewhere in this paper.

We want to apply Theorem 2 of [B2] to the curve $C = C_3(\mathbf{k})$, with $K = k = \mathbf{Q}$. This result states that there is a constant $\gamma(C)$ such that the points $z$ of $C(K)$ either have length $|z|$ with respect to the Néron-Tate form on the Jacobian bounded by $\gamma(C)$ or they belong to a finite set of cardinality at most

$$|\mathrm{tors}(A(K))| 7^{\rho} (1 + \log \gamma(C)/\log 2)\,,$$

where $A$ is the Jacobian of $C$ and $\rho$ is the rank of the Mordell-Weil group $A(K)$.

Actually, what is proved there is a more precise result. First of all, the term $|\mathrm{tors}A(K)|$ can be omitted altogether, since the application of Mumford's Theorem requires only that $(z, w)$ be distinct points of $C$ rather than having distinct images in $A(K) \otimes \mathbf{R}$. Taking this remark into account, what is proved there is that solutions either have length $|z|$ at most $\gamma_1(C)$, or they belong to an explicitly constructed finite set $Z$, or they belong to a finite set of cardinality

$$7^\rho(1 + \log\gamma_2(C)/\log 2)\,,$$

where $\gamma_1(C)$ and $\gamma_2(C)$ are two constants with the following property:

*For every pair of points $z, w \in C(\bar{k})$, $z, w \notin Z$, satisfying*

$$\gamma_1(C) \leqq |z|, \quad \gamma_2(C)|z| \leqq |w|$$

*we have*

$$<z, w> \;\leqq \frac{3}{4}|z||w|\,.$$

*Here $<\,,\,>$ is the Néron-Tate form on the Jacobian of $C$.*

We also want $\gamma_1(C) \geqq c_{20}/\epsilon$ and, in order to apply Mumford's Theorem, we need $\gamma_1(C) \geqq \beta_0$ for a constant $\beta_0$.

In [B2] we take $\gamma_1(C) = \gamma_2(C)$, but this restriction is unnecessary. A more important point however arises as follows. In [B2] we choose an auxiliary divisor $P$ of degree 1 and use the map $j(Q) = \mathrm{cl}(Q - P)$ to embed the curve $C$ in its Jacobian. This requires the knowledge of the divisor $P$, whose existence requires the vanishing of the Manin obstruction in the Brauer group of $C$, and an effective control of the height of $P$ appears to be problematic. A discussion of the problem of the existence of 0-cycles of degree 1 on varieties can be found in [L3], Ch. X, pp.250-258. Thus we must modify the construction of [B2] by allowing $P$ to be a $\mathbf{Q}$-divisor with rational coefficients, choosing a divisor $P_{m_0}$ of known degree $m_0 > 0$ and of known height $h(P_{m_0})$ and setting $P = \frac{1}{m_0}P_{m_0}$. The curve $C$ is in fact given as a projective curve defined over a number field $k$, hence if $m_0 = \deg(C)$ we may take $P_{m_0}$ to be a linear section of $C$, for example with a co-ordinate hyperplane.

This time we map the curve $C$ into its Jacobian $A = \mathrm{Pic}_0(C)$ by associating to a point $Q$ the divisor class $j_{m_0}(Q) = cl(m_0Q - P_{m_0})$, and denote by $j_{m_0} : C \to A$ this map, which is again an embedding of $C$ into its Jacobian. Since the Jacobian is a divisible group, there is a divisor $P_1$ of degree 1 defined over a finite extension $k_1$ of $k$ such that we have the linear equivalence of divisors $P_{m_0} \sim m_0P_1$. If $j : C \to A$ is the embedding determined by $j(Q) = cl(Q - P_1)$ and $[m_0] : A \to A$ is multiplication by $m_0$, we have $j_{m_0} = [m_0] \circ j$. This corresponds to taking the Albanese map (defined over $k_1$) with respect to the base divisor $P_1$, followed by multiplication by $m_0$. The overall change, with respect to the calculations in [B2], is to produce a rescaling of the formulas as follows.

Let $\Theta$ be the theta divisor associated to the embedding $j$, namely

$$\Theta = \{x \in A \mid x = x_1 + \cdots + x_g\,,\ x_i \in j(C)\}, \quad \theta = cl(\Theta),$$

and let

$$\Theta_{m_0} = \{x \in A \mid x = x_1 + \cdots + x_g\,,\ x_i \in j_{m_0}(C)\}, \quad \theta_{m_0} = cl(\Theta_{m_0}).$$

We perform the construction of section 3 of [B2] in a modified way. We define

$$\begin{aligned}\Delta'_{m_0} &= m_0\Delta - P_{m_0}\times C - C\times P_{m_0},\\ B_{m_0} &= sP_{m_0}\times C + sC\times P_{m_0} - m_0\Delta,\\ V_{m_0} &= d_1P_{m_0}\times C + d_2C\times P_{m_0} + d\Delta'_{m_0},\\ \delta_1 &= (d_1+sd)/\overline{N}, \quad \delta_2 = (d_2+sd)/\overline{N}\end{aligned}$$

so that

$$V_{m_0} = \delta_1\overline{N}P_{m_0}\times C + \delta_2 C\times\overline{N}P_{m_0} - dB_{m_0},$$

and denote by $\delta_m$ the divisor class on $A\times A$ given by

$$\delta_{m_0} = (s_1^* + s_2^* - s_{12}^*)\theta_{m_0}.$$

With this understanding, the only change in section 3 of [B2] consists in putting a suffix $m_0$ to the corresponding quantities.

The main change occurs in section 5 of [B2]. The linear equivalences of Lemma 1 become

$$\begin{aligned}j_{m_0}^*(\theta_{m_0}^-) &= m_0^{2g-1}gcl(P_{m_0}),\\ (j_{m_0}\times j_{m_0})^*\delta_{m_0} &= m_0^{2g-1}cl(\Delta'_{m_0}).\end{aligned}$$

If we define

$$< x,y >_{m_0} = \hat{h}_{\theta_{m_0}}(x+y) - \hat{h}_{\theta_{m_0}}(x) - \hat{h}_{\theta_{m_0}}(y), \quad |x|_{m_0}^2 = < x,x >_{m_0},$$

we obtain

$$\begin{aligned}h_{V_{m_0}}(z,w) =& m_0^{1-2g}\Big(\frac{d_1}{2g}|j_{m_0}(z)|_{m_0}^2 + \frac{d_2}{2g}|j_{m_0}(w)|_{m_0}^2 - d < j_{m_0}(z), j_{m_0}(w) >_{m_0}\Big) +\\ & O(d_1|j_{m_0}(z)|_{m_0} + d_2|j_{m_0}(w)|_{m_0}) + O(d_1) + O(d_2) + O(1),\end{aligned}$$

which replaces Lemma 2 in [B2]. It follows that the formulas of [B2] hold replacing $P$ by $P_{m_0}$, $\theta$ with $\theta_{m_0}$, and $|\ |^2$, $<\ ,\ >$ with $m_0^{1-2g}|\ |_{m_0}^2$, $m_0^{1-2g} <\ ,\ >_{m_0}$, and identifying $z$, $w$ with $j_{m_0}(z)$, $j_{m_0}(w)$, which we may because $j_{m_0}$ is an embedding.

With these identifications and modifications in mind, we verify that the calculations in [B2] suffice to prove that

$$\gamma_1(C) \ll \sqrt{h(C)} + 1\,, \quad \gamma_2(C) = 1600(n+1)^2\overline{N}^4\frac{\sqrt{g+1}}{g}$$

where $h(C)$ denotes the lowest upper bound for the height of a set of generators of the homogeneous ideal of $C$ in the projective embedding; the constant involved in the symbol $\ll$ depends on the genus $g$, degree $\overline{N}m_0$ and embedding dimension $n = \overline{N}m_0 - g$ of $C$ by means of the linear system $|\overline{N}P_{m_0}|$. Since the height in projective space of a point $z$ is proportional to $|z|^2$, we have:

*Let $C$ be a non-singular projective curve of genus at least 2 defined over a number field $k$ and let $h(C)$ be the lowest upper bound for the height of a set of generators for the homogeneous ideal of $C$ relative to the projective embedding. Let $K$ be a finite extension of $k$. Then the number of rational points $z \in C(K)$ with height $h(z) \geqq \lambda_1(h(C)+1)$ is at most*

$$12(\log(\deg(C))+1)7^\rho$$

*where $\lambda_1$ depends only on the degree and embedding dimension of $C$ and where $A(K)$ is the Mordell-Weil group of the Jacobian of $C$ and $\rho$ is its rank.*

In order to compute $\gamma_i(C)$ we retrace the various steps in [B2]. All constants $c_i$ in what follows refer to the constants in [B2].

The proof of [B2], Theorem 1 shows that we can choose $\gamma_2(C) = 1/\epsilon$ where $\epsilon$ is so small and $\gamma_1(C)$ is so large that

$$\frac{\sqrt{g+\gamma_0}}{g} + c_4\sqrt{g+\gamma_0}8\overline{N}\epsilon + c_{19}(\frac{1}{|z|}+\frac{1}{|w|}) + \frac{c_{18}}{\gamma_0|z|^2} \leqq \frac{3}{4}$$

whenever $|z| \leqq \epsilon|w|$ and $|z| \geqq \gamma_1(C)$. Here $\gamma_0$ is a parameter at our disposal. For example, we can choose

$$\epsilon = \frac{1}{200c_4\overline{N}\sqrt{g+1}}$$

and $\gamma_0 = 10^{-2}$, and we verify that this choice works as soon as

$$|z| \geqq \frac{c_{20}}{\epsilon} + 1 + 10^2(2c_{19}+\sqrt{c_{18}}) + \beta_0\,.$$

This yields admissible values

$$\gamma_2(C) = 200\overline{N}c_4\sqrt{g+1}, \quad \gamma_1(C) = 200\overline{N}c_{20}c_4\sqrt{g+1} + 1 + 10^2(2c_{19}+\sqrt{c_{18}}) + \beta_0\,.$$

We need a bound for the constant $c_4$ which appears in [B2], Lemma 6, p.628. Actually, it is slightly better to amend the statement of Lemma 6 by replacing the term $-c_4(i_1^*|z|^2 + i_2^*|w|^2 + i_1^* + i_2^*)$ with $-c_4(i_1^*|z|^2 + i_2^*|w|^2) - \beta_1(i_1^*+i_2^*)$ and a new constant $\beta_1$; this does not affect our preceding calculation for $\gamma_1(C)$ and $\gamma_2(C)$ as long as we keep in mind that the constant $c_{17}$ appearing in the proof of Theorem 1 contains the contribution of $\beta_1$. We need to majorize

$$c_5 i_1^* h(x_1/x_0) + c_6 i_1^* + 2i_1^* \sum_{\nu j} h((g_{\nu j})_\xi(x_\nu/x_j, x_1/x_0))$$

and this is at most

$$(c_5 + 2(n+1)^2 d_0) i_1^* h_{\overline{N}P_{m_0}}(z) + c_6 i_1^* + 2(n+1)^2(\max\, h(g_{\nu j}) + 3\log(d_0)) i_1^*$$

where $d_0 \leqq 2\overline{N}^2$ is an upper bound for the degree of each polynomial $g_{\nu j}$. We have

$$h_{\overline{N}P_{m_0}}(z) = \frac{\overline{N}}{2g}|z|^2 + O(|z|) + O(1)\,,$$

so that there is a bound

$$|h_{\overline{N}P_{m_0}}(z) - \frac{\overline{N}}{2g}|z|^2| \leqq \beta_2|z| + \beta_3 \leqq \frac{\overline{N}}{4g}|z|^2 + \frac{g}{\overline{N}}\beta_2^2 + \beta_3$$

for constants $\beta_2$, $\beta_3$ depending only on $C$. This shows that we can take

$$c_4 = (c_5 + 4(n+1)^2\overline{N}^2)\overline{N}/g\,.$$

The constant $c_5$ comes from the inequality

$$2i_1^* \sum_{\nu j} \sum_{v} \log^+ |\text{coefficient of } p_{\nu j}|_v + 5i_1^* \log(2d_0) \leqq c_5 i_1^* h(x_1/x_0) + c_6 i_1^*\,.$$

The polynomial $p_{\nu j}$ is simply $g_{\nu j}(\xi, \zeta + x_1/x_0)$, so that crude estimates for $c_5$ and $c_6$ are

$$\begin{aligned} c_5 &\leqq 4(n+1)^2\overline{N}^2 \\ c_6 &\leqq 5\log(4\overline{N}^2) + (n+1)^2(\max\, h(g_{\nu j}) + 3\overline{N}^2)\,. \end{aligned}$$

This yields at last $c_4 \leqq 8(n+1)^2\overline{N}^3/g$ and the explicit bound

$$\gamma_2(C) \leqq 1600(n+1)^2\overline{N}^4 \frac{\sqrt{g+1}}{g} < 1400\overline{N}^6\,.$$

For the application we have in mind in this paper we have $n = 4$, $m_0 = 1$, $\overline{N} = 8$ and $g = 5$, therefore $\gamma_2(C) < 2^{27}$ and $1 + \log\gamma_2(C)/\log 2 < 28$.

It remains to estimate $\gamma_1(C)$ and our goal is to prove

$$\gamma_1(C) \ll \sqrt{h(C)} + 1\,.$$

We give only a bare indication of the steps in the proof.

It is fairly easy to show that if $C$ has a presentation as a projective curve of logarithmic height $h(C)$ then we can ensure that the auxiliary construction of the $\mathbf{Q}$-divisor $P$ of degree 1 and the basic embeddings $\phi_{\overline{N}P_{m_0}} : C \to \mathbf{P}^n$ and $\phi_{B_{m_0}} : C \times C \to \mathbf{P}^m$ all have heights bounded by $\ll h(C) + 1$, and that $\phi_{\overline{N}P_{m_0}}$ is also sufficiently generic as needed in [B2]. Then it is also easy to prove that the exceptional set $Z$ consists only of points with height at most $\ll h(C) + 1$ (note that the definition of $Z$ in [B2] should be modified to include all zeros of the discriminants $D_{\nu j}$). By retracing the steps in the proof, keeping in mind our preceding remarks about the statement of [B2], Lemma 6, one sees that the required bound for $\gamma_1(C)$ is a consequence of:

$$\begin{aligned} &|h_{\overline{N}P_{m_0}}(z) - \frac{\overline{N}m_0^{1-2g}}{g}(\hat{h}_{\theta^-_{m_0}} \circ j_{m_0})(z)| \ll h(C) + 1\,, \\ &|\frac{s}{\overline{N}}h_{\overline{N}P_{m_0}}(z) + \frac{s}{\overline{N}}h_{\overline{N}P_{m_0}}(w) - h_{B_{m_0}}(z,w) - (\hat{h}_\delta \circ (j_{m_0} \times j_{m_0}))(z,w)| \ll h(C) + 1\,, \\ &\frac{s}{\overline{N}}h_{\overline{N}P_{m_0}}(z) + \frac{s}{\overline{N}}h_{\overline{N}P_{m_0}}(w) - h_{B_{m_0}}(z,w) \gg -h(C) - 1\,, \\ &|h_{\theta-\theta^-}(z)| \ll (\sqrt{h(C)} + 1)|z|\,. \end{aligned}$$

The third estimate is needed to compute the constant $\beta_0$ and the others are needed to compute $c_1$, $c_2$ in [B2], Lemma 2.

The first three estimates are a consequence of a quantitative form of Weil's Theorem on heights on projective varieties, and the last one can be deduced from the others as in [L2], Ch. 5, Proposition 5.4. In order to obtain the quantitative form of Weil's Theorem we need, one could proceed as in [L2], Ch. 4 keeping track of constants, but since we are dealing with projective varieties it is more convenient to replace [L2], Ch. 4, Lemma 2.2 with a systematic use of Segre embeddings, so that one always deals with complete linear systems. It is essential for our purposes to have a reasonably explicit description of the Jacobian as a projective variety, and this can be achieved in various ways, for example using Chow's construction [Ch], or using a $|3\Theta_{m_0}|$ embedding. The important thing to keep in mind in these considerations is that as long as we stay with constructive algebraic geometry all estimates for heights will remain linear in $h(C)$.

V. We are now in position to use a simple combinatorial argument in estimating $Q(N)$. Let us fix $q > e^{\sqrt{N}}$ and $a$ coprime with $q$ and let $\mathcal{Z}$ be a set of $Z$ integers $n$ in the interval $[1, N]$ such that $qn + a$ is a square. Let $d$ be an integer with $D < d$ and let us define

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

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

Let $\mathbf{n} = (n_0, \cdots, n_4)$ be a quintuple of distinct points of $\mathcal{Z}(d, l)$. Then $\mathbf{n}$ determines a point $\mathbf{m}$ on the curve $C_3(\mathbf{k})$ and by Lemma 4 the point $\mathbf{m}$ has large height, $h(\mathbf{m}) > \frac{1}{2}\sqrt{N}$. If $n_i \in \mathcal{Z}(d, l)$ for $i = 0, \cdots, 4$ then each $k_{ij} = n_j - n_i$ is divisible by $d$, therefore we may replace $\mathbf{k}$ with the new vector with integral co-ordinates $\mathbf{k}^* = \mathbf{k}/d$, and now $k^*_{ij} \leqq N/D$ for every $i$, $j$. Conversely, let $\mathbf{k}$ be a vector of integers $k_{ij}$ with $k_{ij} + k_{ji} = 0$, $k_{ij} + k_{jl} + k_{li} = 0$ and $k_{ij} \neq 0$ if $i \neq j$ and let $\mathbf{m}$ be a rational point on the curve $C_3(\mathbf{k})$ with $m_i \neq \pm m_j$ for $i \neq j$. Then the remark at the beginning of section II shows that if $q > 2N$ there is at most one point $\mathbf{n}$ such that, for some rational number $c$ and each $i$, we have $qn_i + a = (cm_i)^2$.

Lemma 6. *Let $N(\mathbf{k})$ be the number of rational points of the curve $C_3(\mathbf{k})$ with height at least $\frac{1}{2}\sqrt{N}$. Then*

$$\sum_{d>D} \sum_{l=1}^{d} \binom{Z(d, l)}{5} \leqq \sum_{\mathbf{k}: k_{4,0} \leq N/D} N(\mathbf{k})\,.$$

Proof. On the left side of the equation above we are counting the number of tuples $(n_0, n_1, \cdots, n_4, d)$ such that each $n_j \in \mathcal{Z}$, $n_0 < n_1 < \cdots < n_4$, $d > D$ and $d$ divides each $n_j - n_i$. Writing $n_j - n_i = dk_{ij}$ and $qn_i + a = m_i^2$ we see, as above, that we have (projectively speaking) a point $\mathbf{m}$ on $C_3(\mathbf{k})$. By Lemma 4 and our hypothesis $q > e^{\sqrt{N}}$ we see that $h(\mathbf{m}) > \frac{1}{2}\sqrt{N}$. So we may count the number of tuples by counting for each such curve $C_3(\mathbf{k})$, and for each (projective) point $\mathbf{m}$ on $C_3(\mathbf{k})$ with $h(\mathbf{m}) > \frac{1}{2}\sqrt{N}$, the number of $d > D$ for which $d = (n_j - n_i)/k_{ij}$ for each $i \neq j$ and $qn_i + a = (cm_i)^2$ for some rational $c$ and each $i$. Now, by the comment immediately preceding Lemma 6, there can be no more than one value of $d > D$, and Lemma 6 follows.

Lemma 5 and Lemma 3 show that

$$N(\mathbf{k}) \ll \prod_{0 \leq i < j \leq 4} 7^{3\omega(k_{ij})}$$

hence Lemma 6 yields

$$\sum_{d>D} \sum_{l=1}^{d} \binom{Z(d, l)}{5} \ll \sum{}' \prod_{0 \leq i < j \leq 4} 7^{3\omega(k_{ij})}$$

where $\sum'$ runs over the possible sets of gaps $k_{ij}$. Since $k_{01}$, $k_{12}$, $k_{23}$, $k_{34}$ determine the $k_{ij}$'s and $k_{ij} \leqq N/D$, from the inequality between arithmetic and geometric means we deduce

$$\sum_{d>D} \sum_{l=1}^{d} \binom{Z(d, l)}{5} \ll (\frac{N}{D})^3 \sum_{k \leq N/D} 7^{30\omega(k)}$$

and finally

$$\sum_{d>D}\sum_{l=1}^{d}\binom{Z(d,l)}{5} \ll (\frac{N}{D})^4(\log N)^c$$

with $c = 7^{30} - 1$, by a standard estimate of the average of powers of the divisor function.

Let $\Lambda_0(d)$ be the set of $l$'s for which $Z(d,l) \leqq 5$ and let $\Lambda_1(d)$ be the set where $Z(d,l) \geqq 6$. Clearly on $\Lambda_1(d)$ we have $\binom{Z(d,l)}{5} \geqq Z(d,l)$, hence the last displayed inequality yields

$$\sum_{d>D}\sum_{\Lambda_1(d)} Z(d,l) \ll (\frac{N}{D})^4(\log N)^c\,.$$

On the other hand, we have

$$\sum_{\Lambda_0(d)} Z(d,l) \leqq 5d$$

and

$$\sum_{l=1}^{d} Z(d,l) = Z\,,$$

therefore we get

$$\begin{aligned} DZ = \sum_{D<d\leq 2D} Z &= \sum_{D<d\leq 2D}\sum_{\Lambda_0(d)} Z(d,l) + \sum_{D<d\leq 2D}\sum_{\Lambda_1(d)} Z(d,l) \\ &\leqq \sum_{D<d\leq 2D} 5d + O((\frac{N}{D})^4(\log N)^c)\,. \end{aligned}$$

The proof of our main result is completed choosing for example $D = Z/20$.

VI. Rather similar considerations apply to the study of $Q_k(N)$, where we work now with Fermat type curves

$$(n_1 - n_2)m_0^k + (n_2 - n_0)m_1^k + (n_0 - n_1)m_2^k = 0\,.$$

The main difference lies in the study of the Mordell-Weil group of these curves. We cannot do the descent on the Jacobian by working over $\mathbf{Q}$, and one possibility consists in working instead in the cyclotomic field $\mathbf{Q}(\sqrt[k]{1})$, which fortunately does not depend on the $n_i$'s. Every point $(u, v, w)$ with $u$, $v$, $w$ a $k$-th root of unity lies on the Fermat curve and the differences between these points generate a subgroup of the Mordell-Weil group of the Jacobian.

Let $T_k$ be the subgroup of $k$-division points of the Jacobian obtained in this way; for example, if $k = 3$, it may be verified directly that $|T_3| \geqq 3$ and that in most cases $T_3 \cong \mathbf{Z}/(3)$, while the Jacobian is an elliptic curve. We expect, but we have not verified, that $T_k$ may be sufficiently large so to be able to perform a $k$-descent using an isogeny with kernel a subgroup of $T_k$, and this should provide us with a good bound for the rank of the Mordell-Weil group. This in turn will give the bounds for $Q_k(N)$ stated in the introduction of this paper.

## References

[ACGH] Arbarello, E., Cornalba, M., Griffiths P. and J. Harris, *Geometry of Algebraic Curves, I.* Springer-Verlag, Berlin-Heidelberg-New York 1985.

[B] Bombieri, E. *Le Grand Crible dans la Théorie Analytique des Nombres.* Astérisque n° 18, 2nd edition 1987/1974, Société Mathématique de France.

[B2] Bombieri, E. The Mordell Conjecture Revisited. *Annali Scuola Normale Sup. Pisa, Cl. Sci.*, S. IV, **17** (1990), pp. 615-640.

[B3] Bombieri, E. On the Number of Rational Points of an Algebraic Curve, in preparation.

[C] Cassels, J. W. S. Diophantine equations with special references to elliptic curves. *Jour. London Math. Soc.* **41** (1966), pp. 193-291.

[Ch] Chow, W. L. The Jacobian Variety of an Algebraic Curve. *American Jour. of Math.* **76** (1954), pp. 453-476.

[E-G] Erdös, P. and R. Graham. *Old and New Problems and Results in Combinatorial Number Theory.* Monographie N° 28 de L'Enseignement Mathématique, Genève 1980.

[H] Hirzebruch, F. *Topological Methods in Algebraic Geometry*, third edition. Springer-Verlag, Berlin-Heidelberg -New York 1966.

[L] Lang, S. *Elliptic Curves–Diophantine Analysis.* Springer-Verlag, Berlin-Heidelberg-New York 1978.

[L2] Lang, S. *Fundamentals of Diophantine Geometry.* Springer-Verlag, New York-Berlin-Heidelberg-Tokyo 1983.

[L3] Lang, S. (Ed.) *Number Theory III. Diophantine Geometry* Encyclopaedia of Mathematical Sciences, Vol. 60, Springer- Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona 1991.

[S] Szemerédi, E. The number of squares in an arithmetic progression. *Studia Sci. Math. Hungar.* **9** (1974), p. 417.