ACTA ARITHMETICA
110.1 (2003)

Almost squares in arithmetic progression (II)

by

Anirban Mukhopadhyay (Allahabad) and T. N. Shorey (Mumbai)

1. Introduction. For an integer $\nu > 1$, we denote by $P(\nu)$ and $\omega(\nu)$ the greatest prime factor of ν and the number of distinct prime divisors of ν, respectively. Further we put $P(1) = 1$ and $\omega(1) = 0$. Let n, d, k, b, y be positive integers such that b is square free, $d > 1$, $k \geq 3$ and $P(b) \leq k$. We consider the equation

$$n(n+d)\dots(n+(k-1)d) = by^2 \quad \text{in } n, d, k, b, y \text{ with } P(b) \leq k. \tag{1}$$

For an account of results on (1), we refer to [8] and [9]. Shorey and Tijdeman [10] proved that (1) with $\gcd(n, d) = 1$ implies that k is bounded by an effectively computable number depending only on $\omega(d)$. Further Shorey [8, p. 489] showed that the assumption $\gcd(n, d) = 1$ can be relaxed to $d \nmid n$ in the preceding result. On the other hand, we observe that (1) may have infinitely many solutions in the case $d \mid n$. Next Saradha and Shorey [7] showed that (1) with $b = 1$ and $k \geq 4$ is not possible whenever $\omega(d) = 1$. It has also been shown in [7] that (1) with $P(b) < k$, $d \nmid n$, $\omega(d) = 1$ and $k \geq 10$ does not hold. In this paper, we prove

Theorem 1. *Let $4 \leq k \leq 9$, $P(b) < k$ and $\omega(d) = 1$ such that $d \nmid n$. Then* (1) *does not hold unless $n = 75$, $d = 23$, $k = 4$, $b = 6$, $y = 4620$.*

The case $k = 3$ remains open even when $b = 1$. Next we consider (1) with $P(b) = k$. Saradha and Shorey [7] showed that (1) with $P(b) = k$, $\gcd(n, d) = 1$ and $\omega(d) = 1$ implies that $k \leq 29$. We prove

Theorem 2. *Let $7 \leq k \leq 29$ and $P(b) = k$. Assume that $\omega(d) = 1$ and $d \nmid n$. Then* (1) *does not hold.*

As stated above, the assumption $d \nmid n$ is necessary in the above theorems. The case $k = 5$ in Theorem 2 remains unresolved. The proofs of Theorems 1 and 2 depend on the theory of linear forms in logarithms. This is a new element in the proof. By combining the results stated above, we have

2000 *Mathematics Subject Classification*: Primary 11D61.

THEOREM 3. *Let $k \neq 3, 5$. Then (1) with $\omega(d) = 1$ and $d \nmid n$ implies that $n = 75$, $d = 23$, $k = 4$, $b = 6$, $y = 4620$.*

Fermat (see [4, p. 21]) stated that there are no four squares in an arithmetic progression and Euler (see [3, p. 635]) proved that (1) with $\gcd(n, d) = 1$, $k = 4$, $b = 1$ is not possible. Further Obláth [5] showed that (1) with $\gcd(n, d) = 1$, $k = 5$, $b = 1$ does not hold. We obtain the following extension of the result of Obláth.

THEOREM 4. *Equation (1) with $\gcd(n, d) = 1$, $k = 5$, $P(b) < k$ does not hold.*

We compute using SIMATH the Mordell group of an elliptic curve for the proof of Theorem 4. By (1), we write

$$n + id = a_i x_i^2, \quad P(a_i) \leq k, \ a_i \text{ square free for } 0 \leq i < k, \tag{2}$$

where x_i are positive integers. Further we put $R = \{a_0, a_1, \ldots, a_{k-1}\}$.

We thank Professor Frits Beukers for his remarks. We also thank the referee for his comments on an earlier draft of this paper.

2. Lemmas. We start with an estimate of Baker and Wüstholz [2] from the theory of linear forms in logarithms. The *height* of an algebraic number is defined as the maximum of the absolute values of the coefficients of its minimal polynomial with relatively prime integer coefficients. Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers different from $0, 1$ and let $\log \alpha_1, \ldots, \log \alpha_n$ be the principal logarithms. Let K be the field generated by $\alpha_1, \ldots, \alpha_n$ over $\mathbb{Q}$ and d be the degree of K over $\mathbb{Q}$. Assume that the heights of $\alpha_1, \ldots, \alpha_n$ do not exceed $A_1, \ldots, A_n$, respectively, where $A_i \geq e$ for $1 \leq i \leq n$. Let $b_1, \ldots, b_n$ be rational integers of absolute values not exceeding B where $B \geq e$. We put

$$\Lambda = b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n.$$

We have

LEMMA 1. *If $\Lambda \neq 0$, then*

$$\log |\Lambda| > -(16nd)^{2(n+2)} \log A_1 \ldots \log A_n \log B.$$

The next result is due to Baker and Davenport [1].

LEMMA 2. *Let θ, β, C be real numbers with $C > 1$. Suppose $K > 6$. For any positive integer M, let p and q be integers satisfying*

$$1 \leq q \leq KM, \quad |\theta q - p| < 2(KM)^{-1}.$$

Then, if

$$\|q\beta\| \geq 3K^{-1},$$

there is no solution of

$$|m\theta - n + \beta| < C^{-m}$$

in the range

$$\frac{\log K^2 M}{\log C} < m < M.$$

Now we apply Lemmas 1 and 2 to solve certain simultaneous Pell's equations as in Baker and Davenport [1].

LEMMA 3. *Let $\delta \in \{-1, 1\}$. Consider the following set of simultaneous Pell's equations*:

$$X^2 + 2 = 6Y^2, \qquad (X+\delta)^2 + 2 = 3Z^2; \tag{3}$$

$$X^2 - 6 = 3Y^2, \qquad (X+\delta)^2 - 2 = 2Z^2; \tag{4}$$

$$X^2 - 3 = 6Y^2, \qquad (X+2\delta)^2 + 1 = 2Z^2; \tag{5}$$

$$X^2 + 2 = 3Y^2, \qquad (X+\delta)^2 + 2 = 2Z^2; \tag{6}$$

$$X^2 + 4 = 2Y^2, \qquad (X+2\delta)^2 + 6 = 6Z^2. \tag{7}$$

These equations have no solutions in positive integers X, Y, Z other than $X = 2$, $Y = 1$, $Z = 1$ with $\delta = -1$ for (3), *$X = 9$, $Y = 5$, $Z = 7$ with $\delta = 1$ and $X = 3$, $Y = 1$, $Z = 1$ with $\delta = -1$ for* (4), *$X = 3$, $Y = 1$, $Z = 1$ with $\delta = -1$ for* (5), *$X = 1$, $Y = 1$, $Z = 1$ with $\delta = -1$ for* (6), *$X = 2$, $Y = 2$, $Z = 1$ and $X = 14$, $Y = 10$, $Z = 5$ with $\delta = -1$ for* (7).

Proof. We follow Baker and Davenport [1] for the proof. The computations required for the proof are carried out using MATHEMATICA. By factorising the above equations, it is enough to solve the following exponential equations in non-negative integers m and n:

$$(1+\sqrt{3})(2+\sqrt{3})^m + (1-\sqrt{3})(2-\sqrt{3})^m - (2+\sqrt{6})(5+2\sqrt{6})^n - (2-\sqrt{6})(5-2\sqrt{6})^n = 2\delta,$$

$$(2+\sqrt{2})(3+2\sqrt{2})^n + (2-\sqrt{2})(3-2\sqrt{2})^n - (3-\sqrt{3})(2+\sqrt{3})^m - (3+\sqrt{3})(2-\sqrt{3})^m = 2\delta,$$

$$(1+\sqrt{2})(3+2\sqrt{2})^m + (1-\sqrt{2})(3-2\sqrt{2})^m - (3+\sqrt{6})(5+2\sqrt{6})^n - (3-\sqrt{6})(5-2\sqrt{6})^n = 4\delta,$$

$$\sqrt{2}(3+2\sqrt{2})^n - \sqrt{2}(3-2\sqrt{2})^n - (1+\sqrt{3})(2+\sqrt{3})^m - (1-\sqrt{3})(2-\sqrt{3})^m = 2\delta,$$

$$(2+2\sqrt{2})(3+2\sqrt{2})^m + (2-2\sqrt{2})(3-2\sqrt{2})^m - \sqrt{6}(5+2\sqrt{6})^n + \sqrt{6}(5-2\sqrt{6})^n = -4\delta.$$

We check that $m > n$. By Lemma 1, we derive that $m < 10^{26}$. Next we apply Lemma 2 with $M = 10^{26}$ and $K = 10^{13}$ to conclude that $m < 90$. By

a computer search we find that all the solutions are given in the statement of Lemma 3. ∎

For the further proofs it may be convenient to mention some standard arguments which are used repeatedly, sometimes without further reference. A square cannot be congruent to 2 modulo 3. If d is odd, it cannot happen that $a_i = a_{i+2} = 1$ since it would follow that $x_{i+2}^2 - x_i^2 = 2d$, whereas the difference of two squares can never be 2 modulo 4. If p divides n, we see from (2) that $\left(\frac{id}{p}\right) = \left(\frac{a_i}{p}\right)$. In particular, if $p = 7$ and $a_i \in \{1, 2, 3, 6\}$, then 3 divides a_i if and only if $\left(\frac{id}{p}\right) = -1$. Also, if 3 divides $n + id$, then neither $a_{i-1} = a_{i+1}$ nor $a_{i+1} = a_{i+2}$ is possible.

As stated in Section 1, we have the following result of Euler and we include the proof for the sake of completeness.

LEMMA 4. *Equation* (1) *with* $k = 4$, $b = 1$ *is not possible.*

Proof. The proof depends on the result that the equation

$$x^4 - x^2y^2 + y^4 = z^2 \quad \text{in positive integers } x, y, z \text{ with } \gcd(x, y) = 1 \tag{8}$$

has no solution other than $x = y = z = 1$ (see Mordell [4, p. 20]). Assume (1) with $k = 4$ and $b = 1$. There is no loss of generality in assuming that $\gcd(n, d) = 1$. Then we see from (2) that $a_0 = 3$, $a_1 = 2$, $a_2 = 1$, $a_3 = 6$ or $a_0 = 6$, $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ or $a_0 = a_1 = a_2 = a_3 = 1$. The last possibility is excluded since it implies (8) with $z > 1$ (see Mordell [4, p. 21]). Next we exclude the first possibility and the proof for the second is similar. By using $3(n + d) = 2n + (n + 3d)$, we observe that $x_1^2 = x_0^2 + x_3^2$. Since x_0 is odd and x_3 is even, we derive that $x_0 = r^2 - s^2$ and $x_3 = 2rs$ where $r > s > 0$ are integers such that $\gcd(r, s) = 1$ and $r \not\equiv s \pmod 2$. Then $d = 2x_3^2 - x_0^2 = 10r^2s^2 - r^4 - s^4$ and $x_2^2 = 3x_0^2 + 2d = r^4 + s^4 + 14r^2s^2$. Next we write $x = r + s$, $y = r - s$ and we observe that $x > y > 0$ with $\gcd(x, y) = 1$ since $\gcd(r, s) = 1$ such that $r \not\equiv s \pmod 2$. Then we obtain (8) with $z = x_2 > 1$ and this is a contradiction. ∎

There are infinitely many pairs (n, d) of relatively prime integers satisfying (1) with $k = 4$ (see Tijdeman [11]). On the other hand, we apply Lemma 3 to show that there is no pair (n, d) of relatively prime integers other than $(75, 23)$ satisfying (1) with $k = 4$ whenever d is a power of an odd prime.

LEMMA 5. *Let* d *be an odd prime power. Then* (1) *with* $\gcd(n, d) = 1$, $k = 4$ *implies that* $n = 75$, $d = 23$, $b = 6$, $y = 4620$.

Proof. We observe that $R \subset \{1, 2, 3, 6\}$. By Lemma 4, we derive that $|R| \neq 1, 4$. If $|R| = 2$, we again use Lemma 4 to observe that exactly three a_i's are equal to 1 implying that d is even. Thus $|R| = 3$. Then at least one a_i is divisible by 3. Suppose that 3 divides a_0 and a_3. Then $\left(\frac{a_1}{3}\right) = \left(\frac{d}{3}\right)$ and

$\left(\frac{a_2}{3}\right) = -\left(\frac{d}{3}\right)$. So either $a_1 = 1$, $a_2 = 2$ or $a_1 = 2$, $a_2 = 1$. Thus

$$a_0 = 3,\ a_1 = 2,\ a_2 = 1,\ a_3 = 3 \quad \text{or} \quad a_0 = 3,\ a_1 = 1,\ a_2 = 2,\ a_3 = 3.$$

From the first possibility, we observe from (2) that

$$n = 3x_0^2, \quad n + d = 2x_1^2, \quad n + 2d = x_2^2, \quad n + 3d = 3x_3^2. \tag{9}$$

So $d = x_3^2 - x_0^2$ implying $d = x_3 + x_0$ and $x_3 - x_0 = 1$ since d is an odd prime power. Thus $d = 2x_0 + 1$ and we obtain from (9) the following equations:

$$X^2 + 2 = 6Y^2, \quad (X+1)^2 + 2 = 3Z^2$$

with $X = 3x_0 + 1$, $Y = x_1$, $Z = x_2$. This is (3) of Lemma 3 with $\delta = 1$. Thus by Lemma 3 we conclude that this case is not possible. From the other possibility we get the following equations:

$$X^2 + 2 = 6Y^2, \quad (X-1)^2 + 2 = 3Z^2$$

with $X = 3x_0 + 2 \geq 5$, $Y = x_2$, $Z = x_1$. This is (3) of Lemma 3 with $\delta = -1$, which is not possible.

Thus we may suppose that 3 divides exactly one a_i. Let $3 \mid a_0$. We apply Legendre symbols as above to get the following two possibilities:

$$a_0 = 3,\ a_1 = 2,\ a_2 = 1,\ a_3 = 1 \quad \text{or} \quad a_0 = 3,\ a_1 = 2,\ a_2 = 1,\ a_3 = 2.$$

The first one gives the equations

$$X^2 - 6 = 3Y^2, \quad (X+1)^2 - 2 = 2Z^2$$

with $X = x_2 - 2$, $Y = x_0$, $Z = x_1$. Now we apply Lemma 3 with (4), $\delta = 1$ to conclude that $x_2 = 11,\ x_0 = 5,\ x_1 = 7$. Thus $n = 75,\ d = 23,\ b = 6$ and $y = 4620$. The second possibility gives

$$X^2 - 3 = 6Y^2, \quad (X+2)^2 + 1 = 2Z^2$$

with $X = 2x_1 - 1$, $Y = x_0,\ Z = x_2$ contradicting Lemma 3.

We proceed as above to observe that $3 \mid a_1$ gives (6) with $\delta = 1$ such that $X = x_0 + 1$, $Y = x_1$, $Z = x_2$ or $X = 3x_0 + 1$, $Y = 3x_1$, $Z = 3x_2$; $3 \mid a_2$ gives (6) with $\delta = -1$ such that $X = x_0 + 2$, $Y = x_2,\ Z = x_1$ or $X = 3x_0 + 2$, $Y = 3x_2$, $Z = 3x_1$; $3 \mid a_3$ gives (4) with $\delta = -1$, $X = x_0 + 3$, $Y = x_3$, $Z = x_2$ or (5) with $\delta = -1$, $X = 2x_0 + 3$, $Y = x_3,\ Z = x_1$. This is not possible by Lemma 3. ∎

LEMMA 6. *Let* $11 \leq k \leq 29$ *be prime. Then* (1) *with* $\gcd(n, d) = 1$, $P(b) = k$ *and* $|R| \geq k - 1$ *does not hold.*

Proof. Let $k = 29$. Then $|R| \geq 28$. We observe that the primes 29, 23, 19, 17, 13, 11, 7 divide at most 1, 2, 2, 2, 3, 3, 5 distinct a_i's respectively. Thus there are at least 10 distinct a_i's composed only of primes 2, 3 and 5, a contradiction.

Thus $11 \leq k \leq 23$. If $k = 17, 19, 23$ and $|R| = k$, we observe that the number of distinct a_i's composed only of 2, 3, 5 is at least 9. If $k = 11, 13$

and $|R| = k$, we see that the number of distinct a_i's composed of $2, 3$ is at least 5. This is not possible. Therefore $|R| = k - 1$.

Let $k = 23$. There are exactly 8 distinct a_i's composed of 2, 3 and 5. Therefore the primes 23, 19, 17, 13, 11, 7 divide exactly 1, 2, 2, 2, 3, 4 distinct a_i's, respectively, such that none of these a_i's is divisible by more than one of the above primes. Now we observe that 11 divides a_0, a_{11}, a_{22}. Therefore 7 cannot divide four a_i's. This is a contradiction.

Let $k = 19$. Now the primes 19, 17, 13, 11, 7, 5 divide 1, 2, 2, 2, 3, 4 distinct a_i's, respectively. Moreover these a_i's are divisible by only one of the primes given above. Let 17 divide a_0, a_{17}. If 5 divides a_1, a_6, a_{11}, a_{16}, we observe that 7 cannot divide three a_i's, a contradiction. Thus 5 divides a_3, a_8, a_{13}, a_{18}. Then 7 divides a_2, a_9, a_{16}; 13 divides a_1, a_{14}; 11 divides a_4, a_{15}. Thus one of the elements $a_5, a_6, a_7, a_{10}, a_{11}, a_{12}$ is divisible by 19 and the others are composed only of 2 and 3. Further we observe that

$$\left(\frac{a_5}{7}\right) = \left(\frac{a_7}{7}\right) = \left(\frac{a_{12}}{7}\right) = -\left(\frac{d}{7}\right), \quad \left(\frac{a_6}{7}\right) = \left(\frac{a_{10}}{7}\right) = \left(\frac{a_{11}}{7}\right) = \left(\frac{d}{7}\right).$$

Let 19 divide a_5. Then either $a_7, a_{12} \in \{3, 6\}$ or $a_6, a_{10}, a_{11} \in \{3, 6\}$, a contradiction. The possibilities of 19 dividing $a_6, a_7, a_{10}, a_{11}, a_{12}$ are excluded similarly. Hence 17 divides a_1, a_{18}. If 5 divides a_2, a_7, a_{12}, a_{17}, then 7 cannot divide three a_i's, a contradiction. Therefore 5 divides a_0, a_5, a_{10}, a_{15}. This is excluded as in the case 17 dividing a_0, a_{17} and 5 dividing a_3, a_8, a_{13}, a_{18}.

Let $k = 17$. The proof depends again as in the cases $k = 23$ on that there are exactly 8 distinct a_i's composed only of 2, 3 and 5. We observe that 5 divides a_0, a_5, a_{10}, a_{15} or a_1, a_6, a_{11}, a_{16}. In the former possibility, 7 divides a_2, a_9, a_{16} and 13 divides a_1, a_{14}, which is not possible since 11 cannot divide two a_i's. The latter possibility is excluded similarly.

Let $k = 11, 13$. There are exactly four distinct a_i's composed only of 2 and 3. First we consider the case $k = 13$. Then the primes $13, 11, 7, 5$ divide exactly $1, 2, 2, 3$ distinct a_i's respectively. Thus 11 divides a_0, a_{11} or a_1, a_{12}. Let 11 divide a_0, a_{11}. Then 5 divides a_2, a_7, a_{12} and 7 divides a_1, a_8 or a_3, a_{10}. Let 7 divide a_1, a_8. Then one of $a_3, a_4, a_5, a_6, a_9, a_{10}$ is divisible by 13 and others are composed of 2 and 3. Considering Legendre symbols modulo 7 and using $|R| = 12$, we see that $a_4, a_6 \in \{1, 2\}$. Further, if 13 divides a_3, then $a_5, a_9, a_{10} \in \{3, 6\}$, a contradiction. Similarly we see that 13 cannot divide any of a_5, a_9, a_{10}. The other possibility of 7 dividing a_3, a_{10} leads to a similar contradiction. The case of 11 dividing a_1, a_{12} is excluded similarly.

Let $k = 11$. Then 5 divides a_0, a_5, a_{10}. Further 7 divides a_1, a_8 or a_2, a_9. Let 7 divide a_1, a_8. Then 11 divides one of $a_2, a_3, a_4, a_6, a_7, a_9$ and the remaining ones are divisible by 2 and 3 only. Let 11 divide a_6. Then we use Legendre symbols modulo 7 as in the case $k = 19$ to derive that $a_4, a_7 \in \{3, 6\}$ and $a_2, a_3, a_9 \in \{1, 2\}$. Thus $\left(\frac{a_3}{3}\right) = \left(\frac{a_9}{3}\right) = -\left(\frac{d}{3}\right)$. Then $a_3 = a_9 = 1$ or

$a_3 = a_9 = 2$. Let $a_3 = a_9 = 1$. Then $a_2 = 2$, implying that n is even and so d is odd. Thus $n+3d$ and $n+9d$ are odd squares, hence congruent to 1 modulo 8. This implies that $4 \mid 6d$, a contradiction. Therefore $a_3 = a_9 = 2$. Further $\left(\frac{a_3}{11}\right) = -\left(\frac{d}{11}\right)$ and $\left(\frac{a_9}{11}\right) = \left(\frac{d}{11}\right)$ since 11 divides a_6. This is not possible. Let 11 divide a_3. Then $a_2, a_9 \in \{3, 6\}$ or $a_4, a_6, a_7 \in \{3, 6\}$ by using Legendre symbols modulo 7. This is not possible. The possibilities of 11 dividing a_4, a_7, a_9 are excluded similarly to $11 \mid a_3$. If 11 divides a_2, then $a_3, a_9 \in \{3, 6\}$ and $a_4, a_6, a_7 \in \{1, 2\}$. Hence $a_4 = a_6 = 1$, $a_7 = 2$ since either a_3 or a_9 is 6. Now we observe that $n + 4d$ and $n + 6d$ are odd squares. Therefore 8 divides $2d$, which is not possible. Hence 7 does not divide $a_1 a_8$. Similarly we conclude that 7 does not divide $a_2 a_9$. ∎

The next result is due to Pocklington [6].

LEMMA 7. *The equation*

$$r^4 + s^4 + 10r^2 s^2 = z^2 \tag{10}$$

does not have any solution in positive integers r, s, z *with* $\gcd(r, s) = 1$ *and* $r \not\equiv s \pmod 2$.

Next we prove Theorem 4 apart from two exceptional cases.

LEMMA 8. *Equation* (1) *with* $\gcd(n, d) = 1$, $k = 5$ *and* $P(b) < k$ *implies that either*

$$n = x_0^2, \quad n+d = 3x_1^2, \quad n+2d = 2x_2^2, \quad n+3d = x_3^2, \quad n+4d = 2x_4^2 \tag{11}$$

or

$$n = 2x_0^2, \quad n+d = x_1^2, \quad n+2d = 2x_2^2, \quad n+3d = 3x_3^2, \quad n+4d = x_4^2. \tag{12}$$

Proof. Assume (1) with $\gcd(n, d) = 1$, $k = 5$ and $P(b) < k$. Let d be even. Then $a_i = 1$ or 3. If $a_0 = 3$, then $a_1 = a_2 = 1$, which is not possible since $1 = \left(\frac{a_1}{3}\right) = \left(\frac{d}{3}\right)$ and $1 = \left(\frac{a_2}{3}\right) = \left(\frac{2d}{3}\right) = -\left(\frac{d}{3}\right)$. Thus $a_0 \neq 3$. Similarly we observe that none of the a_i's is equal to 3. This contradicts Lemma 4. Thus d is odd. Let 3 divide d. Then $a_i = 1$ or 2. This is not possible since there are at least two odd terms. Thus $d \equiv \pm 1 \pmod 6$. We assume that $d \equiv -1 \pmod 6$ and we show that (11) holds. Since (12) is the mirror image of (11), it can be shown similarly that $d \equiv 1 \pmod 6$ implies (12). Thus we restrict ourselves to the case $d \equiv -1 \pmod 6$.

Now we observe that none of the $n + id$ with $0 \leq i \leq 4$ is congruent to 5 (mod 6). Therefore $n \equiv 4 \pmod 6$ since $d \equiv -1 \pmod 6$. We exclude all the possibilities other than (11) and

$$a_0 = 1, \quad a_1 = 3, \quad a_2 = 2, \quad a_3 = 1, \quad a_4 = 1, \tag{13}$$

$$a_0 = 1, \quad a_1 = 3, \quad a_2 = 2, \quad a_3 = 1, \quad a_4 = 3, \tag{14}$$

$$a_0 = 1, \quad a_1 = 3, \quad a_2 = 2, \quad a_3 = 1, \quad a_4 = 6.$$

The last possibility is excluded by Lemma 4. Next we consider (13). We observe that x_0, x_4 are even, x_2 is odd and

$$x_2^2 = \left(\frac{x_0}{2}\right)^2 + \left(\frac{x_4}{2}\right)^2.$$

Let $4 \mid x_0$. Then $n + 4d \equiv 4 \pmod 8$ and $n + d \equiv 3 \pmod 8$, implying that $d \equiv 3 \pmod 8$. Then $2x_2^2 = n + 2d \equiv 6 \pmod 8$, which is not possible. Thus $x_0/2$ is odd and $x_4/2$ is even. Then

$$\frac{x_0}{2} = r^2 - s^2, \quad \frac{x_4}{2} = 2rs, \quad x_2 = r^2 + s^2$$

where $r > s$ are positive integers such that $\gcd(r, s) = 1$ and $r \not\equiv s \pmod 2$. Now we use the relation $2x_3^2 = 2x_2^2 + x_4^2$ to conclude that $r^4 + s^4 + 10r^2s^2 = x_3^2$, which is not possible by Lemma 7. Finally, assume (14). Then $d = x_4^2 - x_1^2 = 3x_1^2 - x_0^2$, implying that $4x_1^2 = x_0^2 + x_4^2$. Also $4x_2^2 = x_0^2 + 3x_4^2$. This implies (10) again as above, which is not possible by Lemma 7. ∎

The possibilities (11) and (12) are ruled out by using the following result.

LEMMA 9. *If x and y are rational numbers satisfying*

$$y^2 = x^3 - 3504x - 76160, \tag{15}$$

then

$$(x, y) \in \{(-40, 0), (-28, 0), (68, 0)\}. \tag{16}$$

Proof. Using SIMATH, we find that the rank of Mordell group of the elliptic curve (15) is 0 and the torsion points are given by (16). ∎

For the next result we introduce the following polynomials:

$$f_1(X) = X^6 + 20X^5 + 158X^4 + 684X^3 + 1755X^2 + 2700X + 2250,$$
$$f_2(X) = X^6 + 10X^5 + 33X^4 - 24X^3 - 430X^2 - 1200X - 1000,$$
$$f_3(X) = f_1(5X) \quad \text{and} \quad f_4(X) = f_2(5X).$$

We apply the method of Runge to obtain the following result:

LEMMA 10. *Let $1 \le i \le 4$ and X be a positive integer. If $f_i(X)$ is a square of a positive integer, then $X \le 85$.*

Proof. We give a proof for $i = 1$. The proofs for the other cases are similar. First we consider $f_1(X) = Y_1^2$ where Y_1 is a positive integer. We observe that

$$(X^3 + 10X^2 + 29X + 52)^2 > Y_1^2.$$

Further

$$Y_1^2 - (X^3 + 10X^2 + 29X + 51)^2 = 2X^3 - 106X^2 - 258X - 351 > 0$$

for $X > 55$. Thus

$$X^3 + 10X^2 + 29X + 51 < Y_1 < X^3 + 10X^2 + 29X + 52$$

for $X > 55$. This is not possible since Y_1 is an integer. Hence $X \le 55$. ∎

3. Proof of Theorem 4. Assume (1) with $\gcd(n, d) = 1$, $k = 5$ and $P(b) < k$. Then either (11) or (12) holds by Lemma 8. Assume (11). Then $x_4^2 + x_2^2 = x_3^2$ where x_2, x_3 are odd and x_4 is even. Then $x_4 = 2rs$, $x_2 = r^2 - s^2$ and $x_3 = r^2 + s^2$ where $r > s$ are positive integers such that $\gcd(r, s) = 1$ and $r \not\equiv s \pmod 2$. Now $d = x_4^2 - x_2^2$ gives $d = 6r^2s^2 - r^4 - s^4$ and $3d = x_3^2 - x_0^2$ gives $n = x_0^2 = 4(r^4 + s^4 - 4r^2s^2)$. Using $n + d = 3x_1^2$ we get $3r^4 + 3s^4 - 10r^2s^2 = 3x_1^2$. Now we obtain an elliptic equation from this relation. Putting $X_1 = r/s$, $Z_1 = x_1/s^2$ we get

$$Z_1^2 = X_1^4 - \frac{10}{3} X_1^2 + 1. \tag{17}$$

We derive (17) with $Z_1 = x_3/s^2$ from (12) in a similar way. Thus (17) is always valid. Now we multiply both sides of (17) by $4X_1^2$ to get

$$v^2 = 4u^3 - \frac{40}{3} u^2 + 4u$$

where $u = X_1^2$, $v = 2Z_1X_1$. By putting $u = (x + 40)/36$ and $v = y/108$ we get

$$y^2 = x^3 - 3504x - 76160.$$

By Lemma 9 we get $x = -40, -28, 68$, which gives $u = 0, 1/3, 3$. Hence $X_1^2 = 0, 1/3, 3$, a contradiction as $X_1 > 0$ is rational. ∎

4. Proofs of Theorems 1 and 2. Let d be a power of 2. We note that p always denotes an odd prime in [7] and in particular in [7, Theorems 2, 3]. By [7, Theorem 2], we may assume that $P(b) = k$ and then the assertion of the theorems follows from [7, Theorem 3]. Thus we may suppose that $d = p^\alpha$ where $\alpha > 0$ is an integer and $p > 2$ is a prime. Then $\gcd(n, d) = p^\beta$ with $0 \le \beta < \alpha$ since $d \nmid n$. By dividing both the sides of (1) by $p^{\beta k}$, we may assume that $\gcd(n, d) = 1$. This is clear if βk is even. If βk is odd, then we see that p divides b and the assumption $\gcd(n, d) = 1$ is again clear. By Lemma 5 and Theorem 4, we may also suppose that $k \ge 6$. Further we derive from [7, Corollary 1] that $d > 104$. Thus $d \ge k - 1$ since $k \le 29$. Let $|R| \le k - 2$. Suppose that there exist $\mu_0 > \mu_1 > \mu_2$ such that $a_{\mu_0} = a_{\mu_1} = a_{\mu_2}$. Then

$$(\mu - \nu)d = a_\nu(x_\mu - x_\nu)(x_\mu + x_\nu)$$

whenever

$$(\mu, \nu) \in \{(\mu_0, \mu_1), (\mu_0, \mu_2), (\mu_1, \mu_2)\}. \tag{18}$$

In fact the above relation is valid with some (μ, ν) satisfying (18) such that $d \mid (x_\mu - x_\nu)$. Therefore $k - 1 \ge \mu - \nu \ge x_\mu + x_\nu > d$, which is not possible. Now the assumption (7.5) of [7, Lemma 10] is satisfied since $|R| \le k - 2$ and we

apply [7, Lemma 10] with $h_1 = 1$, $h_2 = p^\alpha$, $c = \varepsilon_1 = \varepsilon_2 = \chi_1 = 1$. Therefore $d < 4(k-1)$. Consequently, $k = 29$ and $d = 107, 109$. Then $n < 28(k-1)^2$ by (7.8) of [7, Lemma 10]. Now we apply the algorithm of [7, Section 9] to show that (1) does not hold. The details of the application of this algorithm in some particular cases are explained in [7, Lemma 15]. Finally we remark that the arguments from [7] applied above are valid under the assumption $P(b) \le k$ in place of $P(b) < k$. Hence $|R| \ge k-1$.

4.1. *Proof of Theorem 1.* Assume that $P(b) < k$. As mentioned above, we may suppose that $k \ge 6$. Let $|R| = k$. Consider $k = 6$. Then 5 divides a_0, a_5 and a_1, a_2, a_3, a_4 is a permutation of $1, 2, 3, 6$. Now the assertion follows from Lemma 4. The case $k = 8$ is excluded similarly. Further $k \ne 7, 9$, otherwise there are at least five distinct a_i's composed only of 2 and 3. Thus we may assume that $|R| = k-1$. The case $k = 9$ is excluded as in [7, Lemma 7, $k = 9$].

Let $k = 8$. The cases of 7 dividing a_0, a_7 and 5 dividing a_0, a_5 or a_1, a_6 or a_2, a_7 are excluded as in [7, Lemma 7, $k = 8$]. Thus it remains to consider the following cases.

(a) 7 divides only one a_i and 5 divides two distinct a_i's not divisible by 7.

(b) 7 divides a_0, a_7 and 5 divides only one a_i other than a_0, a_7.

(a) Let 5 divide a_0, a_5. Suppose $7 \mid a_6$. Then a_1, a_2, a_3, a_4 are composed of 2 and 3. This is not possible by Lemma 5 with n replaced by $n+d$. Thus $7 \nmid a_6$. Similarly $7 \nmid a_7$. Let 7 divide a_1. Then $a_2, a_3, a_4, a_6, a_7 \in \{1, 2, 3, 6\}$. Now $\left(\frac{a_2}{7}\right) = \left(\frac{a_3}{7}\right) = \left(\frac{d}{7}\right)$, $\left(\frac{a_4}{7}\right) = \left(\frac{a_6}{7}\right) = \left(\frac{a_7}{7}\right) = -\left(\frac{d}{7}\right)$. So either $a_2, a_3 \in \{3, 6\}$ or $a_4, a_6, a_7 \in \{3, 6\}$. This is not possible. Let 7 divide a_2. Then $a_1, a_3, a_4, a_6, a_7 \in \{1, 2, 3, 6\}$. Using Legendre symbols modulo 7 we observe that $a_1, a_7 \in \{3, 6\}$ and $a_3, a_4, a_6 \in \{1, 2\}$. Further we see that $\left(\frac{a_1}{5}\right) = \left(\frac{a_4}{5}\right) = \left(\frac{a_6}{5}\right) = \left(\frac{d}{5}\right)$, $\left(\frac{a_3}{5}\right) = \left(\frac{a_7}{5}\right) = -\left(\frac{d}{5}\right)$. Therefore $a_1, a_4, a_6 \in \{1, 6\}, a_3, a_7 \in \{2, 3\}$ or $a_1, a_4, a_6 \in \{2, 3\}, a_3, a_7 \in \{1, 6\}$. Thus we conclude $a_1 = 6$, $a_3 = 2$, $a_4 = 1$, $a_6 = 1$, $a_7 = 3$ or $a_1 = 3$, $a_3 = 1$, $a_4 = 2$, $a_6 = 2$, $a_7 = 6$. Since d is odd, we observe that the relations $a_4 = a_6 = 1$ and $a_6 = 2$, $a_7 = 6$ do not hold. Therefore both the possibilities are ruled out. We exclude similarly by using Lemma 5 and congruences as above the cases when 5 divides a_0, a_5 and 7 divides a_4; 5 divides a_1, a_6; 5 divides a_2, a_7 and 7 divides $a_0 a_1 a_3 a_5 a_6$. It remains to consider only the cases where 5 divides a_0, a_5 and 7 divides a_3; 5 divides a_2, a_7 and 7 divides a_4. Let 5 divide a_0, a_5 and 7 divide a_3. Then we derive as above that either $a_1 = 1, a_2 = 2, a_4 = 6, a_6 = 1, a_7 = 3$ or $a_1 = 2, a_2 = 1, a_4 = 3, a_6 = 2, a_7 = 6$. The latter possibility is excluded since $a_1 = a_6 = 2$ is not possible by d odd. The former one gives $x_6^2 - x_1^2 = 5d$ by (2). Thus

$$d = 2x_1 + 5 \quad \text{or} \quad d = \frac{2x_1 + 1}{5}.$$

Also

$$(n+2d)(n+4d)(n+7d) = (6x_2x_4x_7)^2 =: Y_1^2,$$

hence we get the following two equations:

$$x_1^6 + 20x_1^5 + 158x_1^4 + 684x_1^3 + 1755x_1^2 + 2700x_1 + 2250 = Y_1^2,$$
$$x_1^6 + 4x_1^5 + \frac{158}{25}\,x_1^4 + \frac{684}{125}\,x_1^3 + \frac{351}{125}\,x_1^2 + \frac{108}{125}\,x_1 + \frac{18}{125} = Y_1^2.$$

The left hand side of the first one is $f_1(x_1)$ of Lemma 10, and that of the second one becomes $f_1(5x_1)$ on multiplication by 125^2. Thus in both the cases Lemma 10 implies $x_1 \le 85$. Now we observe that $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{n}{p}\right) = 1$ since $a_5 = 5$, $a_3 = 7$. Therefore $p \ge 311$, implying $x_1 \ge 150$, a contradiction. The case of 5 dividing a_2, a_7 and $7 \mid a_4$ is ruled out similarly using Lemma 10 with $i = 2$. We shall apply Lemma 10 again in the proof of Theorem 2. It is remarkable that 1 is the repeated term among a_i's in all these instances and this is crucial for applying Lemma 10.

(b) By looking modulo 7, we find that either $5 \mid a_2$ or $5 \mid a_5$. These possibilities are excluded by applying Lemma 5 to products $(n+3d)(n+4d) \times (n+5d)(n+6d)$ and $(n+d)(n+2d)(n+3d)(n+4d)$, respectively.

Let $k = 7$. Then $|R| = 6$ and 5 divides two distinct a_i's. Thus 5 divides a_0, a_5 or a_1, a_6. These cases are excluded by Lemma 5.

Let $k = 6$. Then $|R| = 5$. The possibility of 5 dividing a_0, a_5 is excluded by Lemma 5. Thus 5 divides exactly one a_i. Now we may assume that 5 divides a_2 or a_3 by Lemma 5. Let $5 \mid a_2$. By using Legendre symbols modulo 5, we observe that either $a_0, a_4, a_5 \in \{1, 6\}$, $a_1, a_3 \in \{2, 3\}$ or $a_0, a_4, a_5 \in \{2, 3\}$, $a_1, a_3 \in \{1, 6\}$. Assume the first possibility. Then $a_5 = 6$, implying neither a_1 nor a_3 is equal to 3. This is not possible. Similarly we see from the second possibility that $a_1 = a_3 = 1$, contradicting $|R| = 5$. The case of 5 dividing a_3 is excluded similarly. ∎

4.2. *Proof of Theorem 2.* Assume that $P(b) = k$. By Lemma 6, it remains to consider only the case $k = 7$. Then $|R| \ge 6$. We observe that at least one a_i is divisible by 5. We divide the proof into the following two parts:

(a) 5 divides exactly two elements.

(b) 5 divides only one element.

(a) Let 5 divide a_0, a_5. Then we derive from Lemma 5 that 7 does not divide a_0, a_5, a_6. By applying Legendre symbols modulo 7 and 5 as in the proof of the case $k = 8$, $5 \mid a_0, a_5$, $7 \mid a_2$ of Theorem 1, the possibilities of 7 dividing a_1, a_2, a_4 are excluded and 7 dividing a_3 gives

$$a_1 = a_6 = 1, \quad a_2 = 2, \quad a_4 = 6. \tag{19}$$

Further we conclude as above that $5 \nmid a_1a_6$ unless 7 divides a_3 and

$$a_0 = a_5 = 1, \quad a_2 = 6, \quad a_4 = 2. \tag{20}$$

(b) We observe that $|R| = 6$ such that 7 and 5 do not divide the same a_i. Let 7 divide a_0. Then we derive from Lemma 5 that 5 cannot divide a_1, a_2, a_5, a_6. The remaining cases $5 \mid a_3$ and $5 \mid a_4$ are excluded by considering Legendre symbols modulo 7 and 5. Thus 7 does not divide a_0. Let 7 divide a_1. By considering Legendre symbols modulo 7 and 5 we get

$$a_0 = 2, \quad a_2 = 6, \quad a_4 = 1, \quad a_5 = 3, \quad a_6 = 2.$$

By (2), we have

$$n(n+2d)(n+4d)(n+6d) = 6(2x_0x_2x_4x_6)^2.$$

We observe that n and x_4 are even. We divide both sides by 2^4 to obtain

$$\frac{n}{2}\left(\frac{n}{2}+d\right)\left(\frac{n}{2}+2d\right)\left(\frac{n}{2}+3d\right) = 6\left(x_0x_2\,\frac{x_4}{2}\,x_6\right)^2$$

and $\gcd(n/2, d) = 1$. By Lemma 5 we get $n/2 = 75$ and $d = 23$, implying $x_0^2 = 75$, which is not possible. Similarly we show that none of the other a_i is divisible by 7 unless

$$a_0 = a_5 = 1, \quad a_1 = 2, \quad a_3 = 6, \quad a_6 = 3 \tag{21}$$

in the case $7 \mid a_2$, $5 \mid a_4$ and

$$a_0 = 3, \quad a_1 = a_6 = 1, \quad a_3 = 6, \quad a_5 = 2 \tag{22}$$

in the case $7 \mid a_4$, $5 \mid a_2$. Further we observe that $a_2 = 7$, $a_4 = 5$ and $a_2 = 5$, $a_4 = 7$ in (21) and (22), respectively.

It remains to show that the relations (19)–(22) are not valid. First we consider (19). From (2) we get

$$n + d = x_1^2, \quad n + 2d = 2x_2^2, \quad n + 4d = 6x_4^2, \quad n + 6d = x_6^2.$$

So $5d = x_6^2 - x_1^2$, implying either $x_6 - x_1 = 1$, $x_6 + x_1 = 5d$ or $x_6 - x_1 = 5$, $x_6 + x_1 = d$. In the first case $5d = 2x_1 + 1$, which gives the following equations:

$$X^2 + 4 = 2Y^2, \quad (X+2)^2 + 6 = 6Z^2$$

with $X = 5x_1 + 1$, $Y = 5x_2$ and $Z = 5x_4$. In the latter case $d = 2x_1 + 5$ and we get the same pair of Pell's equations with $X = x_1 + 1$, $Y = x_2$ and $Z = x_4$. This is not possible by Lemma 3. The case (20) is excluded similarly again by Lemma 3. Next, we consider (21). By (2), we have

$$n = x_0^2, \quad n + d = 2x_1^2, \quad n + 2d = 7x_2^2, \quad n + 3d = 6x_3^2,$$
$$n + 4d = 5x_4^2, \quad n + 5d = x_5^2, \quad n + 6d = 3x_6^2,$$

which implies that

$$\left(\frac{n}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = 1, \tag{23}$$

where $d = p^\alpha$ with positive integer α. Further either $5d = 2x_0 + 1$ or $d = 2x_0 + 5$. We also observe that

$$(n+d)(n+3d)(n+6d) = (6x_1x_3x_6)^2.$$

Putting the expressions for n and d in terms of x_0, we get

$$f_1(X) = Y^2 \quad \text{with} \quad X = x_0,\ Y = 6x_1x_3x_6 \tag{24}$$

if $d = 2x_0 + 5$, or

$$f_1(X) = Y^2 \quad \text{with} \quad X = 5x_0,\ Y = 750x_1x_3x_6 \tag{25}$$

if $5d = 2x_0 + 1$. We observe that (22) is the mirror image of (21), and therefore, it implies similarly

$$f_2(X) = Y^2 \quad \text{with} \quad X = x_1,\ Y = 6x_0x_3x_5 \tag{26}$$

and

$$f_2(X) = Y^2 \quad \text{with} \quad X = 5x_1,\ Y = 750x_0x_3x_5. \tag{27}$$

We recall that (24) and (25), together with (23), are excluded by Lemma 10 with $i = 1$ in the proof of the case (a) of $k = 8$ in Theorem 1. Further (26) and (27) are excluded similarly by applying Lemma 10 with $i = 2$. ∎

References

[1] A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford Ser. (2) 20 (1969), 129–137.

[2] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. 442 (1993), 19–62.

[3] L. E. Dickson, *History of the Theory of Numbers*, *Vol. II*, Chelsea, 1952.

[4] L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.

[5] R. Obláth, *Über das Produkt fünf aufeinander folgender zahlen in einer arithmetischen Reihe*, Publ. Math. Debrecen 1 (1950), 222–226.

[6] H. C. Pocklington, *Some Diophantine impossibilities*, Proc. Cambridge Philos. Soc. 17 (1912), 108–121.

[7] N. Saradha and T. N. Shorey, *Almost squares in arithmetic progression*, Compositio Math., to appear.

[8] T. N. Shorey, *Exponential diophantine equations involving products of consecutive integers and related equations*, in: Number Theory, R. P. Bambah, V. C. Dumir and R. J. Hans-Gill (eds.), Hindustan Book Agency, 1999, 463–495.

[9] —, *Powers in arithmetic progression,* in: A Panorama in Number Theory or The View from Baker's Garden, G. Wüstholz (ed.), Cambridge Univ. Press, 2002, 325–336.

[10] T. N. Shorey and R. Tijdeman, *Perfect powers in products of terms in an arithmetical progression*, Compositio Math. 75 (1990), 307–344.

[11] R. Tijdeman, *Diophantine equations and diophantine approximations*, in: Number Theory and Applications (Banff, AB, 1988), R. A. Mollin (ed.), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. 265, Kluwer, 1989, 215–243.

Harish-Chandra Research Institute
Allahabad 211019, India
E-mail: anirban@mri.ernet.in

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai 400005, India
E-mail: shorey@math.tifr.res.in

Received on 27.11.2001
and in revised form on 5.3.2003 (4159)