数理解析研究所講究録 1274 巻 2002 年 202-214

Powers in arithmetic progressions (II)

T.N. Shorey

0. Introduction

We refer to survey papers Shorey (1999, 2002) for an account of the topics under discussion. This article may be considered as a continuation of section 2 of Shorey (2002). An exhaustive list of references is enclosed at the end. A paper which is not yet published is referred as (2003). I shall restrict only to squares in arithmetic progressions in my talk. I shall divide this talk in two sections. The first section is on consecutive integers. Observe that consecutive integers are arithmetic progressions with common difference one. I shall consider arithmetic progressions with common difference greater than one in section 2. First, we introduce some notation. For an integer $\nu > 1$, we denote by $P(\nu)$ and $\omega(\nu)$ the greatest prime factor and the number of distinct prime divisors of ν, respectively. Further we put $P(1) = 1$ and $\omega(1) = 0$. Let $d \geq 1, n \geq 1$ and $k \geq 3$ be integers such that gcd $(n, d) = 1$. We write

$$\triangle(n, k, d) = n(n + d) \cdots (n + (k - 1)d)$$

and

$$\triangle(n, k) = \triangle(n, k, 1).$$

1. Consecutive integers

An old result of Sylvester (1892) states

Theorem 1. *We have*

$$P(\triangle(n,k)) > k \text{ for } n > k.$$

Thus a product of k consecutive positive integers each greater than k is divisible by a prime exceeding k. The assumption $n > k$ in Theorem 1 is necessary since

$$P(\triangle(1,k)) = P(1 \times 2 \cdots \times k) \leq k.$$

Erdös (1934) gave another proof of Theorem 1. The proof admits the following refinement due to Saradha and Shorey (2003a).

Theorem 2. *Let $n > k \geq 3$. Then the inequality*

$$\omega(\triangle(n,k)) \geq \pi(k) + [\frac{1}{3}\pi(k)] + 2$$

holds unless

$n \in \{4,6,7,8,16\}$ *if* $k = 3$; $n \in \{6\}$ *if* $k = 4$;
$n \in \{6,7,8,9,12,14,15,16,23,24\}$ *if* $k = 5$;
$n \in \{7,8,15\}$ *if* $k = 6$;
$n \in \{8,9,10,12,14,15,24\}$ *if* $k = 7$;
$n \in \{9,14\}$ *if* $k = 8$.

According to Theorem 2, $\triangle(n,k)$ is divisible by at least $[\frac{1}{3}\pi(k)]+2$ distinct primes exceeding k. We record the following consequence of Theorem 2.

Corollary 1. *Let $n > k \geq 3$. Then*

$$\omega(\triangle(n,k)) \geq \pi(k) + 2$$

$$n \in \{4,6,7,8,16\} \text{ if } k=3;\ n \in \{6\} \text{ if } k=4; n \in \{6,8\} \text{ if } k=5.$$

The next result gives more information on the assertion of Theorem 1.

Theorem 3. *Let* $(n,k) \neq (48,3)$. *There exists a prime* $p > k$ *such that*

$$\text{ord}_p(\triangle(n,k)) \not\equiv 0 \pmod 2$$

whenever

$$P(\triangle(n,k)) > k. \tag{1}$$

Theorem 3 with (1) replaced by $n > k^2$ implies Theorem 3. For showing this, we may suppose that there exists a prime $q > k$ such that $q^2 \mid \triangle(n,k)$ otherwise the assertion follows. Since $q > k$, there is unique i with $0 \leq i < k$ such that $q \mid (n+i)$. Therefore $q^2 \mid (n+i)$. Thus

$$n+k-1 \geq n+i \geq q^2 \geq (k+1)^2$$

which implies that $n > k^2$. The assumption $(n,k) \neq (48,3)$ is necessary. For this, we observe that

$$48 = 3.2^4, 49 = 7^2, 50 = 2.5^2.$$

Thus, in this example, there is no prime > 3 dividing $\triangle(n,k)$ to an odd power. Theorem 3 with $p \geq k$ was proved by Erdös and Selfridge (1975) developing on the method of Erdös (1939) and Rigge (1939). The conclusion $p \geq k$ was replaced by $p > k$ by Saradha (1997).

Theorem 3 has been sharpened by Saradha and Shorey (2003a) as follows:

Theorem 4. *Let $k \geq 4$ and $n > k^2$. Assume that*

$$(n, k) \notin \{(24, 4), (47, 4), (48, 4)\}.$$

Then there exist distinct primes $p_1 > k$ and $p_2 > k$ such that

$$\mathrm{ord}_{p_i}(\triangle(n, k)) \not\equiv 0 \pmod 2 \text{ for } i = 1, 2.$$

We consider Theorem 4 with $k = 3$. We have

$$\triangle(p-1, 3) = (p-1)p(p+1) = p(p^2-1) = 2py^2$$

if

$$p^2 - 1 = 2y^2 \tag{2}$$

and the assertion of Theorem 4 is not valid. We do not know whether (2) has finitely or infinitely many solutions in p and y. Thus the case $k = 3$ of Theorem 4 remains open.

Let g be the number of i with $0 \leq i \leq k-1$ such that $n+i$ is divisible by a prime exceeding k to odd power. Thus $\triangle(n, k)$ is divisible by at least g distinct primes greater than k to odd powers. The next sharpening of Theorem 4 has been obtained by Mukhopadhyay and Shorey (2003b) by induction on g.

Theorem 5. *Let $k \geq 10$ and $n > k^2$. Then*

$$g \geq 8$$

unless

$k = 10$:

$n = 103 - 105, 112, 116 - 126, 135, 138 - 144, 159 - 162, 166 - 168, 187 - 189,$

$191, 192, 216, 234 - 245, 247 - 250, 280, 285 - 288, 315, 334 - 336, 354 - 360,$
$375, 441, 477 - 484, 498 - 500, 503, 504, 667 - 672, 717 - 722, 726,$
$836-841, 959, 960, 1080, 1343-1344, 1436-1440, 1443-1444, 1673-1681, 2016,$
$2019 - 2023, 2518 - 2520, 2879 - 2883, 3355 - 3360, 4796 - 4800, 5034 - 5041,$
$6718 - 6724, 10077 - 10080, 13447 - 13448, 15116 - 15123, 6375621;$

$k = 11$:

$n = 122 - 126, 140, 144, 158 - 162, 165 - 168, 188 - 192, 215, 216,$
$235 - 243, 287, 288, 375, 440, 480, 719, 720, 837 - 840, 1680, 2880, 5036 - 5040,$
$6718 - 6720, 15119, 15120;$

$k = 12$:

$n = 158 - 160, 165, 189, 239 - 242;$

$k = 13$:

$n = 188, 189, 240.$

Since $x^2 - 2y^2 = -1$ has infinitely many solutions in integers x and y, we observe that the assumption $k \geq 10$ in Theorem 5 is necessary. Now we state an immediate consequence of Theorem 5.

Corollary 2. *Let $k \geq 10$ and $n > k^2$. There are at least 8 distinct primes exceeding k each dividing $\triangle(n, k)$ to odd power unless*

$n \in \{103 - 105, 112, 116 - 126, 144, 159 - 162, 166 - 168, 188, 189, 191, 192,$
$234 - 243, 287, 288, 354 - 360, 482, 483, 672, 717 - 721, 837 - 841, 1444, 5039\}$
if $k = 10$;
$n \in \{122 - 126, 140, 144, 158 - 162, 165 - 168, 188 - 192, 235, 236, 240, 242,$
$287, 288, 719, 720, 837 - 840, 1680\}$ if $k = 11$;
$n \in \{158 - 160, 165, 189\}$ if $k = 12$;
$n \in \{188, 189, 240\}$ if $k = 13$.

Hence we have

Corollary 3. *Let $k \geq 10$ if $n > 5039$ and $k \geq 14$ otherwise. Assume that $n > k^2$. Then $\Delta(n,k)$ is divisible by at least 8 distinct primes greater than k to odd powers.*

Sharper lower bounds for g have been obtained whenever k is sufficiently large. Erdös (1955) observed that his proof for a product of two or more consecutive positive integers is never a square yields

$$g \geq C_1 \frac{k}{\log k}$$

where $C_1 > 0$ is an effectively computable absolute constant. Further Shorey (1987) improved the above inequality to

$$g \geq C_2 \frac{k \log\log k}{\log k} \tag{3}$$

where $C_2 > 0$ is an effectively computable absolute constant. The constant C_2 turns out to be small and therefore (3) is of interest only if k is large. Apart from the elementary arguments of Erdös and Rigge, the improvement (3) depends on a theorem of Baker (1969) that a hyper-elliptic equation, under necessary assumptions, has only finitely many solutions and an explicit bound for the magnitude of the solutions can be given. This is the first time that result proved by Transcendence methods has been applied in the topic under consideration in this section. As an immediate consequence of the theorem of Baker (1969) stated above, we have

$$g \geq k - 2$$

whenever $n \geq n_0(k)$ and $n_0(k)$ is sufficiently large.

The proof of Theorem 5 is elementary and combinatorial. The elliptic equations

$$X(X+p)(X+q) = by^2 \quad \text{with } 1 \leq p < q \leq 12, P(b) \leq 7$$

are solved by using SIMATH in the proof of Theorem 5. We remark that this package depends on the theory of elliptic logarithms as developed by Noriko Hirata - Kohno and Sinnou David. SIMATH has been applied for the first time in a similar context by Filakovszky and Hajdu (2001).

2. Arithmetic progressions with common difference greater than one

We consider arithmetic progressions with common difference $d > 1$. Tijdeman and Shorey (1990), improving on the results of Sylvester (1892) and Langevin (1976), showed that

$$P(\triangle(n,k,d)) > k \text{ if } (n,k,d) \neq (2,3,7).$$

We compare this inequality with the one given in Theorem 1 and we see that the situation between consecutive integers and arithmetic progressions with common difference greater than one is quite different. Let b be a positive integer such that $P(b) < k$ and $d > 1$. We consider the equation

(4) $\triangle(n,k,d) = by^2$ in integers $n > 0, y > 0, k \geq 3$ with gcd $(n,d) = 1$.

We begin with a conjecture on (4) due to Erdös.

Conjecture 1. *Equation* (4) *implies that* k *is bounded by an absolute constant.*

A stronger conjecture states

Conjecture 1'. *Equation* (4) *implies that* $k = 4$.

On the other hand, it is known that (4) with $k = 4$ has infinitely r solutions in n, d and y, see Tijdeman (1988). Shorey and Tijdeman (1 proved that (4) implies that k is bounded by an effectively computable n ber depending only on $\omega(d)$. Thus conjcture 1 is confirmed whenever $\omega($ bounded.

Next we consider (4) with $\omega(d) = 1$. Let $k = 3$ and $b = 1$. We have

I		II
$n = y_0^2$		$n = 2y_0^2$
$n + d = y_1^2$	or	$n + d = y_1^2$
$n + 2d = y_2^2$		$n + 2d = 2y_2^2$

First we exclude the possibility I. Let d be odd. We have

$$d = y_1^2 - y_0^2 = (y_1 - y_0)(y_1 + y_0).$$

Thus

$$y_1 - y_0 = 1$$

implying that

$$d = 2y_0 + 1.$$

Similarly

$$d = 2y_1 + 1.$$

Thus $y_0 = y_1$ which is a contradiction. If $d = 2^\alpha$, we observe as above

$$y_0 = 2^{\alpha-2} - 1, y_1 = 2^{\alpha-2} + 1, y_2 = 2^{\alpha-2} + 3$$

contradicting I. Next we consider II. Then d is odd. We have

$$2d = 2(y_2^2 - y_0^2)$$

$$d = y_2^2 - y_0^2$$

implying that

$$y_2 - y_0 = 1, d = 2y_0 + 1.$$

Thus

$$2y_0^2 + 2y_0 + 1 = y_1^2$$

i.e.

$$4y_0^2 + 4y_0 + 2 = 2y_1^2$$

i.e.

$$(2y_0 + 1)^2 + 1 = 2y_1^2$$

i.e.

$$d^2 - 2y_1^2 = -1.$$

We do not know whether the above equation has finitely or infinitely many solutions in d and y_1 with d prime. Thus the case $k = 3$ of (4) is open.

For $k \geq 4$, we have

Theorem 6. *Equation* (4) *with* $\omega(d) = 1$ *and* $k \geq 4$ *does not hold unless* $n = 75, d = 23, k = 4$.

Theorem 6 with $k > 9$ was proved by Saradha and Shorey (2003b) and with $4 \leq k \leq 9$ by Mukhopadhyay and Shorey (2003a). The assumption gcd $(n, d) = 1$ has been relaxed to $d \nmid n$ which is necessary. Furthermore, the assumption $d \nmid n$ is not required if $b = 1$. We have

Theorem 7. *A product of four or more terms in arithmetic progression with common difference a prime power is not a square.*

Theorem 7 was proved by Saradha and Shorey (2003b). We give a proof of Theorem 7 when $d \mid n$. Let $d = p^\alpha$. We have

$$n(n + d) \cdots (n + (k - 1)d) = y^2.$$

$$p^{\alpha k} n'(n'+1)\cdots(n'+k-1) = y^2$$

where

$$n' = n/d.$$

As already stated a product of two or more consecutive positive integers is never a square. Therefore k and αk are odd. Then

$$n'(n'+1)\cdots(n'+k-1) = py_1^2 \tag{5}$$

where $y_1 > 0$ is an integer. Let $n' > k$. By Corollary 1, the left hand side of (5) is divisible by at least two distinct primes $> k$ unless $(n', k) = (6, 5), (8, 5)$. Further we observe that (5) is not satisfied whenever $(n', k) = (6, 5), (8, 5)$. Therefore $n' > k^2$ by (5). Now we apply Theorem 4 to conclude that the left hand side of (5) is divisible by at least two distinct primes with odd powers. This is not possible. Let $n' \leq k$. We check that (5) does not hold when $n' + k \leq 12$. Thus we assume that $n' + k > 12$. Then

$$n' \leq \frac{n'+k}{2} \leq n' + k - 1$$

and there are at least 2 distinct primes between $\frac{n'+k}{2}$ and $n' + k - 1$ dividing the left hand side of (5) to the first power. This is again not possible.

Let

$$\mathcal{D} = \{\chi p^\alpha \mid 1 < \chi \leq 12, \chi \neq 11, \ \gcd(\chi, p) = 1\}$$

where $p \geq 2$ prime. Let $k \geq 4$ if $d = 7p^\alpha$. The case $k = 3, d = 7p^\alpha$ is again an open problem as in the case $d = p^\alpha$. Saradha and Shorey (2003b) showed that (4) with $d \in \mathcal{D}$ does not hold unless $(n, k, d) = (1, 3, 24)$. Further we observe that if $d \neq p^\alpha, d \notin \mathcal{D}$, then $d \geq 105$. Thus (4) does not hold whenever $k \geq 4$ and $d \leq 104$ unless $(n, k, d) = (75, 4, 23)$. The assumption $k \geq 4$ can be relaxed to $k \geq 3$ in the preceding result if $(n, k, d) \neq (1, 3, 24)$. Hence (4) with $k \geq 3$ and $d \leq 104$ implies that $(n, k, d) = (1, 3, 24)$ or $(75, 4, 23)$. This

was already proved by Saradha (1998) for $d \leq 22$ and for $23 \leq d \leq 30$ by Filakovszky and Hajdu (2001).

REFERENCES

Baker, A. (1969), Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.* **65**, 439-444.

Erdös, P. (1934), A Theorem of Sylvester and Schur, *Jour. London Math. Soc.* **9**, 283-288.

Erdös, P. (1939), Note on the product of consecutive integers (I), *Jour. London Math. Soc.* **14**, 194-198.

Erdös, P. (1955), On the product consecutive integers III, *Indag. Math.* **17**, 85-90.

Erdös P. & J.L. Selfridge (1975), The product of consecutive integers is never a power, *Illinois Jour. Math.* **19**, 292-301.

Filakovszky, P. & L. Hajdu (2001), The resolution of the diophantine equation $x(x+d)\cdots(x+(k-1)d) = by^2$ for fixed d, *Acta Arith.* **98**, 151-154.

Langevin, M. (1977), Plus grand facteur premier d'entiers en progression arithmétique, *Sém Delange-Poitou*, **18** année, 1976/77, No.3, 6pp.

Mukhopadhyay, Anirban & T.N. Shorey (2003a), Almost squares in arithmetic progression (II), to appear

Mukhopadhyay, Anirban & T.N. Shorey (2003b), Almost squares and factorisations in consecutive integers (II), to appear.

Rigge, O. (1939), Über ein diophantisches Problem, in *9th Congress Math. Scand. Helsingfors,* 1938, Mercator, 155-160.

Saradha, N. (1997), On perfect powers in products with terms from arithmetic progressions, *Acta Arith.* **82**, 147-172.

Saradha, N. (1998), Squares in products with terms in an arithmetic progression, *Acta Arith.* **86**, 27-43.

Saradha, N. & T.N. Shorey (2003a), Almost squares and factorisations in consecutive integers,*Compositio Math.,* to appear.

Saradha, N. & T.N. Shorey (2003b), Almost squares in arithmetic progression,*Compositio Math.,* to appear

Shorey, T.N. (1987), Perfect powers in products of integers from a block of consecutive integers, *Acta Arith.* **49**, 71-79.

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

Shorey, T.N. (2002), Powers in arithmetic progression, A Panorama in Number Theory or The View from Baker's Garden, ed. by G. Wüstholz, *Cambridge University Press,* 325-336.

Shorey, T.N. & R. Tijdeman (1990a), On the greatest prime factor of an arithmetical progression. In *A Tribute to Paul Erdös,* A. Baker, B. Bolobás & A. Hajnal (eds.), Cambridge University Press, 385-389.

Shorey, T.N. & R. Tijdeman (1990b), Perfect powers in products of terms in an arithmetical progression, *Compositio Math.* **75**, 307-344.

Sylvester, J.J. (1892), On arithmetical series, *Messenger Math.* **21**, 1-19, 87-120.

Tijdeman, R. (1988). In Diophantine Equations and diophantine Approximations, Richard A. Mollin (ed.), Kluwer, 215-233.

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai 400 005, India
shorey@math.tifr.res.in