数理解析研究所講究録
第 708 巻 1989 年 51-62

On the product of the terms of a finite arithmetic progression

by

R. Tijdeman

(Leiden, The Netherlands)

Let a, d and k be positive integers, $k \geq 3$. We consider the arithmetic progression $a, a+d, a+2d, \ldots, a+(k-1)d$ and in particular the product $\Delta = a(a+d)\ldots(a+(k-1)d)$.

There are two circles of problems we shall consider:

I: What can be said about the greatest prime factor $P(\Delta)$ of Δ and the number of distinct prime divisors $\omega(\Delta)$ of Δ?

II: Can Δ be an (almost) perfect power? Can each of $a, a+d, \ldots, a+(k-1)d$ be an ℓ-th power for some $\ell \geq 2$?

This lexture reports on joint work with T.N. Shorey. It can be considered as an updating of my first lecture given in Banff in 1988, [20]. Almost all results have effective proofs, but for this aspect I refer to the original papers. I am grateful to Shorey for his remarks on an earlier draft of the present paper.

I. Without loss of generality we may assume $\gcd(a, d) = 1$. A first general result on

I was obtained by Sylvester [19] in 1892. He proved

(1) $$\text{if} \quad a \geq d + k \quad \text{then } P(\Delta) > k.$$

Suppose $d = 1$. Then we consider the product of a block of k integers. If $a \geq 1 + k$, then there is apparently at least one number in the block $a, a+1, \ldots, a+k-1$ which is not composed of primes $\leq k$. If $a = 1 + k$, this is Bertrand's Postulate. If $a < 1 + k$, the last term of the block is less than $2k$. Then the question becomes whether $k+1, \ldots, a+k-1$ contains a prime. This is the classical problem on gaps between consecutive primes. The theorem of Hoheisel, Ingham as improved by many others says that if $a > k^{23/42}$ and k is sufficiently large then there is a prime. (The exponent $23/42$ has been slightly improved, see [7]). Probably $a > (1+\epsilon)(\log k)^2$ for large k is sufficient according to a hypothesis of Cramér, but it will be extremely hard to prove this.

Suppose $d > 1$. Then (1) was slightly improved by Langevin in 1977 as follows.

(2) $$\text{If } a > k, \quad \text{then } P(\Delta) > k.$$

Shorey and I showed that in fact $2, 9, 16$ is the only exception:

Theorem 1. ([14]). *Let $d > 1, k > 2, \gcd(a, d) = 1, (a, d, k) \neq (2, 7, 3)$. Then $P(\Delta) > k$.*

The proof rests on a sharp upper bound for $\pi(x)$ due to Rosser and Schoenfeld and is further computational.

If a becomes large, then much better lower bounds are possible. Shorey and I improved upon some estimate of Langevin [5].

Theorem 2. ((a) and (c) in [15], (b) unpublished). *Let* $\chi = a + (k-1)d$, $\chi_0 = \max(\chi/k, 3)$,

$\epsilon > 0$.

(a) $$P(\Delta) >> k \log\log \chi_0 \qquad (\geq k \log\log d).$$

(b) $$\text{if } \chi > k(\log k)^{\epsilon} \text{ then } \quad P(\Delta) >>_{\epsilon} k \log\log a.$$

(c) $$\text{if } \chi > k^{1+\epsilon} \quad \text{then} \quad P(\Delta) >>_{\epsilon} k \log\log \chi.$$

The proof is based on Baker's method, in particular a result on the Thue equation by Győry [4]. Note that some conditions in (b) and (c) are necessary. In (b) we can take $a = [k/2], d = 1$ and it follows that $P(\Delta) \leq a + (k-1)d < 3k/2 = o(k \log\log a)$. In (c) we can take $a = 1, d = [(\log\log \chi)^{1/2}]$ and it follows that $P(\Delta) \leq a + (k-1)d < k(\log\log \chi)^{1/2} = o(k \log\log \chi)$.

Very recently we studied $\omega(\Delta)$. If $a = d = 1$, then $\omega(\Delta) = \omega(k!) = \pi(k)$. There are more examples with $\omega(\Delta) = \pi(k)$, for example $1, 625, 1249$, and $1, 3, 5, 7, 9$.

Theorem 3. [16]

$$\omega(\Delta) \geq \pi(k).$$

The proof is similar to that of Theorem 1. Here only limited improvement is possible if a becomes large. We cannot exclude that there are $k-1$ primes $p_1, \ldots, p_{k-1}$ in such a way that $1, p_1, \ldots, p_{k-1}$ are in arithmetic progression, so that we cannot prove anything better than $\omega(\Delta) \geq k-1$.

Theorem 4. (a) *For any positive integer $t > 1$ we have*

$$\text{if} \quad \chi \geq k^{\frac{k}{t-1}+1} \qquad \text{then} \quad \omega(\Delta) > k - t.$$

(b) *there are infinitely many instances with $\chi \geq k^{2.7}$ and $\omega(\Delta) < ck$ with $c < 1$.*

The proof of (a) is elementary. For (b) we use estimates for the Dickman function $\psi(x, y)$. If we take $t = .6k$ in (a), then we find that $\omega(\Delta) > .4k$ if $\chi \geq k^{2.7}$ and (b) shows that ck for some c with $0 < c < 1$ is the actual order of magnitude.

II. How many ℓth powers can be in arithmetic progression? If $\ell = 2$, then there are infinitely many triples of squares in arithmetic progression, but Fermat proved that there are no four squares in arithmetic progression. Dénes [1] proved in 1952 that there are no three ℓ–th powers in arithmetic progression for $3 \leq \ell \leq 30$ and for 60 other prime values of ℓ and he conjectured that this is true for all ℓ. He used Kummer theory and his method is not applicable for irregular primes. The celebrated result of Faltings [3] implies that for any $\ell \geq 5$ there are only finitely many triples of coprime ℓ–th powers in arithmetic progression, but his result does not provide any bound for k independent of ℓ. In the sequel we assume $\gcd(a, d) = 1, k \geq 3$ and $\ell \geq 2$. Let d_1 be the maximal divisor of d composed of prime factors $\equiv 1 \pmod{\ell}$.

Theorem 5. ((a), (c) and (d) from [12], (b) from [13]).

Suppose $a, a+d, \ldots, a+(k-1)d$ are all ℓ–th powers. Then

(a) *if d is odd, then $k = 3$,*

(b) $k < (1+\epsilon)2^{\omega(d_1)}$ *for* $k \geq k_0(\epsilon)$,

(c) $k << \omega(d) \log \omega(d)$,

(d) $k << \sqrt{\log d}$.

A much weaker condition is that not each of the numbers is an ℓ–th power, but that the product of the numbers is an ℓ–th power. If $d = 1$ we find that

$$a(a+1)(a+2)\ldots(a+k-1) = y^\ell \qquad (\ell > 1). \tag{3}$$

It was proved by Erdös and Selfridge [2] in 1975, 36 years after Erdös started this research, that (3) has no solution in positive integers $a, k > 2, y, \ \ell > 1$. Later Erdös conjectured that if

$$a(a+d)(a+2d)\ldots(a+(k-1)d) = y^\ell \tag{4}$$

then k is bounded by an absolute constant. Still later he conjectured $k \leq 3$. Some special cases are in the literature. Euler proved that the product of four numbers in arithmetic progression cannot be a square. Of course, this implies Fermat's result that there are no four squares in arithmetic progression. Obláth [8] proved the result for the product of five numbers in arithmetic progression. He [9] also proved that the product of three numbers in arithmetic progression cannot be a third, fourth of fifth power. Marszalek [6] was the first to deal with the general problem. He proved that k is bounded by a number depending only on d. He gave rather refined estimates, but a rough simplification of his result gives:

$$\begin{array}{rll} k \leq \exp(2d^{3/2}) & \text{if} & \ell = 2, \\ k \leq \exp(2d^{7/3}) & \text{if} & \ell = 3, \\ k \leq Cd^{5/2} & \text{if} & \ell = 4, \\ k \leq Cd & \text{if} & \ell \geq 5, \quad \text{where} \quad \mathrm{C} = 3 \cdot 10^4. \end{array}$$

Shorey [10] proved that k is bounded by a number depending on $P(d)$, the greatest prime factor of d, provided that $\ell > 2$. Shorey [10] further proved that $d_1 > 1$ if $m > k$ and k large.

Shorey and I have obtained many results on equation (4). Actually we proved these results under the following weaker assumption.

$$(5) \qquad \begin{cases} \text{Let } a, d, k, b, y, \ell \text{ be positive integers such that } \gcd(a, d) = 1, \\ \qquad k > 2, \ell > 1, P(b) \leq k, P(y) > k \quad \text{and} \\ \qquad a(a+d)\dots(a+(k-1)d) = by^\ell. \end{cases}$$

In the sequel we assume that (5) holds.

Theorem 6. $\log k << \dfrac{\log d_1}{\log\log d_1}$.

Proof. For $\ell \geq 7$, see [18]. For $\ell \leq 5$ see [17], formula (2.14).

Observe that this is a considerable improvement of Marszalek's result. We see that $k/d \to 0$ as $d \to \infty$ and even $\log k/\log d \to 0$ as $d \to \infty$.

Theorem 7. [17] $\quad k << d_1^{1/(\ell-2)}$.

This implies Shorey's estimate $d_1 > 1$ for $\ell > 2$ and k large.

Theorem 8. [17]

$$\frac{k}{\log k} << \ell^{\omega(d)} \qquad (\text{even} << \ell^{\omega(d_1)} \text{for } \ell \geq 7).$$

Thus k is bounded by a number depending only on ℓ and $\omega(d)$. Actually we tried to prove that k is bounded by a number depending only on $\omega(d)$, but we did not succeed.

Suppose $\ell > 2$ and $P(d)$ is bounded. Then k is bounded or every prime factor of d_1 is bounded by Theorem 7. However, by definition every prime factor of d_1 is larger than ℓ. So we obtain that $\omega(d)$ and ℓ are bounded, hence, by Theorem 8, k is bounded. Thus Theorems 7 and 8 generalize the results of Shorey mentioned above.

Theorems 7 and 8 imply a slightly weaker inequality than Theorem 6 gives. It is well known that $\omega(n) << \log n / \log\log n$ for all $n > e$. Suppose $\ell \geq 7$. If $\ell \leq \log\log k / \log\log\log k$ then Theorem 8 implies

$$\log k << \frac{\log d}{\log\log d_1} . \log\log\log k$$

and if $\ell > \log\log k / \log\log\log k$ then Theorem 7 implies

$$\log k << \frac{\log d_1}{\ell} < \log d_1 \frac{\log\log\log k}{\log\log k}.$$

Theorems 7 and 8 have proofs based on multiple application of the box principle. For $\ell = 2$ the proof is elementary, but complicated. For $\ell \geq 3$ the proof is completely different. For $\ell \geq 7$ we obtain the best results via elementary arguments, but for $\ell = 3$ and 5 we reach the best estimates when we use Brun's sieve and some result of Evertse on the number of solutions of the equation $ax^\ell - by^\ell = c$, proved by using hypergeometric functions. I want to stress that many lemmas and arguments are due to Erdős.

We have proved that $P(d)$, and even $P(d_1)$, tends to ∞ when $k \to \infty$. In fact we can prove

Theorem 9. [18]

$$P(d_1) >> \ell \log k \log\log k \qquad \text{for } \ell \geq 7,$$

$$P(d) >> \ell \log k \log\log k \qquad \text{for } \ell \in \{2, 3, 5\}.$$

In [18] we give also lower bounds for the smallest prime factor and the greatest square free divisor of d_1.

Up to now I have restricted myself to dependence on d, d_1, k and ℓ. Of course, a can also been taken into account.

Theorem 10 [17].

(a) *There is an absolute constant ℓ_0 such that for $\ell \geq \ell_0$ we have*

$$k <<_a 1.$$

(b)

$$k <<_{a,\omega(d)} 1.$$

For (a) see Shorey [11]. Further (b) follows from the combination of (a) and Theorem 8.

The last theorem concerns upper bounds for the largest term in the arithmetic progression.

Theorem 11. [17]. *There is an absolute constant k_0 such that $k \geq k_0$ implies*

$$a + (k-1)d \leq 17d^2k(\log k)^4 \qquad \textit{if} \quad \ell = 2$$

and

$$a + (k-1)d << k(\frac{d}{\ell})^{\ell/(\ell-2)} \qquad \textit{if} \quad \ell > 2.$$

Finally I want to state a conjecture for the general situation in the line of the conjectures of Dénes and Erdős stated above.

<u>Conjecture.</u> If (5) holds, then $k + \ell \leq 6$.

If $k+\ell \leq 6$, then $(k,\ell) = (3,3)$ or $(4,2)$. It is shown in [20] that in these cases there are infinitely many solutions. As a more moderate target I challenge the reader to prove that k is bounded by a function of only $\omega(d)$ if (5) is satisfied.

Mathematical Institute R.U.

Postbox 9512

2300 RA Leiden

The Netherlands.

References

1. P. Dénes, Über die diophantische Gleichung $x^\ell+y^\ell = cz^\ell$, Acta Math. 88(1952), 241-251.

2. P. Erdős and J.L. Selfridge, The product of consecutive integers is never a power, Illinois J. Math. 19(1975), 292-301.

3. G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent.

   Math. 73(1983), 349-366.

4. K. Győry, Explicit upper bounds for the solutions of some diophantine equations, Ann. Acad. Sci. Fenn. Ser. AI5 (1980), 3-12.

5. M. Langevin, Facteurs premiers d'entiers en progression arithmétique, Acta Arith. 39(1981), 241-249.

6. R. Marszalek, On the product of consecutive elements of an arithmetic progression, Monatsh. Math. 100(1985), 215-222.

7. C.J. Mozzochi, On the difference between consecutive primes, J. Number Theory 24(1986), 181-187.

8. R. Obláth, Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reihe, Publ. Math. Debrecen 1(1950), 222-226.

9. R. Obláth, Eine Bemerkung über Produkte aufeinander folgender Zahlen, J. Indian Math. Soc. (N.S.) 15(1951), 135-139.

10. T.N. Shorey, Some exponential diophantine equations, New Advances in Transcendence Theory, ed. by A. Baker, Cambridge University Press, 1988, pp. 352-365.

11. T.N. Shorey, Some exponential diophantine equations II, to appear in Proceedings Bombay Intern. Colloquium held in January 1988.

12. T.N. Shorey and R. Tijdeman, Perfect powers in arithmetical progression, Madras University J., to appear.

13. T.N. Shorey and R. Tijdeman, Perfect powers in arithmetical progression (II), in preparation.

14. T.N. Shorey and R. Tijdeman, On the greatest prime factor of an arithmetical progression, to appear.

15. T.N. Shorey and R. Tijdeman, On the greatest prime factor of an arithmetical progression (II), Acta Arith., to appear.

16. T.N. Shorey and R. Tijdeman, On the number of prime factors of an arithmetical progression, J. Sichuan Univ., to appear.

17. T.N. Shorey and R. Tijdeman, Perfect powers in products of terms in an arithmetical progression, to appear.

18. T.N. Shorey and R. Tijdeman, Perfect powers in products of terms in an arithmetical progression (II), in preparation.

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

20. R. Tijdeman, Diophantine equations and diophantine approximations, 1st Lecture, in: Number Theory and Applications, Ed. by R.A. Mollin, Kluwer, Dordrecht etc., 1989, pp.215-223.