On a problem in divisibility

Amitabha Tripathi

The following problem appeared at the first level of the Indian Mathematical Olympiad in December 2012.

> Let a, b, c be positive integers such that a divides b^5, b divides c^5 and c divides a^5. Prove that abc divides $(a+b+c)^{31}$.

A first step towards solving this problem is to note that a, b, c have the same set of prime divisors. This includes the possibility $a = b = c = 1$. For prime p and positive integer n, let $\mathsf{e}_p(n)$ denote the highest power of p that divides n. For each common prime divisor p of a, b, c, write

$$\mathsf{e}_p(a) = \alpha, \quad \mathsf{e}_p(b) = \beta, \quad \mathsf{e}_p(c) = \gamma.$$

To complete the proof, one can show that

$$\mathsf{e}_p(abc) = \alpha + \beta + \gamma \le (1 + 5 + 5^2)\min\{\alpha, \beta, \gamma\} \le 31 \cdot \mathsf{e}_p(a+b+c).$$

There is another method to approach this problem. If one expands $(a+b+c)^{31}$, the only terms that do not involve all three of a, b, c are terms of the type $a^r b^{31-r}$ with $r \in \{0, 1, 2, \ldots, 31\}$, together with those obtained by replacing a, b with a, c and with b, c. The divisibility conditions now show that abc divides each of these exceptional terms.

The purpose of this note is to extend this problem to any number of variables, with the divisibility condition extended to any uniform positive integer power. We have the following theorem.

Theorem 1 *For any collection $a_1, a_2, \ldots, a_k, n$ of positive integers, with $k > 1$, that satisfy*

$$a_1 \mid a_2^n, \ \ a_2 \mid a_3^n, \ \ \ldots \ \ , \ \ a_{k-1} \mid a_k^n, \ \ a_k \mid a_1^n, \tag{1}$$

the least positive integer N such that

$$a_1 \cdot a_2 \cdots a_k \textit{ divides } (a_1 + a_2 + \cdots + a_k)^N \tag{2}$$

is given by $N_0 = 1 + n + n^2 + \cdots + n^{k-1}$.

Proof. We treat the cases $n = 1$ and $n > 1$ separately.

1.8Case I: ($n = 1$) Suppose $a_1, a_2, \ldots, a_k$ is a collection of positive integers that satisfy (1) with $n = 1$. Then $a_1 \le a_2 \le \ldots \le a_k \le a_1$. Hence $a_i = a$ for each $i \in \{1, 2, \ldots, k\}$, and (2) reduces to the condition $a^k \mid (ka)^N$. This condition is met for all a if $N \ge k$, but not met if $\gcd(a, k) = 1$ for $N < k$. Hence $N_0 = k$ when $n = 1$.

1.8Case II: $(n > 1)$ Suppose $a_1, a_2, \ldots, a_k$ is a collection of positive integers that satisfy (1) with $n > 1$. To show that (2) holds for some positive integer N, we must show that

$$\mathsf{e}_p\Big(a_1 \cdot a_2 \cdots a_k\Big) \le N \cdot \mathsf{e}_p\Big(a_1 + a_2 + \cdots + a_k\Big) \tag{3}$$

for every prime p. Fix a prime p and write $\mathsf{e}_p(a_i) = e_i$ for $i \in \{1, 2, \ldots, k\}$. Since $a_i \mid a_{i+1}^n$ for $i \in \{1, 2, \ldots, k\}$ (where $a_{k+1} = a_1$), we have

$$e_i = \mathsf{e}_p(a_i) \le \mathsf{e}_p\Big(a_{i+1}^n\Big) = n \cdot e_{i+1}$$

for $i \in \{1, 2, \ldots, k\}$. It follows that

$$e_i \le n^{k-i} \cdot e_k$$

for $i \in \{1, 2, \ldots, k\}$, from which we have

$$e_1 + e_2 + \cdots + e_k \le (n^{k-1} + n^{k-2} + \cdots + n + 1)\, e_k.$$

By symmetry, we must also have

$$e_1 + e_2 + \cdots + e_k \le (n^{k-1} + n^{k-2} + \cdots + n + 1)\, e_i$$

for each $i \in \{1, 2, \ldots, k\}$. Hence

$$e_1 + e_2 + \cdots + e_k \le (n^{k-1} + n^{k-2} + \cdots + n + 1) \cdot \min\{e_1, e_2, \ldots, e_k\}. \tag{4}$$

This establishes (3) with $N = 1 + n + n^2 + \cdots + n^{k-1}$, since $\mathsf{e}_p\Big(a_1 \cdot a_2 \cdots a_k\Big) = e_1 + e_2 + \cdots + e_k$ and $\mathsf{e}_p\Big(a_1 + a_2 + \cdots + a_k\Big) \ge \min\{e_1, e_2, \ldots, e_k\}$. Hence, we have both the existence of the positive integer N in (2) as well as the inequality $N_0 \le 1 + n + n^2 + \cdots + n^{k-1}$.

For the reverse inequality, consider the collection of positive integers p, p^n, p^{n^2}, $\ldots, p^{n^{k-1}}$ where p is any prime. If we take $a_i = p^{n^{k-i}}$, then $a_{i+1}^n = \Big(p^{n^{k-i-1}}\Big)^n = p^{n^{k-i}} = a_i$, thereby meeting the requirement in (1). Now

$$\begin{aligned} &\mathsf{e}_p\Big(a_1 \cdot a_2 \cdots a_k\Big) = e_1 + e_2 + \cdots + e_k = 1 + n + n^2 + \cdots + n^{k-1}, \\ &\mathsf{e}_p\Big(a_1 + a_2 + \cdots + a_k\Big) = 1 \end{aligned}$$

imply $N_0 \ge 1 + n + n^2 + \cdots + n^{k-1}$. Therefore $N_0 = 1 + n + n^2 + \cdots + n^{k-1}$ when $n > 1$. ■

Theorem 1 gives the least positive integer N_0 for which (2) holds for each sequence of positive integers satisfying (1). Therefore there must exist at least one sequence of positive integers satisfying (1) for which (2) fails to hold when $N = N_0 - 1$. We follow the argument in Theorem 1 to characterize such extremal sequences.

For $n = 1$, (1) implies $a_i = a$ for $i \in \{1, 2, \ldots, k\}$. So (2) fails to hold for the collection $a_1, a_2, \ldots, a_k$ with $N = N_0 - 1 = k - 1$ is equivalent to the condition $a^k \nmid (ka)^{k-1}$. Thus the only such collections are those in which each term equals a positive integer a, where $a \nmid k^{k-1}$.

Let $n > 1$. Suppose the sequence $a_1, a_2, \ldots, a_k$ satisfies (1) and is such that

$$a_1 \cdot a_2 \cdots a_k \text{ does not divide } (a_1 + a_2 + \cdots + a_k)^{N_0 - 1}.$$

Then there must exist a prime p for which

$$\mathsf{e}_p\Big(a_1 \cdot a_2 \cdots a_k\Big) = e_1 + e_2 + \cdots + e_k > (N_0 - 1) \cdot \mathsf{e}_p\Big(a_1 + a_2 + \cdots + a_k\Big). \quad (5)$$

On the other hand, every sequence $a_1, a_2, \ldots, a_k$ that satisfies (1) also satisfies (4) for each prime p. Combining (4) and (5) gives

$$(N_0 - 1) \cdot \mathsf{e}_p\Big(a_1 + a_2 + \cdots + a_k\Big) < e_1 + e_2 + \cdots + e_k \le N_0 \cdot \min\{e_1, e_2, \ldots, e_k\} \quad (6)$$

for at least one prime p. This characterizes extremal sequences $a_1, a_2, \ldots, a_k$ when $n > 1$.

When the set $\{e_1, e_2, \ldots, e_k\}$ has a *unique* least element, $\mathsf{e}_p\Big(a_1 + a_2 + \cdots + a_k\Big) = \min\{e_1, e_2, \ldots, e_k\}$. This may also hold when the set $\{e_1, e_2, \ldots, e_k\}$ does not have a unique least element, but the equality is not guaranteed. In case of the unique least element, and consequently of the equality $\mathsf{e}_p\Big(a_1 + a_2 + \cdots + a_k\Big) = \min\{e_1, e_2, \ldots, e_k\} = e$, (6) reduces to

$$e(N_0 - 1) < e_1 + e_2 + \cdots + e_k \le eN_0.$$

When $e = 1$, this further reduces to $e_1 + e_2 + \cdots + e_k = N_0$, as is the case with the collection $p, p^n, p^{n^2}, \ldots, p^{n^{k-1}}$ for prime p.

References

[1] David M. Burton, *Number Theory*, Cambridge University Press, 1994.

Amitabha Tripathi
Department of Mathematics
Indian Institute of Technology
Hauz Khas, New Delhi, India
atripath@maths.iitd.ac