Divisibility

Victor Rong

July 3, 2025

1 Bounding

One of the most useful ways to exploit a divisibility condition is to establish an inequality. We can make use of the following simple fact:

Lemma 1.1. If $a, b \in \mathbb{Z}$ and $a \mid b$, then $|a| \leq |b|$ or $b = 0$.

Example 1 (EGMO TST 2025)**.** Consider a sequence of positive integers $a_1, a_2, \ldots, a_k$ satisfying $1 \leq a_1 < a_2 < \ldots < a_k \leq k^2$ for a positive integer k. Determine all possible values of $a_k - a_1$ if for all $i, j \in \{1, 2, 3, \ldots, k\}$, the sum $i + j$ divides $ia_i + ja_j$.

Proof. We claim that the only possible value of $a_k - a_1$ is $k^2 - 1$. This is achieved when $a_i = i^2$, which can be checked to satisfy the conditions.

Now let's prove that this is the only possible value. From the divisibility condition with $j = i + 1$, we have

$$\begin{aligned} & 2i+1 \mid ia_i + (i+1)a_{i+1} \\ \implies & 2i+1 \mid i(a_i - a_{i+1}) \\ \implies & 2i+1 \mid a_{i+1} - a_i. \end{aligned}$$

Note that the last step uses the fact that $\gcd(i, 2i+1) = 1$. As we know that $a_{i+1} > a_i$, we can conclude from this divisibility that that $a_{i+1} - a_i \geq 2i + 1$. Hence,

$$a_k - a_1 = \sum_{i=1}^{k-1} a_{i+1} - a_i \geq k^2 - 1.$$

But we also know $a_k - a_1 \leq k^2 - 1$ as $a_k \leq k^2$ and $a_1 \geq 1$. So we must have $a_k - a_1 = k^2 - 1$. □

Example 2 (ISL 2021)**.** Find all positive integers $n \geq 1$ such that there exists a pair (a, b) of positive integers, such that $a^2 + b + 3$ is not divisible by the cube of any prime, and

$$n = \frac{ab + 3b + 8}{a^2 + b + 3}.$$

Proof. Note that

$$(a + 3) - n = \frac{(a+1)^3}{a^2 + b + 3}.$$

Hence,

$$a^2 + b + 3 \mid (a+1)^3.$$

Since a^2+b+3 is cube-free, we can see that

$$a^2+b+3 \mid (a+1)^2.$$

For any $a, b \in \mathbb{N}$, we have

$$(a+1)^2 < 2(a^2+b+3)$$

so for the divisibility to hold, we must have

$$\begin{aligned} a^2+b+3 &= (a+1)^2 \\ \implies \qquad b &= 2a-2. \end{aligned}$$

Plugging this in yields $n = 2$. □

1.1 Problems

1. (CMO 2011). Consider 70-digit numbers with the property that each of the digits $1, 2, 3, ..., 7$ appear 10 times in the decimal expansion of n (and $8, 9, 0$ do not appear). Show that no number of this form can divide another number of this form.
2. (ToT 2019). Let a and b be distinct positive integers. Prove that there are only finitely many positive integers n such that
$$a^n + b^n \mid a^{n+1} + b^{n+1}.$$
3. (CMO 2019). Let a, b be positive integers such that $a + b^3$ is divisible by $a^2 + 3ab + 3b^2 - 1$. Prove that $a^2 + 3ab + 3b^2 - 1$ is divisible by the cube of an integer greater than 1.
4. (APMO 2002). Find all positive integers a and b such that
$$\frac{a^2+b}{b^2-a} \quad \text{and} \quad \frac{b^2+a}{a^2-b}$$
are both integers.
5. (APMO 2013). Determine all positive integers n for which $\dfrac{n^2+1}{[\sqrt{n}]^2+2}$ is an integer. Here $[r]$ denotes the greatest integer less than or equal to r.

2 p-adic Valuations

The p-adic valuation is an important concept for handling number theory problems.

Definition. Let p be a prime and n be an integer. The p-adic valuation of n, denoted as $v_p(n)$ is the largest power of p which divides n. In other words,

$$p^{v_p(n)} \mid x \quad \text{but} \quad p^{v_p(n)+1} \nmid x.$$

Note that $v_p(0) = \infty$. Let's first establish some basic properties of the p-adic valuation.

Lemma 2.1. We have

(i) For any $a, b \in \mathbb{Z}$, $v_p(ab) = v_p(a) + v_p(b)$.

(ii) For any $a, b \in \mathbb{Z}$, $v_p(a \pm b) \geq \min\{v_p(a), v_p(b)\}$. In particular, if $v_p(a) < v_p(b)$, then $v_p(a \pm b) = v_p(a)$.

The p-adic valuation can also be extended to rational arguments. In particular, $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$.

Example 3 (ISL 2011)**.** Consider a polynomial $P(x) = \prod_{j=1}^{9}(x + d_j)$, where $d_1, d_2, \dots d_9$ are nine distinct integers. Prove that there exists an integer N, such that for all integers $x \geq N$ the number $P(x)$ is divisible by a prime number greater than 20.

Proof. Note that there are eight primes $p_1, p_2, \dots, p_8 \leq 20$. Let T be an integer such that

$$v_{p_i}(d_j - d_k) < T \text{ for all } 1 \leq i \leq 8, 1 \leq j < k \leq 9.$$

Assume for the sake of contradiction that there are infinitely many a such that $P(a)$ only has prime factors in $\{p_1, \dots, p_8\}$. Let a be sufficiently large. Then for each $1 \leq j \leq 9$ we must have $v_{p_i}(a + d_j) \geq T$ for some $1 \leq i \leq 8$. By Pigeonhole Principle, two of these will have the same p_i. Without loss of generality, say

$$v_{p_1}(a + d_1) \geq T, \quad v_{p_1}(a + d_2) \geq T.$$

Then

$$\begin{aligned} v_{p_1}(d_2 - d_1) &= v_{p_1}\left((a + d_2) - (a + d_1)\right) \\ &\geq \min\{v_{p_1}(a + d_1), v_{p_1}(a + d_2)\} \\ &\geq T \\ &> v_{p_1}(d_2 - d_1), \end{aligned}$$

contradiction. □

2.1 Problems

1. (Putnam 2024). Determine all positive integers n for which there exists positive integers a, b, and c satisfying
$$2a^n + 3b^n = 4c^n.$$

2. (ISL 2009). Let f be a non-constant function from the set of positive integers into the set of positive integer, such that $a - b$ divides $f(a) - f(b)$ for all distinct positive integers a, b. Prove that there exist infinitely many primes p such that p divides $f(c)$ for some positive integer c.

3. (IMO 1984). Let a, b, c, d be odd integers such that $0 < a < b < c < d$ and $ad = bc$. Prove that if $a + d = 2^k$ and $b + c = 2^m$ for some integers k and m, then $a = 1$.

4. (APMO 2017). Call a rational number r powerful if r can be expressed in the form $\frac{p^k}{q}$ for some relatively prime positive integers p, q and some integer $k > 1$. Let a, b, c be positive rational numbers such that $abc = 1$. Suppose there exist positive integers x, y, z such that $a^x + b^y + c^z$ is an integer. Prove that a, b, c are all powerful.
5. (ISL 2013). Determine whether there exists an infinite sequence of nonzero digits $a_1, a_2, a_3, \cdots$ and a positive integer N such that for every integer $k > N$, the number $\overline{a_k a_{k-1} \cdots a_1}$ is a perfect square.

3 Lifting the Exponent

Theorem 1 (LTE)**.** Let x and y be integers and let n be a positive integer. Let $p > 2$ be a prime such that $p \mid x - y$ and $p \nmid x, y$. Then

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Proof. We will first consider the case where $p \nmid n$.

Lemma 3.1. If $p \nmid n$, $v_p(x^n - y^n) = v_p(x - y)$.

First note that

$$\begin{aligned} \frac{x^n - y^n}{x - y} &= x^{n-1} + x^{n-2}y + \ldots + y^{n-1} \\ &\equiv nx^{n-1} \pmod p \end{aligned}$$

So we see that $v_p(x^n - y^n) = v_p(x - y)$. Now let's consider $n = p$.

Lemma 3.2. If $p = n$, $v_p(x^n - y^n) = v_p(x - y) + 1$.

Let $x = kp + y$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned} \frac{x^p - y^p}{x - y} &= \frac{(kp + y)^p - y^p}{(kp + y) - y} \\ &= \frac{\sum_{i=1}^{p} \binom{p}{i} (kp)^i y^{p-i}}{kp} \end{aligned}$$

$$\begin{aligned} &= \sum_{i=1}^{p} \binom{p}{i} (kp)^{i-1} y^{p-i} \\ &= py^{p-1} + \binom{p}{2} (kp) y^{p-2} + \ldots \\ &= py^{p-1} + (\ldots) p^2. \end{aligned}$$

So $v_p(x^p - y^p) = v_p(x - y) + 1$. Now say $n = p^k q$ for $p \nmid q$. We can apply the first lemma to see that

$$v_p\left(x^{p^k q} - y^{p^k q}\right) = v_p\left(x^{p^k} - y^{p^k}\right).$$

Then by the second lemma,

$$\begin{aligned}v_p\left(x^{p^k}-y^{p^k}\right) &= v_p\left(x^{p^{k-1}}-y^{p^{k-1}}\right)+1\\ &= v_p\left(x^{p^{k-2}}-y^{p^{k-2}}\right)+2\\ &= v_p(x-y)+k.\end{aligned}$$

Altogether, we have $v_p(x^n-y^n)=v_p(x-y)+v_p(n)$ as desired. □

Example 4 (IMOC 2024)**.** Find all positive integers n such that $n(2^n-1)$ is a perfect square.

Proof. We claim that $n=1$ is the only possibility. For $n>1$, let p be a prime divisor of n, so $n=pr$. Now consider

$$n(2^n-1)=pr(2^p-1)\left(\frac{2^{pr}-1}{2^p-1}\right).$$

Let q be any prime divisor of 2^p-1. Note that $q\neq p$. The key is to consider taking v_q of this product. We have

$$\begin{aligned}v_q\left(n(2^n-1)\right) &= v_q(p)+v_q(r)+v_q(2^p-1)+v_q\left(\frac{2^{pr}-1}{2^p-1}\right)\\ &= 2v_q(r)+v_q(2^p-1)\end{aligned}$$

by applying LTE. Since $n(2^n-1)$ should be a perfect square, we can conclude that $v_q(2^p-1)$ is even. However, q was any prime factor of 2^p-1 so by this argument, we see that 2^p-1 must be a perfect square. But this is impossible since $2^p-1\equiv 3 \pmod 4$ so we are done. □

Example 5 (ISL 2014)**.** Find all triples (p,x,y) consisting of a prime number p and two positive integers x and y such that $x^{p-1}+y$ and $x+y^{p-1}$ are both powers of p.

Proof. If $p=2$, then clearly $x+y=2^k$ works.

Now consider $p>2$. If $p\mid x$, then we quickly run into problems as we must have $v_p(x^{p-1})\neq v_p(y)$ or $v_p(y^{p-1})\neq v_p(x)$. So $p\nmid x,y$. In particular, by FLT,

$$x\equiv y\equiv -1 \pmod p.$$

WLOG $y\geq x$ and so $y^{p-1}+x\geq x^{p-1}+y$. Since they are both powers of p, we must have

$$\begin{aligned}&x^{p-1}+y\mid y^{p-1}+x\\ \Longrightarrow\ &x^{p-1}+y\mid x^{(p-1)^2}+x\\ \Longrightarrow\ &x^{p-1}+y\mid x^{p(p-2)}+1.\end{aligned}$$

Now we can apply LTE to compute

$$v_p\left(x^{p(p-2)}+1\right)=v_p(x+1)+1.$$

Since $x^{p-1}+y$ is supposed to be a prime power, this implies that

$$\begin{aligned} x^{p-1}+y &\mid p(x+1) \\ \implies x^{p-1}+y &\le p(x+1) \\ \implies x^{p-1}+x &\le p(x+1) \\ \implies x^{p-2} &\le p. \end{aligned}$$

However, $x \equiv -1 \pmod p$ so $x \ge p-1$. This is only possible with $p=3$ and $x=2$.

It remains to find y such that $y+4$ and y^2+2 are powers of 3. Let $y=3^a-4$. Then we have

$$\begin{aligned} y^2+2 &= (3^a-4)^2+2 \\ &= 3^{2a}-8\cdot 3^a+18. \end{aligned}$$

For $a \ge 3$, this cannot be a power of 3. Checking $a=1$ and $a=2$, we find that only $a=2$ works, giving solutions $(2,5,3)$ and $(5,2,3)$. □

It may also be useful to know the following theorem, which is citable on olympiads.

Theorem 2 (Zsigmondy's Theorem)**.** Let $a > b \ge 1$ be relatively prime integers. For any $n \ge 2$, $a^n - b^n$ has a prime divisor p which does not divide $a^k - b^k$ for any $1 \le k < n$ except when

- $n=2$ and $a+b$ is a power of 2;
- $(a,b,n)=(2,1,6)$.

3.1 Problems

1. (CMO 2025). Determine all positive integers a, b, c, p, where p and $p+2$ are odd primes and
$$2^a p^b = (p+2)^c - 1.$$
2. (ISL 2010). Find all pairs (m,n) of nonnegative integers for which
$$m^2 + 2\cdot 3^n = m\left(2^{n+1}-1\right).$$
3. (USAJMO 2024). Let $a(n)$ be the sequence defined by $a(1)=2$ and $a(n+1)=(a(n))^{n+1}-1$ for each integer $n \ge 1$. Suppose that $p>2$ is a prime and k is a positive integer. Prove that some term of the sequence $a(n)$ is divisible by p^k.
4. (RMM 2012). Prove that there are infinitely many positive integers n such that $2^{2^n+1}+1$ is divisible by n but 2^n+1 is not.
5. (USATSTST 2018). For which positive integers $b>2$ do there exist infinitely many positive integers n such that n^2 divides b^n+1?

4 !!

Theorem 3 (Legendre's Theorem)**.** For a prime p and natural number n,

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Theorem 4 (Kummer's Theorem)**.** For a prime p and integers $n \geq m \geq 0$, $v_p\left(\binom{n}{m}\right)$ is equal to the number of carries when adding m and $n-m$ in base p.

Example 6 (IMO 2019)**.** Find all pairs (k, n) of positive integers such that

$$k! = (2^n - 1)(2^n - 2)(2^n - 4)\cdots(2^n - 2^{n-1}).$$

Proof. The idea is to consider v_2 of both sides. By Legendre's Theorem, we have

$$v_2(k!) = \sum_{i=1}^{\infty} \left\lfloor \frac{k}{2^i} \right\rfloor < k$$

On the other side, which we denote as R, we have

$$\begin{aligned} v_2(R) &= v_2(2^n - 1) + v_2(2^n - 2) + \ldots + v_2(2^n - 2^{n-1}) \\ &= 0 + 1 + \ldots + (n-1) \\ &= \frac{n(n-1)}{2}. \end{aligned}$$

Hence, $k > \frac{n(n-1)}{2}$. At this point, various bounding approaches work. A particularly clean way to finish, though, is to now consider v_3 of both sides.

On the left, we have

$$v_3(k!) = \sum_{i=1}^{\infty} \left\lfloor \frac{k}{3^i} \right\rfloor \geq \frac{k-2}{3}.$$

For the right side, note that by LTE, $v_3(2^{2j} - 1) = 1 + v_3(j)$. Hence,

$$\begin{aligned} v_3(R) &= \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{6} \right\rfloor + \ldots \\ &< \frac{3n}{4}. \end{aligned}$$

Together, these give $\frac{9n}{4} + 2 > \frac{n(n-1)}{2}$ which only holds for $n \leq 6$. Checking these cases manually gives $n = 1, k = 1$ and $n = 2, k = 3$. □

4.1 Problems

1. (CMO 2024). Jane writes down 2024 natural numbers around the perimeter of a circle. She wants the 2024 products of adjacent pairs of numbers to be exactly the set $\{1!, 2!, \ldots, 2024!\}$. Can she accomplish this?

2. (ISL 2023). For positive integers n and $k \geq 2$, define $E_k(n)$ as the greatest exponent r such that k^r divides $n!$. Prove that there are infinitely many n such that $E_{10}(n) > E_9(n)$ and infinitely many m such that $E_{10}(m) < E_9(m)$.
3. (USAMO 2016). Prove that for any positive integer k,

$$(k^2)! \cdot \prod_{j=0}^{k-1} \frac{j!}{(j+k)!}$$

is an integer.

4. (ISL 2012). Determine all integers $m \geq 2$ such that every n with $\frac{m}{3} \leq n \leq \frac{m}{2}$ divides the binomial coefficient $\binom{n}{m-2n}$.
5. (ISL 2007). For every integer $k \geq 2$, prove that 2^{3k} divides the number

$$\binom{2^{k+1}}{2^k} - \binom{2^k}{2^{k-1}}$$

but 2^{3k+1} does not.

5 Functional Equations

When dealing with divisibility conditions in function equations, there are a few very useful ideas.

1. Make the right side of the divisiblity condition as "forcing" as possible, i.e. prime or prime power
2. If you prove that $f(n) = g(n)$ for some known g and n in infinite set S, you can often choose $N \in S$ arbitrarily large and prove that $f(n) = g(n)$ for all $n << N$.

We will see this recipe in the next example.

Example 7 (ISL 2004)**.** Find all functions $f : \mathbb{N} \to \mathbb{N}$ satisfying

$$f^2(m) + f(n) \mid \left(m^2 + n\right)^2$$

for any two positive integers m and n.

Proof. Let $P(m, n)$ denote the assertion. We will first prove that $f(p-1) = p-1$ for all primes p. From $P(1, 1)$ we see

$$\begin{aligned} & f(1)^2 + f(1) \mid 4 \\ \implies \quad & f(1) = 1. \end{aligned}$$

Now for any prime p, consider $P(1, p-1)$. We have

$$\begin{aligned} & f(1)^2 + f(p-1) \mid p^2 \\ \implies \quad & f(p-1) = p-1 \\ & \text{or } f(p-1) = p^2 - 1. \end{aligned}$$

To resolve this ambiguity, assume for the sake of contradiction that $f(p-1) = p^2 - 1$ for some p and take $P(p-1, p-1)$:

$$\begin{aligned} & f(p-1)^2 + f(p-1) \mid ((p-1)^2 + p - 1)^2 \\ \implies & \qquad (p^2-1)p^2 \mid (p-1)^2 p^2 \end{aligned}$$

which is impossible due to size. Hence, $f(p-1) = p-1$ for all primes p.

Now, consider $P(m, p-1)$ for any $m \in \mathbb{N}$ and any prime p. This gives

$$\begin{aligned} & f(m)^2 + p - 1 \mid (m^2 + p - 1)^2 \\ \implies & f(m)^2 + p - 1 \mid \left(m^2 - f(m)^2\right)^2. \end{aligned}$$

Since this is true for all primes p, the right hand side must be 0 and so $f(m) = m$ for all $m \in \mathbb{N}$. It is easy to check that function indeed works. □

The above strategy is particularly effective when the solution set for f is easy to understand. When this is not the case, more ad-hoc ideas are often necessary.

Example 8 (IMO 2011)**.** Let f be a function from the set of integers to the set of positive integers. Suppose that, for any two integers m and n, the difference $f(m) - f(n)$ is divisible by $f(m-n)$. Prove that, for all integers m and n with $f(m) \leq f(n)$, the number $f(n)$ is divisible by $f(m)$.

Proof. Let $P(m, n)$ denote the assertion. We will first prove that f is even, i.e. $f(n) = f(-n)$.

From $P(m, 0)$, we have

$$\begin{aligned} & f(m) \mid f(m) - f(0) \\ \implies & f(m) \mid f(0) \qquad \forall m \in \mathbb{Z}. \end{aligned}$$

Now take $P(0, n)$:

$$\begin{aligned} & f(-n) \mid f(0) - f(n) \\ \implies & f(-n) \mid f(n). \end{aligned}$$

Similarly, from $P(0, -n)$, we have $f(n) \mid f(-n)$. Hence, $f(n) = f(-n)$, as desired.

Now the key idea is that the problem's divisibility condition is constrained by size. Consider the following:

$$\begin{aligned} P(m, n) &\implies f(m-n) \mid f(m) - f(n) \\ P(m, m-n) &\implies \quad f(n) \mid f(m) - f(m-n) \\ P(m-n, -n) &\implies \quad f(m) \mid f(m-n) - f(-n) \\ &\implies \quad f(m) \mid f(m-n) - f(n) \end{aligned}$$

Hence, we have three natural numbers $\{a, b, c\} = \{f(m), f(n), f(m-n)\}$ for which

$$a \mid b - c, b \mid c - a, c \mid a - b.$$

Say WLOG that $0 < a \leq b \leq c$. Then from $c \mid a - b$, we must have $a = b$ and furthermore, $a \mid c$, $b \mid c$. Thus, $f(m) \leq f(n) \implies f(m) \mid f(n)$. □

5.1 Problems

1. (ISL 2013). Let $\mathbb{Z}_{>0}$ be the set of positive integers. Find all functions $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ such that
$$m^2 + f(n) \mid mf(m) + n$$
for all positive integers m and n.
2. (ISL 2019). Find all functions $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ such that $a + f(b)$ divides $a^2 + bf(a)$ for all positive integers a and b with $a + b > 2019$.
3. (USATSTST 2022). Let $\mathbb{N}$ denote the set of positive integers. A function $f \colon \mathbb{N} \to \mathbb{N}$ has the property that for all positive integers m and n, exactly one of the $f(n)$ numbers
$$f(m+1), f(m+2), \ldots, f(m+f(n))$$
is divisible by n. Prove that $f(n) = n$ for infinitely many positive integers n.
4. (ISL 2011). Let $n \geq 1$ be an odd integer. Determine all functions f from the set of integers to itself, such that for all integers x and y the difference $f(x) - f(y)$ divides $x^n - y^n$.
5. (ISL 2016). Denote by $\mathbb{N}$ the set of all positive integers. Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that for all positive integers m and n, the integer $f(m) + f(n) - mn$ is nonzero and divides $mf(m) + nf(n)$.

6 Order

Definition. Let $n > 1$ be a natural number. For a relatively prime to n, the *order* of a modulo n, denoted as $\operatorname{ord}_n(a)$, is the smallest natural number such that
$$a^{\operatorname{ord}_n(a)} \equiv 1 \pmod{n}.$$

By the pigeonhole principle, such a natural number must exist. Euler's totient function gives a specific example of such an exponent although it may not be the smallest:
$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

The following lemma is crucial for understanding the order.

Lemma 6.1. If $a^k \equiv 1 \pmod{n}$ then $\operatorname{ord}_n(a) \mid k$.

Proof. Let $k = q \operatorname{ord}_n(a) + r$ for $0 \leq r < \operatorname{ord}_n(a)$. Assume for the sake of contradiction that $\operatorname{ord}_n(a)$ does not divide k and hence $r \neq 0$.

We have
$$\begin{aligned} & a^k \equiv 1 \pmod{n} \\ \Longrightarrow\quad & a^{q \operatorname{ord}_n(a) + r} \equiv 1 \pmod{n} \\ \Longrightarrow\quad & \left(a^{\operatorname{ord}_n(a)}\right)^q \cdot a^r \equiv 1 \pmod{n} \\ \Longrightarrow\quad & a^r \equiv 1 \pmod{n}. \end{aligned}$$
However, this contradicts the minimality of $\operatorname{ord}_n(a)$, and so $\operatorname{ord}_n(a)$ must have divided k. □

Remark. This is closely related to the lemma that states $\gcd(a^s-1, a^t-1) = a^{\gcd(s,t)} - 1$.

Example 9. Find all $n \in \mathbb{N}$ such that $n \mid 2^n - 1$.

Proof. Clearly $n = 1$ works. Let's now consider $n > 1$.

Take p to be the minimal prime which divides n. Note that $p \neq 2$. Then we have

$$p \mid 2^n - 1 \implies \operatorname{ord}_p(2) \mid n.$$

However, $\operatorname{ord}_p(2) \leq p - 1 < p$. Since we picked p to be the minimal prime divisor of n, we must have

$$\operatorname{ord}_p(2) = 1 \implies 2^1 \equiv 1 \pmod{p},$$

which is impossible.

Hence, $n = 1$ is the only solution. □

Example 10. Let p be a prime. If q is a prime divisor of $\frac{n^p-1}{n-1}$ for some $n \in \mathbb{N}$, prove that $q = p$ or $q \equiv 1 \pmod{p}$.

Proof. We proceed in two cases.

Case 1. $q \mid n - 1$

In this case, we will prove that $q = p$. Since $n \equiv 1 \pmod{q}$, we have

$$\begin{aligned} \frac{n^p - 1}{n - 1} &\equiv 0 \pmod{q} \\ \implies n^{p-1} + \ldots + 1 &\equiv 0 \pmod{q} \\ \implies \qquad p &\equiv 0 \pmod{q} \end{aligned}$$

and so we must have $q = p$.

Case 2. $q \nmid n - 1$ Since $q \mid n^p - 1$, the order $\operatorname{ord}_q(n)$ must be 1 or p. Since $q \nmid 1$, it must be p. But we also know that $\operatorname{ord}_q(n) \mid q - 1$ and so $q \equiv 1 \pmod{p}$. □

For a prime p, the set of orders are well-understood, thanks to the existence of primitive roots modulo p.

Definition. Let n be a natural number. For g relatively prime to n, g is a *primitive root* if $\operatorname{ord}_n(g) = \phi(n)$.

In particular, $\{1, g, \ldots, g^{\phi(n)-1}\}$ taken modulo n are exactly all the relatively prime elements to n.

Theorem 5. Let p be a prime. There exists a primitive root g such that $\text{ord}_p(g) = p - 1$.

The existence of at least one primitive root actually implies that there are $\phi(p-1)$ primitive roots.

It is often convenient to interpret the set $\{1, 2, \ldots, p-1\}$ as $\{1, g, \ldots, g^{p-2}\}$ modulo p.

Example 11. Let n be a positive integer and let $p > n + 1$ be a prime. Prove that p divides

$$1^n + 2^n + \ldots + (p-1)^n.$$

Proof. Let g be a primitive root. Then

$$\begin{aligned} \sum_{i=1}^{p-1} i^n &\equiv \sum_{j=0}^{p-2} g^{nj} \pmod{p} \\ &\equiv \frac{g^{(p-1)n} - 1}{g^n - 1} \pmod{p} \\ &\equiv 0 \end{aligned}$$

as desired. Crucially, we needed $g^n - 1 \not\equiv 0 \pmod{p}$ since $n < p - 1$. □

6.1 Problems

1. Prove that $n \mid \phi(a^n - 1)$ for all $a, n \in \mathbb{N}$.
2. (USATST 2003). Find all ordered triples of primes (p, q, r) such that

$$p \mid q^r + 1, \quad q \mid r^p + 1, \quad r \mid p^q + 1.$$

3. (China 2006). Find all positive integer pairs (a, n) such that $\frac{(a+1)^n - a^n}{n}$ is an integer.
4. (ISL 2006). Find all integer solutions of the equation

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

5. (IMO 2003). Let p be a prime number. Prove that there exists a prime number q such that for every integer n, the number $n^p - p$ is not divisible by q.

7 Vieta Jumping

Vieta jumping, popularized by the following example, is a technique used to solve polynomial-like Diophantine equations. By interpreting the equation as a polynomial in a single variable, we can "jump" from one solution to another using Vieta's formulas.

Example 12 (IMO 1988)**.** Let a and b be two positive integers such that $ab+1$ divides a^2+b^2. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Proof. Fix $k \in \mathbb{Z}$ and consider the set of solutions $(a,b) \in \mathbb{N}_0^2$ to

$$\frac{a^2+b^2}{ab+1} = k \iff a^2 - kab + b^2 - k = 0.$$

Assume for the sake of contradiction that k is not a perfect square. Let (a_0, b_0) be the solution that minimizes $a+b$ across all solutions. Without loss of generality, say $a_0 \le b_0$. Note that $a_0 \neq 0$ since otherwise, $k = b_0^2$.

Consider the quadratic $x^2 - kxa_0 + a_0^2 - k$. We know that b_0 is one solution. By Vieta's, there is another solution b_* where

$$b_* = ka_0 - b,$$
$$b_* = \frac{a_0^2 - k}{b_0}.$$

From the first equation, we know that $b_* \in \mathbb{Z}$. Furthermore, we must have $b_* > 0$ since $a_0^2 - k \neq 0$ and $\frac{a_0^2+b_*^2}{a_0 b_* + 1} = k > 0$.

Finally, note that

$$b_* = \frac{a_0^2 - k}{b_0} < b_0.$$

This is a contradiction as (b_*, a_0) has a smaller sum than (a_0, b_0) and so we are done.

□

7.1 Problems

1. (Iran 2013). Suppose that a, b are two odd positive integers such that $2ab+1 \mid a^2+b^2+1$. Prove that $a = b$.
2. (IMO 2007). Let a and b be positive integers. Show that if $4ab-1$ divides $(4a^2-1)^2$, then $a = b$.
3. (Romania 2004). Let a, b be two positive integers, such that $ab \neq 1$. Find all the integer values that $f(a,b)$ can take, where

$$f(a,b) = \frac{a^2+ab+b^2}{ab-1}.$$

4. (ISL 2017). Find the smallest positive integer n or show no such n exists, with the following property: there are infinitely many distinct n-tuples of positive rational numbers $(a_1, a_2, \ldots, a_n)$ such that both

$$a_1 + a_2 + \cdots + a_n \quad \text{and} \quad \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

are integers.

5. (ISL 2019). Let a and b be two positive integers. Prove that the integer

$$a^2 + \left\lceil \frac{4a^2}{b} \right\rceil$$

is not a square. (Here $\lceil z \rceil$ denotes the least integer greater than or equal to z.)

8 Problems

A1. (Poland 2023). Given a sequence of positive integers $a_1, a_2, a_3, \dots$ such that for any positive integers k, l we have $k + l \mid a_k + a_l$. Prove that for all positive integers $k > l$, $a_k - a_l$ is divisible by $k - l$.

A2. (IMO 2023). Determine all composite integers $n > 1$ that satisfy the following property: if $d_1, d_2, \dots, d_k$ are all the positive divisors of n with $1 = d_1 < d_2 < \cdots < d_k = n$, then d_i divides $d_{i+1} + d_{i+2}$ for every $1 \le i \le k - 2$.

A3. (Putnam 2018). Find all positive integers $n < 10^{100}$ for which simultaneously n divides 2^n, $n - 1$ divides $2^n - 1$, and $n - 2$ divides $2^n - 2$.

A4. (APMO 2012). Determine all the pairs (p, n) of a prime number p and a positive integer n for which $\frac{n^p+1}{p^n+1}$ is an integer.

A5. (ISL 2022). Find all positive integers $n > 2$ such that

$$n! \mid \prod_{p<q\le n, p,q \text{ primes}} (p+q).$$

A6. (APMO 2022). Find all pairs (a, b) of positive integers such that a^3 is multiple of b^2 and $b - 1$ is multiple of $a - 1$.

A7. (Iran 2024). For a given positive integer number n find all subsets $\{r_0, r_1, \cdots, r_n\} \subset \mathbb{N}$ such that

$$n^n + n^{n-1} + \cdots + 1 | n^{r_n} + \cdots + n^{r_0}.$$

B1. (APMO 2016). A positive integer is called fancy if it can be expressed in the form

$$2^{a_1} + 2^{a_2} + \cdots + 2^{a_{100}},$$

where $a_1, a_2, \cdots, a_{100}$ are non-negative integers that are not necessarily distinct. Find the smallest positive integer n such that no multiple of n is a fancy number.

B2. (USAMO 2012). Find all functions $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ (where $\mathbb{Z}^+$ is the set of positive integers) such that $f(n!) = f(n)!$ for all positive integers n and such that $m - n$ divides $f(m) - f(n)$ for all distinct positive integers m, n.

B3. (ISL 2016). Let n, m, k and l be positive integers with $n \ne 1$ such that $n^k + mn^l + 1$ divides $n^{k+l} - 1$. Prove that $m = 1$ and $l = 2k$; or $l|k$ and $m = \frac{n^{k-l}-1}{n^l-1}$.

B4. (IMO 1990). Determine all integers $n > 1$ such that

$$\frac{2^n + 1}{n^2}$$

is an integer.

B5. (IMO 2003). Determine all pairs of positive integers (a, b) such that

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

is a positive integer.

B6. (IMO 2022). Find all triples (a, b, p) of positive integers with p prime and

$$a^p = b! + p.$$

B7. (CMO 2021). A function f from the positive integers to the positive integers is called Canadian if it satisfies

$$\gcd(f(f(x)), f(x+y)) = \gcd(x, y)$$

for all pairs of positive integers x and y.

Find all positive integers m such that $f(m) = m$ for all Canadian functions f.

B8. (IMO 2018). Let a_1, a_2, $\ldots$ be an infinite sequence of positive integers. Suppose that there is an integer $N > 1$ such that, for each $n \geq N$, the number

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$$

is an integer. Prove that there is a positive integer M such that $a_m = a_{m+1}$ for all $m \geq M$.

B9. (RMM 2024). Consider an infinite sequence of positive integers $a_1, a_2, a_3, \ldots$ such that $a_1 > 1$ and $(2^{a_n} - 1)a_{n+1}$ is a square for all positive integers n. Is it possible for two terms of such a sequence to be equal?

B10. (CMO 2018). Let k be a given even positive integer. Sarah first picks a positive integer N greater than 1 and proceeds to alter it as follows: every minute, she chooses a prime divisor p of the current value of N, and multiplies the current N by $p^k - p^{-1}$ to produce the next value of N. Prove that there are infinitely many even positive integers k such that, no matter what choices Sarah makes, her number N will at some point be divisible by 2018.

B11. (USAMO 2025). Determine, with proof, all positive integers k such that

$$\frac{1}{n+1}\sum_{i=0}^{n}\binom{n}{i}^k$$

is an integer for every positive integer n.

B12. (ISL 2014). Let $c \geq 1$ be an integer. Define a sequence of positive integers by $a_1 = c$ and

$$a_{n+1} = a_n^3 - 4c \cdot a_n^2 + 5c^2 \cdot a_n + c$$

for all $n \geq 1$. Prove that for each integer $n \geq 2$ there exists a prime number p dividing a_n but none of the numbers $a_1, \ldots, a_{n-1}$.

C1. (ISL 2010). The rows and columns of a $2^n \times 2^n$ table are numbered from 0 to $2^n - 1$. The cells of the table have been coloured with the following property being satisfied: for each $0 \leq i, j \leq 2^n - 1$, the j-th cell in the i-th row and the $(i+j)$-th cell in the j-th row have the same colour. (The indices of the cells in a row are considered modulo 2^n.) Prove that the maximal possible number of colours is 2^n.

C2. (CMO 2015). Let p be a prime number for which $\frac{p-1}{2}$ is also prime, and let a, b, c be integers not divisible by p. Prove that there are at most $1 + \sqrt{2p}$ positive integers n such that $n < p$ and p divides $a^n + b^n + c^n$.

C3. (Iran 2013). Do there exist natural numbers a, b and c such that $a^2 + b^2 + c^2$ is divisible by $2013(ab + bc + ca)$?

C4. (ISL 2018). Let $f : \{1, 2, 3, \dots\} \to \{2, 3, \dots\}$ be a function such that $f(m + n)|f(m) + f(n)$ for all pairs m, n of positive integers. Prove that there exists a positive integer $c > 1$ which divides all values of f.

C5. (ISL 2018). Let $n \geq 2018$ be an integer, and let $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ be pairwise distinct positive integers not exceeding $5n$. Suppose that the sequence

$$\frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_n}{b_n}$$

forms an arithmetic progression. Prove that the terms of the sequence are equal.

C6. (IMO 2016). Let $P = A_1A_2 \cdots A_k$ be a convex polygon in the plane. The vertices $A_1, A_2, \dots, A_k$ have integral coordinates and lie on a circle. Let S be the area of P. An odd positive integer n is given such that the squares of the side lengths of P are integers divisible by n. Prove that $2S$ is an integer divisible by n.

C7. (ISL 2011). Let $P(x)$ and $Q(x)$ be two polynomials with integer coefficients, such that no nonconstant polynomial with rational coefficients divides both $P(x)$ and $Q(x)$. Suppose that for every positive integer n the integers $P(n)$ and $Q(n)$ are positive, and $2^{Q(n)} - 1$ divides $3^{P(n)} - 1$. Prove that $Q(x)$ is a constant polynomial.

C8. (Serbia 2017). Let k be a positive integer and let n be the smallest number with exactly k divisors. Given n is a cube, is it possible that k is divisible by a prime factor of the form $3j + 2$?

C9. (ISL 2014). For every real number x, let $||x||$ denote the distance between x and the nearest integer. Prove that for every pair (a, b) of positive integers there exist an odd prime p and a positive integer k satisfying

$$\left|\left|\frac{a}{p^k}\right|\right| + \left|\left|\frac{b}{p^k}\right|\right| + \left|\left|\frac{a+b}{p^k}\right|\right| = 1.$$

C10. (Poland 2017). Integers $a_1, a_2, \dots, a_n$ satisfy

$$1 < a_1 < a_2 < \ldots < a_n < 2a_1.$$

If m is the number of distinct prime factors of $a_1a_2 \cdots a_n$, then prove that

$$(a_1a_2 \cdots a_n)^{m-1} \geq (n!)^m.$$

C11. (China 2010). Let $k > 1$ be an integer, set $n = 2^{k+1}$. Prove that for any positive integers $a_1 < a_2 < \cdots < a_n$, the number $\prod_{1 \leq i < j \leq n}(a_i + a_j)$ has at least $k + 1$ different prime divisors.