Some Techniques to Solve Diophantine Equations

- Parity (Even or Odd) Contradiction
- Factoring Equations
- Bounding (Using Inequalities)
- Modular Contradiction
- Infinite Descent (Minimality Contradiction)
- Vieta Jumping (Minimality Contradiction)

Divisibility Rules

Let x, y, z be integers.

- *If $z|x, y$, then $z|ax + by$ for any integers a, b (possibly negative).*
- *If $x|y$, then either $y = 0$, or $|x| \leq |y|$.*
- *If $x|y$, and $y|x$, then $x = \pm y$, i.e., $|x| = |y|$.*
- *If $x|yz$ and $gcd(x, y) = 1$, then $x|z$.*
- *If p is a prime and $0 < x < p$, then $\binom{p}{x}$ is divisible by p.*

Two Useful Factorization Formulae

If n is a positive integer, then

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$

If n is a positive odd number, then

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1})$$

Division Algorithm

For every integer pair a, b, there exists distinct integer quotient and remainders, q and r, that satisfy

$$a = bq + r, 0 \leq r < b$$

Euclidean Algorithm

For two natural numbers $a, b, a > b$, to find $gcd(a, b)$, we use division algorithm repeatedly

$$a = bq_1 + r_1$$
$$b = r_1q_2 + r_2$$
$$r_1 = r_2q_3 + r_3$$
$$\dots$$
$$r_{n-2} = r_{n-1}q_n + r_n$$
$$r_{n-1} = r_nq_{n+1}$$

We have $gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_{n-1}, r_n) = r_n$

If $a(x) = b(x)q(x) + r(x)$ *with* $deg(r(x)) < deg(b(x))$, *then*

$$gcd\big(a(x), b(x)\big) = gcd\ (b(x), r(x))$$

Fundamental Theorem of Arithmetic

Every integer $n \geq 2$ *has a unique prime factorization.*

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

where $p_1, \dots, p_k$ *are distinct primes and* $\alpha_1, \dots, \alpha_k$ *are positive integers.*

Bezout's Identity

For natural numbers a, b, *there exist* $x, y \in \mathbb{Z}$ *such that* $ax + by = gcd\ (a, b)$.

General Bezout's Identity

For integers $a_1, a_2, \dots, a_n$, *there exist* $x_1, x_2, \dots, x_n \in \mathbb{Z}$ *such that*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = \sum_{i=1}^{n} a_ix_i = gcd\ (a_1, a_2, \dots, a_n)$$

GCD and LCM

For natural numbers, a, m, n,

- $gcd(a^m - 1, a^n - 1) = a^{gcd(m,n)} - 1$
- $gcd(a, b)\ lcm[a, b] = ab$

Let the prime factorizations of two integers a, b *be*

$$a = p_1^{e_1}p_2^{e_2} \dots p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i} = \prod p_k^{e_k}$$

$$b = p_1^{f_1}p_2^{f_2} \dots p_k^{f_k} = \prod_{i=1}^{k} p_i^{f_i} = \prod p_k^{f_k}$$

The exponents above can be zero and the $p_i{}'s$ *are distinct. Then,*

$$gcd(a, b) = p_1^{min\ (e_1, f_1)} p_2^{min\ (e_2, f_2)} \dots p_k^{\min(e_k, f_k)}$$

$$lcm[a, b] = p_1^{max\ (e_1, f_1)} p_2^{max(e_2, f_2)} \dots p_k^{max\ (e_k, f_k)}$$

Let x, y be integers, for every prime p, we have

$$v_p(\gcd(x, y)) = \min\{v_p(x), v_p(y)\}$$

$$v_p(\text{lcm}[x, y]) = \max\{v_p[x], v_p[y]\}$$

Four Number Lemma

Let a, b, c and d be positive integers such that $ad = bc$. There exist positive integers p, q, u, v such that

$$a = pu, b = qu, c = pv, d = qv.$$

Hence, $a + b + c + d$ is not a prime number.

Number and Sum of Divisors

Let $n \in \mathbb{N}$ such that its prime factorization is

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Then, the number of divisors of n,

$$d(n) = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k)$$

Note. The function $d(n)$ is odd if and only if n is a square.

Then, the sum of divisors of n,

$$\sigma(n) = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\right) \dots \left(\sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k}\right) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right) \dots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right)$$

Properties of Modulus

Let a, b and m be integers, with $m \neq 0$. We say that a and b are congruent modulo m, denoted by

$$a \equiv b (mod\ m)$$

if $m \mid a - b$.

1. *Reflexivity: $a \equiv a (mod\ m)$*
2. *Transitivity: If $a \equiv b (mod\ m)$ and $b \equiv c (mod\ m)$, then $a \equiv c (mod\ m)$*
3. *Symmetry: If $a \equiv b (mod\ m)$, then $b \equiv a (mod\ m)$*
4. *Addition: If $a \equiv b (mod\ m)$ and $c \equiv d (mod\ m)$, then $a + c \equiv b + d (mod\ m)$ and $a - c \equiv b - d (mod\ m)$.*
5. *If $a \equiv b (mod\ m)$, then for any integer k, $ka \equiv kb (mod\ m)$.*
6. *Multiplication: If $a \equiv b (mod\ m)$ and $c \equiv d (mod\ m)$, then $ac \equiv bd (mod\ m)$*
   In general, if $a_i \equiv b_i (mod\ m), i = 1, \dots, k$ then $a_1 \dots a_k \equiv b_1 \dots b_k (mod\ m)$
   In particular, if $a \equiv b (mod\ m)$, then for any positive integer k, $a^k \equiv b^k (mod\ m)$.
7. *We have $a \equiv b (mod\ m_i), i = 1, \dots, k$ if and only if $a \equiv b\big(mod\ lcm(m_1, \dots, m_k)\big)$*
   In particular, if $m_1, \dots, m_k$ are pairwise relatively prime, then $a \equiv b (mod\ m_i), i = 1, \dots, k$ if and only if $a \equiv b (mod\ m_1 \dots m_k)$.
8. *Division: If $ac \equiv bc (mod\ m)$, then $a \equiv b \left(mod\ \frac{m}{\gcd(m,c)}\right)$*
   In particular, if $ac \equiv bc (mod\ m)$, $\gcd(c, m) = 1$, then $a \equiv b (mod\ m)$

9. *If* $a \equiv b(mod\ m)$, *and* $d \mid m$, *then* $a \equiv b\ (mod\ d)$.
10. *If* $a \equiv b(mod\ m)$ *and* $d \neq 0$, *then* $da \equiv db\ (mod\ dm)$.

Freshman's Dream

Let a, b be integers and p be a prime. Then

$$(a+b)^p \equiv a^p + b^p\ (mod\ p)$$

Modular Contradictions

Let n *be an integer. Then*

1. $n^2 \equiv 0\ or\ 1\ (mod\ 3)$
2. $n^2 \equiv 0\ or\ 1\ (mod\ 4)$
3. $n^2 \equiv 0\ or \pm 1\ (mod\ 5)$
4. $n^2 \equiv 0\ or\ 1\ or\ 4\ (mod\ 8)\ or\ odd^2 \equiv 1(mod\ 8)$
5. $n^3 \equiv 0\ or \pm 1\ (mod\ 7)$
6. $n^3 \equiv 0\ or \pm 1\ (mod\ 9)$
7. $n^4 \equiv 0\ or\ 1\ (mod\ 16)$

Fermat's Little Theorem

Let a *be any number relatively prime to a prime* p. *Then*

$$a^{p-1} \equiv 1(mod\ p).$$

Alternatively,

Let a *be any number. Then*

$$a^p \equiv a\ (mod\ p)$$

Euler's Totient Theorem

Let a *be any number relatively prime to* n. *Then*

$$a^{\phi(n)} \equiv 1(mod\ n)$$

Euler's Totient Function

Let $n \in \mathbb{N}$ *such that its prime factorization is*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Then, the number of positive integers less than n *that are coprime to* n *are*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$
$$= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_k^{\alpha_k - 1} \cdot (p_1 - 1)(p_2 - 1)\dots(p_k - 1)$$

Gauss

For any positive integer n, we have

$$\sum_{d \mid n} \phi(d) = n.$$

For instance, if $n = 10$, then $\phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10$

General Inverses

Let $n \geq 2$ be any positive integer. Then every number with $gcd(a, n) = 1$ has an inverse, that is a number x such that

$$ax \equiv 1\ (mod\ n).$$

Inverses add and multiply like fractions

Let $b, d \not\equiv 0\ (mod\ p)$. Then for any a, c, we have

$$\frac{a}{b} + \frac{c}{d} \equiv a \cdot b^{-1} + c \cdot d^{-1} \equiv (ad + bc) \cdot (bd)^{-1} \equiv \frac{ad + bc}{bd}\ (mod\ p)$$
$$\frac{a}{b} \cdot \frac{c}{d} \equiv (a \cdot b^{-1}) \cdot (c \cdot d^{-1}) \equiv (ac) \cdot (bd)^{-1} \equiv \frac{ac}{bd}\ (mod\ p)$$

just like normal fractions.

Chinese Remainder Theorem

The system of linear congruences

$$x \equiv a_1 (mod\ b_1)$$
$$x \equiv a_2 (mod\ b_2)$$
$$\dots$$
$$x \equiv a_n (mod\ b_n),$$

where $b_1, b_2, \dots, b_n$ are pairwise relatively prime (aka $\gcd(b_i, b_j) = 1$ iff $i \neq j$) has one distinct solution for x modulo $b_1 b_2 \dots b_n$.

Properties of Floor and Ceiling Functions

For a real number x, there is a unique integer n such that $n \leq x < n + 1$.

We say that n is the greatest integer less than or equal to x.

$$n = \lfloor x \rfloor$$

The difference $x - \lfloor x \rfloor$ is called the fractional part of x and is denoted by $\{x\}$.

$$\{x\} = x - \lfloor x \rfloor$$

The least integer greater than or equal to x is called the ceiling of x and is denoted by $\lceil x \rceil$.

If x is an integer, then $\lfloor x \rfloor = \lceil x \rceil = x, \{x\} = 0$.

If x is not an integer, then $\lceil x \rceil = \lfloor x \rfloor + 1$

1. *If a and b are integers with $b > 0$, and q is the quotient and r is the remainder when a is divided by b, then $q = \left\lfloor \frac{b}{a} \right\rfloor$ and $r = \left\{ \frac{a}{b} \right\} \cdot b$.*
2. *For any real number x and any integer n, $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ and $\lceil x \rceil + n = \lceil x \rceil + n$.*
3. *If x is an integer then $\lfloor x \rfloor + \lfloor -x \rfloor = 0$; if x is not an integer, then $\lfloor x \rfloor + \lfloor -x \rfloor = -1$.*
   If x is an integer then $\lceil x \rceil + \lceil -x \rceil = 0$; if x is not an integer, then $\lceil x \rceil + \lceil -x \rceil = 1$.
   If x is an integer then $\{x\} + \{-x\} = 0$; if x is not an integer, then $\{x\} + \{-x\} = 1$.
4. *The floor function is nondecreasing; that is for $x \le y$, $\lfloor x \rfloor \le \lfloor y \rfloor$.*
5. *$\left\lfloor x + \frac{1}{2} \right\rfloor$ rounds x to its nearest integer.*
6. $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$
7. *$\lfloor x \rfloor \cdot \lfloor y \rfloor \le \lfloor xy \rfloor$ for non-negative real numbers x and y.*
8. *For any positive real number x and any positive integer n the number of positive multiples of n not exceeding x is $\left\lfloor \frac{x}{n} \right\rfloor$.*
9. *For any real number x and any positive integer n,*

$$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor.$$

Hermite Identity

Let x be a real number, and let n be a positive integer. Then

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor$$

Wilson's Theorem

Let p be a prime. Then

$$(p-1)! \equiv -1 \ (mod\ p)$$

Alternatively, more generally,

For any integer n, we have

$$(n-1)! \equiv -1 \ (mod\ n)$$

if and only if n is a prime.

Fermat's Christmas Theorem

Let p be a prime. Then, there exists an x with $x^2 \equiv -1 (mod\ p)$

if and only if $p = 2$ or $p \equiv 1 (mod\ 4)$.

Order

Let p be a prime and $a \not\equiv 0 \ (mod\ p)$. Then the order of a modulo p is defined to be the smallest positive integer n such that $a^n \equiv 1 (mod\ p)$.

Fundamental Theorem of Orders

For a prime p and any integer $a \neq 0 \ (mod\ p)$, we have

$$a^m \equiv 1 \ (mod\ p) \Leftrightarrow ord_p a \mid m.$$

For relatively prime positive integers a and m,

$$order_m a \mid \phi(m)$$

Primitive Roots

Let p be a prime. Then a residue $g \neq 1$ is called primitive root mod p if g has order $(p-1)$ mod p.

$$g^{p-1} \equiv 1 \ (mod\ p)$$

Primitive Roots Generate all Non-zero Residues

Let g be a primitive root modulo p. Then

$$\{g^1, g^2, g^3, \dots, g^{p-1}\} \equiv \{1,2,3,\dots,p-1\} \ (mod\ p)$$

Primitive Roots Always Exists modulo p

Let $p > 2$ be a prime. Then there always exists a primitive root modulo p.

p-adic Valuation/ Largest Exponent

Let p be a prime and n be an integer. Then the p-adic valuation of n is defined to be the largest integer t such that $p^t \mid n$.

If we let $2 = p_1 < p_2 < p_3 < \cdots$ be all the primes, then we can write any integer n as

$$n = \prod_{i \geq 0} p_i^{v_{p_i}(n)} = p_1^{v_{p_1}(n)} p_2^{v_{p_2}(n)} \dots$$

Note.

- *By convention, $v_p(0) = +\infty$*
- *v_p can be positive, 0 or even negative. E.g., $v_7\left(\frac{49}{10}\right) = 2, v_5\left(\frac{20}{15}\right) = 0, v_2\left(\frac{3}{4}\right) = -2$*

Arithmetic Properties in p-adic Valuation

Let x, y be integers, $n \in \mathbb{N}$, and p be a prime.

1. (Divisibility) $x \mid y \Leftrightarrow v_p(x) \leq v_p(y)$ *for all primes p.*
2. *(Product)* $v_p(xy) = v_p(x) + v_p(y)$.
3. *(Exponentiation)* $v_p(x^n) = n v_p(x)$.
4. *(Quotient)* $v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y)$
5. *(Sum)* $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$, *equality holds if $v_p(x) \neq v_p(y)$.*

   i.e., if $v_p(x) > v_p(y)$ then $v_p(x+y) = v_p(y)$

6. *If* $p^n < x < p^{n+1}$, *then* $v_p(x) = n = \lfloor \log_p x \rfloor$.

Legendre's Formula

For all positive integers n *and positive primes* p, *we have*

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

$$v_p(n!) = \frac{n - s_p(n)}{p - 1}$$

Where, $s_p(n)$ *denotes the sum of the digits of* n *in base p.*

Lifting the exponent/ LTE

Let $p > 2$ be a prime and $a, b \in \mathbb{Z}$ be coprime to p such that $p \mid a - b$. Suppose n is a positive integer.

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

Note. Three particular conditions must be satisfied.

1. p must be odd. i.e., $p \neq 2$.
2. $\gcd(p, a) = \gcd(p, b) = 1$. i.e., $p \dagger a, b$.
3. $p \mid a - b$, i.e., $v_p(a - b) \neq 0$

Alternatively,

Let $p > 2$ be a prime and $a, b \in \mathbb{Z}$ be coprime to p such that $p \mid a + b$. Suppose n is an odd positive integer.

$$v_p(a^n + b^n) = v_p(a + b) + v_p(n)$$

Sad case when $p = 2$/ LTE for $p = 2$

Let x, y be odd integers such that $2 \mid x - y$. Let n be an even integer. Then

$$v_2(x^n - y^n) = v_2(x^2 - y^2) + v_2\left(\frac{n}{2}\right) = v_2(x - y) + v_2(x + y) + v_2(n) - 1$$