Number Theory

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$.

a divides b is same as

a is a factor or divisor of b is same as

b is a multiple of a.

Notations: $a|b$ for a divides b.

$a \nmid b$ for a does not divide b.

Examples: $3|6$, $2|-4$, $5|-5$.

Number Theory

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$.

a divides b is same as

a is a factor or divisor of b is same as

b is a multiple of a.

Notations: $a|b$ for a divides b.

$a \nmid b$ for a does not divide b.

Examples: $3|6$, $2|-4$, $5|-5$.

Theorem

Let a, b, c be integers, where $a \neq 0$. Then

i. if $a|b$ and $a|c$, then $a|(b+c)$;

ii. if $a|b$, then $a|bc$ for all integers c;

iii. if $a|b$ and $b|c$, then $a|c$. (transitive property of $|$)

Exercise: Write down a C program to find multiplication of two integers using only addition operation. Can you modify it to two multiply two rational numbers with finite decimal representation.

Corollary

If a, b, c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|bx + cy$ whenever $x, y \in \mathbb{Z}$.

Corollary

If a, b, c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|bx + cy$ whenever $x, y \in \mathbb{Z}$.

Theorem (Division Algorithm)

Let $a \in \mathbb{Z}$ and b a positive integer. Then there exists unique integers q, r, such that

$$a = bq + r \quad \text{with } 0 \leq r < b.$$

Exercise: Write down a C program to find q, r with input a, b.

Proof.

We use $\mathbb{N}$ is a well ordered set (Poset with every nonempty subset has a least element).

Then

$$A = \{a - bq | a - bq \geq 0, q \in \mathbb{Z}\} \neq \phi$$

Let $r_0 = a - bq_0$ be a least element of above set. (*)

Claim: $0 \leq r_0 < b$.

If $r_0 \geq b$, then $r_0 - b \in A$, contradiction to eq^n (*).

Uniqueness: Suppose $bq_1 + r_1 = a = bq_2 + r_2$ with $0 \leq r_1, r_2 < b$.

$\Rightarrow (q_1 - q_2)b = r_2 - r_1$

$\Rightarrow r_1 = r_2$

Division Algorithm: Given $a \in \mathbb{Z}, b \in \mathbb{N}$,

$$a = bq + r \text{ with } 0 \leq r < b.$$

$a =$ dividend, $b =$ divisor, $q =$ quotient, $r =$ remainder.
For $a = -5, d = 3$, $-5 = 3(-2) + 1$, $q = -2, r = 1$.

Definition

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. We say a is congruent to b modulo n ($a \equiv b \mod n$) if

$$n|(a-b)$$

In division algorithm, $a \equiv r \mod b$.

$$a \equiv b \mod n \Leftrightarrow a = b + qn$$

Let $n \in \mathbb{N}$, $a \equiv b \mod n$ and $c \equiv d \mod n$. Then

$$a + c \equiv b + d \mod n$$
$$ac \equiv bd \mod n$$
$$a^m \equiv b^m \mod n$$

Find $5^{25} \bmod (3)$.

Representation of Integers

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

Binary Expansion : b=2
Octal Expansion : b=8
Hexa decimal Expansion : b=16
Decimal Expansion : b=10

$$
\begin{aligned}
(1\ 0101\ 1111)_2 = {} & 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 \\
& + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 351.
\end{aligned}
$$

$$(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8 + 6 = 3598.$$

$$(2AE0B)_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16 + 11 = 175627.$$

Find the hexadecimal expansion of $(177130)_{10}$.

Solution: First divide 177130 by 16 to obtain

$$177130 = 16 \cdot 11070 + 10.$$

Successively dividing quotients by 16 gives

$$\begin{aligned} 11070 &= 16 \cdot 691 + 14, \\ 691 &= 16 \cdot 43 + 3, \\ 43 &= 16 \cdot 2 + 11, \\ 2 &= 16 \cdot 0 + 2. \end{aligned}$$

The successive remainders that we have found, 10, 14, 3, 11, 2, give us the digits from the right to the left of 177130 in the hexadecimal (base 16) expansion of $(177130)_{10}$. It follows that

$$(177130)_{10} = (2B3EA)_{16}.$$

ALGORITHM 2 Addition of Integers.

procedure *add*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}a_{n-2}\dots a_1a_0)_2$
and $(b_{n-1}b_{n-2}\dots b_1b_0)_2$, respectively}
$c := 0$
for $j := 0$ **to** $n - 1$
    $d := \lfloor (a_j + b_j + c)/2 \rfloor$
    $s_j := a_j + b_j + c - 2d$
    $c := d$
$s_n := c$
return $(s_0, s_1, \dots, s_n)$ {the binary expansion of the sum is $(s_ns_{n-1}\dots s_0)_2$}

ALGORITHM 3 Multiplication of Integers.

procedure *multiply*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}a_{n-2}\ldots a_1a_0)_2$
and $(b_{n-1}b_{n-2}\ldots b_1b_0)_2$, respectively}
for $j := 0$ **to** $n-1$
  if $b_j = 1$ **then** $c_j := a$ shifted j places
  else $c_j := 0$
{$c_0, c_1, \ldots, c_{n-1}$ are the partial products}
$p := 0$
for $j := 0$ **to** $n-1$
  $p := p + c_j$
return p {p is the value of ab}

Prime numbers and GCD

$p > 1$ a natural number is said to be prime if it's positive divisors are only 1 and p.
If $n > 1$ is not prime then it is called composite number.
Question: How many are prime numbers?
List all prime numbers: 2, 3, 5, 7, $\cdots$

Theorem

There exists infinitely many prime numbers.

Prime numbers and GCD

$p > 1$ a natural number is said to be prime if it's positive divisors are only 1 and p.
If $n > 1$ is not prime then it is called composite number.
Question: How many are prime numbers?
List all prime numbers: 2, 3, 5, 7, $\cdots$

Theorem

There exists infinitely many prime numbers.

Theorem (Fundamental Theorem of Arithmetic)

Every natural number $n > 1$ can be written uniquely as the product of primes upto the order of prime factors.

$100 = 2 * 2 * 5 * 5 = 2 * 5 * 5 * 2$
Proof by strong form of mathematical induction:
Theorem is true for $n = 2$.
Assume theorem is true for all $n \leq k$. (*)
If $k + 1$ is prime then we are done.
If $k + 1$ is not a prime, then $\exists k \geq a, b > 1$ such that $k + 1 = a * b$.
By $(*)$ a and b both are product of primes in unique way, hence $k + 1$.

Theorem

If n is a composite number > 1, then n has a prime divisor $\leq \sqrt{n}$.

Proof: Suppose $n = ab$, where $1 < a, b$.
Claim: Either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
Suppose not, i.e., $a > \sqrt{n}, b > \sqrt{n}$.
$\Rightarrow n = a * b > \sqrt{n} * \sqrt{n} = n$, a contradiction.
If $a \leq \sqrt{n}$ then any prime divisor of a is $\leq \sqrt{n}$ and divisor of n. $\square$

Question: How to find prime factorization of a natural number?
Question: Give an injective function $f : \mathbb{N} \to \mathbb{N}$ such that $f(n)$ is a prime number.

The largest known prime number is $2^{8,25,89,933} - 1$(Patrick Laroche).

Prime numbers of the form $2^p - 1$ are called Mersenne primes.

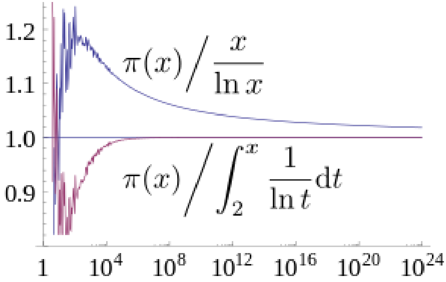
Agrawal-Kayal-Saxena primality test: Deterministic primality-proving polynomial time algorithm in 2002, in a paper titled "PRIMES is in P".

Distribution of Primes

Question: Given $n \in \mathbb{N}$, how many prime numbers are $\leq n$?

Theorem (Prime Number Theorem)

The ratio of number of primes $\leq n$ and $\frac{n}{\log_e n}$ approaches 1 as n grows or tends to ∞.



Goldbach's conjecture [1742] Every even integer > 2 is a sum of two primes.
Proved for all integers less than 4×10^{18}.

Goldbach's conjecture [1742] Every even integer > 2 is a sum of two primes.
Proved for all integers less than 4×10^{18}.
Twin prime conjecture: There are infinitely many pairs $(p, p+2)$ such that $p, p+2$ are primes.

Theorem (Yitang Zhang, 2013)

For some integer $N <$ 70 million, there are infinitely many pairs of primes $(p, p+N)$.

Maynard, Tao improved N to 246.

Mersenne primes: prime numbers of the form $2^p - 1$, where p is also prime.

Great Internet Mersenne Prime Search (GIMPS) Largest Mersenne prime known is $2^{82,589,933} - 1$(2018, Patrick Laroche).

The Lucas–Lehmer test works as follows. Let $M_p = 2^p - 1$ be the Mersenne number to test with p an odd prime. The primality of p can be efficiently checked with a simple algorithm like trial division since p is exponentially smaller than M_p. Define a sequence $\{s_i\}$ as

$$s_i = 4 \ if \ \ i = 0;$$

$$s_i = s_{i-1}^2 - 2 \ \text{ otherwise.}$$

The first few terms of this sequence are 4, 14, 194, 37634,... Then M_p is prime if and only if $s_{p-2} \equiv 0(\bmod M_p)$.

Definition

Let $a, b \in \mathbb{Z} \setminus \{0\}$. The gcd(a,b)= largest integer d such that $d|a$ and $d|b$.

Let $a, b \in \mathbb{N}$. The lcm(a,b)= smallest positive integer l that is divisible by both a and b.

The integers a, b are said to be relatively prime if gcd(a,b)=1.

The integers $a_1, a_2, \ldots, a_n$ are said to be pairwise relatively prime if gcd(a_i, a_j)=1 for $i \neq j$.

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, \;\; b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

gcd(a,b)= $p_1^{min\{\alpha_1,\beta_1\}} p_2^{min\{\alpha_2,\beta_2\}} \cdots p_n^{min\{\alpha_n,\beta_n\}}$

lcm(a,b)= $p_1^{max\{\alpha_1,\beta_1\}} p_2^{max\{\alpha_2,\beta_2\}} \cdots p_n^{max\{\alpha_n,\beta_n\}}$

Euclidean Algorithm: If $a \equiv r$ mod b then

$$\text{gcd } (a, b) = \text{gcd } (b, r)$$

$$42=30(1)+12$$
$$30=12(2)+6$$
$$12=6(2)+0$$

Hence gcd(42, 30)=6: last non zero remainder in successive division algorithm.

6=30-12(2)
=30-[42-30(1)](2)
=30-42(2)+30(2)
6=30(3)+42(-2)

Theorem (BEZOUT'S THEOREM)

Let a, b be two positive integers and $d = gcd\,(a, b)$. Then there exists $x, y \in \mathbb{Z}$ such that $d = ax + by$.

These x, y can be found using Euclidean Algorithm.
gcd(252, 198)=18.
252=1*198+54
198=3*54+36
54=1*36+18
36=2*18

18=54-1*36=54-1*(198-3*54)=4*54-1*198=4*(252-1*198)-1*198=4*252-5*198

Lemma

Let gcd(a, b)=1. Then

1. a and b do not have any common prime in their factorization.

2. If $a|c$ and $b|c$ then $ab|c$.

3. If $b|ac$ then $b|c$

Lemma

If p is a prime and p divides $a_1 a_2 \cdots a_n$, where each a_i is an integer, then p divides a_i for some i.

Theorem

Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc (mod\ m)$ and $gcd(c, m) = 1$, then $a \equiv b (mod\ m)$.

Remark: $gcd(c, m) = 1$ is an important condition, without it theorem does not hold true.

Question: Does there exists x such that $3x \equiv 1 \text{ mod}(5)$?
Let $a, b, m \in \mathbb{Z}$. Then there exists $x \in \mathbb{Z}$ such that $ax \equiv b \text{ mod } m$ if and only if $\gcd(a, m) = 1$.
Question Does there exists $x \in \mathbb{Z}$ such that $x \equiv 1 \text{ mod } 3$ and $x \equiv 2 \text{ mod } 5$?
YES, by Chinese Remainder Theorem, since gcd(3,5)=1.

Theorem (Chinese Remainder Theorem)

Let gcd(a,b)=1 and $0 \leq r < a$ and $0 \leq s < b$. Then there exists unique $x \in \mathbb{Z}$ such that
$0 \leq x < ab$
$x \equiv r \ mod(a)$
$x \equiv s \ mod(b)$.

Let M=ab and x_1, y_1 be such that $ax_1 + by_1 = 1$.
Take $x = s.ax_1 + r.by_1 mod(ab)$
In above example a=3, b=5, r=1, s=2.
3*(2)+5*(-1)=1 which implies $x_1 = 2, x_2 = -1$.
x=2*3*(2)+1*5*(-1) (mod 15)= 7.

THE CHINESE REMAINDER THEOREM Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1},\\
x &\equiv a_2 \pmod{m_2},\\
&\cdot\\
&\cdot\\
&\cdot\\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \le x < m$, and all other solutions are congruent modulo m to this solution.)

Proof: To establish this theorem, we need to show that a solution exists and that it is unique modulo m. We will show that a solution exists by describing a way to construct this solution; showing that the solution is unique modulo m is Exercise 30.

To construct a simultaneous solution, first let

$$M_k = m/m_k$$

for $k = 1, 2, \ldots, n$. That is, M_k is the product of the moduli except for m_k. Because m_i and m_k have no common factors greater than 1 when $i \neq k$, it follows that $\gcd(m_k, M_k) = 1$. Consequently, by Theorem 1, we know that there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

To construct a simultaneous solution, form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

Theorem (Fermat's Little Theorem)

Let p be a prime and a not divisible by p. Then

$$a^{p-1} \equiv 1 \ mod \ p$$

Find $7^{1001}(mod\ 11)$.
$7^{10} \equiv 1(mod\ 11)$ and 1001=10(100)+1.
$7^{1001}(mod\ 11) = 7^{10*100+1}(mod\ 11) = (7^{10})^{100} * 7^1(mod\ 11) = 1 * 7 = 7$.

Definition

The value of the Euler ϕ-function at the positive integer n is defined to be the number of positive integers less than or equal to n that are relatively prime to n. (e.g. $\phi(2) = 1, \phi(3) = 2, \phi(4) = 2$.

For prime p, $\phi(p) = p - 1$

Theorem

If gcd(a, n)=1 then $a^{\phi(n)} \equiv 1(mod\ n)$.

Applications of congruences

1. (Hashing function) Suppose you have to store details of employees of a company on a computer. Each employee is given a unique identification number.
   Store given employee's data at i^{th} place if i is congruent to his/her id. number modulo a permissible number n.
2. (Pseudo-random numbers-Linear Congruential Method:) Choose modulus- m, multiplier-a, increment-c and seed-x_0 with $2 \leq a < m, 0 \leq c < m$ and $0 \leq x_0 < m$
   Generate x_n using the formula
   $$x_{n+1} = (ax_n + c) \bmod m.$$
3. Cryptography: Earliest known uses of cryptography was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet. For instance, using this scheme the letter B is sent to E and the letter X is sent to A.

“MEET YOU IN THE PARK” using the Caesar cipher is encrypted as “PHHW BRX LQ WKH SDUN.”
Caesar cipher: Encryption: f(p)= (p+3) mod 26. Decryption: g(p)=(p-3) mod 26.
The RSA Cryptosystem To encrypt messages using a particular key (n,e), we first translate a plaintext message M into sequences of integers.
To do this, we first translate each plaintext letter into a two-digit number, That is, we include an initial zero for the letters A through J, so that A is translated into 00, B into 01, ..., and J into 09. K into 10,...Z into 25. Then, we concatenate these two-digit numbers into strings of digits.
Next, we divide this string into equally sized blocks of 2N digits, where 2N is the largest even number such that the number 2525...25 with 2N digits does not exceed n. (When necessary, we pad the plaintext message with dummy Xs to make the last block the same size as all other blocks.) After these steps, we have translated the plaintext message M into a sequence of integers $m_1, m_2, ..., m_k$ for some integer k.

Encryption proceeds by transforming each block m_i to a ciphertext block c_i. This is done using the function

$$C = M^e (mod\ n)$$

Encrypt the message STOP using the RSA cryptosystem with key (2537,13).

Since $2525 < 2537 < 252525$, we group these numbers into blocks of four digits

$STOP \rightarrow 1819\ 1415$

Encrypt each block using the mapping $C = M^{13} (mod\ 2537)$.

Computations using fast modular multiplication show that $1819^{13} (mod 2537) = 2081$ and $1415^{13} (mod\ 2537) = 2182$.

The encrypted message is 2081 2182.

Since $2537 = 43 * 59$, $\phi(2537) = 42 * 58$ and gcd(13, ϕ(2537))=1, there exists f such that $e.f \equiv 1 (mod\ \phi(2537))$

For Decryption: $D = C^f (mod\ 2537)$

In above case, $f = 937$, using Euclidean Algorithm.

$2081^{937} (mod\ 2537) = 1819$ (Use following site to verify https://planetcalc.com/8326/)

Exercise: Encrypt Following message-"HELP" using key (2537,13).