Number Theory (Part - 2)

P. Sam Johnson

NITK, Surathkal

Overview

We discuss the following in two lectures :

- the prime factorization factorials
- applications of integers which are relatively prime (the integers have no prime factors in common)
- **Stem-Brocot tree:** a mehod to construct the set of all nonnegative fractions m/n with $gcd(m,n) = 1$
- invertible element in the set of integers modulo m (denoted by $\mathcal{Z}$ and a characterization for existence of inverse in $\mathcal{Z}$
- Solving the congruence relation $ax \equiv 1 \ (mod \ \ m)$
- properties of $\phi(n)$, Euler's totient function of n, the number of integers (between 1 and n) which are relatively prime to n
- Chinese remainder theorem to solve a system of linear congruence relations.

We now look at the prime factorization of some interesting highly composite numbers, the **factorials**:

$$n! = 1.2.\ldots.n = \prod_{k=1}^{n} k, \quad \text{integer } n \geq 0.$$

We define 0! is 1 for our convention for an empty product.

For every positive integer n,

$$n! = (n-1)!\ n.$$

And it is the number of permutations (bijective functions from $\{1, 2, \ldots, n\}$ to itseft) of n distinct objects. That is, $n!$ is the number of ways to arrange n things in a row.

We shall prove that $n!$ is plenty big and the factorial function grows exponentially.

$n!^2 = (1.2.\ldots.n)(n.\ldots.2.1) = \prod_{k=1}^{n} k(n+1-k)$. We have

$$n \leq k(n+1-k) \leq \left(\frac{n+1}{2}\right)^2 \qquad (1)$$

because the quadratic polynomial $k(n+1-k)$ has its smallest value at $k = 1$ and its largest value at $k = \frac{n+1}{2}$.

Apply $\prod_{k=1}^{n}$ in (1), we get

$$\prod_{k=1}^{n} n \leq \prod_{k=1}^{n} k(n+1-k) \leq \prod_{k=1}^{n} \left(\frac{n+1}{2}\right)^2.$$

That is,

$$n^{n/2} \leq n! \left(\frac{n+1}{2}\right)^n.$$

Let p be a prime number. We would like to determine the largest power of p that divides $n!$

That is, in $n!$'s unique prime factorization, we want the **exponent of p in $n!$**

We denote this number by $\varepsilon_p(n!)$.

Example

Let $p = 2$ and $n = 10$. Then $\varepsilon_2(10!)$ can be found by summing the numbers that contribute all possible powers of 2.

We mean "an integer m_1" contributes a power of 2 *(say, 2^ℓ) if there are m_1 integers (between 1 and 10) which are divisible by 2^ℓ.*

Since $n = 10$, starting from 1 to 10, possible powers of 2 are $2, 2^2$ and 2^3.

Calculation of $\varepsilon_p(n!)$

Let a and b be positive integers. Then $\lfloor a/b \rfloor$ helps us to know the number of integers (between 1 and a) which are divisible by b.

	1	2	3	4	5	6	7	8	9	10	powers of 2
divisible by 2		$*$		$*$		$*$		$*$		$*$	$5 = \lfloor 10/2 \rfloor$
divisible by 4				$*$				$*$			$2 = \lfloor 10/4 \rfloor$
divisible by 8								$*$			$1 = \lfloor 10/8 \rfloor$
	0	1	0	2	0	1	0	3	0	1	8

That is, the middle of the last row says that the number of appearences of 2 for any integer k between 1 and 10. This is denoted by $\rho(k)$ (called, the **ruler function**). For example, $\rho(1) = 0, \rho(4) = 2, \rho(10) = 1,$

Hence 2^8 divides 10! but 2^9 does not. Note that

$$\varepsilon_2(10!) = \lfloor 10/2 \rfloor + \lfloor 10/4 \rfloor + \lfloor 10/8 \rfloor = 5 + 2 + 1 = 8.$$

For general n, this method gives

$$\varepsilon_2(n!) = \lfloor n/2 \rfloor + \lfloor n/2^2 \rfloor + \lfloor n/2^3 \rfloor + \cdots = \sum_{k \geq 1} \lfloor n/2^k \rfloor.$$

This summand is actually finite, since the summand is zero when $2^k > n$.

Each term is just the floor of half the previous term. This is true for all n because $\lfloor \frac{n}{2^{k+1}} \rfloor = \lfloor \lfloor \frac{n}{2^k} \rfloor / 2 \rfloor$.

Exercise

Prove that $\sum_{k \geq 1} \lfloor \frac{n}{2^k} \rfloor$ *has only* $\lfloor \log n \rfloor$ *non-zero terms.*

When we write the number n in binary representation, we can find easily $\varepsilon_p(n!)$.

For example, $n = 100$, $p = 2$. Then $n = (1100100)_2$.

$$\begin{aligned}
\lfloor 100/2 \rfloor &= (110010)_2 = 50 \\
\lfloor 100/4 \rfloor &= (11001)_2 = 25 \\
\lfloor 100/8 \rfloor &= (1100)_2 = 12 \\
\lfloor 100/16 \rfloor &= (110)_2 = 6 \\
\lfloor 100/32 \rfloor &= (11)_2 = 3 \\
\lfloor 100/64 \rfloor &= (1)_2 = 1
\end{aligned}$$

Therefore $\varepsilon_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$.

We have $n = 100$. Then $n = (1100100)_2$.

Each 1 contributing 2^m to the value of n contributes

$$2^{m-1} + 2^{m-2} + \cdots + 2^0 = 2^m - 1$$

to the value of $\varepsilon_2(n!)$.

For example, the first 1 in 100 (coefficients of 2^2) contributes $2 + 1 = 2^2 - 1$.

The second 1 in 100 (coefficients of 2^5) contributes $2^4 + 2^3 + 2^2 + 2 + 1 = 2^5 - 1$.

The last 1 in 100 (coefficients of 2^6) contributes $2^5 + 2^4 + 2^3 + 2^2 + 2 + 1 = 2^6 - 1$.

Therefore
$\varepsilon_2(n!) = (2^2 - 1) + (2^5 - 1) + (2^6 - 1) = 3 + 31 + 63 + 97.$

Finding $\varepsilon_p(n!)$ for an arbitrary prime p

The binary representation shows us how to derive another formula

$$\varepsilon_p(n!) = n - v_2(n)$$

where $v_2(n)$ is the number of 1's in the binary representation of n.

This simplification works because each 1 that contributes 2^m to the value of n contributes $2^{m-1} + 2^{m-2} + \cdots + 2^0 = 2^m - 1$ to the value of $\varepsilon_2(n!)$.

The following is a generalization of our findings to an arbitrary prime p.

Exercise

Prove that $\varepsilon_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots = \sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor$ *where* p *is a prime number.*

Relatively Prime

When $gcd(m, n) = 1$, the integers m and n **have no prime factors in common** and we say that they are **relatively prime**.

- A fraction m/n is in lowest terms iff $gcd(m, n) = 1$.
- Since we reduce fractions of lowest terms by casting out the largest common factor of numerator and denominator, we get $m/gcd(m, n)$ and $n/gcd(m, n)$ are relatively prime. Hence

$$gcd(km, kn) = k\ gcd(m, n).$$

- When we use the prime exponent representations of numbers, we have
  - $gcd(m, n) = 1 \iff \min\{m_p, n_p\} = 0$ for all p.
  - $gcd(m, n) = 1 \iff m_p n_p = 0$ for all p.

Moreover,

$$gcd(k, m) = 1 = gcd(k, n) \iff gcd(k, mn) = 1.$$

When we use the prime exponent representations of numbers, we have

$$k_p m_p = 0 \text{ and } \; k_p n_p = 0 \iff k_p(m_p + n_p) = 0$$

when m_p and n_p are non-negative.

Beautiful way to construct the set of all nonnegative fractions : **Stem-Brocot tree**

There is a beautiful way to construct the set of all nonnegative fractions m/n with $gcd(m, n) = 1$, called the **Stem-Brocot tree** because it was discovered independently by Moris Stern, a German mathematician, and Achille Brocot, a French clockmaker.

The idea is to start with the two fractions $(\frac{0}{1}, \frac{1}{0})$ and then to repeat the following operation as many times as desired:

Insert $\frac{m+m'}{n+n'}$ between two adjacent fractions $\frac{m}{n}$ and $\frac{m'}{n'}$.

The new fraction $\frac{(m+m')}{(n+n')}$ is called the **mediant** of $\frac{m}{n}$ and $\frac{m'}{n'}$.

Note that the fraction $\frac{1}{0}$ represents a very big integer.

For example, the first step gives us one new entry between $\frac{0}{1}$ and $\frac{1}{0}$,

$$\frac{0}{1}, \frac{1}{1}, \frac{1}{0};$$

and the next gives two more ;

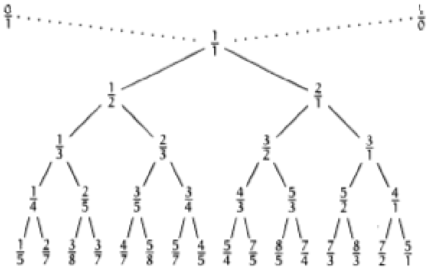
$$\frac{0}{1}, \frac{1}{2}, \frac{1}{1}, \frac{2}{1}, \frac{1}{0}.$$

The next gives four more,

$$\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}, \frac{3}{2}, \frac{2}{1}, \frac{3}{1}, \frac{1}{0};$$

and then we will get $8, 16$, and so on.

The entire array can be regarded as an infinite binary tree structure whose top levels look like this:



Each fraction is $\frac{m+m'}{n+n'}$, where $\frac{m}{n}$ is the **nearest ancestor above to the left**, and $\frac{m'}{n'}$ is the **nearest ancestor above and to the right.** An "ancestor" is a fraction that is reachable by following the braches upward.

'MOD' : The congruence relation

Modular arithmetic is one of the main tools provided by number theory.

The definition $a \equiv b \ (mod \ \ m)$ (can be read "a is congruent to b modulo m") $\iff$ $a - b$ is a multiple of m, makes sense when a, b and m are arbitrary real numbers, but we use the definition with integers only.

Exercise

$a \equiv b \ (mod \ \ m) \iff a \ mod \ \ m = b \ mod \ \ m.$

For example, $9 \equiv -16(mod \ 5)$,

because $9 \ (mod \ 5) = 4 = (-16) \ (mod \ 5)$.

The congruence sign "$\equiv$" looks conveniently like '$=$', because congruences are almost like equations.

For example, congruence is an equivalence relation ; that is, it satisfies the **reflexive law** '$a \equiv a$', the **symmetric law** '$a \equiv b$ implies $b \equiv a$', and the **transitive law** '$a \equiv b$ and $b \equiv c$ implies $a \equiv c$'.

All these properties are easy to prove, because any relation '$\equiv$' that satisfies '$a \equiv b \iff f(a) = f(b)$' for some function f, is an equivalence relation. In our case, $f(x) = x \ (mod \ m)$.

The equivalence relation "$\equiv$ $mod \ m$" splits $\mathbb{Z}$ into m mutually disjoint sets called **residue classes mod** m or **remainder classes mod** m:

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

On $\mathbb{Z}_m$, define addition modulo m and multiplication modulo m as follows :

$$x \oplus y = \begin{cases} x + y & \text{when} \quad 0 \leq x + y < m \\ x + y - m & \text{when} \quad x + y \geq m. \end{cases}$$

and

$$x \otimes x = xy \ (mod \ \ m).$$

Moreover, we can add and subtract congruence elements without losing congruence

$a \equiv b$ and $c \equiv d$ implies $a + c \equiv b + d \ (mod \ \ m)$

$a \equiv b$ and $c \equiv d$ implies $a - c \equiv b - d \ (mod \ \ m)$.

Incidentally, it is not necessary to write '($mod\ m$)' once for every appearance of '$\equiv$' ; if the modulus is constant, we need to name it only once in order to establish the context. This is one of the great conveniences of congruence relation.

When we deal with integers, multiplication works well:

Exercise

Prove that $a \equiv b$ and $c \equiv d$ implies $ac \equiv bd (mod\ m)$.

Repeated application of this multiplication property allows us to take powers: $a \equiv b$ implies $a^n \equiv b^n (mod\ m)$, integers a, b, integer $n \geq 0$.

For example, since $2 \equiv -1 (mod\ 3)$, so $2^n \equiv (-1)^n (mod\ 3)$. This means that $2^n - 1$ is a multiple of 3 iff n is even.

Cancellation property

Combining all these, we have the following :

If $a \equiv b (mod\ \ m)$ and $f(x)$ is any polynomial with integer coefficients, then $f(a) \equiv f(b)(mod\ \ m)$.

Thus, most of the algebraic operations that we customarily do with equations can also be done with congruences. But the operation of division sometimes fails.

If $ad \equiv bd(mod\ \ m)$, we cannot always conclude that $a \equiv b$.

For example, $3.2 \equiv 5.2(mod\ 4)$, but $3 \neq 5$.

When $gcd(d, m) = 1$, the cancellation property holds good : If a, b, d, m are integers and $gcd(d, m) = 1$, then

$$ad \equiv bd\ (mod\ \ m) \iff a \equiv b\ (mod\ \ m).$$

Proof. Since $gcd(d, m) = 1$, there are integers d' and m' such that

$$d'd + m'm = 1. \tag{2}$$

Suppose $ad \equiv bd$. Multiplying both sides of the congruences by d', we get

$$ad'd \equiv bd'd. \tag{3}$$

Since $d'd \equiv 1$ (from the relation (2)), we have $ad'd \equiv a$ and $bd'd \equiv b$, hence $a \equiv b$ (from the relation (3)).

The number d' acts almost like $1/d$ when congruences are considered (mod m).

Therefore we call it the "**inverse of** d **modulo** m".

Invertible element

Let d be a positive integer.

In $\mathbb{Z}_m$, if there exists an integer x' satisfying

$$x \otimes x' \equiv 1 \ (mod \ \ m),$$

we call x' is an **invertible element** (a multiplicative inverse of $x \ mod \ \ m$) and is denoted by x^{-1}.

We can determine all invertible elements in $\mathbb{Z}_m$ with respect to $\otimes \ mod \ \ m$ as follows :

Theorem

Let $x \neq 0$ in $\mathbb{Z}_m$. Then x^{-1} exists iff $gcd(x, m) = 1$.

Proof. Suppose $gcd(x, m) = d > 1$.

Then there are integers x' and m', greater than 1, such that $x = x'd$ and $m = m'd$.

Then $xm' = (x'd)m' = x'(m'd) = x'm$ which is congruent to $0 \pmod{m}$.

Since $xm' \equiv 0 \pmod{m}$, for any integer $m' > 1$, x cannot be invertible.

Conversely, suppose $gcd(x, m) = 1$.

By Euclid's algorithm, find integers x' and m' such that

$$x'x + m'm = 1.$$

Since $x'x \equiv 1 \pmod{m}$, the inverse of x, x^{-1} is nothing but $x' mod\ m$.

This completes the proof.

Let m and n be integers greater than 1. Among all divisors of m and n, only the $gcd(m, n) = d$ has the property that

$$d = m'm + n'n$$

for some integers m' and n'. That is, d is an integer linear combination of m and n.

Euclid's algorithm is the most well-known and effective method of finding m and n.

Example

We calculate $gcd(1072, 147)$ *as follows:*

$$\begin{aligned} gcd(1072, 147) &= gcd(147, 43) = gcd(43, 18) \\ &= gcd(18, 7) = gcd(7, 4) \\ &= gcd(4, 3) = gcd(3, 1) = 1. \end{aligned}$$

Method to find m' and n' so that $m'm + n'n = 1$.

We have the following :

$$\begin{aligned} 1072 &= (147 \times 7) + 43 \\ 147 &= (43 \times 3) + 18 \\ 43 &= (18 \times 2) + 7 \\ 18 &= (7 \times 2) + 4 \\ 7 &= (4 \times 1) + 3 \\ 4 &= (3 \times 1) + 1. \end{aligned}$$

Hence

$$\begin{aligned} 1 &= (4)(1) + (3)(-1) = (4)(1) + (7 - 4 \times 1)(-1) \\ &= (7)(-1) + (4)(2) = (7)(-1) + (18 - 7 \times 2)(2) \\ &= (18)(2) + (7)(-5) = (18)(2) + (43 - 18 \times 2)(-5) \\ &= (43)(-5) + (18)(12) = (43)(-5) + (147 - 43 \times 3)(12) \\ &= (147)(12) + (43)(-41) = (147)(12) + (1072 - 147 \times 7)(-41) \\ &= (1072)(-41) + (147)(299). \end{aligned}$$

Thus $m' = 299$ and $n' = -41$.

Solution of the congruence relation $ax \equiv 1 \ (mod \ m)$

The construction of finding "inverse" is helpful in solving a simple congruence relation : $ax \equiv 1 \ (mod \ m)$.

Here x is nothing but $a^{-1}(mod \ m)$. How to find $a^{-1}(mod \ m)$?

- Find integers x' and m' such that $x'x + m'm = 1$.
- $x'(mod \ m)$ is the required x^{-1}.

Example

Solve $7x \equiv 1(mod \ 25)$.

We have $x' = -7$ and $m' = 2$, so that

$$(-7 \times 7) + (2 \times 25) = gcd(25, 7).$$

Apply mod 25 both sides $-7 \times 7(mod \ 25) \equiv 1$ implies that $7^{-1} = -7(mod \ 25) = 18(mod \ 25)$. Therefore $x = 18$.

Euler's totient function

By the previous theorem, for a fixed integer $m > 1$, the number of invertible elements in $\mathbb{Z}_m$ is same as number of integers (between 1 and m) which are relatively prime to m.

The number is called **Euler's totient function of** m (because Euler was the first person to study it) and is denoted by $\phi(m)$ (read as "phi of m".)

By convention, we have $\phi(1) = 1$. Moreover, $\phi(p) = p - 1$, for any prime p, $\phi(m) < m - 1$, for any composite number m.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12

Theorem

If p is prime, prove that for $\alpha \geq 1$,

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Proof. We have

$$gcd(n, p^\alpha) = 1 \iff p \text{ does not divide } n.$$

The multiples of p in $\{0, 1, 2, \ldots, p^\alpha - 1\}$ are $\{0, p, 2p, \ldots, p^\alpha - p\}$.

Hence there are $p^\alpha - 1$ of them and $\phi(p^\alpha)$ counts what is left:

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Notice that this formula properly gives $\phi(p) = p - 1$ when p is a prime number and $\alpha = 1$.

Multiplicative function

Theorem

Prove that ϕ is a multiplicative function*. That is, if $m, n > 1$ and $gcd(m, n) = 1$, then*

$$\phi(mn) = \phi(m)\phi(n).$$

Moreover, if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ then

$$\phi(n) = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{p_i \backslash n} \left(1 - \frac{1}{p_i}\right).$$

Proof. If $m > 1$ is not a prime power, we can write $n = m_1 m_2$ where $gcd(m_1, m_2) = 1$.

Then the numbers $0 \leq n < m$ can be represented in a residue number system as $(n \ mod \ m_1, n \ mod \ m_2)$. We have

$$gcd(n, m) = 1 \iff gcd(n \ mod \ m_1, m_1) = 1 \ \text{ and } \ gcd(n \ mod m_2, m_2) = 1.$$

Hence, $n \ mod \ m$ is "good" iff $n \ mod \ m_1$ and $n \ mod \ m_2$ are both "good," if we consider relative primality to be virtue.

The total number of good values modulo m can now be computed recursively:

It is $\phi(m_1)\phi(m_2)$, because there are $\phi(m_1)$ good ways to choose the first component $n \ mod \ m_1$ and $\phi(m_1)$ good ways to choose the second component $n \ mod \ m_2$ in the residue representation.

Examples

1. $\phi(100) = \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = 40.$
2. $\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40.$
3. We can find x such that $\phi(x) = 12$ as follows:

$$\begin{aligned} 12 &= 4 \times 3 \\ &= (5^1 - 5^0)(4^1 - 4^0) \\ &= \phi(5 \times 4) = \phi(20) \end{aligned}$$

hence $x = 20$.

Another way to apply division to congruences is to divide the modulus as well as the other numbers:

$$ad \equiv bd \ (mod \ \ md) \iff a \equiv b \ (mod \ \ m)$$

for $d \neq 0$.

This law holds for all real a, b, d, and m, because it depends only on the distributive law $(a \ mod \ \ m) \ d \equiv ad \ (mod \ \ md)$: We have

$$\begin{aligned} a \ (mod \ \ m) = b \ (mod \ \ m) & \iff (a \ mod \ \ m) \ d = (b \ mod \ \ m) \ d \\ & \iff ad \ (mod \ \ md) = bd \ (mod \ \ md). \end{aligned}$$

Moreover, we get a general law that changes the modulus as little as possible : For integers a, b, d, m,

$$ad \equiv bd \ (mod \ \ m) \iff a \equiv b \left(mod \frac{m}{gcd(d,m)} \right).$$

Proof. Find integers d' and m' such that

$$d'd = m'm = gcd(d,m).$$

Multiplying $ad \equiv bd$ by d' gives the congruence

$$a.gcd(d,m) \equiv b.gcd(d,m)(mod \ \ m),$$

which can be divided by $gcd(d,m)$.

The idea of changing the modulus

If we know that $a \equiv b(mod\ \ m)$, then $a \equiv b(mod\ \ d)$, where d is any divisor of m because any multiple of m is a multiple of d.

Moreover, if $a \equiv b$ with respect to two small moduli, say m and n, we can conclude that

$$a \equiv b$$

with respect to the $lcm(m, n)$ (a larger one) :

$$a \equiv b(mod\ \ m) \text{ and } a \equiv b(mod\ \ n) \iff a \equiv b(mod\ lcm(m, n))$$

integers $m, n > 0$ because if $a - b$ is a common multiple of m and n, it is a multiple of $lcm(m, n)$.

For example, if $a \equiv b$ modulo 12 and 18, then $a \equiv b (mod\ 36)$.

Since $lcm(m, n) = mn$ when m and n are relatively prime, we have the following :

$$a \equiv b \ (mod \ \ mn) \iff a \equiv b \ (mod \ \ m) \text{ and } a \equiv b \ (mod \ \ n) \tag{4}$$

if $gcd(m, n) = 1$.

The moduli m and n in (4) can be further decomposed into relatively prime factors until every distinct prime has been isolated. Therefore

$$a \equiv b \ (mod \ \ m) \iff a \equiv b \ (mod \ \ p^{m_p}) \tag{5}$$

if $\prod_p p^{m_p}$ is the prime factorization of m. Thus congruence modulo "powers of primes" are the building blocks for all congruences modulo "integers".

Solving congruence relations

Consider a linear congruence

$$ax \equiv b \ (mod \ \ m) \tag{6}$$

- Does (6) have a solution?
- If there is one solution, can we find all possible solutions of (6)?

If (6) has a soluion, then $\frac{ax-b}{m}$ is an integer, say y.

Hence $ax - my = b$. The problem of finding "x" has become a problem of finding "x" and "y" satisfying $ax - my = b$.

It is observed that if (6) has a solution, then $d = gcd(a, m)$ must divide b, because $d = gcd(a, m)$ divides $ax - my$.

Let d divide b. Then $a = a_1 d, m = m_1 d, b = b_1 d$, and $gcd(a_1, m_1) = 1$. Now

$$\begin{aligned} ax - my &= b \\ a_1 dx - m_1 dy &= b_1 d \\ a_1 x - m_1 y &= b_1 \\ a_1 x &\equiv b_1 \ (mod\ m_1) \quad \text{since } gcd(a_1, m_1) = 1. \end{aligned}$$

By Euclid's algorithm, there are integers α and β such that

$$\begin{aligned} a_1\alpha + m_1\beta &= 1 \\ a_1(b_1\alpha) + m_1(b_1\beta) &= b_1. \end{aligned}$$

Therefore $x = b_1\alpha$ and $y = -b_1\beta$. Reduce mod m if necessary, we have a solution for (6). Hence existence of solution of (6) is answered.

Theorem

Let x_0 be any solution. Then any possible solution of

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

is given by

$$x = x_0 + \left(\frac{m}{d}\right)t,$$

$t = 0, 1, \ldots, d-1$. *These are the only solutions ; the number of such solutions is* d.

Proof. Let x and x' be any two arbitrary solutions :

$$ax \equiv b \ (mod \ \ m) \quad \text{and} \quad ax' \equiv b \ (mod \ \ m).$$

Then $a(x - x') \equiv 0 \ (mod \ \ m)$, hence $\frac{a(x-x')}{m}$ is an integer.

Let $d = gcd(a, m)$. Then $a = a_1 d$ and $m = m_1 d$ for some integers n_1, m_1, so $\frac{a_1(x-x')}{m_1}$ is an integer.

Hence $a_1(x - x') \equiv 0 \ (mod \ n_1)$. Since $gcd(a_1, n_1) = 1$, we can cancel a_1 both sides.

Therefore $x - x' \equiv 0 \ (mod \ n_1)$ which implies that $x - x' \equiv 0 \ (mod \ \frac{n}{d})$.

Thus $x - x' = n_1 t = (\frac{n}{d})t, \quad t = 0, 1, \ldots, d - 1.$

Example

Solve $51x \equiv 34 \ (mod \ 68)$.

Let $a = 51, b = 34, m = 68$. Then $d = gcd(a, m) = 17$. Therefore solution exists since "17 divides 34".

Divide by 17 throughout, we get

$$3x \equiv 2 \ (mod \ 4).$$

By inspection, $x = 2$ is a solution. Therefore $x_0 = 2$.

All other solutions are given by

$$x = x_0 + \frac{68}{17} t, t = 0, 1, \ldots, 16.$$

Hence $x = 2 + 4t, \quad t = 0, 1, \ldots, 16.$

Therefore 17 distinct solutions $\{2, 6, \ldots, 66\}$ exist.

Example

Solve $51x \equiv 33 \ (mod \ 66)$.

Let $a = 51, b = 33, m = 66$. Then
$d = gcd(a, m) = gcd(51, 66) = 3.$

Therefore solution exists since "3 divides 33".

Divide by 3 throughout, we get

$$17x \equiv 11(mod\ 22),$$

so $x = -17^{-1}x11(mod\ 22)$. Using Euclid's algorithm, we get $17^{-1} \equiv -9 \equiv 13$. Hence $x \equiv 11(mod\ 22)$, so $x_0 = 11$.

All solutions are $x = x_0 + (\frac{n}{d})t = 11 + 22t, \quad t = 0, 1, 2$. Therefore $11, 33$ and 55 are the only solutions.

Exercises

Solve the following congruence relations.

1. $117x \equiv 45\ (mod\ 207)$
2. $103x \equiv 79\ (mod\ 199)$.

Chinese remainder theorem (discovered by Sun Tsu in China, about A.D. 350.)

We now consider systems of linear congruences.

Theorem

Let $m_1, m_2, \ldots, m_k$ be given positive integers such that they are all mutually pairwise coprime. Then the following system of congruence has a unique solution modulo M with $M = m_1 m_2 \cdots m_k$:

$$\begin{aligned} x &\equiv r_1 (mod \; m_1) \\ x &\equiv r_2 (mod \; m_2) \\ \vdots \; &\; \vdots \quad \vdots \\ x &\equiv r_k (mod \; m_k). \end{aligned}$$

Proof. Existence. Let $M_i = \frac{m_1 m_2 \cdots m_k}{m_i} = \frac{M}{m_i}, 1 \leq i \leq k$. Then $gcd(M_i, m_i) = 1$. Hence, for each i, there exists y_i such that $M_i y_i \equiv 1 \ (mod \ m_i)$. Let $x = \sum_{i=1}^{k} M_i y_i r_i$. Then $x = \sum_{i=1}^{k} M_i y_i r_i \equiv r_i \ (mod \ m_i)$, for all $1 \leq i \leq k$. Thus x is the desired solution.

Uniqueness: Let x and x' be two solutions. Then $x \equiv r_i \ (mod \ m_i)$ and $x' \equiv r_i \ (mod \ m_i)$ for all $i = 1, 2, \ldots, k$. So $x - x' \equiv 0 \ (mod \ m_i)$ for all $i = 1, 2, \ldots, k$, hence $x - x'$ is divisible by each m_i, $1 \leq i \leq k$.

Since $gcd(m_i, m_j) = 1$, for $i \neq j$, $x - x'$ must be divisible by their product $M = m_1 m_2 \cdots m_k$. Hence $x - x' \equiv 0 \ (mod \ M)$. Thus, in any interval of length M, there exists exactly one solution of the system.

Example

Find least positive integer solution of the following :

$$\begin{aligned} x &\equiv 3 \ (mod \ 4) \\ x &\equiv 2 \ (mod \ 5) \\ x &\equiv 7 \ (mod \ 9). \end{aligned}$$

Let $m_1 = 4, m_2 = 5, m_3 = 9$. Then $M = m_1 m_2 m_3 = 180, M_1 = 45, M_2 = 36, M_3 = 20$. Solving the congruent relations $M_i y_i \equiv 1 \ (mod \ m_i)$, $i = 1, 2, 3$, give $y_1 = 1, y_2 = 1, y_3 = 5$.

Therefore $x = \sum M_i y_i r_i = 907 \ (mod \ 180) = 7 \ (mod \ 180)$. Thus $x = 7 + 180t$, for some integer t.

Exercise

The following problem was posed by Sun Tsu Suan-Ching (4th century AD):
There are certain things whose number is unknown. Repeatedly divided by 3*, the remainder is* 2*; by* 5 *the remainder is* 3*; and by* 7 *the remainder is* 2*. What will be the number?*

Exercise

Find out the smallest number which leaves remainder of 1 *when divided by* $2, 3, 4, 5, 6$ *but divided by* 7 *completely.*

Exercise

Another puzzle with a dramatic element from Brahma-Sphuta-Siddhanta (Brahma's Correct System) by Brahmagupta (born 598 AD):

An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

Exercise

A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

Hint: *We have the following congruence relations:*

$$
\begin{aligned}
x &\equiv 5 \ (mod\ 17) \\
x &\equiv 7 \ (mod\ 16) \\
x &\equiv 0 \ (mod\ 15).
\end{aligned}
$$

Now solve this system.

Some applications

Proposition

Any positive integer n is divisible by 3 iff the sum of digits of n (base 10) is also divisible by 3.

Proof. Let $n = \sum_{i=0}^{\ell} d_i 10^i$, where $d_i \in \{0, 1, \ldots, 9\}$.

$10 \equiv 1 \ (mod \ 3)$

$10^i \equiv 1 \ (mod \ 3)$ $d_i 10^i \equiv d_i \ (mod \ 3)$.

Hence $n = \sum_{i=0}^{\ell} d_i 10^i \equiv \sum_{i=n}^{\ell} d_i \ (mod \ 3)$.

Proposition

Any positive integer n is divisible by 11 iff the following is true : The sum of digits in even position is congruent to the sum of the digits in odd position (mod 11).

Proof. Let $n = \sum_{i=0}^{\ell} d_i 10^i$, where

$$\sum_{i=0}^{\ell} d_{2k} \equiv \sum_{i=0}^{\ell} d_{2k+1} \ (mod\ 11).$$

$10 \equiv -1 \ (mod\ 11)$ $10^i \equiv (-1)^i \ (mod\ 11)$

$$\sum_{i=0}^{\ell} d_i 10^i \equiv \sum_{i=0}^{\infty} d_i (-1)^i \ (mod\ 11).$$

Hence 11 divides n iff $d_0 + d_2 + \cdots \equiv d_2 + d_4 + \cdots \ (mod\ 11)$.

Prime number sieve : a fast type of algorithm for finding primes

A **prime sieve** or **prime number sieve** is a fast type of algorithm for finding primes. There are many prime sieves.

A prime sieve works by creating a list of all integers up to a desired limit and progressively removing composite numbers (which it directly generates) until only primes are left.

This is the most efficient way to obtain a large range of primes; however, to find individual primes, direct primality tests are more efficient.

Furthermore, based on the sieve formalisms, some integer sequences are constructed which they also could be used for generating primes in certain intervals.

Sieve of Eratosthenes

The sieve of Eratosthenes (250s BCE), one of a number of prime number sieves, is a simple, ancient algorithm for finding all prime numbers up to any given limit. It is named after **Eratosthenes of Cyrene**, a Greek mathematician.

It does so by iteratively marking as composite (i.e., not prime) the multiples of each prime, starting with the multiples of 2.

Eratosthenes of Cyrene

Algorithm : Sieve of Eratosthenes

Following is the algorithm to find all the prime numbers less than or equal to a given integer n by Eratosthenes' method:

- Create a list of integers from 2 to n : $\{2, 3, 4, \ldots, n\}$. Initially, let p equal 2, the first prime number.
- Starting from p, count up in increments of p and mark each of these numbers greater than p itself in the list. These numbers will be $2p, 3p, 4p$, etc.; note that some of them may have already been marked.
- Find the first number greater than p in the list that is not marked. If there was no such number, stop. Otherwise, let p now equal this number (which is the next prime), and repeat from step 3.

When the algorithm terminates, all the numbers in the list that are not marked are prime.

The **sieve of Sundaram** is a simple deterministic algorithm for finding all prime numbers up to a specified integer. It was discovered by **Indian mathematician S.P. Sundaram** in 1934.

Theorem

Let $n > 1$ be fixed. Then either n is prrime, or there is a prime p such that $p \backslash n$ and $p \leq \sqrt{n}$.

Proof. Let n be composite, say $n = \ell m$ with $1 < \ell, m < n$.

If both $\ell > \sqrt{n}$ and $m > \sqrt{n}$, then

$$n = \ell m > \sqrt{n}.\sqrt{n} = n.$$

That is, $n > n$, an absurd.

Fermat's Little Theorem

Remark. If we can somehow know that n does not have any divisor (> 1) below $\sqrt{n}$, then surely n is prime. This is the sieve method of tabulating the primes, in use, for long, long time.

Theorem

Given a prime $p > 1$ and any integer $a > 1$, we always have

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

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

Proof. Suppose that $gcd(a, p) = 1$.

Consider the first $(p - 1)$ multiples of a :

$$1a, 2a, 3a, \ldots, (p - 1)a.$$

Claim : These are all distinct *mod* p.

If $k, k' \in \{1, 2, \ldots, p-1\}$ and $ka \equiv ka' \ (mod\ p)$, a and p are coprime, cancel it, we get $k \equiv k' \ (mod\ p)$. This forces $k = k'$.

So these numbers when reduced *mod* p simply give $1, 2, \ldots, p-1$ in a (possibly) difference order.

Hence

$$\begin{aligned} 1.2.3\ldots(p-1) &\equiv 1.a.2.a\ldots(p-1)a \ (mod\ p) \\ a^{(p-1)!} &\equiv (p-1)! \ (mod\ p) \end{aligned}$$

We can cancel $(p-1)!$, hence $a^{p-1} \equiv 1 \ (mod\ p)$.

Euler's theorem

The following result is a generalization of above result, which is useful at present, essence of RSA, crypto-systems.

Theorem (Euler's theorem)

Let a and n be such that, both are greater than 1*, and* $gcd(a, n) = 1$*. Then*

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

Proof. Let $t = \phi(n)$ and denote by $r_1, r_2, \ldots, r_t$ those integers between 1 and n which are coprime with n.

That is, $1 \leq r_i < n$, for all i and $gcd(r_i, n) = 1$. We consider the following t multiples of a: $r_1.a, r_2, a, \ldots, r_t.a$.

Claim: Any two of these are distinct $(mod \ n)$.

If $r_i a \equiv r_j a \ (mod \ \ n)$, simply cancel a since $gcd(a, n) = 1$. Therefore $r_i \equiv r_j \ (mod \ \ n)$.

This forces $r_i = r_j$.

Hence, when reduced $mod \ \ n$, they are all distinct and so, just the numbers $r_1, r_2, \ldots, r_t$ in some other order.

Thus $r_1 a, r_2 a, \ldots, r_t a \equiv r_1 r_2 \ldots r_t \ (mod \ \ n)$.

But all the r_i's are coprime with n, so must be their product. Hence cancel it and get $a^t \equiv 1 \ (mod \ \ n)$ or $a^{\phi(n)} \equiv 1 \ (mod \ \ n)$.

Corollary

Fermat's theorem follows by letting $n = p$, a prime.

Application of Fermat's theorem

Alternate way of finding $a^{-1}(mod\ n)$ if $gcd(a, n) = 1$ is known.

By Fermat's theorem, we have

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

so $a^{\phi(n)-1} \equiv a^{-1}\ (mod\ n)$, since $gcd(a, n) = 1$.

Example : Find 20^{99} $(mod\ 101)$.

Since 101 is prime and $gcd(101, 20) = 1$, by Euler's theorem,

$$20^{100} \equiv 1\ (mod\ 101).$$

Hence

$$20^{99} \equiv 20^{-1}\ (mod\ 101).$$

The problem is reduced to solving the following congruent relation

$$20x \equiv 1\ (mod\ 101).$$

We have discussed earlier a method to solve the above congruent relation. Verifty that $x = 96$ is a solution. Thus

$$20^{99}\ (mod\ 101) = 96.$$

Finding last digit of 27^{982}.

Since

$$27 \equiv 7 \ (mod \ 10)$$

and

$$gcd(10, 7) = 1,$$

$7^{\phi(10)} \equiv 1 \ (mod \ 10)$, so

$$7^4 \equiv 1 \ (mod \ 10).$$

Since

$$27^{982} \equiv 7^{982} \ (mod \ 10),$$

$7^{982} = (7^4)^{245} \times 7^2 = 1 \times 7^2 = 49 \equiv 9 \ (mod \ 10).$

Exercise

Find last 2 digits of 29^{2005}.

Finding x from $39^{2005} \equiv x \ (mod\ 100)$.

Since

$$39^{\phi(100)} \equiv 1 \ (mod\ 100)$$

and

$$\phi(100) = \phi(5^2.2^2) = 40,$$

$39^{40} \equiv 1 \ (mod\ 100)$, by Euler's theorem.

Since $39^{2005} = 39^{2000}.39^5 = (39^{40})^{50}.39^5$,

$$39^{2005} = 39^5 \equiv 99 \ (mod\ 100).$$

Thus

$$x = 99.$$

Wilson's theorem

Theorem

If p is prime, then $(p-1)! \equiv -1 \ (mod \ p)$.

Proof. Since p is prime, $x^2 \equiv 1 \ (mod \ p)$.

Then $(x-1)(x+1) \equiv 0 \ (mod \ p)$.

Since $p \backslash (x-1)$ or $p \backslash (x+1)$, we get $x \equiv 1 \ (mod \ p)$ or $x \equiv -1 \ (mod \ p)$.

Therefore, in the set $\{1, 2, \ldots, p-1\}$, the only solutions are $x = 1$ and $x = p-1$.

Again, stare at the numbers $1, 2, \ldots, p-1$. If $p = 2$, then it is trivial. So let p be odd.

Here, except 1 and $p-1$, pair off each x with its unique inverse $x^{-1} \ (mod \ p)$.

Converse to Wilson is also true.

Hence the product

$$1.2.3.\ldots(p-2)(p-1) = (1)(1)(p-1)(mod\ p) \equiv -1\ (mod\ p).$$

That is, $(p-1)! \equiv -1\ (mod\ p)$.

Theorem

If $(p-1)! \equiv -1\ (mod\ p)$, then p is prime.

Proof. Assume that

$$(n-1)! \equiv -1 (mod\ n). \tag{7}$$

Suppose n is composite, say $1 < d < n$ and $d \backslash n$. Then

$$d \backslash (n-1)! \tag{8}$$

Since $d \backslash n$ and $n \backslash \{(n-1)! + 1\}$,

$$d \backslash \{(n-1)! + 1\}.$$

From (7) and (8), $d \backslash 1$, which gives $d = 1$, a contradiction. Thus n is prime.

Special Numbers : Mersenne numbers

The numbers of the form $2^n - 1$ are called **Mersenne numbers**, denoted by M_n. If $M_p = 2^p - 1$ is prime, it is called **Mersenne prime**.

Theorem

If n is composite, then M_n is composite.

Proof. Let $n = mk$, where $1 < k, m < n$. Then $2^n - 1 = 2^{mk} - 1 = (2^k)^m - 1 = (2^k - 1)(1 + 2^k + \cdots + 2^{(n-1)k})$, a non-trivial factorization.

Convers is not necessarily true. For example, $M_{11} = 2^{11} - 1 = 2047 = 23 \times 87$ is composite whereas 11 is prime.

Conjecture. There exists infinitely many Mersenne primes. The fact that only 43 Mersenne primes are known till date.

Special Numbers : Fermat numbers

Fermat numbers are defined by $f_n = 2^n + 1$.

If f_n is prime, then n must be a power of 2, that is, $n = 2^k$ for some k. Converse need not be true.

Example given by Euler

When $n = 2^5$, f_n is not prime.

Primes of type $2^{2^k} + 1 = F_k$ are called **Fermat primes.**

Fact : Only F_0, F_1, F_2, F_3 and F_4 are known to be primes ; $F_5, F_6, \ldots, F_{14}$ are known to be composite.

Conjecture: There exists only finitely many Fermat primes.

Special Numbers : Carmichael numbers

If n satisfies with an integer a, $gcd(a, n) = 1$ and $a^{n-1} \equiv 1 \ (mod \ \ n)$, then n may or may not be prime.

Proposition

If $gcd(a, n) = 1$ but $a^{n-1} \equiv 1 \ (mod \ \ n)$, then n is a prime.

If n satisfies $a^{n-1} \equiv 1 \ (mod \ \ n)$ for all $a \in \{2, 3, \ldots, n-1\}$ and $gcd(a, n) = 1$, then n is called **Carmichael number**.

The smallest Carmichael number is 561.

Theorem (1998)

There exists infinitely many such Carmichael numbers.

Euclid's proof suggests that we define **Euclid numbers** by the recurrence

$$e_n = e_1 e_2 \cdots e_{n-1} + 1$$

when $n \geq 1$.

All e_n's are not prime numbers.

For example, e_1, e_2, e_3, e_4, e_6 are primes, whereas $e_5, e_7, e_8, e_9, \ldots, e_{17}$ are composite.

References

1. **Graham, Knuth and Patashnik**, *"Concrete Mathematics – A Foundation for Computer Science"*, Pearson Education.
2. **Marko Petkovsek, Herbert S. Wilf and Doron Zeilberger**, "$A = B$", AK Peters Ltd., Wellesley, Massachusetts.
3. **Herbert S. Wilf**, *"Generatingfunctionology"*, Third Edition, AK Peters Ltd., Wellesley, Massachusetts.