maths devoted to study of set of integers and their properties

NUMBER THEORY AND CRYPTOGRAPHY

⊙ Division

- If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$ (or $\frac{b}{a}$) $\quad a|b \equiv \exists c(ac=b)$ where D is set of integers.

* When a divides b, a is a ~~factor~~/divisor of b and b is a multiple of a. If $a|b$, the $\frac{b}{a}$ is an integer
* When a does not divide b, it is denoted by $a \nmid b$

① Determine whether

ⓐ $3|7$

$\frac{7}{3} = 2.33$

$3 \nmid 7$ bcz $\frac{7}{3}$ is not an integer

ⓑ $3|12$

$\frac{12}{3} = 4$

$3|12$ bcz $\frac{12}{3}$ is an integer

- Properties of Divisibility.

① Let a, b and c be integers, where $a \neq 0$. Then

ⓘ if $a|b$ and $a|c$, then $a|(b+c)$ $\quad b=ak \quad c=al \quad b+c=a(k+l) \quad b+c=(k+l)a \quad \therefore a|b+c$

ⓘⓘ if $a|b$, then $a|bc$ for all integers c

ⓘⓘⓘ if $a|b$ and $b|c$, then $a|c$.

* Proofs are done using proof methods learned earlier.

② If a, b and c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|mb+nc$ whenever m and n are integers.

Using (ii)

$a|mb$ and $a|nc$

Using (i)

$a|mb+nc$

Note:

- When an integer is divided by a positive integer, there is quotient and remainder, as shown by the

DIVISION ALGORITM

dividend, divisor

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$,

quotient, remainder

such that

$$a = dq + r \qquad \therefore \quad q = a \text{ div } d \quad \frac{a}{d}$$

$$r = a \bmod d \quad a - d$$

Dividend = (Divisor)(Quotient) + Remainder

Note: • Divisor is always positive integer.

• The divison algorithm is a theorem, not an algorithm.

Q Find quotient and remainder when (i) 101 is divided by 11?

q = a div d = $\frac{101}{11}$ = 9

r = a mod d = 2.

```
   9
11|101
  -99
   2
```

USING ~~QUOTIT~~ DIVISION ALGORITHM

$101 = 11 \cdot 9 + 2$

Step 1: Find a multiple of d such that it is as close to a possible

Step 2: Add the r according to the difference b/w d.q and a.

(ii) -11 is divided by 3

~~$-11 = 3(-3)+$~~

$-11 = 3(-4) + 1$ +

Note: Remainder can never be negative. so when finding a multiple ~~dos~~ of d as close to a as possible we find a number greater than a than smaller.

3(-4) is -12

* Can also use rules of -ve integers to understand as $-12 < -11$.

• a is divisible by d iff the remainder is zero

Q Why cant the remainder be -ve?

The range for r is $0 \leq r < d$ and -ve integer does not fit in the range

Q Can two integers have the same remainder when they are divided by the positive integer m?

- If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides a - b.

$$a \equiv b \pmod{m}$$ — RELATION

CONGRUENCE RELATION

where m = modulus (plural moduli)

* a and b have same remainder when divided by m.

$$a \bmod m = b \bmod m.$$ — FUNCTION

* If a and b are not congruent modulo m.

$$a \not\equiv b \pmod{m}.$$

(3) Determine whether

(i) 17 is congruent to 5 modulo 6

Step 1: Write in congruence relation form

$$17 \equiv 5 \pmod{6}$$

Step 2: Divide a-b by 6

$$\frac{17-5}{6} = \frac{12}{6} = 2$$

So 17 is congruent to 5 modulo 6 bcz a-b is divided by m

(ii) 24 and 14 are congruent modulo 6.

$$= \frac{24-14}{6} = \frac{10}{6} = 1.66$$

$24 \not\equiv 14 \pmod{6}$ 24 & 14 not congurent

Q Is there another way to establish congurence between two integers

- Let m be a positive integer The integers a and b are congurent modulo m iff there is an integer k such that

$$a = b + km$$

$$a \equiv b \pmod{m} \quad \text{iff} \quad m \mid a - b$$

So,

$$a - b = km$$
$$a = b + km$$

Q Can two congurent relations ~~be~~ with modulo m be

(i) Added.

let m be a positive iuteger. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

validity is preserved when $d = c$

$$a + c \equiv b + d \pmod{m}.$$

(ii) Multiplied.

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

Validity is preserved when $d = c$

$$ac = bd \pmod{m}.$$

Note: Some properties expected to be true are not always valid.

- Let m be a positive integer and let a and b be integers then - ARITHMETIC MODULO M

* The operations $+_m$ and $\cdot_m$ satisfy many ordinary addition and multiplication properties

① Associativity ② Commutativity ③ Identity elements ④ Additive Inverse ⑤ Distributivity

$a +_m 0 = a$ $\quad a +_m (m-a) = 0$ $\quad a \cdot_m 1 = a$ $\quad 0 \cdot_m 0 = 0$

Addition modulo

$$a +_m b = (a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$7 +_{11} 9 = (7+9) \bmod 11 = 16 \bmod 11 = 5$

and

$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

$$a \cdot_m b = ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Multiplication modulo

- Dividing a congurence by an integer doesnt always give valid congruence

④ Find the values of $(19^3 \bmod 31)^4 \bmod 23$.

Using BODMAS

$19^3 \bmod 31$

$6859 \bmod 31$

Using DIVISION ALGORITHM.

$6859 = 31 \cdot 221 + 8$

So,

$(6859 \bmod 31)^4 \bmod 23$

$(8)^4 \bmod 23$

$4096 \bmod 23$

$4096 = 23 \cdot 178 + 2.$

So,

$4096 \bmod 23 = 2.$

Q What is the use of congurences?

① Hasling Function assigns a memory location to the record that has a unique key.

* Customer Records are identified using social security Number of the customer as the key. A hasling function h assigns memory location h(k) to the record that has k as its key.

• A common hasling function is

$$h(k) = k \bmod m$$ where m = no. of available memory locations

* The hasling function is auto, so all memory locations are possible

⑤ (i) Find the memory locations assigned by the hasling function h(k) = k mod 111 to records of customers with social Security Numbers 064212848 and 037149212.

$$h(064212848) = 064212848 \bmod 111$$
$$= 14$$ → memory location of record 064212848.

$$h(037149212) = 037149212 \bmod 111$$
$$= 65$$

Note:

• When the hasling function is not one-to-one, ~~memory is ass~~ data is assigned to the first free location following the occupied memory

location assigned by the hash function - collision when more than one file is assigned to the same memory location.

LINEAR PROBING FUNCTION

(ii) Assign a memory location to the record of the customer with Social Security number 107405723

$h(10740523) = 10740523 \bmod 111 = 14$

14 already assigned SS 064212 48

Total memory locations are 111 with 14 and 65 filled so since the next empty location after 14 is 15

10740523 is stored in memory location 15

$h(k, i) = h(k) + i \bmod m$. where looks for first free memory location $0 < i < m-1$

② Pseudorandom Numbers are not truly random numbers since they are generated by systematic methods but is used for generating random numbers

Q How to generate pseudorandom numbers?

- We use LINEAR CONGRUENTIAL METHOD

Step 1: Choose four integers:

① modulus ; m ② multiplier ; a $2 \leq a < m$

③ increment ; c $0 \leq c < m$ ④ seed ; x_0 $0 \leq x_0 < m$

Step 2: Generate sequence using congurence

A sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by successively using the recursively defined function.

$$x_{n+1} = (ax_n + c) \bmod m.$$

⑥ Find the sequence of pseudorandom numbers generated by linear congruential method with $m = 9$, $a = 7$, $c = 4$, $x_0 = 3$

$$x_{n+1} = (7x_n + 4) \bmod 9$$

So,

$$x_1 = (7x_0 + 4) \bmod 9$$

$$x_1 \equiv (7 \cdot 3 + 4) \bmod 9 = 7$$

$x_2 = (7 \cdot 7 + 4) \bmod 9 = 8$

$x_3 =$

$\vdots$

$x_9 = (7x_8 + 4) \bmod 9 = (7 \cdot 5 + 4) \bmod 9 = 3.$

Sequence of pseudorandom numbers:

3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3

9 diff numbers before repition

Note: • when $c = 0$ a pure multiplicative generator is created. Such generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16807$ generates $2^{31} - 2$ numbers before repeating.

* It is imp to show only till c repitions

(3) Check Digits are used to check for errors in digit strings by adding an extra digit at the end of the string.

* Can be 0-9 and X (10)

(i) Universal Product Codes (UPCs)

• Most common is a 12 digits UPC. The first digit identifies product category, the next five the manufacturer, and the following five the particular product. and the last gives check digit.

• The check digit is determined by congurence.

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} = 0 \pmod{10}.$$

* Multiply odd places by 3 and the sum all values.

• We can calculate the check digit and then check it to make sure it is valid.

(7) (a) Suppose the first 11 digits of a UPC are 79357343104. What is the check digit?

$0 \pmod{10} = 3\cdot7+9+3\cdot3+5+3\cdot7+3+4\cdot3+3+1\cdot3+0+4\cdot3+x_{12}$

$0 \pmod{10} = \underbrace{98}_{\text{need to make 98 divisible by 10 so we add 2}} + x_{12}$

$98+x_{12}$ should give remainder 0 when divided by 10

$x_{12} = 2 \pmod{10}$.

~~$98 = 0 \pmod{10}$.~~

$$\begin{array}{r|l} & 9 \\ 10 & 98 \\ & -90 \\ \hline & 8 \end{array} \quad \rightarrow 8+x=10, \; x=2.$$

So check digit is 2.

(b) Check whether 041331021641 is valid?

$3\cdot0+4+1\cdot3+3+3\cdot3+1+0\cdot3+2+1\cdot3+6+4\cdot3+1 \equiv 0 \pmod{10}$

$44 \equiv 0 \pmod{10}$.

$$\begin{array}{r|l} & 4 \\ 10 & 44 \\ & -40 \\ \hline & 4 \end{array}$$

44 mod 10 gives remainder 4

So 1 is not the valid ~~UPC~~ check digit of the UPC.

(ii) International ~~Boo~~ Standard Book Number (ISBN)

- ISBN-10 is a ~~ten~~ digit code.

$$\underbrace{x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, x_7\, x_8\, x_9}_{\text{identify language, publisher, book}}\ \ x_{10}$$

x_{10}: check digit

- Check digit is determined by congurence

$$x_{10} = \sum_{i=1}^{9} i x_i \pmod{11}.$$

(8)(a) Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

Multiply by weights

$$x_{10} = 1\cdot 0 + 2\cdot 0 + 3\cdot 7 + 4\cdot 8 + 5\cdot 8 + 6\cdot 8 + 7\cdot 0 + 8\cdot 0 + 9\cdot 8 \pmod{11}$$

$$x_{10} = 189 \pmod{11}. = 2$$

(b) Is 084930149X valid ISBN-10?

X means 10.

$$= 1\cdot 0 + 8\cdot 1 + 4\cdot 2 + 9\cdot 3 + 3\cdot 4 + 0\cdot 5 + 1\cdot 6 + 4\cdot 7 + 9\cdot 9 + 10\cdot 10 \pmod{11}$$

$$= 299 \pmod{11} = 2 \neq 0$$

Since 299 divided by 11 does not give remainder 0 so ISBN-10 check digit is not valid.

Note:

- several kinds of errors often arise in identification numbers

Single error
An error in one digit of an identification number

Transposition error
an accidental interchanging of two digits.

* Both errors can be detected by the check digit for ISBN-10.

(9) Check single error for a valid ISBN-10

0-306-40615-2.

$0 \cdot 10 + 3 \cdot 9 + 0 \cdot 8 + 6 \cdot 7 + 4 \cdot 6 + 0 \cdot 5 + 6 \cdot 4 + 1 \cdot 3 + 5 \cdot 2 + 2 \cdot 1 = 88$

$88 \bmod 11 = 0$ so valid.

Now if 3 becomes 5

0-506-40615-2.

$0 \cdot 10 + 5 \cdot 9 + 0 \cdot 8 + 6 \cdot 7 + 4 \cdot 6 + 0 \cdot 5 + 6 \cdot 4 + 1 \cdot 3 + 5 \cdot 2 + 2 \cdot 1 = 106$

$106 \bmod 11 = 7$ not 0 so error detected.

* Same concept with transposition error.

⊙ Primes

- An integer p greater than 1 is called prime iff positive factors of p are 1 and p. &

* A +ve integer that is greater than 1 and not a prime is called composite.

n is composite if there is an integer a such that $a|n$ and $1 < a < n$

Q Why is 1 not prime?

Because it has only one +ve factor.

Note:

- Primes are building blocks of +ve integers as shown by THE FUNDAMENTAL THEOREM OF ARITHMETIC:

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size

① The prime factorizations of

(a) $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

2	100
2	50
5	25
5	5
	1

(b) 641 is a prime number itself.

(c) $999 = 3^3 \cdot 37$

3	999
3	333
3	111
37	37
	1

(d) $1024 = 2^{10}$

Q How to show that an integer is prime?

- If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
- n is not divisible by an prime less than or equal to its square root, then n is prime — TRIAL DIVISION. (inefficient method)

(2) Show that 101 is prime.

$\sqrt{101} = 10.05$

so primes less than $\sqrt{101}$ are 2, 3, 5, 7

101 is not divisible by any of these primes so 101 is a prime number.

Q How to find all primes not exceeding a specified +ve integer?

Using sieve of Eratosthenes

Step 1: List down all numbers till the specified +ve integer.

Step 2: Delete all integers, other than 2, divisible by 2

Step 3: Delete all integers, other than 3, divisible by 3

Step 4: Delete all integers, other than 5, divisible by 5

Step 5: Delete all integers, other than 7, divisible by 7.

The remaining integers are primes till that specified +ve integer.

Note:

- There are infinitely many primes

Using proof by contradiction

There are finite primes

$$Q = p_1 p_2 \cdots p_n + 1$$

Q is a prime unless it can be written as the product of two or more primes but none of the primes p_i divide Q as if $p_j \mid Q$. then $Q - p_1 p_2 \cdots p_n = 1$

So there is a prime not in this list, which is either Q or a prime factor of Q.

- Prime numbers of the form $2^p - 1$, where p is prime, are called Mersenne primes. (only prime when p prime)

$2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$ and $2^7 - 1 = 127$.

$2^{11} - 1 = 2047$ not a prime bcz $2047 = 23 \cdot 89$

* The larges Mersenne prime is $2^{43112609} - 1$ with nearly 13 million digits

⊙ Greatest Common Divisor (gcd):

- Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the gcd of a and b. $\gcd(a, b)$

① Find gcd of 24 and 36.

$24 = 1, 2, 12, 3, 8, 4, 6, 24$

$36 = 1, 2, 18, 3, 12, 4, 9, 6, 36.$

positive common divisors $= 1, 2, 3, 4, 6, 12.$

$\gcd(24, 36) = 12.$

* The integers a and b are relatively prime if their gcd is 1.

- The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

② Determine whether 10, 17 and 21 are pairwise relatively prime

① $10 = 1, 2, 5, 10$ $\quad 17 = 1, 17.$

$\gcd(10, 17) = 1$

$21 = 1, 3, 7, 21$

$\gcd(10, 21) = 1$ $\quad \gcd(17, 21) = 1$ ~~, 10~~,

So 10, 17 and 21 are pairwise relatively prime.

(ii) Using prime

$10 = 2, 5$ $\quad 21 = 3, 7$

$17 = 17$

$\gcd(10, 17) = 1$ $\quad \gcd(17, 21) = 1.$

$\gcd(10, 21) = 1$

(5) Find $\gcd(120, 500)$ using prime factorization

$120 = 2^3 \cdot 3 \cdot 5$ $\quad 500 = 2^2 \cdot 5^3$

$$\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)}$$

$$= 2^2 \cdot 3^0 \cdot 5^1 = 2^2 \cdot 5 = 20.$$

⊙ Least Common Multiple (LCM):

• Two positive integers a and b ~~is the~~'s least common multiple is the smallest positive integer that is divisible by both a and b. lcm(a, b).

Q How to find LCM?

Using prime factorizations.

$$\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

(1) Find lcm of $2^3 3^5 7^2$ and $2^4 3^3$?

$$= 2^{\max(3,4)} \cdot 3^{\max(5,3)} \cdot 7^{\max(2,0)}$$

$$= 2^4 \cdot 3^5 \cdot 7^2$$

Q What is the relationship b/w gcd and lcm?
Let a and b be positive integers then

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$$

Q Is there a more efficient way to compute gcd?

- We use Euclidian algorithm – based on the idea that gcd(a,b) is equal to gcd(a,c) when a > b and c is the remainder when a is divided by b.

* Time complexity is O(log b), where a > b

② Find gcd (91, 287) greater will be divided

Divide 287 by 91

$287 = 91 \cdot 3 + 14$

Divide 91 by 14

$91 = 14 \cdot 6 + 7$

Divide 14 by 7

~~$7 = 14 \cdot$~~

$14 = 7 \cdot 2 + 0$ ← remainder 0 so reached stopping condition

$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7.$

Q Can gcd be represented as a linear combination?

BEZOUTS THEOREM

- If a and b are +ve integers, then there exists integers s and t such that

$$\gcd(a,b) = sa + tb$$ - BEZOUT IDENTITY

s, t: Bezout coefficients

③ Express gcd (252, 198) = 18 as a linear combination of 252 and 198

TWO PASS METHOD

Use Euclidean algorithm to show gcd (252, 198) = 18

i. $252 = 198 \cdot 1 + 54$

ii. $198 = 54 \cdot 3 + 36$

iii. $54 = 36 \cdot 1 + 18$

iv. $36 = 18 \cdot 2 + 0$

Work backwards from iii to i

Rearranging

Rewriting eqs interms of r = 18

$18 = 54 - 1 \cdot 36$

$36 = 198 - 54 \cdot 3$

Subsitute 2nd eq to 1st

$18 = 54 - 1(198 - 54 \cdot 3)$

$18 = 4 \cdot 54 - 198$ ~~= 252 - 198~~

Subsitute the above eq

$$18 = 4 \cdot (252 - 198) - 198$$

$$= 4 \cdot 252 - 5 \cdot 198$$
$$\quad\ s \qquad\quad t$$

Note:

- Let m be a +ve integer and a, b, c be integers. If $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod m$
- If a, b, c are +ve integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Q How to solve linear congurencies?

- The solution to a linear congurence $ax \equiv b \pmod m$ (x: variable) are all integers x that satisfy the congurence

- The method to find such integers is called

Inverse Modulo m

Step 1: Find inverses modulo m by working backwards through the steps of Euclidean algorithm.

Q What is the inverse of a modulo m?

An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod m$ is said to be an inverse of a modulo m.

For 3 modulo 7.

$$3(\bar{a}) \equiv 1 \pmod 7$$

when $\bar{a} = 5$

$$3 \cdot 5 \equiv 1 \pmod 7$$

$$15 \equiv 1 \pmod 7$$

$$\begin{array}{r} 2 \\ 7 \overline{)\ 15} \\ \underline{+14} \\ 1 \end{array}$$

Q Does the inverse always exist?

- Inverse of a modulo m exists whenever a and m are relatively prime and $m > 1$. ($\gcd(a, m) = 1$)

* The inverse is a unique modulo m ($\bar{a}$ is unique and less than m and every other inverse of a modulo m is congurent to $\bar{a}$ modulo m).

$ax \equiv b \pmod m$

$3x \equiv 4 \pmod 7$

1.1: Verify that inverse exists

$a = 3 \quad m = 7$

$3 = 1, 3 \quad 7 = 1, 7$

$\gcd(3, 7) = 1$ so inverse exists.

$7 = 3 \cdot 2 + 1$

1.2: Using Euclidian algorithm and working backwards to make linear combination of $\gcd(a, b)$

$\gcd(a, m) = 1 = as + tm$

$7 = 3 \cdot 2 + 1$

$3 = 1 \cdot 3 + 0$

$-2 \cdot 3 + 1 \cdot 7 = 1$

$sa + tm = 1$

$s = -2 \qquad t = 1$

$\therefore tm \equiv 0 \pmod m$

$\therefore sa \equiv 1 \pmod m$

So, $\bar{a} = s = -2$

* Every integer congurent to -2 modulo 7 is an inverse of 3 modulo 7

$b \equiv a \pmod m$

$b - a = kn.$

$b = a + kn.$

$b = -2 + 7k$

so,

$k = 0$	$k = 1$	$k = 2$	$k = -1$
$b = -2$	$b = 5$	$b = 12$	$b = -9$

Step 2: Solve congurence by multiplying both sides of the congurence by $\bar{a}$

2.1: Find x $\quad \bar{a} = 2$

is an inverse of 3 mod 7

$$(-2)3x \equiv (-2)4 \pmod 7$$

$$-6x = -8 \pmod 7$$

as 3 mod 7 has inverse 2.

$$3(-2) \equiv -6 \equiv 1 \pmod 7 \quad \therefore 3 \equiv 1 \pmod 7$$

Replacing -6 by 1 bcz -6 and 1 are congurent

$$1 \cdot x \equiv -8 \pmod 7 \qquad -8 = 7 \cdot (-2) + 6.$$

$$1x = 6$$

$$x = 6 \pmod 7$$

2.2: Verify modular equivalences

$$-6 \equiv 1 \pmod 7$$

$$-6 + 7 = 1$$

so -6 and 1 are congurent to modulo 7

$$-8 \equiv 6 \pmod 7$$

$$-8+7 = -1$$

$$-1+7 = 6$$

So, -8 and 6 are congruent modulo 7

As seen $3x = 3 \cdot 6 = 18 = 4 \pmod 7$ verified.

2·3: Conclude $(x \equiv 6 \bmod 7)$.

As $-6 \equiv 1 \pmod 7$ and $-8 \equiv 6 \pmod 7$, the solution to the congruence is

$$x \equiv 6 \pmod 7$$

i.e $x = 6+7k$.

where k is any integer

$k=0$	$k=1$	$k=-1$	$k=2$	$k=-2$
$x=6$	$x=13$	$x=-1$	$x=20$	$x=-8$

all satisfy $3x \equiv 4 \pmod 7$

$ax \equiv b \pmod{m}$.

① Solve linear congruence $19x \equiv 4 \pmod{141}$ using modular inverse.

~~141 = 19~~

19 mod 141.

$\gcd(19, 141) = 1$ so inverse exists

$141 = 19 \cdot 7 + 8$
$19 = 8 \cdot 2 + 3$
$8 = 3 \cdot 2 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$

gives →

$3 - 2 \cdot 1 = 1$
$8 - 3 \cdot 2 = 2$
$19 - 8 \cdot 2 = 3$
$141 - 19 \cdot 7 = 8$

↓ substituting gives

$3 - (8 - 3 \cdot 2) = 1$
$3 - 8 + 3 \cdot 2 = 1$
$3 \cdot 3 - 8 = 1$
$3 \cdot (19 - 8 \cdot 2) - 8 = 1$
$3 \cdot 19 - 8 \cdot 6 - 8 = 1$
$3 \cdot 19 - 8 \cdot 7 = 1$
$3 \cdot 19 - (141 - 19 \cdot 7) \cdot 7 = 1$
~~$3 \cdot 19 - 987 + 7 \cdot 19$~~
$3 \cdot 19 - 141 \cdot 7 + 19 \cdot 49 = 1$

$19 \cdot 52 - 141 \cdot 7 = 1$
$as + bt = 1.$
$\bar{a} = 52$

$52 \cdot 19 \equiv 1 \pmod{141}$

So it is an inverse.

$$52 \cdot 19x = 52 \cdot 4 \pmod{141}$$

Since

$$52 \cdot 19 \equiv 1 \pmod{141}$$

$$1x = 52 \cdot 4 \pmod{141}$$

$$x = 208 \pmod{141}$$

$$x = 67 \pmod{141}.$$

$$x = 67 + 141k.$$

So,

$$x = 67 + 0 = 67.$$
$$x = 67 + 141(1) = 208$$

Q How to solve a system of linear congurences?

- We make use of the

CHINESE REMAINDER THEOREM.

Let $m_1, m_2, \cdots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \cdots, a_n$ an arbitary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$

* There is a solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution

Q How to apply the Chinese Remainder Theorem?

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7$$

Step 1: Compute the product of all moduli M

$$M = m_1 \cdot m_2 \cdot \cdots \cdot m_k$$

$$= 3 \cdot 5 \cdot 7 = 105$$

Step 2: Compute partial products for each modulus m_i.

$$M_i = \frac{M}{m_i}$$

$$M_1 = \frac{105}{3} = 35, \quad M_2 = \frac{105}{5} = 21, \quad M_3 = \frac{105}{7} = 15$$

Step 3: Find modular inverse (N_i) for each M_i

$$M_i \cdot N_i \equiv 1 \pmod{m_i}$$

For M_1

$$35 \cdot N_1 \equiv 1 \pmod 3$$

Since $35 \equiv 2 \pmod 3$

$$2 \cdot N_1 \equiv 1 \pmod 3$$

$N_1 = 2$

$2 \cdot 2 \equiv 4 \equiv 1 \pmod 3$

For M_2

$$21 \cdot N_2 \equiv 1 \pmod 5$$

since $21 \equiv 1 \pmod 5$

$$1 \cdot N_1 \equiv 1 \pmod 5$$

$N_1 = 1$

$1 \cdot 1 = 1 \pmod 5$

OR

For M_3

$15 \cdot N_3 \equiv 1 \pmod 7$

Since $15 \equiv 1 \pmod 7$

$1 \cdot N_3 = 1 \pmod 7$

$N_3 = 1$

$1 = 1 \pmod 7$

$N_1 : y_1 = 35 \bmod 3$

$35 = 3 \cdot 11 + 2$

$3 = 2 \cdot 1 + 1$

So,

$1 = 3 - 2 \cdot 1$

$35 - 3 \cdot 11 = 2$

$1 = 3 - 2(35 - 3 \cdot 11)$

$1 = 3 \cdot 12 - 35 \cdot (2)$

$\bar{a} = 2$

Can be done for M_2 and M_3

Step 4: Construct the solution using formula

$$x = a_1 M_1 N_1 + a_2 M_2 N_2 + a_3 M_3 N_3 \pmod M$$

$a_1 = 2, \; a_2 = 3, \; a_3 = 2$

So,

$$x = (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1) \pmod{105}$$

$$x = 140 + 63 + 30 \pmod{105}$$

$$= 233 \pmod{105}$$

Step 5: Simplify modulo m

$\frac{233}{105} = 2$ remainder 23

So

$X = 23$.

Step 6: Verify solution

$\frac{23}{3} = 7$ remainder 2 $\Rightarrow x \equiv 2 \pmod 3$

$\frac{23}{5} = 4$ remainder 3 $\Rightarrow x \equiv 3 \pmod 5$

$\frac{23}{7} = 3$ remainder 2 $\Rightarrow x \equiv 2 \pmod 7$

Shows that all congruences are satisfied. So,

$$x = 23 \pmod{105}$$

* 23 is the smallest +ve integer that is a simultaneous solution

① Solve for x

$x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 3 \pmod 5$

$M = 3 \times 4 \times 5 = 60$

$M_1 = \frac{60}{3} = 20$, $M_2 = \frac{60}{4} = 15$, $M_3 = \frac{60}{5} = 12$.

For y_1

20 mod 3

$20 = 3 \cdot 6 + 2$

$3 = 2 \cdot 1 + 1$

So,

$3 - 2 \cdot 1 = 1$

$20 - 3 \cdot 6 = 2$

$3 - (20 - 3 \cdot 6) \cdot 1 = 1$

$3 \cdot 7 - 20 \cdot 1 = 1$

$y_1 = \bar{a} + m = -1 + 3 = 2$

OR $20 \equiv 2 \pmod 3$.

$y_1 = 2$.

$2 \cdot 2 = 4 \equiv 1 \pmod 3$

For y_2

$15 \bmod 4$

$15 = 3 \pmod 4$

So,

$3 \cdot 3 = 1 \pmod 4$

$9 = 1 \pmod 4$.

$y_2 = 3$

For y_3

$12 \bmod 5$

$12 = 2 \pmod 5$

So,

$2 \cdot 3 = 1 \pmod 5$

$6 = 1 \pmod 5$

$y_3 = 3$.

$$x = (2 \times 20 \times 2) + (1 \times 15 \times 3) + (3 \times 12 \times 3) \pmod{60}$$

$$= 233 \pmod{60}$$

$$= 53$$

$\frac{53}{3} = 17$ remainder 2

$\frac{53}{4} = 13$ remainder 1

$\frac{53}{5} = 10$ remainder 3

So,

$x = 53 \pmod{60}$

Q How to find remainders of large power integers?

- We use

FERMAT'S LITTLE THEOREM.

If p is a prime and a is an integer not divisible by p, then

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

Furthermore, for every integer a we have

$$a^{p} \equiv a \pmod{p}$$

① Find $7^{222} \bmod 11$

$a = 7 \quad p = 11$

So,

$$7^{10-1} \equiv 1 \pmod{11}.$$

$$7^{10} \equiv 1 \pmod{11}.$$

Thus,

$$(7^{10})^{k} \equiv 1 \pmod{11}$$ for every positive integer k

~~when k = 22~~

$$222 = 10 \cdot 22 + 2.$$

Thus,

$$(7^{10})^{22} + 7^{2} \equiv (1)^{22} \cdot 49 \pmod{11}$$

$$\equiv 4950 \pmod{11}$$

$$\equiv 5$$

So, $7^{222} \bmod 11 = 5.$

(a) Find $2^{50} \bmod 17$

$$2^{17-1} \equiv 1 \pmod{17}$$

$$2^{16} \equiv 1 \pmod{17}$$

~~$16 = 17 \cdot 1 + 1$.~~

$50 = 16 \cdot 3 + 2$.

So,

$$(2^{16})^3 \cdot 2^2 \equiv (1)^3 \cdot 4 \pmod{17}$$

$$\equiv 4 \pmod{17}$$

So,

$2^{50} \bmod 17 = 4$.

Q What is the application of modular arithmetics?

CRYPTO GRAPHY
is the concept of encoding and decoding messages

- The method for encoding messages is known as cipher and the encoded message is known as ciphertext.
- The original message to be encoded is known as plaintext
- The process for encoding messages is known as encryption while the process of decoding messago

is known as decryption.

⊙ TYPES OF CIPHERS

① Caesar Cipher (subsitution)

- Subsitute each letter of the message by the letter coming three letters after it in the alphabet.

$$f(p) = (p+3) \bmod 26$$

* Example of encryption.

① Encrypt "MEET YOU IN THE PARK" using Caesar Cipher.

Step 1: Write position of each letter in the alphabet

M	E	E	T	Y	O	U		I	N
12	4	4	19	24	14	20		8	13

T	H	E	P	A	R	K
19	7	4	15	0	17	10

Step 2: Replace each number by $f(p) = (p+3) \bmod 26$

M	E	E	T	Y	O	U		I	N
15	7	7	22	1	17	23		11	16

T	H	E	P	A	R	K
22	10	7	18	3	20	13

Step 3: Translate numbers back to letters

P H H W B R X L Q W K H S D U N

Q How to recover the original message? - Decrypt the msg.

- To recover the original message use

$$f^{-1}(p) = (p-3) \bmod 26.$$

* Shift each letter back by three digits

Note:

- Caesar Cipher is an example of shift ciphers

* Letter are shifted by an integer k called a key with

- ENCRYPTION FUNCTION

$$f(p) = (p+k) \bmod 26$$

- DECRYPTION FUNCTION

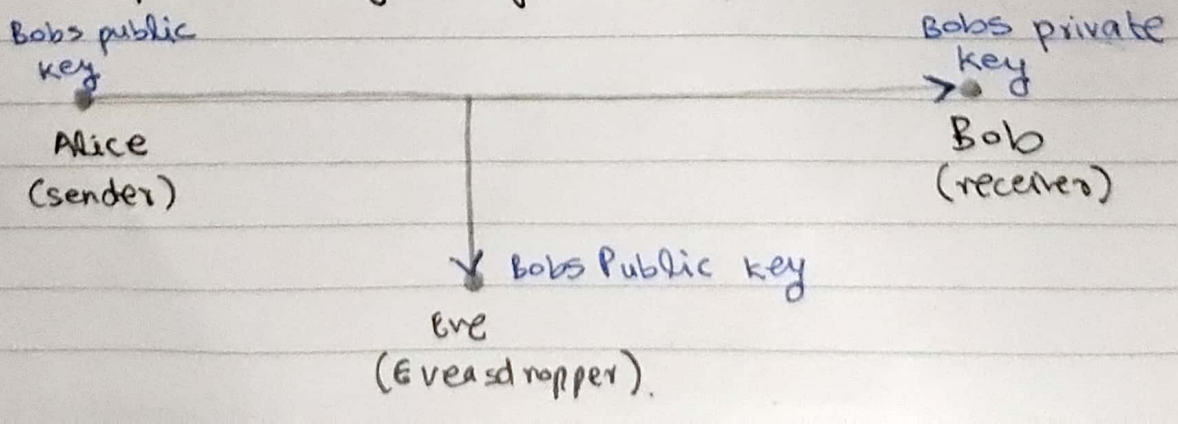
$$f^{-1}(p) = (p-k) \bmod 26$$

⊙ TYPES OF CRYPTOGRAPHY

① Public key cryptography (Asymmetric Cryptosystems)

- Uses the concept of two keys
  - (i) Public key - available to everyone
  - (ii) Private key - secret key known only to receipient.

Q How does public key crypto graph work?



① Alice encrypts the message using Bob's public key, creating a ~~cypht~~ ciphertext
② Bob decrypts the ciphertext using his private key to retrieve the original message

Q Why use public key cryptography?
- Even if the message is intercepted by an eavesdropper, it cannot be decrypted as only Bob is able to do it.

* Thus no need for a shared secret key in advance for decryption.

② Symmetric Cryptosystems
- Uses the concept of sharing same secret key for encryption and decryption.
- Requires a secure way to exchange the secret key before communication which could be intercepted by Eve the Eveasdropper.

* Can be done using Advanced Encryption Standard (AES)

Q How to implement public key cryptography?
Using RSA. algorithm

Q How to generate a key using RSA?

Step 1: Choose two prime numbers (p and q)
- Should be chosen at random and of similar bit-length
- The numbers should remain private.

$n = p \times q$ would give n; the public key

Step 2: Compute Euler's Totient $\phi(n)$

$$\phi(n) = (p-1) \times (q-1)$$

represents the number of integers less than n that are coprime with n.

Step 3: Choose public exponent e

- Select e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$ to ensure e is coprime with $\phi(n)$.

Step 4: Compute private key d

- d is the multiplicative inverse of e mod $\phi(n)$ i.e. $e \cdot d \equiv 1 \pmod{\phi(n)}$. – use euclidean algorithm.

Note:

- The public key is (e, n)
- The private key is (d, n).

Q How to encrypt the message?

Use the public key (e, n) to encrypt M

$$C = M^e \bmod n \quad \text{where } C = \text{ciphertext}$$

Q How to decrypt the message?

Use the private key (d, n) to decrypt C

$$M = C^d \bmod n.$$

① Perform RSA. for message = 19

$p = 7$ and $q = 17$

$n = 7 \times 17 = 119$

$f(n) = \phi(n) = (7-1)(17-1) = 6(16) = 96$

$\gcd(e, \phi(n)) = \gcd(5, 96) = 1$

$e = 5$ (a relatively prime of $f(n)$)

$ed = 1 \bmod (f(n))$

$5d = 1 \bmod (96)$.

$96 = 5 \cdot 19 + 1$

$5 = 1 \cdot 5 + 0$

$5d - 96k = 1$

$96 = 19 \cdot 5 + 1$

$\gcd(5, 96) = 1$

$1 = 96 - 19 \cdot 5$

$-5 \cdot 19 + 96 \cdot 1 = 1$

$d = -19$ $k = 1$

$d = -19 + 96 = 77$ ✓

OR

$96 = 5 \cdot 19 + 1$

$96 - 5 \cdot 19 = 1$

$d = -19 + 96 = 77$

public key (5, 119)
private key (77, 119).

Encryption :

$19^5 \bmod 119 = 66$

Decryption:

$66^{77} \bmod 119 = 19$