Number Theory & Cryptography

Division:

If a & b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$ or equivalently if $\frac{b}{a}$ is an integer. When a divides b we say that a is a factor or divisor of b, & b is multiple of a.

Theorem (1)

"Let a, b & c be integer, where $a \neq 0$. Then

(i) if $a|b$ & $a|c$ then $a|b+c$

(ii) if $a|b$ & $a|c$ then $a|bc$ for all integers c

(iii) if $a|b$ & $b|c$ then $a|c$

$\Rightarrow$ $a|b \Rightarrow b = at_1$

$a|c \Rightarrow c = at_2$

$b+c = at_1 + at_2$

$b+c = a(t_1+t_2)$

$b+c = at_3$

$a|b+c$ prove

$\Rightarrow$ $b = at$

multiply by c on both sides

$bc = atc$

$bc = a(t \times c)$

$bc = a(t_2)$

$a|bc$ proved

$\Rightarrow \quad b = at, \quad c = bt \qquad \Rightarrow c = at$

$b + c = at_1 - bt_2$

$b - c = t(a - b)$

$b - c = tl$

$b + c = at_1 + bt_2$

$c = at_1 + bt_2 - b$

$c = at + b(t_2 - 1)$

$c = at + bt_3$

$c = at + t_4$

$c = a(t_1 + t_4)$

$c = at_5$

Quotient:

$q = a \text{ div } d \qquad \Rightarrow q = a/d$

Remainder:

$r = a \text{ mod } d \qquad \Rightarrow r = a - d$

Example:

Quotient & remainder when 101 is divided by 11

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

$r = a \text{ mod } d = 101 \text{ mod } 11 = 2$

Modular Arithmetic:

let a & b integer, let m be a positive integer. Then $a \equiv b \pmod m$ if & only if

$$a \bmod m = b \bmod m$$

$$a \equiv b \pmod m$$

$$m \mid a-b$$

Theorem: $a \equiv b \pmod m$ & $c \equiv d \pmod m$

$$a+c = b+d \pmod m$$

$$ac = bd \pmod m$$

$a \equiv b \pmod m \Rightarrow m \mid a-b \Rightarrow (a-b) = mt_1$

$c \equiv d \pmod m \Rightarrow m \mid c-d \Rightarrow (c-d) = mt_2$

adding

$$(a-b)+(c-d) = mt_1 + mt_2$$

$$(a-b)+(c-d) = mt_1 + mt_2$$

$$(a+c)-(b-d) = m(t_1+t_2)$$

$$(a+c) = mt_3 + (b+d)$$

$$mt_3 \quad a+c = b+d \pmod m$$

$$\Rightarrow ac = bd \pmod m$$

$$(a-b)(c-d) = (mt_1)(mt_2)$$

$$ac - ad - bc + bd = m^2 t_3$$

$$ac = m^2 t_3 + ad + bc + bd$$

$$ac = bd + m^2 t_3 + ad + bc$$

$$ac = bd + m(t_3 + ad + bc)$$

$$ac = bd \pmod m$$

Example:

$7 \equiv 2 \pmod 5$ $\quad 4 \equiv 1 \pmod 5$

$5 \mid (7-2) \Rightarrow (7-2) = 5$

From Theorem

$a=7,\ b=2,\ c=11,\ d=1 \quad \text{mod}(5)$

$\Rightarrow a+c \equiv b+d \pmod m$

$7+11 = 2+1 \pmod 5$

$18 = 3 \pmod 5$

$= (\text{mod } 5) \mid 18-3$

$18-3 = \text{mod } 5$

$15 = \text{mod } 5$ ✓

$\Rightarrow ac = bd \pmod m$

$71 = 7 \cdot 11 = 2 \cdot 1 = 2 \pmod 5$

$71 = 2 \pmod 5$

$77-2 = \text{mod}(5)$ ✓

$75 = (\text{mod } 5)$

Defination of addition & multiplication.

let a & b are integers & m is a positive integer then

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

&

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

Example:

$7+11\ 9 \quad \& \quad 7 \cdot 11\ 9$

$a=7, \quad b=9 \quad \text{mod} = 11$

$-4 \quad -2 \quad -6 \quad -11$

Addition: $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

$(7+9) \bmod 11 = (16) \bmod 11 = 5$ Ans. $((-4)+(-2)) \bmod m$

$-6 \bmod 11$

Multiplication: $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$ $11-6=5$

$(7 \cdot 9) \bmod 11 = ((7 \bmod 11)(9 \bmod 11)) \bmod 11$

$(63) \bmod 11 = ((-4)(-2)) \bmod 11$

$63 \pmod{11} = 8 \pmod{11}$

Addition:

$(7+9) \bmod 11 = ((7 \bmod 11) + (9 \bmod 11)) \bmod 11$

$= (+4+2) \bmod 11$

$= (-6) \bmod 11$

$= (-6) - (11) =$

$a \neq b$ is a positive integer.

Exercise

Q1: Does ... ?

a: 68 $\Rightarrow$ Yes

c: 357 $\Rightarrow$ Yes

Q2: what are quotient & remainder.

a: 19 is divided by 7?

$q = 2$

$r = 5$

$$\begin{array}{r} 2 = q \\ 7 \overline{)\,19} \\ \underline{14} \\ 5 = r \end{array}$$

c: 0 is divided by 19?

$q = 0$

$r = 0$

$$\begin{array}{r} 0 = q \\ 19 \overline{)\,0} \\ \underline{0} \\ 0 = r \end{array}$$

h: 4 is divided by 1

$$q = 4$$

$$r = 0$$

$$1 \overline{)\,4}\quad 4,\ 4,\ 0$$

Q11: What time does a 12 hour take read a. 80 hours after it reads 11:00

$$a = 11,\ b = 80 \qquad \text{mod } m = 12$$

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

$$= ((a \bmod m) + (b \bmod m)) \bmod 12$$

$$= ((11 \bmod 12) + (80 \bmod 12)) \bmod 12$$

$$= ((11-12) + (80-12)) \bmod 12$$

$$= (-1 + 68) \bmod 12 \quad = (67) \bmod 12$$

$$= 7 \text{ : clock}$$

$$12 \overline{)\,67}\quad 5,\ 60,\ 7$$

or $(11+80) \bmod 12$

7 : clock

b. 40 hours before it reads 12:00

$$a = 12,\ b = 40,\ m = 12$$

$$(12-40) \bmod m = (-28) \bmod 12$$

$$12 \overline{)\,-28}\quad -3,\ -36,\ 8$$

$$= 8 \text{ : clock}$$

Q13: $a=4$, mod 13 = m, $b=9$, $c=$

$\Rightarrow c = 9a \pmod{13}$

$= 9(4) \pmod{13}$

$= 36 \pmod{13}$

$= (9(4 \bmod 13)) \bmod 13$

$13 \overline{)36}$ (2, 26, 10)

$c = 10$ Ans.

$\Rightarrow c \equiv a + b \pmod{13}$

$\equiv (4 \pmod{13} + 9 \pmod{13}) \pmod{13}$

$= \bmod 13 (4 + 9 (\bmod 13))$

$= 13 \pmod{13}$

$= 0$

$13 \overline{)13}$ (1, 13, 0)

$\Rightarrow c \equiv a^3 - b^3 \pmod{13}$

$= (4^3 - 9^3) \bmod 13$

$= (64 - 729) \bmod 13$

$= -665 \bmod 13$

$= 11$

$13 \overline{)-665}$ (-52, +676, 11)

Q20:

a: $-17 \bmod 2$

$= (-17 - 2)$

$= -19 = 1$

$2 \overline{)-17}$ (9, +18, 1)

b: $144 \bmod 7$

$144 - 7 =$

$= 137$

Q21:

a: $13 \bmod 3$

1

$3 \overline{)13}$ (4, 12, 1)

Q23: Find a div m & a mod m

a: a = 228 , m = 119

a div m = 1

a mod m = 109

$$\begin{array}{r} 1 \\ 119\overline{)228} \\ 119 \\ \hline 109 \end{array}$$

Q25: Find the integer a such that

$a \equiv -15 \pmod{27}$ & $-26 \le a \le 0$

$$\begin{array}{r} -0 \\ 27\overline{)-15} \\ +0 \\ \hline -15 \end{array}$$

~~$-26 \equiv -15 \pmod{27}$~~

~~-26~~

$a = -15 - 27 \Rightarrow -42 \pmod{27}$

$a = -15 + 27 = 14 \pmod{27}$

∴ Since -15 is b/w -26 & 0

So -15 is answer

$\Rightarrow a \equiv 99 \pmod{41}$ 100 — 140

$99 + 41 = 140$

$= 140$ Ans.

Q31: Find each of these values.

a. $(-133 \bmod 23 + 27 \bmod 31) \bmod 31$

$(5 + 8) \bmod 23$

$(13) \bmod 23$

13 Ans.

$$\begin{array}{r} 0 \\ 23\overline{)13} \\ 0 \\ \hline 13 \end{array}$$

$6.\ (457 \bmod 23 \cdot 182 \bmod 23) \bmod 23$

$(20 \cdot 21) \bmod 23$

$(420) \bmod 23$

6 Ans

$$23 \overline{)420}\ 18,\ 414,\ 6$$

Q33: $(99^2 \bmod 32)^3 \bmod 15$

$(9801 \bmod 1089)^3 \bmod 15$

$(9)^3 \bmod 15$

$(729) \bmod 15$

$= 9$ Ans.

$$15 \overline{)729}\ 48,\ 720,\ 9$$

4.2 Integer Representation & Algorithms.

Integer representation :

Decimal (base 10)

Binary (base 2)

Octal (base 8)

hexadecimal (base 16)

Binary to decimal

$(10101\ 1111)_2$

$= 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^1$

$= 256 + 64 + 16 + 8 + 4 + 2 + 1$

$= 351$

Scanned with CamScanner

Decimal to ocial.

(7016)8

7 0 1 6

$= 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0$

$= 3584 + 8 + 6$

$= 3598$

Decimal to nexadecimal

(2AE0B)16

2 A E 0 B

$= 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0$

$= 175627$

Octal Expansion of

(12345)10

First divide by 8, multiply quotient by 8 & divide by remainder

n q r

$12345 = 8 \cdot 1543 + 1$ ←

$1543 = 8 \cdot 192 + 7$ ←

$192 = 8 \cdot 24 + 0$ ←

$24 = 8 \cdot 3 + 0$ ←

$3 = 8 \cdot 0 + 3$ ←

$(12345)_{10} = (30071)_8$

$8 \overline{)12345}$ (1543)

12344

1

Find hexadecimal Expansion

$(177130)_{10}$

$177130 = 16 \cdot 11070 + 10 \Rightarrow A$

$11070 = 16 \cdot 691 + 14 \Rightarrow E$

$691 = 16 \cdot 43 + 3 \Rightarrow 3$

$43 = 16 \cdot 2 + 11 \Rightarrow B$

$3 = 16 \cdot 0 + 2 \Rightarrow 2$

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

Find binary Expansion.

$(241)_{10}$

$241 = 2 \cdot 120 + 1$

$120 = 2 \cdot 60 + 0$

$60 = 2 \cdot 30 + 0$

$30 = 2 \cdot 15 + 0$

$15 = 2 \cdot 7 + 1$

$7 = 2 \cdot 3 + 1$

$3 = 2 \cdot 1 + 1$

$1 = 2 \cdot 0 + 1$

$(241)_{10} = (11110001)_2$

Adding Algorithm

To add a & b, first add right most bits.

This gives

$a_0 + b_0 = c_0 \cdot 2 + s_0$

where s_0 is the rightmost bit of binary expansion of "a+b" & c_0 is the carry which is either

0 & 1. Then add the next pair of bits & carry.

Example

Add $a = (1110)_2$ & $b = (1011)_2$

$a_0 + b_0 = 0+1 = 0.2 + 1$ $\quad 2\overline{)1}$ $\quad 0 = c_0$, $\frac{0}{1} = s_0$

$a_1 + b_1 = 1+1 = 1.2 + 0$

$a_2 + b_2 + c_1 = 1+0+1 = 1.2 + 0$ $\quad 2\overline{)2}$ $\quad 1 = c_1$, $\frac{2}{0} = s_1$

$a_3 + b_3 + c_2 = 1+1+1 = 1.2 + 1$ $\quad 2\overline{)3}$ $\quad 1 = c_2$, $\frac{2}{1} = s_2$

Here $c_0 = 0$ & $s_0 = 1$

$s = (a+b)_2 = (11001)_2$

Multiplication Algorithm:

$$ab = a(b_0 2^0 + b_1 2^1 + b_2 2^2 \cdots b_n 2^n + b_{n-1} 2^{n-1})$$

$$= a(b_0 2^0) + a(b_1 2^1) + a(b_2 2^2) \cdots a(b_{n-1} 2^{n-1})$$

Example

$a = (110)_2$, $b = (101)_2$

$ab = (110)(1.2^0) + (110)(0.2^1) + (110)(1.2^2)$

$= (110)(1.1) + (110)(0) + (110)_2(2^2)$

$= (110)_2 + (000)_2 + (11000)_2$

$= 11000$
$\quad\ 0000$
$\quad\ 110$
$\overline{11110}$

$ab = (11110)_2$

Primes & Greatest Common Divisior.

What is Prime?

Every integer greater ~~great~~ than 1 & only be divisbly by at least two integer 1 & itself is called primes.

Composite:

Integer greater than 1 but not a prime is called composite.

Fundamental Theorem of Arithmetic

It state that:=

"Every integer greater than 1 can be written uniquely as a prime or the product of two or more primes where the prime factors are written in non-decreasing size."

Example: Prime Factorization of

$71 = 71$

$70 = 2.5.7$

$30 = 2.3.5$

$100 = 2^2.5^2$

2 | 30
3 | 15
5 | 5
1	

71 | 71
1

2 | 70
5 | 35
7 | 7
1	

2 | 100
2 | 50
5 | 25
5 | 5
1	

Scanned with CamScanner

what is trial division?

A brute force method of finding a division of an integer by simply plugging in one or set of integer 4 seeing if they divide is called trial division.

what is meant by Mersenne prime?

A prime number that is one less than power of two is called mersenne prime

$$M_p = 2^p - 1$$

Example:

Any prime number other than 2, 3, 5, 47 is not a mersene prime number

take 13,

$2^{13} - 1 = 8192 - 1 = 8191/13$

not a merscenne prime

$2^{17} - 1 = 131,056 - 1 = 131,055/17$

not a merscenne prime

$2^{19} - 1 = 524,224 - 1 = 524223/19$

not a merscenne prime

Scanned with CamScanner

what is meant by goldbatch conjuctive

Every even integer $n, n>2$ is the sum of two primes is called goldbatch conjuctive.

Example:

$4 = 2+2$ $\quad\quad$ $12 = 7+5$

$6 = 3+3$ $\quad\quad$ $14 = 7+7$

$8 = 3+5$ $\quad\quad$ $16 = 11+5$

$10 = 5+5$ $\quad\quad$ $18 = 11+7$

What is meant by twin primes?

The prime numbers having a gap of two or less is called twin primes

Example: 2 & 3, 5 & 7, 11 & 13, 17 & 19, 29 & 31

Define greatest common division & least common division;

The largest integer that divides both of two integers is called greatest common division. 24 & 36

e.g 12 is greatest common divisor

The smallest non-zero integer that divides both of two integer is called least common divisor.

in case of any two positive integers least common multiple is always 1

Scanned with CamScanner

What is meant by relatively prime?

The common divisor of any two integer is 1 Then it is called relatively prime

e.g 17 & 22

only 1 can divide both.

Maximum Common multiple & least common multiple:

Prime Factorization of 120 & 150

$120 = 2^3 \cdot 3^1 \cdot 5^1$

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

$LCM = 2^{(\min(3,2)} \times 3^{\min(1,0)} \times 5^{\min(1,3)}$

$= 2^2 \times 3^0 \times 5^1 = 2^2 4 \times 1 \times 5 = 20$

$GCM = 2^{\max(3,2)} \times 3^{(\max(1,0)} \times 5^{\max(1,3)}$

$= 2^3 \times 3^1 \times 5^3 = 8 \times 3 \times 125 = 300$

what is Euclidean Algorithm?

A method of finding the greatest common divisor of two numbers by diving the larger by smaller, the smaller by the remainder, the first remainder by the second remainder, so on until the exact division is obtained is called euclidean Algorithm.

⇒.

⇒ 287 & 91

① $287 = 91.3 + 14$

② S number by Remainder 1

$91 = 14.6 + 7$

③ First remainder by 2nd Remainder

$14 = 7.2 + 0$

7 is the gcd.

$$\begin{array}{r} 3 \\ 91\overline{)287} \\ 273 \\ \hline 14 = R_1 \end{array}$$

② S number by R_1

$$\begin{array}{r} 6 \\ 14\overline{)91} \\ 84 \\ \hline 7 = R_2 \end{array}$$

4.4

SOLVING CONGRUENCES

What is linear congruences?

A congruence in the form

$$ax \equiv b \pmod m$$

where m is positive integer, & a & b are integers, & x is variable is called linear congruences.

Find inverse of 101 modulo 4620

$$4620 = 45 \cdot 101 + 75$$

$$101 = 1 \cdot 75 + 26$$

$$75 = 2 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3$$

$$23 = 7 \cdot 3 + 2$$

~~$3 = 0 \cdot 2 + 0$~~ 2

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

$$2 = 2 \cdot 1 + 0$$

Scanned with CamScanner

inverse :

$1 = 3 - 1 \cdot 2$

$= 3 - 1 \cdot (23 - 7 \cdot 3) = 2 \cdot (23 - 21) = 2 \cdot 2 = 4$

$= 4 \cdot (26 - 1 \cdot 23) = 4 (3) = 12$

$= 12 \cdot (75 - 2 \cdot 26) = 12 (75 - 52) = 12 (23) = 266$

$= 266 \cdot (101 - 1 \cdot 75) = 266 (26) = 6916$

$= 6916 (4620 - 45 \cdot 101)$

Remainder 1 start point $3 = 1 \cdot 2 + (1) R$

$1 = 3 - 1 \cdot 2$, move backward

Sub 2 = $23 - 7 \cdot 3$ $23 = 7 \cdot 3 + (2) R$

$1 = 1 \times 3 \boxed{- 1 \cdot (23 - 7 \cdot 3)}$

add x

$= -1 \cdot 23 + 8 \cdot 3$

Sub 3 = $26 - 1 \cdot 23$ $26 = 1 \cdot 23 + (3) R$

$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23)$

$= 8 \cdot 26 - 9 \cdot 23$

Sub 23 = $75 - 2 \cdot 26$ $75 = 2 \cdot 26 + (23) R$

$1 = 8 \cdot 26 \boxed{- 9 \cdot (75 - 2 \cdot 26)}$

$= 8 - 9 \cdot 75 + 26 \cdot 26$

Sub 26 = $101 - 1 \cdot 75$

$1 = -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75)$

$= 26 \cdot 101 - 35 \cdot 75$

Sub 75 = $4620 - 45 \cdot 101$

$1 = 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$

$= -35 \cdot 4620 + 1601 \cdot 101$

-35 & 1601 = Bezout function

1601 is an inverse of 101 modulo 4620

Scanned with CamScanner

Chinese Remainder Theorem:

It state that

"If one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisor are pairwise coprime."

Fermat Little Theorem:

If p is prime & a is an integer not divisible by p then

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

or for every integer

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

Fermat Little Theorem tells that $a \in Z_p$, then $a^{p-1} = 1$ in Z_p

Example : $7^{222} \bmod 11$

we know $7^{10} = 1 \pmod{11}$

$7^{222/10} = 7^{\frac{22 \cdot 10 + 2}{}}$ $\quad 22 \cdot 10 + 2$

$7^{222} = 7^{22 \cdot 10 + 2} = 7^{22 \cdot 10} \cdot 7^2$

$= (7^{10})^{22} \cdot (7)^2 = (1)^{22} \cdot 49 = 49$

$49 = 5 \pmod{11}$

5 is answer

$$10 \overline{)222}\ (22,\ 220,\ 2)$$

$$4 \overline{)49}\ (4,\ 44,\ -5\ (R))$$

What is Pseudo Prime

A prime integer that is actualy not prime, there are composite integer n such that $2^{n-1} = 1 \pmod n$. Such integers are called pseudoprime.

e.g: 6 is a composite no

$2^{6-1} = 1 \pmod 6$

$2^5 = 1 \pmod 6$

$32 = 1 \pmod 6$

$$6 \overline{)32} \quad 5, \ 30, \ 2 \times$$

3 is a prime no

$2^{3-1} = 1 \pmod 3$

$2^2 = 1 \pmod 3$

$4 = 1 \pmod 3$

$$3 \overline{)4} \quad 1, \ 3, \ 1 \checkmark$$

$2^{8-1} = 1 \pmod 8$

$2^7 = 1 \pmod 8$

$128 = 1 \pmod 8$

$$8 \overline{)128} \quad 16, \ 128, \ 0 \times$$

Scanned with CamScanner

"CryptoGraphy"

"The study of secure communication techniques that allows only the sender & intended recepient of a message"
The term is derived from greek word kryptos, which means hidden.
The widely used public key system is RSA cryptosystem.

Classical Cryptography:

Presented by Julius Caesar, it state that Alaphbets 0 to 25 ⇒ A to Z
replace Alphabets by integers for encypt & decrypt
$7(p) = (p + 3) \bmod 26$

Encaption:

Process of convertion data or information into code.

e.g: "Help Me"

① Replace with integers

H	E	L	P		M	E
8	5	12	16		13	5

② Formula $7(p) = (p+k) \bmod 26$

③ Here p is the integer of your message & k is the converting code integer.
let $k = 3$

④ $7(8) = (8+3) \bmod 26 = (11) \bmod 26$
at u its k, do for all code you

get encopted code as

HELP ME = KHOS PH

↓ ↓

Normal Encrypted.

Deeryption:

Conversion of encrypted data into original form is called deeryption.

Formula: $7(p) = (p-k) \bmod 26$

" KHOS PH "

$7(\overset{N}{14}) = (14-3) \bmod 26$

$11 = K$

KHOS PH = HELP ME

u