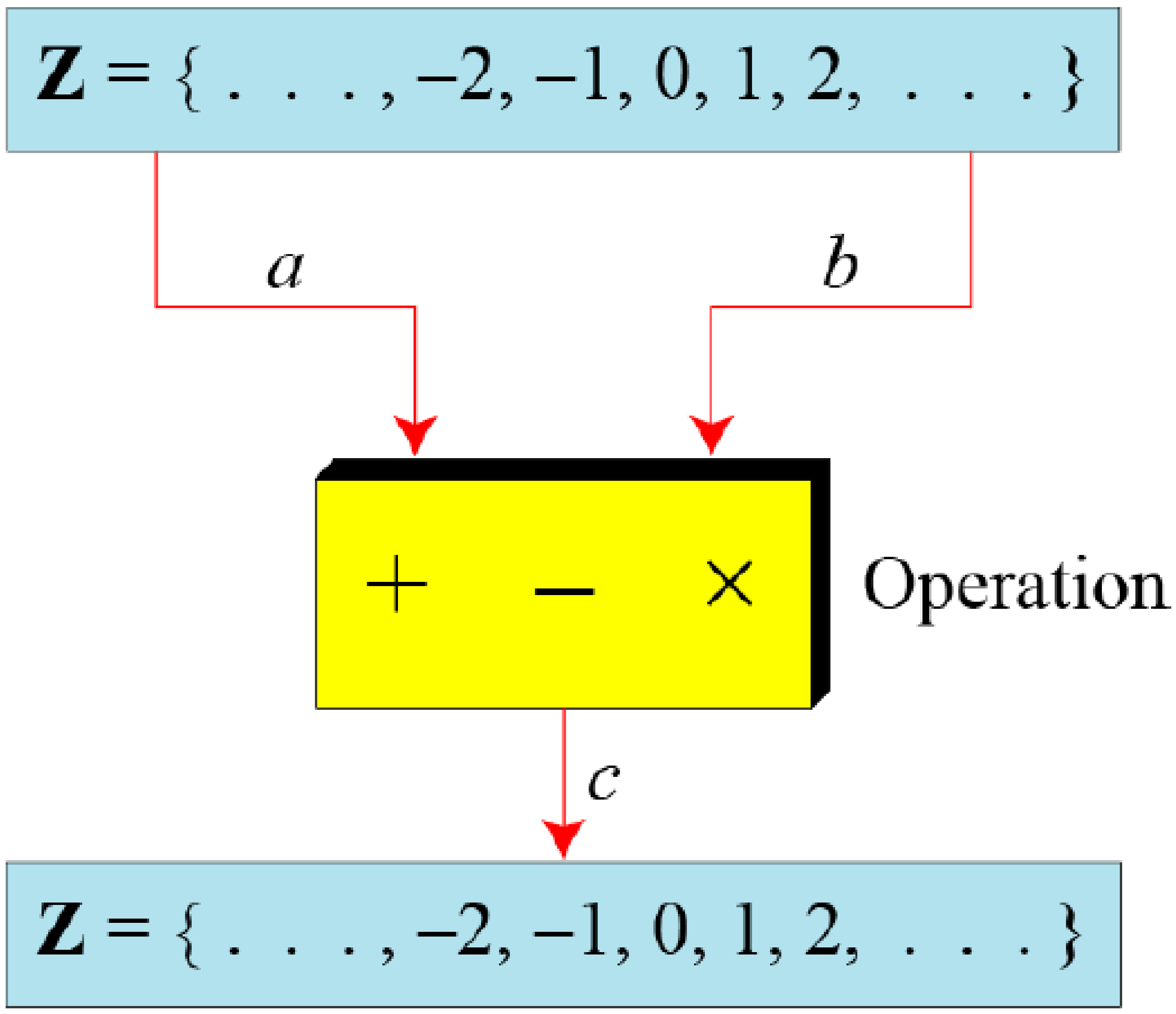
Integer Arithmetic

- Consists of a set of Integers and operations on it.



Integer Division

- If $b|a$ and $b \neq 0$, then $a = q * b$; where $a, b, q \in Z$
- If $b \nmid a$ and $b \neq 0$, then $a = q * b + r$; where $a, b, q, r \in Z$

$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \quad \leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

Properties of Integer Division

- If $b|a$ and $a|b$, then $a=\pm b$.
- If $b|1$, then $b=\pm 1$.
- If $a|b$ and $b|c$, then $a|c$.
- If $a|b$ and $a|c$, then $a|(m*b+n*c)$, where $a, b, c, m, n \in Z$.

MODULAR ARITHMETIC

Modular Arithmetic

- For $a = q * b + r$,
- $a \; mod \; b \;=\; r; \; where \; a, b, q, r \;\in\; Z.$
- $Z_n \;=\; \{0, 1, 2, 3, 4, \ldots\ldots\; (n-1)\}$

$\boxed{\mathbf{Z}_2 = \{0, 1\}}$ $\boxed{\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}}$ $\boxed{\mathbf{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}}$

Modular Arithmetic (Examples)

- 27 mod 5 = 2
- 36 mod 7 = 1
- -13 mod 6 = 5
- -29 mod 12 = 7

Basic Operations in Modular Arithmetic

- If $a, b \in Z_n, then\ (a+b)\ mod\ n = c \in Z_n$
- $If\ a, b \in Z_n, then\ (a-b)\ mod\ n = c \in Z_n$
- If $a, b \in Z_n\ then\ (a * b) mod\ n = c \in Z_{\mathrm{n}}$

Basic Operations in Modular Arithmetic (Examples)

- $(17 + 19) \; mod \; 23 \; = \; 13 \; \in Z_{23}$
- $(3 - 5) \; mod \; 6 \; = \; 4 \; \in \; Z_6$
- $(13 * 14) \; mod \; 15 \; = \; 2 \; \in \; Z_{15}$
- $(8 * 9) \; mod \; 13 \; = \; 7 \; \in \; Z_{13}$

Properties of Modular Arithmetic

$$(a + b)\ mod\ n\ =\ [(a\ mod\ n) + (b\ mod\ n)]\ mod\ n;\ a, b\ \in\ Z$$

$$(a - b)\ mod\ n\ =\ [(a\ mod\ n) - (b\ mod\ n)]\ mod\ n;\ a, b\ \in\ Z$$

$$(a * b)\ mod\ n\ =\ [(a\ mod\ n) * (b\ mod\ n)]\ mod\ n;\ a, b\ \in\ Z$$

Properties of Modular Arithmetic (Examples)

$$(8+7)\ mod\ 5\ =\ [(8\ mod\ 5)\ +\ (7\ mod\ 5)]\ mod\ 5\ =\ (3+2)\ mod\ 5\ =\ 0\ \in\ Z_5$$

$$(28-16)\ mod\ 8\ =\ [(28\ mod\ 8)\ -\ (16\ mod\ 8)]\ mod\ 8\ =\ (4-0)\ mod\ 8\ =\ 4\ \in\ Z_8$$

$$(23*25)\ mod\ 20\ =\ [(23\ mod\ 20)*(25\ mod\ 20)]\ mod\ 20\ =\ (3*5)\ mod\ 20\ =\ 15\ \in\ Z_{20}$$

Modular Additive Inverse

$For\ a, b\ \in\ Z_n, b\ is\ the\ additive\ inverse\ of\ a\ if\ (a + b)\ \equiv\ 0\ (mod\ n)$

Additive Inverse pairs of $Z_{10}\ =\ \{(0,0), (1,9), (2,8), (3,7), (4,6), (5,5)\}$

Additive Inverse pairs of $Z_9\ =\ \{(0,0), (1,8), (2,7), (3,6), (4,5)\}$

Additive Inverse pairs of $Z_{11}\ =\ \{(0,0), (1,10), (2,9), (3,8), (4,7), (5,6)\}$

Modular Multiplicative Inverse

$For\ a, b\ \in\ Z_n, b\ is\ the\ Multiplicative\ Inverse\ of\ a, if\ (a * b)\ \equiv\ 1\ (mod\ n)$

$Multiplicative\ Inverse\ pairs\ in\ Z_5\ =\ \{(1,1), (2,3), (4,4)\}$

$Multiplicative\ Inverse\ pairs\ in\ Z_6\ =\ \{(1,1), (5,5)\}$

$Multiplicative\ Inverse\ pairs\ in\ Z7\ =\ \{(1,1), (2,4), (3,5), (6,6)\}$

Properties of Congruences

1) Reflexive Property:- $a \equiv a \ (mod\ n)$
2) Symmetric Property:- $If\ a \equiv b\ (mod\ n), then\ b \equiv a\ (mod\ n)$
3) Transitive Property:- $If\ a \equiv b\ (mod\ n)\ and\ b \equiv c\ (mod\ n), then\ a \equiv c\ (mod\ n)$
4) Addition Property:- $If\ a \equiv b\ (mod\ n)\ and\ c \equiv d\ (mod\ n), then\ (a + c) \equiv (b + d)\ mod\ n$
5) Subtraction Property:- $If\ a \equiv b\ (mod\ n)\ and\ c \equiv d\ (mod\ n), then\ (a - c) \equiv (b - d)\ mod\ n$
6) Multiplication Property:- $If\ a \equiv b\ (mod\ n), then\ (a * c) \equiv (b * c)\ mod\ n;\ c \in Z$
7) Exponential Property:- $If\ a \equiv b\ (mod\ n), then\ am \equiv bm\ (mod\ n)$

Properties of Congruences (Examples)

- $7 \equiv 7 \pmod{5}$
- $8 \equiv 3 \pmod{5}$; Hence, $3 \equiv 8 \pmod{5}$
- $18 \equiv 11 \pmod{7}$; $11 \equiv 4 \pmod{7}$; Hence, $18 \equiv 4 \pmod{7}$
- $19 \equiv 10 \pmod{9}$; $25 \equiv 16 \pmod{9}$; Hence, $44 \equiv 26 \pmod{9}$
- $44 \equiv 26 \pmod{9}$; $25 \equiv 16 \pmod{9}$; Hence, $19 \equiv 10 \pmod{9}$
- $18 \equiv 11 \pmod{7}$; Hence, $90 \equiv 55 \pmod{7}$
- $8 \equiv 3 \pmod{5}$; Hence, $64 \equiv 9 \pmod{5}$;

PRIMES AND GCD

Prime Numbers

- In Cryptography, only positive primes have significance, though some Mathematicians extend the idea of primes and composites to negative numbers as well.
- In Cryptography, large primes are required for algorithms like RSA, Diffie Hellman, etc.

2039568783564019774057658669290345772801939933143482630947726464532830627
2270127763293661606314408817331237288267712387953870940015830656733832827
9154499698366071906766440037074217117805690872792848149112022286332144876
1833763265120835748216479339929612499173198362193042742802438031040150005
63790123

Prime Factorization

- Expressing a positive composite number as a product of primes.
- Prime factorization of a number is harder than multiplying the primes to generate the number.
- $10 = 2 * 5$
- $100 = 2^2 * 5^2$
- $1000 = 2^3 * 5^3$
- $120 = 2^3 * 3 * 5$
- $5040 = 2^4 * 3^2 * 5 * 7$

GCD (HCF)

- In Cryptography, typically only positive numbers are used.
- $If\ c|a\ and\ c|b, the\ GCD(a,b) = c;\ where\ a,b,c\ \in\ N.$
- GCD(5,10) = 5
- GCD(8,12) = 4
- GCD(24, 60) = 12
- GCD(10, 45) = 5
- GCD(28, 70) = 14

Co-Primes

- a and b are co-prime if $GCD(a,b) = 1$; $a,b \in N$;
- 1 is co-prime with all the Natural numbers.
- For $a \equiv b \pmod{n}$, if $GCD(d,n)=1$, then $(a/d) \equiv (b/d) \pmod{n}$; where $d \in N$.
- Examples of some co-prime pairs: (8,15), (12,25), (17,20)

EUCLIDEAN ALGORITHM

Euclidean Algorithm to Calculate GCD (Pseudocode)

```
GCD(a,b)
{
if(b==0)
    return a;
else
    return GCD(b, a mod b)
}
```

- Here a,b ∈ N and a ≥ b.

GCD (48, 18) = ?

a	**b**
48	18
18	12
12	6
6	0

GCD (198, 121) = ?

a	b
198	121
121	77
77	44
44	33
33	11
11	0

GCD (584, 248) = ?

a	b
584	248
248	88
88	72
72	16
16	8
8	0

GCD (66348, 18042) = ?

a	**b**
66348	18042
18042	12222
12222	5820
5820	582
582	0

GCD (868, 795) = ?

a	**b**
868	795
795	73
73	65
65	8
8	1
1	0

EXTENDED EUCLIDEAN ALGORITHM (EEA)

EEA for gcd(a,b)=d

```
EEA(a, b)
{
u1=1, u2=0, v1=0, v2=1;
while(b≠0)
{
    q=a/b; r=a mod b; u=u1-q*u2; v=v1-q*v2;
   a=b; b=r; u1=u2; u2=u; v1=v2; v2=v;
}
d=a; x=u1; y=v1;
return(d, x, y)
}
```

- Here $d=a*x+b*y$; where $x,y \in Z$.

Calculate GCD(48,18), x, y

q	a	b	r	u1	u2	u	v1	v2	v
2	48	18	12	1	0	1	0	1	-2
1	18	12	6	0	1	-1	1	-2	3
2	12	6	0	1	-1	3	-2	3	-8
	6	0		**-1**	3		**3**	-8	

- GCD(48, 18) = 6 = 48 * (-1) + 18 * (3)

Calculate GCD(848, 596), x, y

q	a	b	r	u1	u2	u	v1	v2	v
1	848	596	252	1	0	1	0	1	-1
2	596	252	92	0	1	-2	1	-1	3
2	252	92	68	1	-2	5	-1	3	-7
1	92	68	24	-2	5	-7	3	-7	10
2	68	24	20	5	-7	19	-7	10	-27
1	24	20	4	-7	19	-26	10	-27	37
5	20	4	0	19	-26	149	-27	37	-212
	4	0		**-26**	149		**37**	-212	

- GCD(848, 596) = 4 = 848 * (-26) + 596 * (37)

Calculate GCD(165,68), x, y

q	a	b	r	u1	u2	u	v1	v2	v
2	165	68	29	1	0	1	0	1	-2
2	68	29	10	0	1	-2	1	-2	5
2	29	10	9	1	-2	5	-2	5	-12
1	10	9	1	-2	5	-7	5	-12	17
9	9	1	0	5	-7	68	-12	17	-165
	1	0		**-7**	68		**17**	-165	

- GCD(165,68) = 1 = 165*(-7)+68*(17)
- Hence, MI(165) mod 68 = -7 mod 68 = 61

MI(485) mod 812 = ?

q	a	b	r	v1	v2	v
1	812	485	327	0	1	-1
1	485	327	158	1	-1	2
2	327	158	11	-1	2	-5
14	158	11	4	2	-5	72
2	11	4	3	-5	72	-149
1	4	3	1	72	-149	221
3	3	1	0	-149	221	-812
	1	0		**221**	-812	

- MI(485) mod 812 = 221

MI(608) mod 73 = ?

q	a	b	r	u1	u2	u
8	608	73	24	1	0	1
3	73	24	1	0	1	-3
24	24	1	0	1	-3	73
	1	0		**-3**	73	

- MI(608) mod 73 = -3 mod 73 = 70

MODULAR EXPONENTIAL ALGORITHM

$7^{13} \bmod 20 = ?$

- $7^4 \bmod 20 = 1$
- $7^{13} \bmod 20 = [7^{12} \bmod 20 * 7 \bmod 20] \bmod 20$
- $7^{13} \bmod 20 = (7^4 \bmod 20)^3 \bmod 20 * 7 \bmod 20 = 7$

$13^{27} \bmod 48 = ?$

- $27 = 16+8+2+1$
- $13^2 \bmod 48 = 25$
- $13^8 \bmod 48 = (13^2 \bmod 48)^4 \bmod 48 = 25^4 \bmod 48 = 1$
- $13^{16} \bmod 48 = (13^8 \bmod 48)^2 \bmod 48 = 1^2 \bmod 48 = 1$
- $13^{27} \bmod 48 = (13^{16} \bmod 48 * 13^8 \bmod 48 * 13^2 \bmod 48 * 13) \bmod 48 = (1*1*25*13) \bmod 48 = 37$

$106^{239} \bmod 54 = ?$

- $239 = 128 + 64 + 32 + 8 + 4 + 2 + 1$
- $106^2 \bmod 54 = 4$
- $106^4 \bmod 54 = (106^2 \bmod 54)^2 \bmod 54 = 4^2 \bmod 54 = 16$
- $106^8 \bmod 54 = (106^4 \bmod 54)^2 \bmod 54 = 16^2 \bmod 54 = 40$
- $106^{32} \bmod 54 = (106^8 \bmod 54)^4 \bmod 54 = 40^4 \bmod 54 = 22$
- $106^{64} \bmod 54 = (106^{32} \bmod 54)^2 \bmod 54 = 22^2 \bmod 54 = 52$
- $106^{128} \bmod 54 = (106^{64} \bmod 54)^2 \bmod 54 = 52^2 \bmod 54 = 4$
- $106^{239} \bmod 54 = (106^{128} \bmod 54 * 106^{64} \bmod 54 * 106^{32} \bmod 54 * 106^8 \bmod 54 * 106^4 \bmod 54 * 106^2 \bmod 54 * 106) \bmod 54$

$106^{239} \bmod 54 = ?$ (Contd..)

- $106^{239} \bmod 54 = (4*52*22*40*16*4*106) \bmod 54$
- $106^{239} \bmod 54 = [(4*52*22*40) \bmod 54 * (16*4*106) \bmod 54] \bmod 54$
- $106^{239} \bmod 54 = (34 * 34) \bmod 54 = 22$

FERMAT’S THEOREM

Fermat's Theorem

- $a^{p-1} \equiv 1 \pmod{p}$; where $a \in N$, $GCD(a,p)=1$, and p is a prime.
- $7^{18} \bmod 19 = 1$
- $48^{28} \bmod 29 = 1$
- $65^{96} \bmod 97 = 1$

Fermat's Theorem (Proof)

Consider the set of positive integers less than p: $\{1, 2, \ldots, p - 1\}$ and multiply each element by a, modulo p, to get the set $X = \{a \bmod p, 2a \bmod p, \ldots, (p - 1)a \bmod p\}$. None of the elements of X is equal to zero because p does not divide a. Furthermore, no two of the integers in X are equal. To see this, assume that $ja \equiv ka(\bmod p))$, where $1 \leq j < k \leq p - 1$. Because a is relatively prime to p, we can eliminate a from both sides of the equation resulting in $j \equiv k(\bmod p)$. This last equality is impossible, because j and k are both positive integers less than p. Therefore, we know that the $(p - 1)$ elements of X are all positive integers with no two elements equal. We can conclude the X consists of the set of integers $\{1, 2, \ldots, p - 1\}$ in some order. Multiplying the numbers in both sets (p and X) and taking the result mod p yields

$$a \times 2a \times \cdots \times (p - 1)a \equiv [(1 \times 2 \times \cdots \times (p - 1)](\bmod p)$$
$$a^{p-1}(p - 1)! \equiv (p - 1)! \ (\bmod p)$$

Fermat's Theorem (Proof)

- Dividing both the sides of the equation by (p-1)! (Since its coprime with p), we get $a^{p-1} \equiv 1 \pmod{p}$, which represents the Fermat's theorem
- If we multiply both the sides of the equation representing the Fermat's theorem by a, then we also get $a^p \equiv a \pmod{p}$

Fermat's Theorem (Examples)

- $7^{19} \bmod 19 = 7$
- $48^{29} \bmod 29 = 48 \bmod 29 = 19$
- $140^{73} \bmod 73 = 140 \bmod 73 = 67$

$200^{192} \bmod 97 = ?$

- $200^{96} \bmod 97 = 1$
- $200^{192} \bmod 97 = (200^{96} \bmod 97)^2 \bmod 97 = 1^2 \bmod 97 = 1$

$3^{1026} \bmod 103 = ?$

- $3^{102} \bmod 103 = 1$
- $3^{1020} \bmod 103 = (3^{102} \bmod 103)^{10} \bmod 103 = 1^{10} \bmod 13 = 1$
- $3^{1026} \bmod 103 = (3^{1020} \bmod 103 * 3^{6} \bmod 103) \bmod 103$
- $3^{1026} \bmod 103 = (1*8) \bmod 103 = 8$

EULER’S THEOREM

Euler Totient Function ($\phi(n)$)

- $\phi(n)$ = Number of natural numbers less than n which are relatively prime with n.
- $\phi(p) = p-1$; p is a prime.
- If $n = p*q$, then $\phi(n) = (p-1)*(q-1)$, where p and q are primes and $p \neq q$
- If $n=p^m$, $\phi(n) = p^m-p^{m-1}$

Proof for ϕ(n)=ϕ(p*q)=ϕ(p)*ϕ(q)

To see that $\phi(n) = \phi(p) \times \phi(q)$, consider that the set of positive integers less than n is the set $\{1, \ldots, (pq - 1)\}$. The integers in this set that are not relatively prime to n are the set $\{p, 2p, \ldots, (q - 1)p\}$ and the set $\{q, 2q, \ldots, (p - 1)q\}$. To see this, consider that any integer that divides n must divide either of the prime numbers p or q. Therefore, any integer that does not contain either p or q as a factor is relatively prime to n. Further note that the two sets just listed are non-overlapping:

Proof for $\phi(n)=\phi(p*q)=\phi(p)*\phi(q)$(Contd..)

Because p and q are prime, we can state that none of the integers in the first set can be written as a multiple of q, and none of the integers in the second set can be written as a multiple of p. Thus the total number of unique integers in the two sets is $(q - 1) + (p - 1)$. Accordingly,

$$\begin{aligned}
\phi(n) &= (pq - 1) - [(q - 1) + (p - 1)] \\
&= pq - (p + q) + 1 \\
&= (p - 1) \times (q - 1) \\
&= \phi(p) \times \phi(q)
\end{aligned}$$

Euler's Theorem

If GCD(a,n) = 1, then $a^{\phi(n)} \equiv 1 \pmod{n}$

Euler's Theorem (Proof)

Equation is true if n is prime, because in that case, $\phi(n) = (n - 1)$ and Fermat's theorem holds. However, it also holds for any integer n. Recall that $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. Consider the set of such integers, labeled as

$$R = \{x_1, x_2, \ldots, x_{\phi(n)}\}$$

That is, each element x_i of R is a unique positive integer less than n with $\gcd(x_i, n) = 1$. Now multiply each element by a, modulo n:

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots, (ax_{\phi(n)} \bmod n)\}$$

The set S is a permutation of R, by the following line of reasoning:

1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.

Euler's Theorem (Proof)

2. There are no duplicates in S. If $ax_i \bmod n = ax_j \bmod n$, then $x_i = x_j$.

Therefore,

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i (\bmod n)$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i \right] \equiv \prod_{i=1}^{\phi(n)} x_i (\bmod n)$$

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

33^{40} mod 100 = ?

- GCD(33,100) = 1
- $\phi(100) = \phi(2^2) * \phi(5^2) = (2^2-2)*(5^2-5) = 40$
- Hence 33^{40} mod 100 = 1

77^{1218} mod 240 = ?

- GCD(77, 240)=1
- $\phi(240) = \phi(2^4) * \phi(3) * \phi(5) = 8*2*4 = 64$
- 77^{64} mod 240 = 1
- 77^{1218} mod 240 = [(77^{64} mod 240$)^{19}$ * 77^2 mod 240] mod 240
- 77^{1218} mod 240 = (1*169) mod 240 = 169

PRIMALITY TESTING

Primality Testing (Properties)

The **first property** is stated as follows: If p is prime and a is a positive integer less than p, then $a^2 \bmod p = 1$ if and only if either $a \bmod p = 1$ or $a \bmod p = -1 \bmod p = p - 1$. By the rules of modular arithmetic $(a \bmod p)(a \bmod p) = a^2 \bmod p$. Thus, if either $a \bmod p = 1$ or $a \bmod p = -1$, then $a^2 \bmod p = 1$. Conversely, if $a^2 \bmod p = 1$, then $(a \bmod p)^2 = 1$, which is true only for $a \bmod p = 1$ or $a \bmod p = -1$

The **second property** is stated as follows: Let p be a prime number greater than 2. We can then write $p - 1 = 2^k q$ with $k > 0$, q odd. Let a be any integer in the range $1 < a < p - 1$. Then one of the two following conditions is true.

1. a^q is congruent to 1 modulo p. That is, $a^q \bmod p = 1$, or equivalently, $a^q \equiv 1 \pmod{p}$.
2. One of the numbers $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to -1 modulo p. That is, there is some number j in the range $(1 \le j \le k)$ such that $a^{2^{j-1}q} \bmod p = -1 \bmod p = p - 1$ or equivalently, $a^{2^{j-1}q} \equiv -1 \pmod{p}$.

Miller Rabin Algorithm (MLA)

TEST (n)

1. Find integers k, q, with $k > 0$, q odd, so that ($n - 1 = 2^k q$);
2. Select a random integer $a, 1 < a < n - 1$;
3. **if** $a^q \bmod n = 1$ **then** return("inconclusive");
4. **for** $j = 0$ **to** $k - 1$ **do**
5. **if** $a^{2^j q} \bmod n = n - 1$ **then** return("inconclusive");
6. return("composite");

Miller Rabin Algorithm (Proof)

Fermat's theorem states that $a^{n-1} \equiv 1 \pmod{n}$ if n is prime. We have $p - 1 = 2^k q$. Thus, we know that $a^{p-1} \bmod p = a^{2^k q} \bmod p = 1$. Thus, if we look at the sequence of numbers

$$a^q \bmod p,\ a^{2q} \bmod p,\ a^{4q} \bmod p,\ \ldots,\ a^{2^{k-1}q} \bmod p,\ a^{2^k q} \bmod p$$

we know that the last number in the list has value 1. Further, each number in the list is the square of the previous number. Therefore, one of the following possibilities must be true.

1. The first number on the list, and therefore all subsequent numbers on the list, equals 1.
2. Some number on the list does not equal 1, but its square mod p does equal 1. By virtue of the first property of prime numbers defined above, we know that the only number that satisfies this condition is $p - 1$. So, in this case, the list contains an element equal to $p - 1$.

This completes the proof.

MLA on 105

- $n = 105$
- $n\text{-}1 = 2^k * q$
- $104 = 2^3 * 13$; where $k=3$ and $q=13$
- Select $a = 2$
- $a^q \bmod n = 2^{13} \bmod 105 = 2$
- $a^{2*q} \bmod n = (a^q \bmod n)^2 \bmod n = 2^2 \bmod 105 = 4$
- $a^{4*q} \bmod n = (a^{2*q} \bmod n)^2 \bmod n = 4^2 \bmod 105 = 16$
- Hence, 105 is composite

MLA on 35

- $n = 35$
- $n-1 = 2^k * q$ i.e. $34 = 2^1 * 17$; where k=1 and q=17
- Select a=2
- $a^q \bmod n = 2^{17} \bmod 35 = 32$
- Hence 35 is composite

MLA on 233

- $n = 233$
- $n-1 = 2^k * q$ i.e. $232 = 2^3 * 29$; where $k=3$ and $q=29$
- Select $a = 2$
- $a^q \bmod n = 2^{29} \bmod 233 = 1$
- Hence, 233 is a prime

MLA on 61

- $n = 61$
- $n\text{-}1 = 2^k * q$ i.e. $60 = 2^2 * 15$; where $k=2$ and $q=15$
- Select $a = 2$
- $a^q \bmod n = 2^{15} \bmod 61 = 11$
- $a^{2*q} \bmod n = (a^q \bmod n)^2 \bmod n = 11^2 \bmod 61 = 60$
- Hence, 61 is prime

MLA on 241

- $n = 241$
- $n-1 = 2^k * q$ i.e. $240 = 2^4 * 15$; where k=4 and q=15
- Select a = 2
- $a^q \bmod n = 2^{15} \bmod 241 = 233$
- $a^{2*q} \bmod n = (a^q \bmod n)^2 \bmod n = 233^2 \bmod 241 = 64$
- $a^{4*q} \bmod n = (a^{2*q} \bmod n)^2 \bmod n = 64^2 \bmod 241 = 240$
- Hence, 241 is prime

CHINESE REMAINDER THEOREM (CRT)

CRT algorithm

- Let $m_1, m_2, m_3, \ldots\ldots\ldots\ldots\ m_k$, be a pairwise relatively prime integers. If $a_1, a_2, \ldots\ldots.a_k \in Z$, then there exists $x \in Z$, which satisfies the linear set of congruences:-

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

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

$$\ldots\ldots\ldots$$

$$x \equiv a_k \pmod{m_k}$$

where $M = m_1 * m_2 * \ldots\ldots.. * m_k$

- $M_i = M/m_i$
- $x = (a_1 * M_1 * N_1 + a_2 * M_2 * N_2 + \ldots\ldots\ldots\ldots + a_k * M_k * N_k) \bmod M$

where $N_i = MI(M_i) \bmod m_i$

CRT Example 1:-

- Solve for x:-

$$x \equiv 1 \pmod{5}$$

$$x \equiv 2 \pmod{6}$$

$$x \equiv 3 \pmod{7}$$

- $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $m_1 = 5$, $m_2 = 6$, $m_3 = 7$;
- $M = m_1 * m_2 * m_3 = 5*6*7 = 210$
- $M_1 = M/m_1 = 210/5 = 42$
- $M_2 = M/m_2 = 210/6 = 35$
- $M_3 = M/m_3 = 210/7 = 30$

CRT Example 1 (Contd..)

- $N_1 = MI(M_1) \pmod{m_1}$
- $N_1 = MI(42) \pmod{5}$

q	a	b	r	u1	u2	u
8	42	5	2	1	0	1
2	5	2	1	0	1	-2
2	2	1	0	1	-2	5
	1	0		**-2**	5	

- $N_1 = -2 \pmod{5} = 3$

CRT Example 1 (Contd..)

- $N_2 = MI(M_2) \pmod{m_2}$
- $N_2 = MI(35) \pmod{6}$

q	a	b	r	u1	u2	u
5	35	6	5	1	0	1
1	6	5	1	0	1	-1
5	5	1	0	1	-1	6
	1	0		**-1**	6	

- $N_2 = -1 \bmod 6 = 5$

CRT Example 1 (Contd..)

- $N_3 = MI(M_3) \pmod{m_3}$
- $N_3 = MI(30) \pmod 7$

q	a	b	r	u1	u2	u
4	30	7	2	1	0	1
3	7	2	1	0	1	-3
2	2	1	0	1	-3	7
	1	0		**-3**	7	

- $N_3 = -3 \bmod 7 = 4$

CRT Example 1 (Contd..)

- $x = (a_1*M_1*N_1 + a_2*M_2*N_2 + a_3*M_3*N_3) \bmod M$
- $x = (1*42*3 + 2*35*5 + 3*30*4) \bmod 210 = 206$

CRT Example 2:-

- Solve for x:-

x	$\equiv$	3	(mod 5)
x	$\equiv$	4	(mod 8)
x	$\equiv$	11	(mod 13)
x	$\equiv$	6	(mod 17)

- $a_1 = 3$, $a_2 = 4$, $a_3 = 11$, $a_4 = 6$ $m_1 = 5$, $m_2 = 8$, $m_3 = 13$, $m_4 = 17$;
- $M = m_1 * m_2 * m_3 * m_4 = 5*8*13*17 = 8840$
- $M_1 = M/m_1 = 8840/5 = 1768$
- $M_2 = M/m_2 = 8840/8 = 1105$
- $M_3 = M/m_3 = 8840/13 = 680$
- $M_4 = M/m_4 = 8840/17 = 520$

CRT Example 2 (Contd..)

- $N_1 = MI(M_1) \pmod{m_1}$
- $N_1 = MI(1768) \pmod{5}$

q	a	b	r	u1	u2	u
353	1768	5	3	1	0	1
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
	1	0		**2**	-5	

- $N_1 = 2$

CRT Example 2 (Contd..)

- $N_2 = MI(M_2) \pmod{m_2}$
- $N_2 = MI(1105) \pmod{8}$

q	a	b	r	u1	u2	u
138	1105	8	1	1	0	1
8	8	1	0	0	1	-8
	1	0		**1**	-8	

- $N_2 = 1$

CRT Example 2 (Contd..)

- $N_3 = MI(M_3) \pmod{m_3}$
- $N_3 = MI(680) \pmod{13}$

q	a	b	r	u1	u2	u
52	680	13	4	1	0	1
3	13	4	1	0	1	-3
4	4	1	0	1	-3	13
	1	0		**-3**	13	

- $N_3 = -3 \bmod 13 = 10$

CRT Example 2 (Contd..)

- $N_4 = MI(M_4) \pmod{m_4}$
- $N_4 = MI(520) \pmod{17}$

q	a	b	r	u1	u2	u
30	520	17	10	1	0	1
1	17	10	7	0	1	-1
1	10	7	3	1	-1	2
2	7	3	1	-1	2	-5
3	3	1	0	2	-5	17
	1	0		**-5**	17	

- $N_4 = -5 \bmod 17 = 12$

CRT Example 2 (Contd..)

- $x = (a_1{*}M_1{*}N_1 + a_2{*}M_2{*}N_2 + a_3{*}M_3{*}N_3 + a_4{*}M_4{*}N_4) \bmod M$
- $x = (3{*}1768{*}2 + 4{*}1105{*}1 + 11{*}680{*}10 + 6{*}520{*}12) \bmod 8840 = 3508$

DISCRETE LOGARITHMS

Order of an Integer a mod n

- $Order_n(a)$= smallest natural number k such that a^k mod n = 1; where GCD(a,n)=1, $1 \le a < n$, and $1 \le k \le \phi(n)$.
- $Order_7(2) = 3$ $(2)^3 mod 7 = 1$
- $Order_5(3) = 4$ $(3)^4 mod 5 = 1$
- $Order_{15}(8) = 4$ $(8)^4 mod 15 = 1$
- $Order_9(8) = 2$ $(8)^2 mod 9 = 1$
- $Order_8(1) = 1$

$Ord_9(4) = ?$

- $GCD(4,9) = 1$
- $4^1 \bmod 9 = 4$
- $4^2 \bmod 9 = 7$
- $4^3 \bmod 9 = 1$
- Therefore $Ord_9(4) = 3$

$\text{Ord}_{11}(8) = ?$

- GCD(8,11) = 1
- $\phi(11) = 10$
- $8^1 \bmod 11 = 8$
- $8^2 \bmod 11 = 9$
- $8^3 \bmod 11 = 6$
- $8^4 \bmod 11 = 4$
- $8^5 \bmod 11 = 10$
- $8^6 \bmod 11 = 3$
- $8^7 \bmod 11 = 2$
- $8^8 \bmod 11 = 5$
- $8^9 \bmod 11 = 7$
- $8^{10} \bmod 11 = 1$
- Therefore $\text{Ord}_{11}(8) = 10$

$\mathrm{Ord}_{12}(8) = ?$

- $\mathrm{GCD}(8,12) = 4$.
- Therefore $\mathrm{Ord}_{12}(8)$ doesn’t exist.

Primitive Roots of n

- ‘a’ is a primitive root of n if $Ord_n(a) = \phi(n)$.
- All n don’t have primitive roots. For n to have primitive roots, n=2, 4, p^α, $2*p^\alpha$, where p is any odd prime, α is a natural number
- Examples of natural numbers having primitive roots are 2,3,4,5,6,7,9,10,11, etc.
- Examples of natural numbers which don’t have primitive roots are 8, 12, 15, etc.
- Primitive roots of 7 are 3 and 5.
- Primitive roots of 5 are 2 and 3.

Primitive Roots of 11

- $\phi(11) = 10$

<u>a=1</u>:-

- $1^1 \bmod 11$
- $Ord_{11}(1) = 1$
- Hence 1 is not a primitive root of 11

<u>a=2</u>:-

- $2^1 \bmod 11 = 2$
- $2^2 \bmod 11 = 4$
- $2^3 \bmod 11 = 8$
- $2^4 \bmod 11 = 5$
- $2^5 \bmod 11 = 10$
- $2^6 \bmod 11 = 9$

Primitive Roots of 11 (Contd..)

- $2^7 \bmod 11 = 7$
- $2^8 \bmod 11 = 3$
- $2^9 \bmod 11 = 6$
- $2^{10} \bmod 11 = 1$
- $Ord_{11}(2) = 10$
- Hence 2 is a primitive root of 11

a=3:-

- $3^1 \bmod 11 = 3$
- $3^2 \bmod 11 = 9$
- $3^3 \bmod 11 = 5$
- $3^4 \bmod 11 = 4$
- $3^5 \bmod 11 = 1$
- $Ord_{11}(3) = 5$
- Hence, 3 is not a primitive root of 11

Primitive Roots of 11 (Contd..)

a=4:-

- $4^1 \bmod 11 = 4$
- $4^2 \bmod 11 = 5$
- $4^3 \bmod 11 = 9$
- $4^4 \bmod 11 = 3$
- $4^5 \bmod 11 = 1$
- $Ord_{11}(4) = 5$
- Hence 4 is not a primitive root of 11

a=5:-

- $Ord_{11}(5) = 5$
- Hence , 5 is not a primitive root of 11.

Primitive Roots of 11 (Contd..)

a=6:-

- $Ord_{11}(6) = 10$
- Hence , 6 is a primitive root of 11.

a=7:-

- $Ord_{11}(7) = 10$
- Hence , 7 is a primitive root of 11.

a=8:-

- $Ord_{11}(8) = 10$
- Hence , 8 is a primitive root of 11.

Primitive Roots of 11 (Contd..)

a=9:-

- $Ord_{11}(9) = 5$
- Hence , 9 is not a primitive root of 11.

a=10:-

- $Ord_{11}(10) = 2$
- Hence , 10 is not a primitive root of 11.

- Therefore, the primitive roots of 11 are 2, 6, 7, and 8

Primitive Roots of 2

- $n = 2$
- $\phi(2) = 1$
- $1^1 \bmod 2 = 1$
- Hence, $Ord_2(1) = 1$
- The primitive root of 2 is 1.

Primitive Roots of 4

- n = 4
- $\phi(4) = 2$
- $Ord_4(1) = 1$
- GCD(2,4) = 2; Hence 2 can’t be a primitive root of 4
- $Ord_4(3) = 2$
- Hence 3 is a primitive root of 4

Primitive Roots of 9

- $n = 9 = 3^2$; Here $p = 3$, and $\alpha=2$
- $\phi(9) = 3^2 - 3 = 6$
- $Ord_9(1) = 1$
- $Ord_9(2) = 6$; Hence 2 is a primitive root
- $GCD(3,9) = 3$
- $Ord_9(4) = 3$
- $Ord_9(5) = 6$; Hence 5 is a primitive root
- $GCD(6,9) = 3$
- $Ord_9(7) = 3$
- $Ord_9(8) = 2$
- The primitive roots of 9 are 2 and 5.

Primitive Roots of 20

- 20 cannot be expressed as p^α or $2*p^\alpha$
- Hence 20 doesn’t have any primitive root.

Observations Regarding Primitive Roots

- If **a** is a primitive root of n, then the set $\{a^1, a^2, \ldots\ldots\ldots, a^{\phi(n)}\} \pmod{n}$ contain unique elements and are relatively prime to n.
- For example, the set $\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6\} \pmod{9} = \{2, 4, 8, 7, 5, 1\}$ contains unique elements which are relatively prime to 9.

Discrete Logarithms

- If $b = a^x \bmod n$, then discrete logarithm is given by $x = dlog_{a,n}(b)$, where $GCD(b,n) = 1$ and ‘a’ is a primitive root of n.
- Calculating Discrete Logarithms is a relatively harder problem than exponentiation.

<u>Calculate the Discrete logarithm x, where $3^x \bmod 7 = 4$:-</u>

- $GCD(4,7) = 1$
- $Ord_7(3) = 6$;
- Min value of $x = 4$.
- Therefore, $x = 4+6*k$, where $k \in W$.

Solve for x:- $5^x \pmod{18} = 11$

- $GCD(11,18) = 1$
- $Ord_{18}(5) = 6$
- Min value of $x = 5$
- Therefore, $x = 5+6*k$, where $k \in W$.