TUTORIAL

CSCI361 – Computer Security

Sionggo Japit

sjapit@uow.edu.au

17 January 2020

NUMBER THEORY

Divisor, common divisor, and greatest common divisor (GCD)

Some number theory

- Let *a*, *b* be integers, then *a* divides *b* if there exists an integer *c* such that *b* = *ac*. In another words, *a* is a divisor of *b*, or *a* is a factor of *b*.
  - E.g., 10 = 2 ´ 5

- If *a* divides *b*, then this is denoted by *a*|*b*.
  - E.g., 2 | 10

Some number theory

- An integer *c* is *common divisor* of *a* and *b* if *c*|*a* and *c*|*b*.
  - E.g., $2 \mid 12$ and $2 \mid 8$, hence 2 is a common divisor of 12 and 8

Some number theory

- A non-negative integer *d* is the *greatest common divisor* of integers *a* and *b*, denoted *d = gcd(a, b)*, if
  - *d* is a common divisor of *a* and *b*; and
  - whenever $c|a$ and $c|b$, then $c|d$.
    - E.g., $1|12$ and $1|8$,

      $2|12$ and $2|8$,

      $4|12$ and $4|8$

      4 is the greatest common divisor because

      whenever, $1|12$ and $1|8$, then $1|4$, and

      $2|12$ and $2|8$, then $2|4$, and

      $4|12$ and $4|8$, then $4|4$.

Some number theory

- Equivalently, $\gcd(a, b)$ is the largest positive integer that divides both a and b, with the exception that $\gcd(0,0) = 0$

Hence $4 = \gcd(8, 12)$

Some number theory

- Two integers a and b are said to be $\mathit{relatively\ prime}$ or $\mathit{coprime}$ if $\gcd(a, b) = 1$.

E.g., 3 and 7 are coprime; that is, gcd(3,7) = 1 because 1|3 and 1|7. There is no other common divisor that divides both 3 and 7.

Similarly, 3 and 4 are coprime; that is, gcd(3,4) = 1 because 1|3 and 1|4, and there is no other common divisor that divides both 3 and 4.

Euclidean algorithm

- Euclidean algorithm for computing the greatest common divisor (gcd) of two integers:

INPUT: two non-negative integers a and b with $a \geq b$.
OUTUT: the greatest common divisor of a and b.

```
While $b \neq 0$ do the following:
    Set $r \leftarrow a\ mod\ b$,
        $a \leftarrow b$,
        $b \leftarrow r$.
Return (a)
```

Euclidean algorithm

```
While $b \neq 0$ do the following:
        Set $r \leftarrow a \bmod b$,
            $a \leftarrow b$,
            $b \leftarrow r$.
Return (a)
```

- Example: $\gcd(4864, 3458) = 38$

a	b	q	r
4864	3458	1	1406
3458	1406	2	646
1406	646	2	114
646	114	5	76
114	76	1	38
76	38	2	0
38	0		

NUMBER THEORY

Modular Arithmetic

Modular Arithmetic

- Modular arithmetic provides Cryptography with a practical way of handling very large whole numbers.
  - It allows large numbers to be constrained and easily managed.
- Both RSA and El Gamal use modular arithmetic.
  - Also known as modulo, or clock arithmetic.
  - Arithmetic system for integers where numbers "wrap around" after a certain value.
    - E.g., Clock with 12 hours, time with 24 hours.

Modular Arithmetic

- In this system, valid integers go from $0 - 11$ or $0 - 23$
- Does not matter how many times we go round the clock
  - 1700 hours is always 5pm, and even if we add another 2400 hours to it to make it 4100 hours, it is still 5 pm.
  - We are only interested in the hours within the day.
- Widely used in fields such as number theory, ring theory, cryptography, chemistry and even music.

Modular m

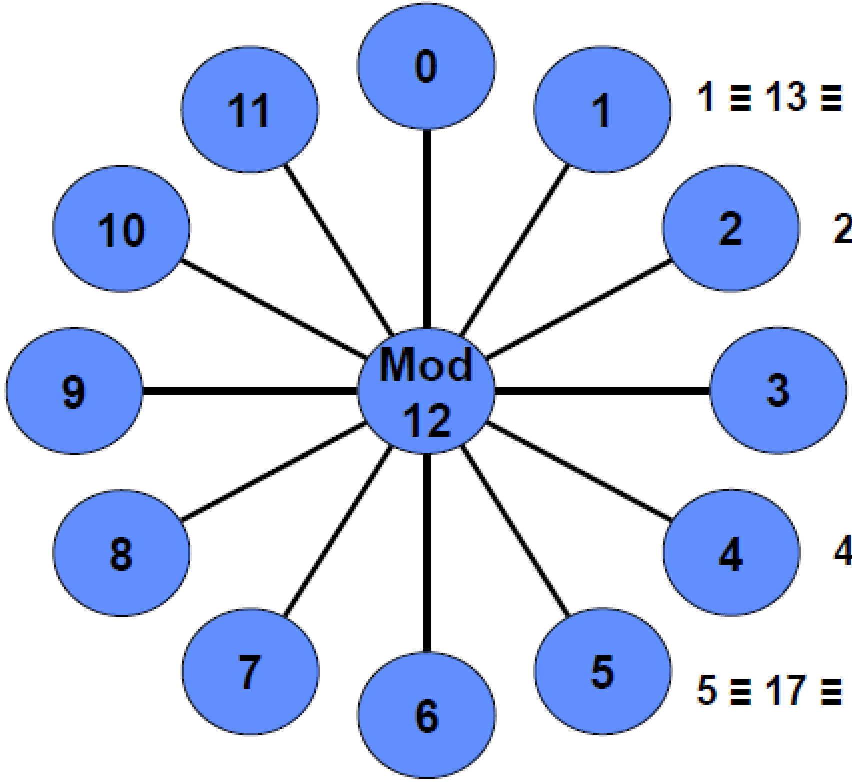
- In a modulo m system,
  - We limit the field of integers to $mod\ m$.
    - E.g., for a $12 - hour$ clock, $m = 12$, and all numbers are constrained from $0 - 11$.
    - All numbers n can be written as $n = km + r$ where $0 \leq r \leq m - 1$.
      - km generally plays no part in computations

Modular m

- Integers resulting from computations always in range of 0 to $m-1$.
  - To do so
    - If answer is $+$ and $\geq m$, we *subtract as many multiples of m as needed*.
    - If answer is $-$, we *add as many multiples as needed*.

Equivalence Classes

$0 \equiv 12 \equiv 24 \equiv 36 \equiv 48, \ldots(\text{mod } 12) = [0]_{12}$



$1 \equiv 13 \equiv 25 \equiv 37 \equiv 49, \ldots(\text{mod } 12) = [1]_{12}$

$2 \equiv 14 \equiv 26 \equiv 38 \equiv 50, \ldots(\text{mod } 12) = [2]_{12}$

$3 \equiv 15 \equiv 27 \equiv 39 \equiv 51, \ldots(\text{mod } 12) = [3]_{12}$

$4 \equiv 16 \equiv 28 \equiv 40 \equiv 52, \ldots(\text{mod } 12) = [4]_{12}$

$5 \equiv 17 \equiv 29 \equiv 41 \equiv 53, \ldots(\text{mod } 12) = [5]_{12}$

$6 \equiv 18 \equiv 30 \equiv 42 \equiv 54, \ldots(\text{mod } 12) = [6]_{12}$

Equivalence Classes

- The *equivalence class* of a modulo m is the set:
  $\{\dots, a-2m, a-m, a, a+m, a+2m, \dots\}$
- Examples
  - $5\ mod\ 12$ has the equivalence set
    $\{\dots, -19, -7, 5, 17, 29, 41, 53, \dots\}$
- All the members of an equivalence are *congruent* to each other
  - $a \equiv a-2m \equiv a-m \equiv a+m \equiv a+2m \dots$

Congruence

- Two numbers a and b are said to be $congruent\ mod\ m$ if

  $a\ mod\ m = b\ mod\ m$

- We can also think of congruence as

  $r = (a - b) mod\ m$

  Where r must be a multiple of m, i.e., $(0, m, 2m, 3m, \ldots)$

- We write congruence as $a \equiv b(mod\ n)$
- E.g., $38 \equiv 14(mod\ 12)$

  $38 \equiv 2(mod\ 12)$

  $-3 \equiv 2(mod\ 5)$

Congruence

- The congruence relation is a binary equivalence relation:
- E.g., we read:

$$38 \equiv 14 (mod\ 12)$$

as “38 is congruent to $14 (mod\ 12)$”

Residue

- Modular arithmetic is related to finding the integer remainder in division
  - E.g., $2 = 14 (mod\ 12)$, or more commonly: $14\ mod\ 12 = 2$
  - The equality sign is used.
  - The $remainder$ is called the $common\ residue$, which is the $smallest\ non - negative$ member of an equivalence class.
  - Correct to say:

$$38 \equiv 14 (mod\ 12)$$

$$2 \equiv 14 (mod\ 12)$$

and $2 = 14 (mod\ 12)$

It is incorrect to say:

$$38 = 14 (mod\ 12)$$

Residue

- Residue classes
  - This refers to the set of numbers congruent to $a\ mod\ m$ where a is the common residue and can be denoted as the set of numbers $[a]_m$
  - Residue classes sometimes denoted as $[a]_n$
  - There are exactly n different sets of $[a]_n$
    - $[0]_n, [1]_n, [2]_n, [3]_n, \dots [n-1]_n$

Important Modular Arithmetic Relations

- Addition:

  $[a]_n + [b]_n = [a + b]_n$

  i.e., $a(mod\, n) + b(mod\, n) = (a + b)(mod\, n)$
- Subtraction:

  $[a]_n - [b]_n = [a - b]_n$

  i.e., $a(mod\, n) - b(mod\, n) = (a - b)(mod\, n)$
- Multiplication:

  $[a]_n \times [b]_n = [a \times b]_n$

  i.e., $a(mod\, n) \times b(mod\, n) = (a \times b)(mod\, n)$

Basic Modular Arithmetic

- $(u + v) mod\ m = \big((u\ mod\ m) + (v\ mod\ m)\big)\ mod\ m$
- $(u \times v) mod\ m = \big((u\ mod\ m) \times (v\ mod\ m)\big)\ mod\ m$
- Example:

$\big(31 \times (23 + 16)\big)\ mod\ 9$

$=\Big((31\ mod\ 9) \times \big((23\ mod\ 9) + (16\ mod\ 9)\big)\Big)\ mod\ 9$

$=\Big(\big(4 \times (5 + 7)\big)\Big)\ mod\ 9$

$=\big(4 \times (12\ mod\ 9)\big)\ mod\ 9$

$=(4 \times 3)\ mod\ 9$

$=12\ mod\ 9$

$=3$

Computational Complexity of Modular Multiplication

- Computational complexity of $(u \times v)\ mod\ m$
    - We note that $(u \times v)\ mod\ m = \big((u\ mod\ m) \times$

Computational Complexity of Modular Multiplication

- If $u', v'$and m are all of bitsize b, the complexities are:
  - $O(b^2)$ for multiplication operation, and
  - $O(b^2)$ for the modulus operation
- Since both operations happen independent of each other, the overall complexity is $O(b^2 + b^2) = O(2b^2)$ or $O(b^2)$ if n is very large.

Modular Division

- However, unfortunately division cannot always be defined.
- Three possible cases:
    - There are cases where there is $a\ unique\ answer$:
        - E.g., what is $\frac{[5]_{12}}{[7]_{12}} = ?$
        - We translate that to: $? \times [7]_{12} = [5]_{12}$
        - We try all possible answers one-by-one:
            - $? \times [7]_{12} = [5]_{12}$
            - $? \times [7]_{12} = [17]_{12}$
            - $? \times [7]_{12} = [29]_{12}$
            - $? \times [7]_{12} = [41]_{12}$
            - $? \times [7]_{12} = [65]_{12}$
            - $[11]_{12} \times [7]_{12} = [77]_{12}$

Only $[11]_{12}$ satisfies the equation: $? \times [7]_{12} = [5]_{12}$.

Modular Division

- There are cases where there is $\mathit{no\ unique\ answer}$.
- E.g., What is $\frac{[5]_{10}}{[5]_{10}} = ?$
  - We translate that to: $? \times [5]_{10} = [5]_{10}$
  - We try all possible answers one-by-one:
    - $[1]_{10} \times [5]_{10} = [5]_{10}$
    - $[3]_{10} \times [5]_{10} = [5]_{10}$
    - $[5]_{10} \times [5]_{10} = [5]_{10}$
    - $[7]_{10} \times [5]_{10} = [5]_{10}$
    - $[9]_{10} \times [5]_{10} = [5]_{10}$
    - …

There is an infinite number of possible answers $\Longrightarrow$ no unique answer.

Modular Division

- There are cases where there are $no\ answers$!
- E.g., What is $\frac{[1]_{10}}{[5]_{10}} = ?$
  - We translate that to: $? \times [5]_{10} = [1]_{10}$
  - We try all possible answers one-by-one:
    - $? \times [5]_{10} = [1]_{10}$
    - $? \times [5]_{10} = [11]_{10}$
    - $? \times [5]_{10} = [21]_{10}$
    - $? \times [5]_{10} = [31]_{10}$
    - $? \times [5]_{10} = [41]_{10}$
    - $? \times [5]_{10} = [51]_{10}$
    - …

There is no answer at all!

Modular Inverse

- The multiplicative inverse a^{-1} of a number a satisfies

$$a \times a^{-1} = 1$$

- Similarly, the modular multiplicative inverse of $a\ mod\ m$ is the number a^{-1} where $1 \leq a^{-1} \leq m - 1$ such that

$$a \times a^{-1} = 1\ (mod\ m)$$

Example,

- The modular inverse $2\ mod\ 17$ is 9, since $2 \times 9\ mod\ 17 = 1$
- Conversely, the modular inverse of $9\ mod\ 17$ is 2, since $9 \times 2\ mod\ 17 = 1$
- This is because modular multiplication is commutative.

Use of Modular Inverses

- If modulus m is prime, then all numbers between 1 and $m - 1$ will have modular inverse mod m
- If modulus m is composite, then all numbers which are co-prime with m will have modular inverse mod m
- If they exist, modular inverse are very useful in modular division
  - Example:
  - If $M \times S = C\ mod\ p$

➢ $M = \frac{C}{S}\ mod\ p$

➢ $M = C \times S^{-1} mod\ p$

So instead of doing a modular division, we simply find the modular inverse of $S\ (mod\ p)$ and multiply it with C to get M.

NUMBER THEORY

Extended Euclidean algorithm

Extended Euclidean algorithm

- While it is possible to work out modular inverses by trial and error for small numbers, this will not work for large numbers.
- Euclid’s algorithm provides a very efficient way to find modular inverses, and is of complexity $O(b^2)$
- To find the inverse of a number $n \ mod \ m$:
    - Find two integers a and b such that

$$1 = an - bm$$

Extended Euclidean algorithm

The Euclidean algorithm can be extended so that it not only yields the *greatest common divisor* d of two integers a and b, but also integers *x* and *y* satisfying $ax + by = d$; where $d = \gcd(a, b)$. In other words,

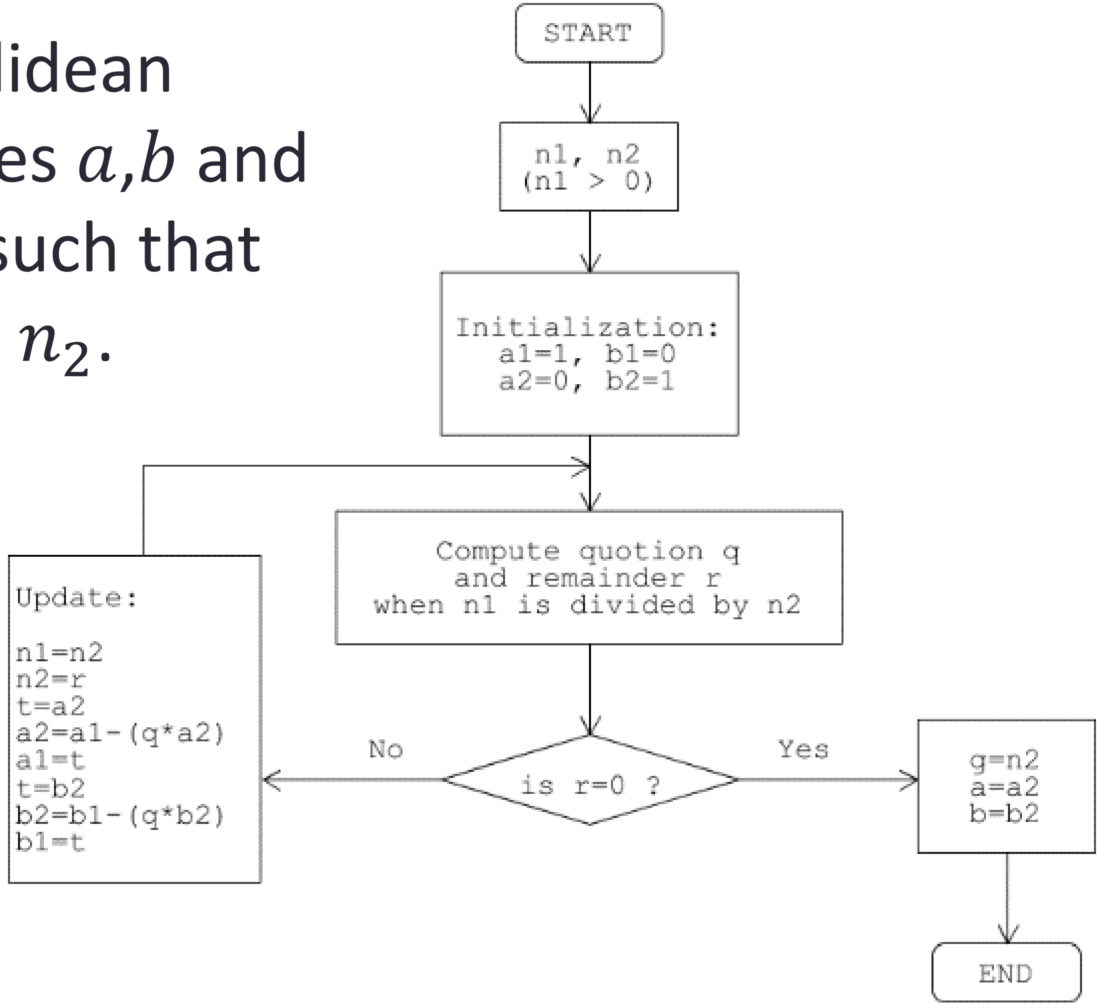
gcd(a,b) = ax + by

If *gcd(a,b) = 1*, then *ax + by = 1*. In such a case,

- x is known as $a^{-1}\ mod\ b$ (inverse multiplicative modulo b), and
- y is known as $b^{-1}\ mod\ a$ (inverse multiplicative modulo a)

Extended Euclidean algorithm

The Extended Euclidean algorithm calculates a,b and $g = gcd(n_1, n_2)$ such that $g = a \times n_1 + b \times n_2$.



START

n1, n2
(n1 > 0)

Initialization:
a1=1, b1=0
a2=0, b2=1

Compute quotion q
and remainder r
when n1 is divided by n2

is r=0 ?

No

Update:

n1=n2
n2=r
t=a2
a2=a1-(q*a2)
a1=t
t=b2
b2=b1-(q*b2)
b1=t

Yes

g=n2
a=a2
b=b2

END

Extended Euclidean algorithm

Find gcd(4864,3458) and a, b such that

$$4864a + 3458b = \gcd(4864,3458)$$

Extended Euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458			1	0	0	1

Extended Euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1

Extended Euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406			0	1		

n1 = n2, n2 = r

a1 = a2, b1 = b2

Extended Euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1

a2 = a1 – q * a2

b2 = b1 – q * b2

Extended Euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646			1	-1		

n1 = n2, n2 = r

a1 = a2, b1 = b2

Extended Euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646	114	2	1	-1	-2	3

a2 = a1 – q * a2

b2 = b1 – q * b2

Extended Euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646	114	2	1	-1	-2	3
646	114	76	5	-2	3	5	-7

Extended Euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646	114	2	1	-1	-2	3
646	114	76	5	-2	3	5	-7
114	76	38	1	5	-7	-27	38

Extended Euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646	114	2	1	-1	-2	3
646	114	76	5	-2	3	5	-7
114	76	38	1	5	-7	-27	38
76	38	0	2	-27	38	32	-45

$$\gcd(4864, 3458) = 38, \textit{ thus } 4864 \times 32 + 3458 \times -45 = 38$$

Extended Euclidean algorithm

Find 121^{-1} mod 654.

How?

Recall that the Euclidean algorithm can be extended so that it not only yields the *greatest common divisor d* of two integers *a* and *b*, but also integers *x* and *y* satisfying *ax* + *by* = *d*; where d = gcd(a,b). In other words,

$$\gcd(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{ax} + \boldsymbol{by}$$

Extended Euclidean algorithm

Find 121^{-1} mod 654

n1	n2	r	q	a1	b1	a2	b2
654	121			1	0	0	1

Extended Euclidean algorithm

Find 121^{-1} mod 654

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1

Extended Euclidean algorithm

Find 121^{-1} mod 654

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5

Extended Euclidean algorithm

Find 121^{-1} mod 654

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5
49	23	3	2	1	-5	-2	11

Extended Euclidean algorithm

Find 121^{-1} mod 654

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5
49	23	3	2	1	-5	-2	11
23	3	2	7	-2	11	5	-27

Extended Euclidean algorithm

Find 121^{-1} mod 654

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5
49	23	3	2	1	-5	-2	11
23	3	2	7	-2	11	5	-27
3	2	1	1	5	-27	-37	200

Extended Euclidean algorithm

Find 121^{-1} mod 654

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5
49	23	3	2	1	-5	-2	11
23	3	2	7	-2	11	5	-27
3	2	1	1	5	-27	-37	200
2	1	0	2	-37	200	42	-227

Extended Euclidean algorithm

Thus $n1 ´ \; a2 \; + \; n2 ´ \; b2 \; = \; \mathrm{gcd}(n1, n2)$

$654 ´ \; 42 \; + \; 121 ´ \; -227 = 1$

$1 = 1$

Extended Euclidean algorithm

$$\text{Since gcd}(654,121) = 1\text{, there exist multiplicative inverse:}$$

$$a2 = \text{multiplicative inverse n1 mod n2, and}$$
$$b2 = \text{multiplicative inverse n2 mod n1}$$

$$n1 \times a2 \ + \ n2 \times b2 \ = \ \text{gcd}(n1, n2)$$
$$654 \times 42 \ + \ 121 \times -227 = 1$$

$$Thus\ 121^{-1} \text{ mod } 654 = -227 \text{ mod } 654 = 427 \text{ mod } 654$$

$$Check: 427 \times 121 \text{ mod } 654 = 1 \text{ mod } 654$$

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234			1	0	0	1

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3
619	615	4	1	1	-3	-1	4

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3
619	615	4	1	1	-3	-1	4
615	4	3	153	-1	4	2	-7

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3
619	615	4	1	1	-3	-1	4
615	4	3	153	-1	4	2	-7
4	3	1	1	2	-7	-307	1075

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3
619	615	4	1	1	-3	-1	4
615	4	3	153	-1	4	2	-7
4	3	1	1	2	-7	-307	1075
3	1	0	3	-307	1075	309	-1082

Extended Euclidean algorithm

From the above, we have:

$$4321 ´ 309 + 1234 ´ -1082 = 1$$

Thus the multiplicative inverses of $1234 \mod 4321$ are:

$$x = 309 \mod 1234, \textit{ and}$$

$$y = -1082 \mod 4321 = 3239 \mod 4321$$

Check:

$$309 ´ 4321 \mod 1234 = 1 \mod 1234$$

$$3239 ´ 1234 \mod 4321 = 1 \mod 4321$$

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 120.

n1	n2	r	q	a1	b1	a2	b2
1234	120			1	0	0	1

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 120.

n1	n2	r	q	a1	b1	a2	b2
1234	120	34	10	1	0	0	1

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 120.

n1	n2	r	q	a1	b1	a2	b2
1234	120	34	10	1	0	0	1
120	34	18	3	0	1	1	-10

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 120.

n1	n2	r	q	a1	b1	a2	b2
1234	120	34	10	1	0	0	1
120	34	18	3	0	1	1	-10
34	18	16	1	1	-10	-3	31

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 120.

n1	n2	r	q	a1	b1	a2	b2
1234	120	34	10	1	0	0	1
120	34	18	3	0	1	1	-10
34	18	16	1	1	-10	-3	31
18	16	2	1	-3	31	4	-41

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 120.

n1	n2	r	q	a1	b1	a2	b2
1234	120	34	10	1	0	0	1
120	34	18	3	0	1	1	-10
34	18	16	1	1	-10	-3	31
18	16	2	1	-3	31	4	-41
16	2	0	8	4	-41	-7	72

Extended Euclidean algorithm

Find the multiplicative inverse of 1234 mod 120.

n1	n2	r	q	a1	b1	a2	b2
1234	120	34	10	1	0	0	1
120	34	18	3	0	1	1	-10
34	18	16	1	1	-10	-3	31
18	16	2	1	-3	31	4	-41
16	2	0	8	4	-41	-7	72

Since GCD(1234, 120) = 2, there is no multiplicative inverse exist.

Extended Euclidean algorithm

Alternative method: (back substitution)

$1 = an - bm$

$\Rightarrow an = 1 + bm$

$\Rightarrow an(mod\ m) = (1 + bm)(mod\ m)$

$\Rightarrow an(mod\ m) = \Big(\big(1(mod\ m)\big) + \big(bm(mod\ m)\big)\Big)\ mod\ m$

$\Rightarrow an(mod\ m) = \big(1(mod\ m)\big) mod\ m$

$\Rightarrow an(mod\ m) = 1(mod\ m)$

$\Rightarrow an = 1(mod\ m)$

$\Rightarrow a\ is\ the\ modular\ inverse\ of\ n\ mod\ m$

Note: $bm\ (mod\ m) = 0$

Why?

Extended Euclidean algorithm

Example

- Find the inverse of 223 mod 660
  - Look for a and b such that $1 = a(223) - b(660)$
  - Work forwards

1. $660 = 2(223) + 214 \quad \Rightarrow 214 = 660 - 2(223)$
2. $223 = 1(214) + 9 \quad \Rightarrow 9 = 223 - 1(214)$
3. $214 = 23(9) + 7 \quad \Rightarrow 7 = 214 - 23(9)$
4. $9 = 1(7) + 2 \quad \Rightarrow 2 = 9 - 1(7)$
5. $7 = 3(2) + 1 \quad \Rightarrow 1 = 7 - 3(2)$

Extended Euclidean algorithm

- Work backwards
  - $1 = 7 - 3(2)$
  - $1 = 7 - 3\big(9 - 1(7)\big) = 7 + 3(7) - 3(9) = 4(7) - 3(9)$
  - $1 = 4\big(214 - 23(9)\big) - 3(9) = 4(214) - 92(9) - 3(9) = 4(214) - 95(9)$
  - $1 = 4(214) - 95\big(223 - 1(214)\big) = 99(214) - 95(223)$
  - $1 = 99\big(660 - 2(223)\big) - 95(223) = -293(223) + 99(660)$
- So the modular inverse of 223 mod 660 is
  - $a = -293\ mod\ 660 = (660 - 293)\ mod\ 660 = 367\ mod\ 660$
  - Quick check by making sure that $223(367) - 1$ is divisible by 660.

NUMBER THEORY

Finite Fields and Euler Phi Function

Finite Fields of the Form GF(p)

Finite Fields of Order p

- For a given prime, p, the finite field of order p, $GF(p)$, is the set Z_p of integer $\{0, 1, \ldots, p-1\}$ together with the arithmetic operations modulo p.

Euler Phi Function – φ(n)

- Euler Phi Function φ(n) is defined s the **count** of natural numbers in a set S that are **coprime** with the number n, where the set S simply consists of all the natural numbers from 1 to n.

Explanation:

- Every natural number greater than one has a unique factorization in terms of prime number. For example:

$$n = 6 \rightarrow 6 = 2 \times 3$$
$$n = 30 \rightarrow 30 = 2 \times 3 \times 5$$
$$n = 72 \rightarrow 72 = 2 \times 2 \times 2 \times 3 \times 3 = 2^3 \times 3^2$$

Euler Phi Function – φ(n)

- For n = 30, the set S contains {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14,…, 28, 29, 30}. In this set S, according to Euler Phi Function, there are 8 numbers – 1, 7, 11, 13, 17, 19, 23 and 29 that are coprime or relatively prime with 30.

- How to determine this number 8?

1. Determine the prime factors of the number 30; that is, 30 = 2 x 3 x 5.
2. Define 3 sets – one for each prime factor – such that each set contains the integers from S that each of the prime factor divides into evenly.

Euler Phi Function – φ(n)

- For example:

$$S_2 = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30\}$$
$$S_3 = \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}$$
$$S_5 = \{5, 10, 15, 20, 25, 30\}$$

What are the numbers in each set means with respect to the number 30? These numbers have common factors with the number 30.

We notice that in each set, the numbers are the prime factor and its multiples. For example, in set S_2, the numbers are 2 and all its multiples; in set S_3, the numbers are 3 and its multiples, and in set S_5, the numbers are 5 and its multiples.

Euler Phi Function – φ(n)

- If the numbers in set S_2 contains the prime number 2 and all its multiples, what is the probability that a number is chosen from set S, and the number is from set S_2? It is $^1/_2$. (Note, set S contains the numbers 1, 2, 3, …, 29, 30.)

- Similarly, the probability that a number is chosen from set S, and the number is from set S_3 is $^1/_3$.

- Likewise for set S_5, the probability is $^1/_5$.

Euler Phi Function – φ(n)

- Next, what is the probability that a number chosen randomly from set S, the number is not in (outside) the set S_2? It is $\left(1 - \frac{1}{2}\right)$.

- Likewise, the probability that a number is chosen randomly from set S, and the number is outside set S_3 is $\left(1 - \frac{1}{3}\right)$ and the probability that a number is chosen randomly from set S, and the number is outside set S_5 is $\left(1 - \frac{1}{5}\right)$.

Euler Phi Function – φ(n)

- Hence, base on these observation, if we randomly choose a number from set S, and the number chosen is outside $S_2, S_3, \text{and } S_5$ is $30 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right) \times \left(1-\frac{1}{5}\right)$.

- So what does this mean?
- This mean the numbers chosen from set S are outside the sets $S_2, S_3\ and\ S_5$, and these numbers do not have common factor with the number $n = 30$; this is what $\varphi(30)$ means.

- We can now write a general formula for Euler's Totient in terms of prime factors:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right).$$

Euler Phi Function – $\varphi(n)$

- For example,

$$\begin{aligned}\varphi(30) &= 30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\\ &= 30\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\\ &= 30\left(\frac{8}{30}\right) = 8\end{aligned}$$

Euler Phi Function – φ(n)

- $\varphi(11) = 11\left(1 - \frac{1}{11}\right)$
  $= 11\left(\frac{10}{11}\right) = 10$

Euler Phi Function – φ(n)

- The Euler Phi function is multiplicative, that is, if gcd(m, n) = 1, then $\varphi(mn) = \varphi(m) \times \varphi(n)$.

- For example, $\varphi(7{,}11) =?$

$$\begin{aligned}\varphi(7{,}11) &= \varphi(7) \times \varphi(11) \\ &= 7 \times \left(1 - \frac{1}{7}\right) \times 11 \times \left(1 - \frac{1}{11}\right) \\ &= 7 \times \left(\frac{6}{7}\right) \times 11 \times \left(\frac{10}{11}\right) \\ &= 6 \times 10 = 60\end{aligned}$$