DTS203TC
Design and Analysis of Algorithms

Lecture 18: Number Theory

Dr. Qi Chen
School of AI and Advanced Computing

Learning Outcome

- Divisibility and Primes
- Modular arithmetic
- Euclid's GCD algorithm
- Modular Multiplicative Inverses
- Euler's totient function

Divisibility and divisors

- The notion of one integer being divisible by another is key to the theory of numbers.

- If a and d are integers with $d \neq 0$, we say that d divides a if there is an integer k such that $a = k \cdot d$.
  - The notation $d \mid a$ (read "d divides a")
  - d is a divisor of a.
  - For example, the divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

- Every positive integer a is divisible by the trivial divisors 1 and a. The nontrivial divisors of a are the factors of a.

Prime and Composite Numbers

- An integer $a > 1$, whose only divisors are trivial divisors 1 and a is a Prime number.
- An integer $a > 1$, which is not a Prime number, is called Composite Number.
- 1 is called unit, and it is neither prime nor composite. Similarly, 0 and all negative integers are neither prime nor composite.

Exercise

- Find all the first 10 prime numbers.
  - 2,3,5,7,11,13,17,19,23,29

- Is 39 a composite number?
  - Yes. 39=3*13

Division Theorem

- "For any integer a and any positive integer n, there exist unique integers q and r such that $0 \le r < n$ and $a = qn + r$".

- The value $q = \lfloor a/n \rfloor$ is the quotient of the division.
- The value $r = a \bmod n$ is the remainder of the division.
  - $n \mid a$ (n divides a), if and only if $a \bmod n = 0$

Find the quotient and the remainder of 12 and 67.

The quotient: 5

The remainder: 7

Common Divisors

- If d is a divisor of a and d is also divisor of b then d is a common divisor of a and b.
  - '1' is a common divisor of any two integers.
  - If $a \mid b$ and $b \mid a$ then $a = \pm b$

- Important Property:
  - If $d \mid a$ and $d \mid b$ then $d \mid (a + b)$ & $d \mid (a - b)$

    More generally, if $d \mid a$ and $d \mid b$ then $d \mid (ax + by)$

Find all the common divisors of 24 and 30.

1, 2, 3, 6

Greatest Common Divisor (GCD)

- The GCD of two integers a and b , not both Zero, is the largest of the common divisors of a and b.
  - gcd(24, 30) = 6
  - gcd(5, 7) = 1

- Elementary properties of the GCD function:
  - gcd(a, b) = gcd(b, a)
  - gcd(a, b) = gcd(-a, b)
  - gcd(a, b) = gcd(|a|,|b|)
  - gcd(a, 0) = |a|
  - gcd(a, ka) = |a| for any k ϵ $\mathbb{Z}$

Relatively Prime Integers

- Two integers a and b are relatively prime (also called co-prime) if their only common divisor is 1.

$$\gcd(a, b) = 1$$

- For example, 8 and 15 are relatively prime.

Are 10 and 21 relatively prime?

Unique factorization

- There is exactly one way to write any composite integer a as a product of the form:

$$a = p_1^{e_1}\, p_2^{e_2} \ldots p_r^{e_r}$$

Where the p_i are prime, and the e_i are positive integers.

For example, the number 6000 is uniquely factored into primes as $2^4 \cdot 3 \cdot 5^3$

What is the unique factorization of the number 770 ?

$2 \cdot 5 \cdot 7 \cdot 11$

Greatest Common Divisors (GCD)

Let there are two positive integers a and b

$$a = p_1^{e_1}\, p_2^{e_2} \ldots p_r^{e_r}$$

$$\mathrm{b} = p_1^{f_1}\, p_2^{f_2} \ldots p_r^{f_r}$$

Here, $$\gcd(a, b) = p_1^{\min(e_1, f_1)}\, p_2^{\min(e_2, f_2)} \ldots p_r^{\min(e_r, f_r)}$$

Find the value of gcd(90, 150) using the above rule.

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

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

So, gcd(a, b) = $2 \cdot 3 \cdot 5 = 30$

Exercise

- Find the value of gcd(24, 30)

GCD recursion theorem

For any non-negative integer a and any positive integer b, we have

$$\gcd(a,b) = \gcd(b, a \bmod b)$$

Proof

- We shall show that gcd(a, b) and gcd(b, a mod b) divide each other.

- Case 1: gcd(a, b) | gcd(b, a mod b)

Let d = gcd(a, b), then d | a and d | b.

Here, a mod b = a - qb where q = $\lfloor a/b \rfloor$

Since, a mod b is a linear combination of a and b, we can say that d | (a mod b).

So, d | b and d | (a mod b) => d | gcd(b, a mod b)

=> gcd(a, b) | gcd(b, a mod b)

Proof

- Case 2: gcd(b, a mod b) | gcd(a, b)

Let d = gcd(b, a mod b), then d | b and d | a mod b.

Here, a = qb + (a mod b)   where q = $\lfloor a/b \rfloor$

Since, a is a linear combination of b and (a mod b), we can say that d | a.

So, d | a and d | b => d | gcd(a, b)

=> gcd(b, a mod b) | gcd(a, b)

From Case 1 and 2, we can say that:

gcd (a,b) = gcd (b, a mod b)

Euclid’s Algorithm

- Let a and b are non-negative integers.

```
EUCLID(a, b)
    if (b == 0)
        return a
    else  return EUCLID(b, a mod b)
```

Find the value of gcd(30, 21) using Euclid Alogrithm.

EUCLID(30,21) = EUCLID (21,9)
= EUCLID (9,3)
= EUCLID (3,0)
= 3.

Extended Euclid's Algorithm

- In this algorithm, we find additional information like the values of x and y, where

$$d = \gcd(a, b) = ax + by$$

```
EXTENDED-EUCLID(a, b)
If b = = 0
   return (a,1,0)
else
   (d', x', y')  =  EXTENDED-EUCLID(b, a mod b)
   (d, x, y) = (d', y', x' - ⌊a/b⌋y')
   return   (d, x, y)
```

Extended Euclid's Algorithm

In the algorithm,

$$d = ax + by$$

$$d' = bx' + (a \bmod b)\, y'$$

Because d = d', we have

$$\begin{aligned} ax + by &= bx' + (a \bmod b)\, y' \\ &= bx' + (a - b\lfloor a/b \rfloor)\, y' \\ &= ay' + b\,(x' - \lfloor a/b \rfloor\, y') \end{aligned}$$

So, $x = y'$ and $y = (x' - \lfloor a/b \rfloor y')$

Exercise

- Find the value of $gcd(99, 78)$ and corresponding x, y values using Extended-Euclid Algorithm.

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78				

Exercise

gcd(99, 78)

a = 99, b = 78, $\lfloor a/b \rfloor$ = 1

gcd(99, 78) = gcd(78,21)

```
EXTENDED-EUCLID(a, b)
If b = = 0
    return (a,1,0)
else
    (d', x', y')  =  EXTENDED-EUCLID(b, a mod b)
    (d, x, y) = (d', y', x' - ⌊a/b⌋y')
    return   (d, x, y)
```

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			

Exercise

gcd(78, 21)

a = 78, b = 21, $\lfloor a/b \rfloor$ = 3

gcd(78, 21) = gcd(21,15)

```
EXTENDED-EUCLID(a, b)
If b = = 0
    return (a,1,0)
else
    (d', x', y')  =  EXTENDED-EUCLID(b, a mod b)
    (d, x, y) = (d', y', x' - ⌊a/b⌋y')
    return   (d, x, y)
```

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			

Exercise

gcd(21, 15)

a = 21, b = 15, $\lfloor a/b \rfloor$ = 1

gcd(21, 15) = gcd(15,6)

```
EXTENDED-EUCLID(a, b)
If b = = 0
   return (a,1,0)
else
   (d', x', y') = EXTENDED-EUCLID(b, a mod b)
   (d, x, y) = (d', y', x' - ⌊a/b⌋y')
   return (d, x, y)
```

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			

Exercise

gcd(15, 6)

a = 15, b = 6, $\lfloor a/b \rfloor$ = 2

gcd(15, 6) = gcd(6,3)

```
EXTENDED-EUCLID(a, b)
If b = = 0
    return (a,1,0)
else
    (d', x', y')  =  EXTENDED-EUCLID(b, a mod b)
    (d, x, y) = (d', y', x' - ⌊a/b⌋y')
    return   (d, x, y)
```

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2			

Xi'an Jiaotong-Liverpool University 西交利物浦大学

Exercise

$gcd(6, 3)$

$a = 6, b = 3, \lfloor a/b \rfloor = 2$

$gcd(6, 3) = gcd(3,0)$

```
EXTENDED-EUCLID(a, b)
If b = = 0
    return (a,1,0)
else
    (d', x', y')  =  EXTENDED-EUCLID(b, a mod b)
    (d, x, y) = (d', y', x' - ⌊a/b⌋y')
    return   (d, x, y)
```

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2			

Exercise

```
EXTENDED-EUCLID(a, b)
If b = = 0
    return (a,1,0)
else
    (d', x', y')  =  EXTENDED-EUCLID(b, a mod b)
    (d, x, y) = (d', y', x' - ⌊a/b⌋y')
    return   (d, x, y)
```

gcd(3, 0)

a = 3, b = 0, $\lfloor a/b \rfloor$ = -

Return: d = 3, x=1 , y=0

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2			
3	0	-	3	1	0

Exercise

```
EXTENDED-EUCLID(a, b)
If b = = 0
   return (a,1,0)
else
   (d', x', y')  =  EXTENDED-EUCLID(b, a mod b)
   (d, x, y) = (d', y', x' - ⌊a/b⌋y')
   return   (d, x, y)
```

$d' = 3, x'=1 , y'=0$

$(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$

So, $d = 3, x = 0, y = 1$

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2	3	0	1
3	0	-	3	1	0

Exercise

```
EXTENDED-EUCLID(a, b)
If b = = 0
    return (a,1,0)
else
    (d', x', y') = EXTENDED-EUCLID(b, a mod b)
    (d, x, y) = (d', y', x' - ⌊a/b⌋y')
    return (d, x, y)
```

$d' = 3, x'=0, y'=1$

$(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$

So, $d = 3, x = 1, y = -2$

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

Exercise

```
EXTENDED-EUCLID(a, b)
If b = = 0
    return (a,1,0)
else
    (d', x', y') = EXTENDED-EUCLID(b, a mod b)
    (d, x, y) = (d', y', x' - ⌊a/b⌋y')
    return (d, x, y)
```

$d' = 3, x'=1, y'=-2$

$(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$

So, $d = 3, x = -2, y = 3$

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

Exercise

$d' = 3$, $x'=-2$, $y'=3$

$(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$

So, $d = 3$, $x = 3$, $y = -11$

```
EXTENDED-EUCLID(a, b)
If b = = 0
   return (a,1,0)
else
   (d', x', y') = EXTENDED-EUCLID(b, a mod b)
   (d, x, y) = (d', y', x' - ⌊a/b⌋y')
   return (d, x, y)
```

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

Exercise

EXTENDED-EUCLID(a, b)
If b = = 0
  return (a,1,0)
else
  (d', x', y') = EXTENDED-EUCLID(b, a mod b)
  (d, x, y) = (d', y', x' - $\lfloor a/b \rfloor$y')
  return (d, x, y)

d' = 3, x'=3, y'=-11

(d, x, y) = (d', y', x' - $\lfloor a/b \rfloor$y')

So, d = 3, x = -11, y = 14

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

Exercise

$gcd(99, 78) = 3$

$= -11 * 99 + 14 * 78$

d x a y b

```
EXTENDED-EUCLID(a, b)
If b = = 0
   return (a,1,0)
else
   (d', x', y') = EXTENDED-EUCLID(b, a mod b)
   (d, x, y) = (d', y', x' - ⌊a/b⌋y')
   return (d, x, y)
```

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

Modular Arithmetic

- We can partition the integers into n equivalence classes according to their remainders modulo n. The equivalence class modulo n containing an integer a is:

$$[a]_n = \{a + kn : k \in \mathbb{Z}\}$$

- For Example, $[3]_7$={…,-11,-4,3,10,17,…}; we can also denote this set by $[-4]_7$ and $[10]_7$.
- We can write $a \in [b]_n$ or $a \equiv b \pmod{n}$. *a* and *b* are said to be **congruent** modulo *n*

(mod *n*) applies to the entire equation

Modular Arithmetic

- *Examples:*
  - $2 \equiv -3 \ (mod\ 5)$
  - $-8 \equiv 7 \ (mod\ 5)$
  - $-3 \equiv -8 \ (mod\ 5)$
  - $38 \equiv 14 \ (mod\ 12)$

$$[a]_n = \{a + kn : k \in \mathbb{Z}\}$$

Properties

Properties [edit]

The congruence relation satisfies all the conditions of an equivalence relation:

- Reflexivity: $a \equiv a \pmod{n}$
- Symmetry: $a \equiv b \pmod{n}$ if $b \equiv a \pmod{n}$ for all a, b, and n.
- Transitivity: If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, or if $a \equiv b \pmod{n}$, then:[1]

- $a + k \equiv b + k \pmod{n}$ for any integer k (compatibility with translation)
- $k\,a \equiv k\,b \pmod{n}$ for any integer k (compatibility with scaling)
- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ (compatibility with addition)
- $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$ (compatibility with subtraction)
- $a_1\,a_2 \equiv b_1\,b_2 \pmod{n}$ (compatibility with multiplication)
- $a^k \equiv b^k \pmod{n}$ for any non-negative integer k (compatibility with exponentiation)
- $p(a) \equiv p(b) \pmod{n}$, for any polynomial $p(x)$ with integer coefficients (compatibility with polynomial evaluation)

If $a \equiv b \pmod{n}$, then it is generally false that $k^a \equiv k^b \pmod{n}$. However, the following is true:

- If $c \equiv d \pmod{\varphi(n)}$, where φ is Euler's totient function, then $a^c \equiv a^d \pmod{n}$—provided that a is coprime with n.

For cancellation of common terms, we have the following rules:

- If $a + k \equiv b + k \pmod{n}$, where k is any integer, then $a \equiv b \pmod{n}$
- If $k\,a \equiv k\,b \pmod{n}$ and k is coprime with n, then $a \equiv b \pmod{n}$
- If $k\,a \equiv k\,b \pmod{kn}$, then $a \equiv b \pmod{n}$

From wikipedia

Modular Multiplicative Inverse

- A modular multiplicative inverse of an integer a is an integer x such that ax is congruent to 1 modular some modulus n.

$$ax \equiv 1 \ (mod\ n)$$

We will also denote x with a^{-1} mod n

Find the multiplicative inverses of the following, where n = 7

	1	2	3	4	5	6
Answer:	1	4	5	2	3	6

Modular Multiplicative Inverse

- Modular inverse doesn't always exist. E.g., a = 2 and n = 4.
- The modular inverse exists if and only if a and n are relatively prime (i.e. gcd(a, n) = 1).
- Multiplicative group of integers modulo n:

$0 \leq a < n$

$$Z_n^* = \{a \in Z_n : \gcd(a, n) = 1\}$$

Exercise

- What is Z_{12}^*?

$Z_n^* = \{a \in Z_n : \gcd(a,n) = 1\}$

$Z_{12}^* = \{1,5,7,11\}$

- What is Z_{15}^*?

$Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Question: How many elements are there in Z_n^*?

Euler's totient function

- Also called Euler's phi function

$$\phi(n) = |Z_n^*| = n \prod_{p:p \text{ is prime and } p|n} (1 - \frac{1}{p})$$

Example

$Z_{12}^* = \{1,5,7,11\}$

$$|Z_{12}^*| = \phi(12) = 12 * \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$$

$Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$$|Z_{15}^*| = \phi(15) = 15 * \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8$$

Back to Modular Multiplicative Inverse

- How to find modular inverse?

- Consider the equation (with unknown x and y):

$$ax + ny = 1$$

When gcd(a,n)=1, the equation has a solution which can be found using the Extended Euclid Algorithm.

If we take modulo n of both sides, we can get rid of ny, and the equation becomes:

$$ax \equiv 1 \ (mod\ n)$$

x is the modular inverse of a

Exercise

Evaluate 17^{-1} mod 91

```
EXTENDED-EUCLID(a, b)
If b = = 0
    return (a,1,0)
else
    (d', x', y')  =  EXTENDED-EUCLID(b, a mod b)
    (d, x, y) = (d', y', x' - ⌊a/b⌋y')
    return   (d, x, y)
```

a	b	$\lfloor a/b \rfloor$	d	x	y

Xi'an Jiaotong-Liverpool University 西交利物浦大学

Exercise

```
EXTENDED-EUCLID(a, b)
If b = = 0
    return (a,1,0)
else
    (d', x', y')  =  EXTENDED-EUCLID(b, a mod b)
    (d, x, y) = (d', y', x' - ⌊a/b⌋y')
    return   (d, x, y)
```

Evaluate 17^{-1} mod 91

gcd(17,91) = gcd(91, 17) = 1

= 91 * 3 + 17*(-16)

We have $17^{-1} \equiv -16 \equiv$ 75 (mod 91), Since 17 * 75 = 1275 = 14 * 91 +1 $\equiv$ 1 (mod 91),

a	b	$\lfloor a/b \rfloor$	d	x	y
91	17	5	1	3	-16
17	6	2	1	-1	3
6	5	1	1	1	-1
5	1	5	1	0	1
1	0	-	1	1	0

Learning Outcome

- Divisibility and Primes
- Modular arithmetic
- Euclid's GCD algorithm
- Modular Multiplicative Inverses
- Euler's totient function