

# COMP2711 Discrete Math for CS

## [Number Theory] Review Notes

### 1. Divisibility and Modular Arithmetic

- **divisibility:** if  $b = ac$ , then  $a \mid b$ ; otherwise,  $a \nmid b$
- Properties:

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

- (i) if  $a \mid b$  and  $a \mid c$ , then  $a \mid (b + c)$ ;
- (ii) if  $a \mid b$ , then  $a \mid bc$  for all integers  $c$ ;
- (iii) if  $a \mid b$  and  $b \mid c$ , then  $a \mid c$ .

- **The Division Algorithm :** Let  $a$  be an int and  $d$  a +ve int. Then there're **unique** int  $q$  and  $r$ , with  $0 \leq r < d$ , such that  $a = dq + r$ .
- **Congruence**
  - $a \equiv b \pmod{m}$  :  $a$  is congruent to  $b$  modulo  $m$ .
  - $a \equiv b \pmod{m} \Leftrightarrow \exists k, a = b + km$ . (**often used in proof.**)
  - If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$ , and  $ac \equiv bd \pmod{m}$ .
- Arithmetic Modulo  $m$ .
  - $a +_m b = (a + b) \pmod{m}$ .
  - $a \cdot_m b = (a \cdot b) \pmod{m}$ .
- **Modular Exponentiation**
  - Find  $b^n \pmod{m}$  efficiently.
    - $n = (a_{k-1} \dots a_1 a_0)_2$ .
    - $b^n = b^{a_{k-1} \cdot 2^{k-1} + \dots + a_1 \cdot 2 + a_0} = b^{a_{k-1} \cdot 2^{k-1}} \dots b^{a_1 \cdot 2} \cdot b^{a_0}$
    - Thus, only need to find  $b, b^2, b^4, \dots, b^{2^{k-1}} \pmod{m}$

#### ALGORITHM 5 Modular Exponentiation.

```
procedure modular_exponentiation( $b$ : integer,  $n = (a_{k-1}a_{k-2} \dots a_1a_0)_2$ ,  
                                 $m$ : positive integers)  
 $x := 1$   
 $power := b \bmod m$   
for  $i := 0$  to  $k - 1$   
    if  $a_i = 1$  then  $x := (x \cdot power) \bmod m$   
     $power := (power \cdot power) \bmod m$   
return  $x$  { $x$  equals  $b^n \bmod m$ }
```

## 2. Primes and GCD

- **Prime**

- **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.

- If  $n$  is a composite integer, it has a prime divisor  $\leq \sqrt{n}$ .

- **Theorem :** There are infinitely many primes.

[Proof] Use proof by contradiction. Assume there're finitely many primes,  $p_1, \dots, p_n$ .

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

By the *fundamental theorem of arithmetic*,  $Q$  is prime or else it can be written as the product of two or more primes. However, none of the primes  $p_j$  divides  $Q$ , for if  $p_j \mid Q$ , then  $p_j \mid Q - \prod p_i = 1$ .

Hence, there's a prime not in the list  $p_1, p_2, \dots, p_n$ . Contradiction found!

**Note that  $Q$  is not necessary a prime. The prime not in the list is either  $Q$ , if it is prime, or a prime factor of  $Q$ .**

- **Greatest Common Divisors**

- $\gcd(a, b)$  is the largest  $d$  such that  $d \mid a$  and  $d \mid b$ .

- if  $\gcd(a, b) = 1$ , they are **relatively prime**.

- if  $\gcd(a_i, a_j) = 1$  whenever  $1 \leq i < j \leq n$ , then  $a_1, \dots, a_n$  are **pairwise relatively prime**.

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

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

- **The Euclidean Algorithm**

- Let  $a = bq + r$ , then  $\gcd(a, b) = \gcd(b, r)$ .

[Proof] Suppose  $d$  divides both  $a$  and  $b$ , then  $d$  must also divides  $a - bq = r$ .

Hence, any common divisor of  $a$  and  $b$  is also a common divisor of  $b$  and  $r$ .

Conversely, suppose  $d$  divides both  $b$  and  $r$ , then  $d$  must also divides  $bq + r = a$ .

Hence, any common divisor of  $b$  and  $r$  is also a common divisor of  $a$  and  $b$ .

- The GCD is the last **nonzero remainder** in the sequence of divisions.

- **Bezout's Theorem**

- If  $a, b$  are positive integers, then there exist integers  $s, t$  such that  $sa + tb = \gcd(a, b)$

- $s, t$  are called **Bezout coefficients** of  $a, b$ .

- Use **extended Euclidean algorithm** to find Bezout coefficient

Express  $\gcd(252, 198) = 18$  as a linear combination of 252 and 198.

**Solution:** To show that  $\gcd(252, 198) = 18$ , the Euclidean algorithm uses these divisions:

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

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

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

$$36 = 2 \cdot 18.$$

Using the next-to-last division (the third division), we can express  $\gcd(252, 198) = 18$  as a linear combination of 54 and 36. We find that

$$18 = 54 - 1 \cdot 36.$$

The second division tells us that

$$36 = 198 - 3 \cdot 54.$$

Substituting this expression for 36 into the previous equation, we can express 18 as a linear combination of 54 and 198. We have


$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

The first division tells us that

$$54 = 252 - 1 \cdot 198.$$

Substituting this expression for 54 into the previous equation, we can express 18 as a linear combination of 252 and 198. We conclude that

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198,$$

completing the solution. 

- Useful **lemmas**.


If  $a$ ,  $b$ , and  $c$  are positive integers such that  $\gcd(a, b) = 1$  and  $a \mid bc$ , then  $a \mid c$ .

**Proof:** Because  $\gcd(a, b) = 1$ , by Bézout's theorem there are integers  $s$  and  $t$  such that

$$sa + tb = 1.$$

Multiplying both sides of this equation by  $c$ , we obtain

$$sac + tbc = c.$$

We can now use Theorem 1 of Section 4.1 to show that  $a \mid c$ . By part (ii) of that theorem,  $a \mid tbc$ . Because  $a \mid sac$  and  $a \mid tbc$ , by part (i) of that theorem, we conclude that  $a$  divides  $sac + tbc$ . Because  $sac + tbc = c$ , we conclude that  $a \mid c$ , completing the proof. 

**LEMMA 3**

If  $p$  is a prime and  $p \mid a_1 a_2 \cdots a_n$ , where each  $a_i$  is an integer, then  $p \mid a_i$  for some  $i$ .

We can now show that a factorization of an integer into primes is unique. That is, we will show that every integer can be written as the product of primes in nondecreasing order in at most one way. This is part of the fundamental theorem of arithmetic. We will prove the other part, that every integer has a factorization into primes, in Section 5.2.

**Proof (of the uniqueness of the prime factorization of a positive integer):** We will use a proof by contradiction. Suppose that the positive integer  $n$  can be written as the product of primes in two different ways, say,  $n = p_1 p_2 \cdots p_s$  and  $n = q_1 q_2 \cdots q_t$ , each  $p_i$  and  $q_j$  are primes such that  $p_1 \leq p_2 \leq \cdots \leq p_s$  and  $q_1 \leq q_2 \leq \cdots \leq q_t$ .

When we remove all common primes from the two factorizations, we have

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v},$$

where no prime occurs on both sides of this equation and  $u$  and  $v$  are positive integers. By Lemma 3 it follows that  $p_{i_1}$  divides  $q_{j_k}$  for some  $k$ . Because no prime divides another prime, this is impossible. Consequently, there can be at most one factorization of  $n$  into primes in nondecreasing order. ◀

Although we cannot divide both sides of a congruence by any integer to produce a valid congruence, we can if this integer is relatively prime to the modulus. Theorem 7 establishes this important fact. We use Lemma 2 in the proof.

Let  $m$  be a positive integer and let  $a$ ,  $b$ , and  $c$  be integers. If  $ac \equiv bc \pmod{m}$  and  $\gcd(c, m) = 1$ , then  $a \equiv b \pmod{m}$ .

**Proof:** Because  $ac \equiv bc \pmod{m}$ ,  $m \mid ac - bc = c(a - b)$ . By Lemma 2, because  $\gcd(c, m) = 1$ , it follows that  $m \mid a - b$ . We conclude that  $a \equiv b \pmod{m}$ . ◀

### 3. Solving Congruences

- **Multiple inverse**

- If  $a$  and  $m > 1$  are relatively prime, then an inverse of  $a$  **modulo**  $m$  exists, such that  $a \cdot \bar{a} \equiv 1 \pmod{m}$ .
  - Proof of existence: use bezout identity
  - Proof of uniqueness: omit here. (to be completed.)
- Example: Find an inverse of 101 modulo 4620.

[Ans] By extended Euclidean algorithm,  $1 = -35 \cdot 4620 + 1601 \cdot 101$ .

So that  $1601 \cdot 101 \equiv 1 \pmod{4620}$ , thus 1601 is an inverse of 101 modulo 4620.

- **Solve linear congruence**

- Multiply both sides by inverse
- $3x \equiv 4 \pmod{7} \Leftrightarrow -2 \cdot 3x \equiv -2 \cdot 4 \pmod{7} \Leftrightarrow x \equiv -8 \equiv 6 \pmod{7}$ .

- **Solve system of linear congruence**

- **The Chinese Remainder Theorem:**

Let  $m_1, m_2, \dots, m_n$  be **pairwise relatively prime positive integers**, and  $a_1, a_2, \dots, a_n$  arbitrary.

Then the system

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

has a **unique** solution modulo  $m = m_1 m_2 \dots m_n$ .

- **Proof** of CRT:

**Proof:** To establish this theorem, we need to show that a solution exists and that it is unique modulo  $m$ . We will show that a solution exists by describing a way to construct this solution; showing that the solution is unique modulo  $m$  is Exercise 30.

To construct a simultaneous solution, first let

$$M_k = m/m_k$$

for  $k = 1, 2, \dots, n$ . That is,  $M_k$  is the product of the moduli except for  $m_k$ . Because  $m_i$  and  $m_k$  have no common factors greater than 1 when  $i \neq k$ , it follows that  $\gcd(m_k, M_k) = 1$ . Consequently, by Theorem 1, we know that there is an integer  $y_k$ , an inverse of  $M_k$  modulo  $m_k$ , such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

To construct a simultaneous solution, form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n.$$

We will now show that  $x$  is a simultaneous solution. First, note that because  $M_j \equiv 0 \pmod{m_k}$  whenever  $j \neq k$ , all terms except the  $k$ th term in this sum are congruent to 0 modulo  $m_k$ . Because  $M_k y_k \equiv 1 \pmod{m_k}$  we see that

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k},$$

for  $k = 1, 2, \dots, n$ . We have shown that  $x$  is a simultaneous solution to the  $n$  congruences. ◀

- **Fermat's Little Theorem**

- If  $p$  is prime and  $a$  is **not divisible** by  $p$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .
- $a^p \equiv a \pmod{p}$  for **any**  $a$ .
- Example: Find  $7^{222} \pmod{11}$ .

$$[\text{Ans}] 7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 49 \pmod{11}.$$

## 4. Applications of Congruences

- Hashing functions
- Pseudorandom Numbers
- Check digits

## 5. Cryptography

- Shift cipher
  - $A \sim Z$  replaced by  $0 \sim 25$
  - $f(p) = (p + k) \pmod{26}$
  - $f^{-1}(p) = (p - k) \pmod{26}$
- Affine cipher
  - $f(p) = (ap + b) \pmod{26}$
  - Need to guarantee that  $f$  is a bijection, that is, **if and only if**  $\gcd(a, 26) = 1$ .
  - decrypt:
    - Suppose  $c = (ap + b) \pmod{26}$
    - solve congruence:  $c - b \equiv ap \pmod{26}$
    - $p \equiv a^{-1}(c - b) \pmod{26}$
- Block cipher : transposition cipher
  - Use a permutation  $\sigma$  of set  $\{1, 2, \dots, m\}$  to itself.
  - If  $\sigma(1) = 3$ , it means that the first letter in plaintext will be transported to the third position.
- RSA
  - each individual has an encryption key  $(n, e)$ , where modulus  $n = pq$ , exponent  $e$  is relatively prime to  $(p - 1)(q - 1)$ .
  - The product of large primes, with approx 400 digits, **cannot be factored** in a reasonable length of time.
  - **Encryption:**
    - Translate each letter into a two-digit number
    - divide string into blocks of  $2N$  digits, which is the **largest even** number that  $2525 \dots 25$  with  $2N$  digits does not exceed  $n$ . (When necessary, add dummy nums)
    - ciphertext block  $C = M^e \pmod{n}$ .
    - calculate using **fast modular exponentiation**.
  - Example: Encrypt `STOP` using key  $(2537, 13)$ .

[Ans] Since  $2525 < 2537 < 252525$ , we group numbers into blocks of 4.

1819 1415

Then encrype,  $1819^{13} \pmod{2537} = 2081, 1415^{13} \pmod{2537} = 2182$

Encrypted message is 2081 2182.
  - **Decryption:**
    - decryption key  $d = e^{-1} \pmod{(p - 1)(q - 1)}$ .
    - $C^d = (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}$ .
    - By **Fermat's little theorem**,  $M^{p-1} \equiv 1 \pmod{p}, M^{q-1} \equiv 1 \pmod{q}$
    - Thus  $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \pmod{p} \equiv M \pmod{q}$ .
    - Since  $\gcd(p, q) = 1$ , by **Chinese remainder theorem**,  $C^d \equiv M \pmod{pq}$ .
- Cryptographic protocols

- Two parties exchange a secret key over an insecure communications channel without having shared any infos before.
- **Diffie-Hellman key agreement protocol (DH):**
  - Computations done in  $\mathbb{Z}_p$
  - First choose prime  $p$ , a primitive root  $a$  of  $p$ .
    - Alice chooses  $k_1$ , sends  $a^{k_1} \pmod{p}$  to Bob.
    - Bob chooses  $k_2$ , sends  $a^{k_2} \pmod{p}$  to Alice.
    - Shared key is  $a^{k_1 k_2} \pmod{p}$ .
  - **Viewable to public :**  $p, a, a^{k_1} \% p, a^{k_2} \% p$
  - Even with these four numbers, one cannot calculate  $a^{k_1 k_2} \pmod{p}$ .
- Digital Signatures
  - Alice use **private** key to **encrypt** message. (which was used to decrypt in RSA)
  - Receivers use Alice's **public** key to decrypt message.
  - So that receivers know it's Alice who sent the message.