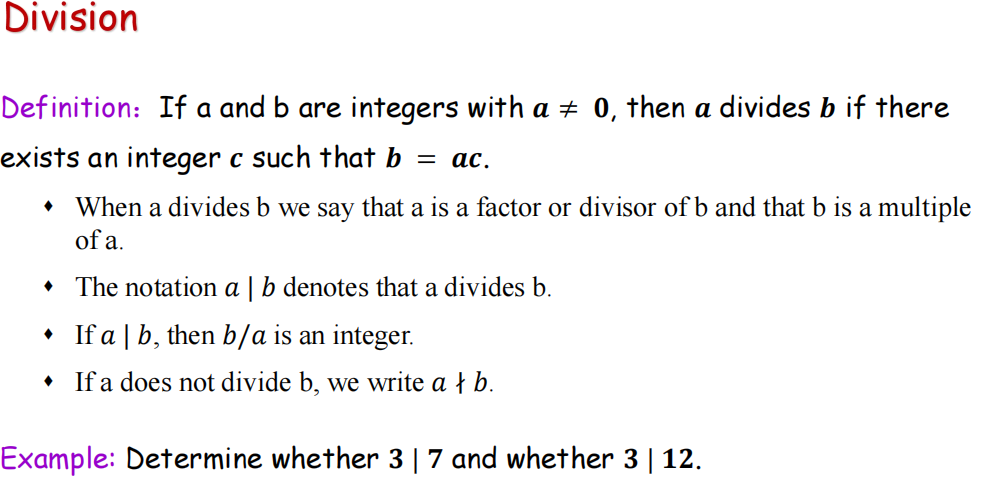
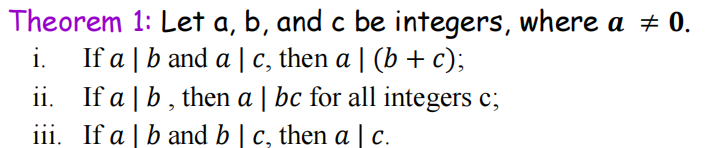
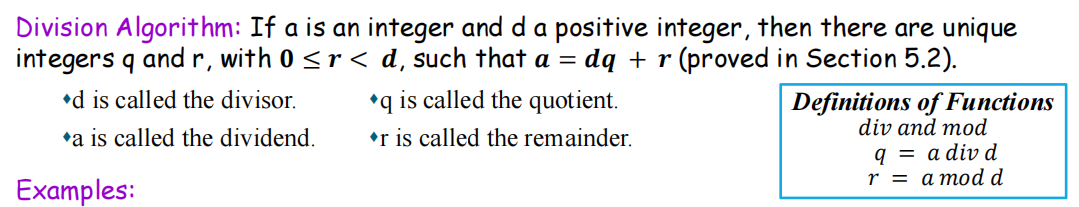
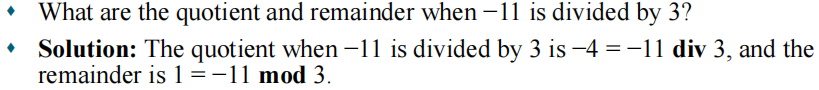
**（4.1）Divisibility and Modular**

**Arithmetic（整除性和模运算）**

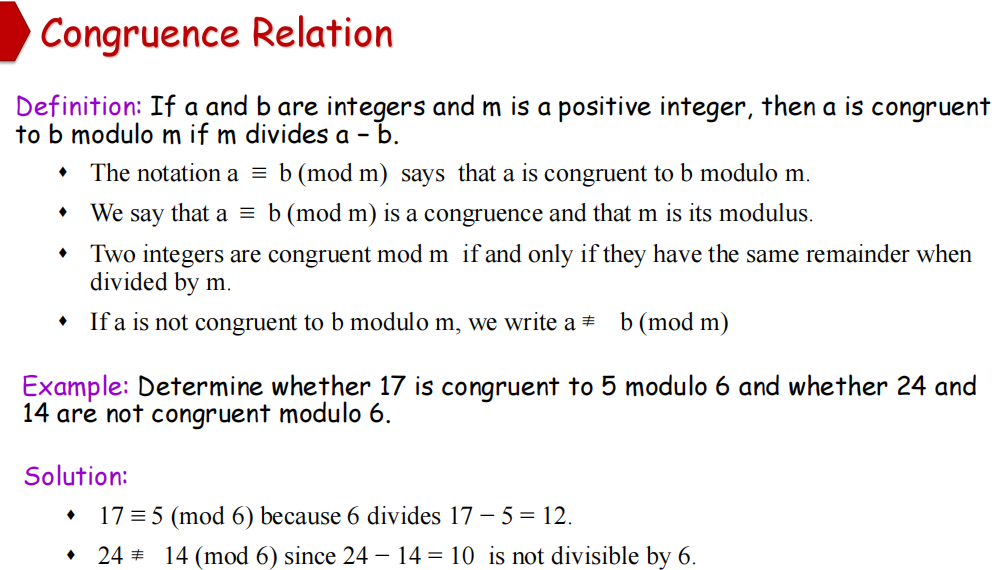


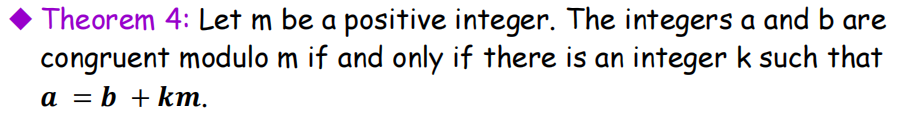


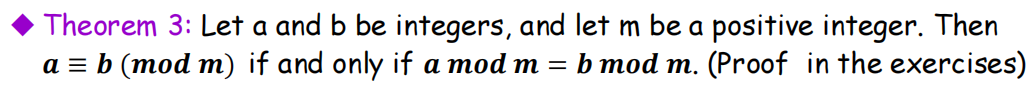


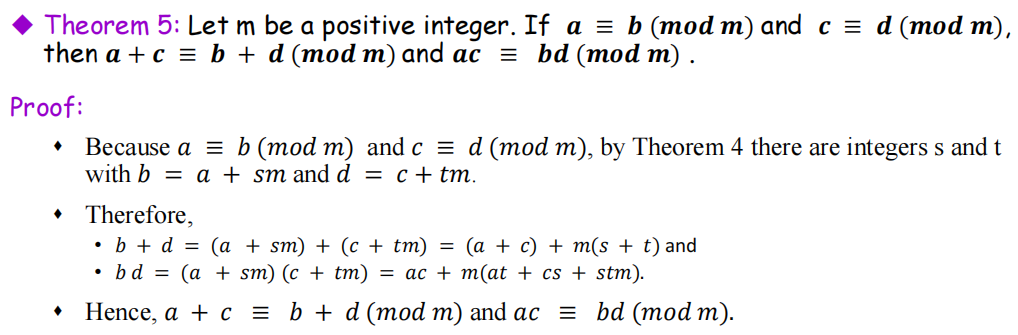


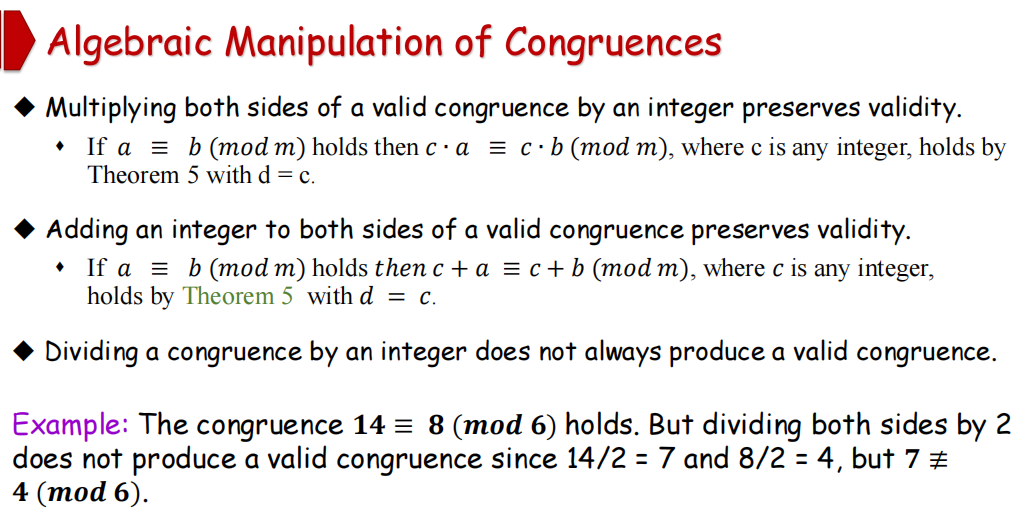
**同余**

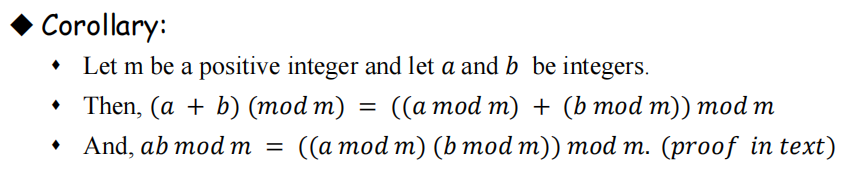


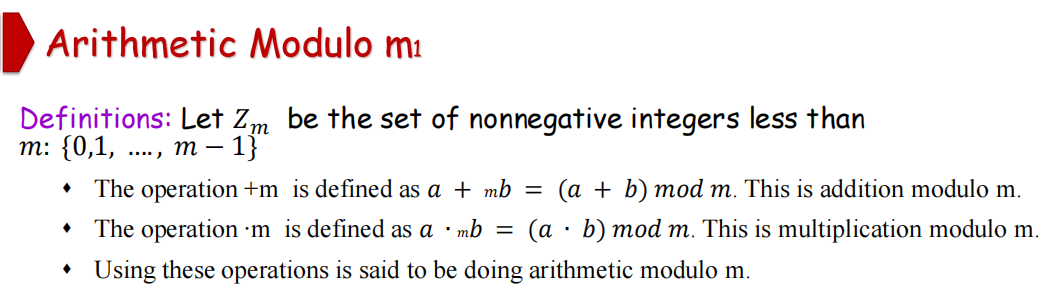


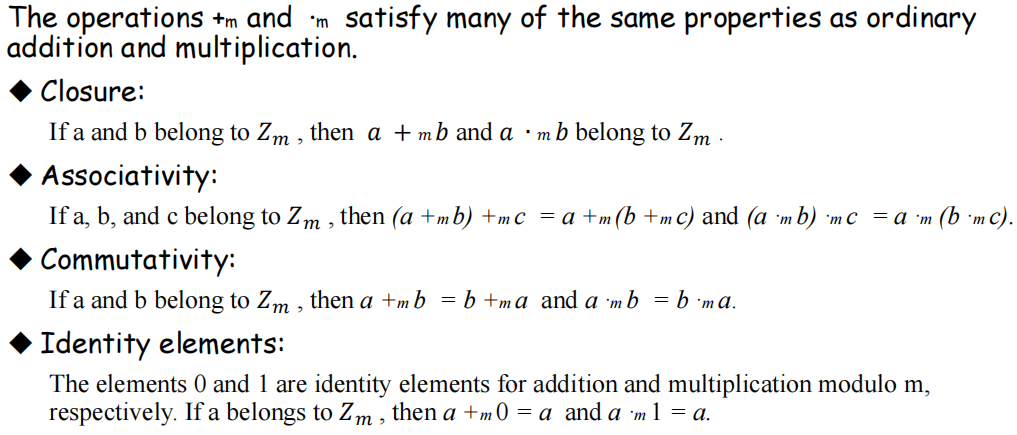


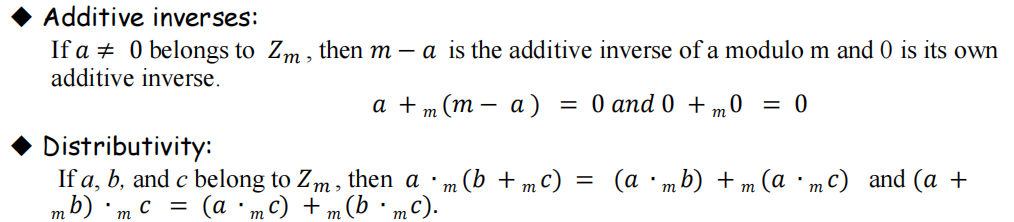


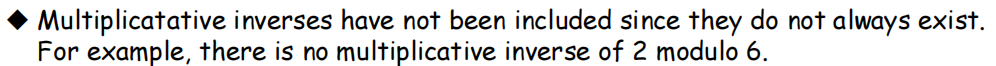










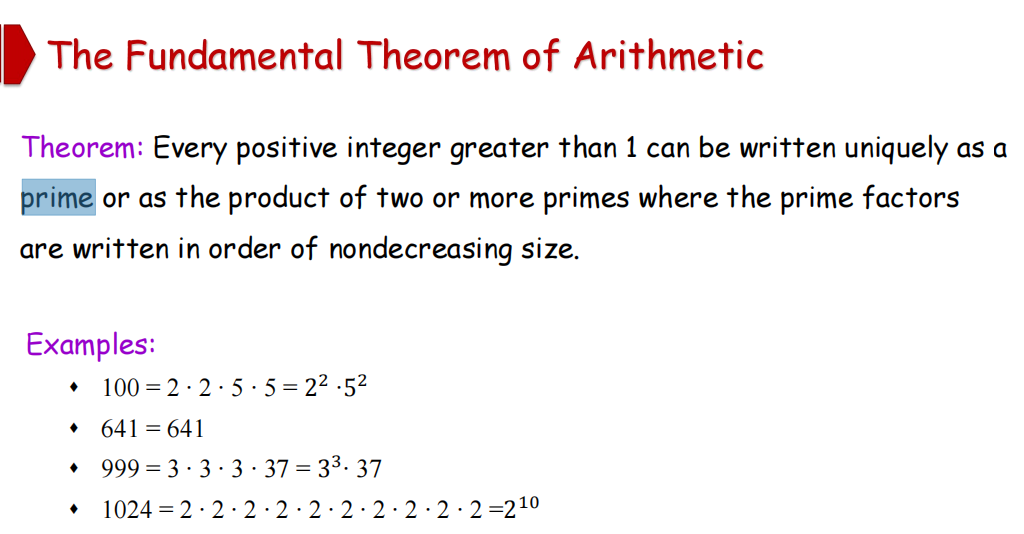


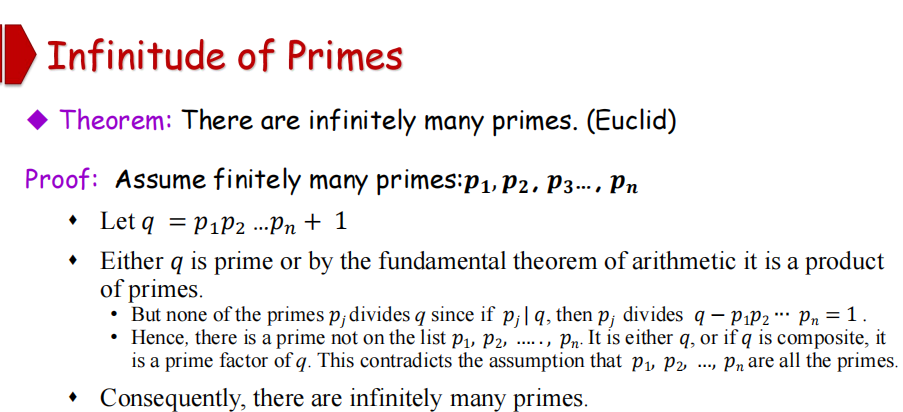
**（4.3）Primes and Greatest**

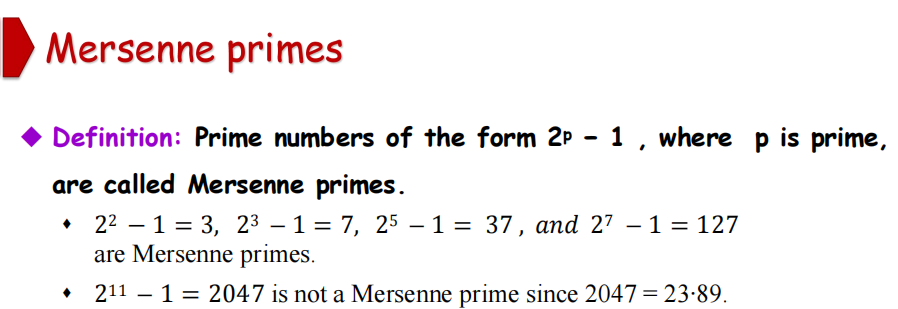
**Common Divisors**

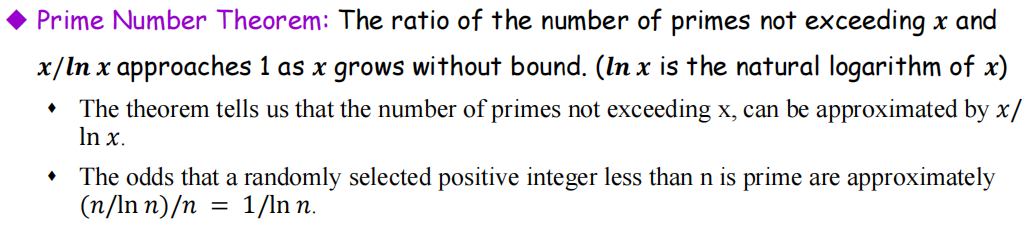
Composite（合数）prime（质数）

prime factorization（质因数分解）



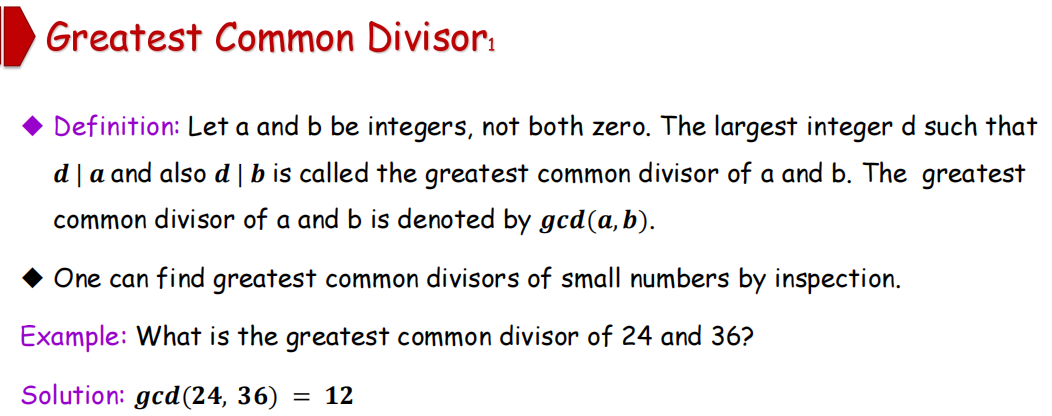


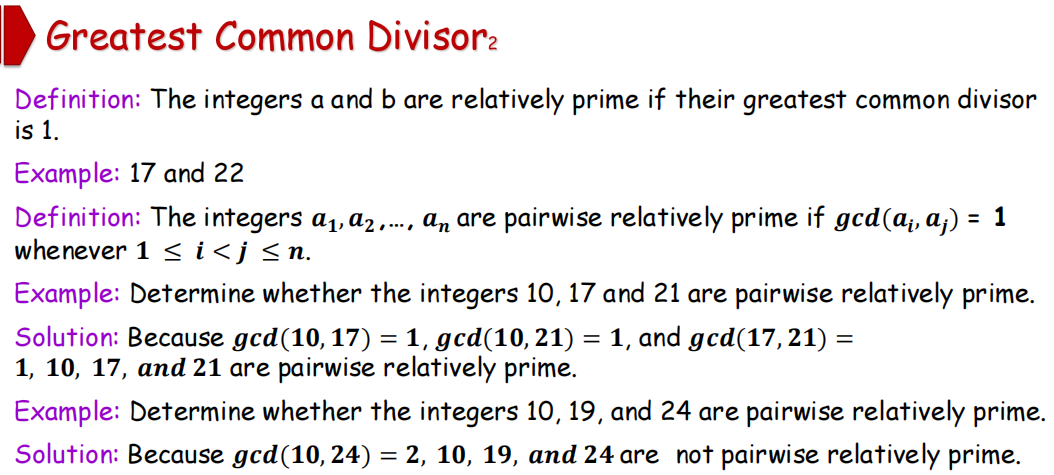


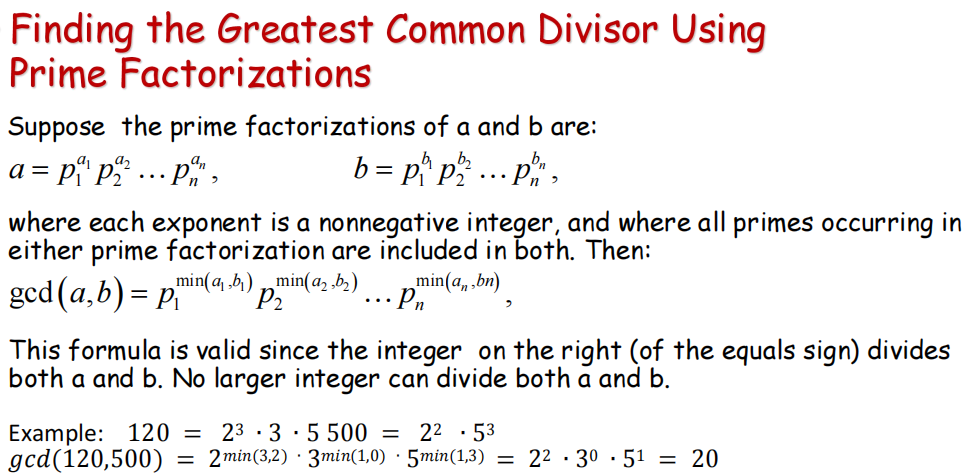


翻译：不超过x的素数的个数和x/lnx 的比值接近于1（当x趋于很大时）

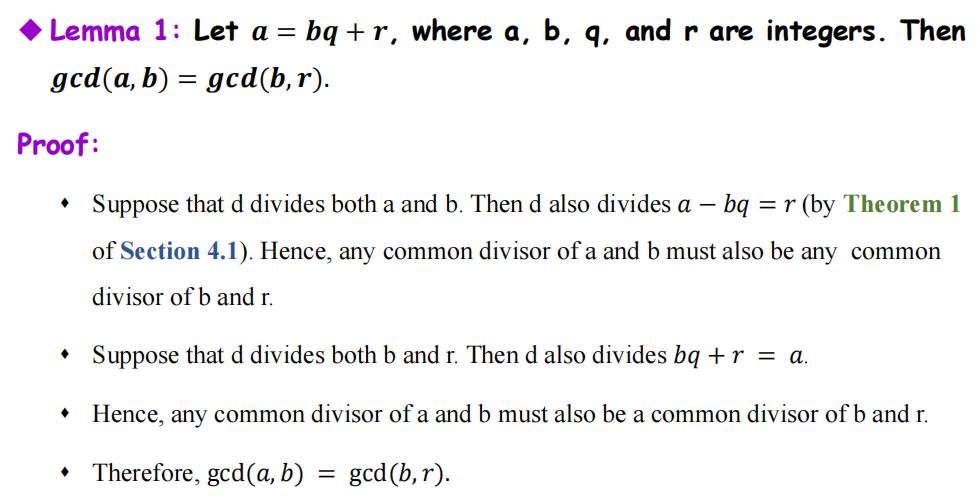
随机选择的小于n的正整数为素数的概率约为（n/ln n)/n= 1/ln n

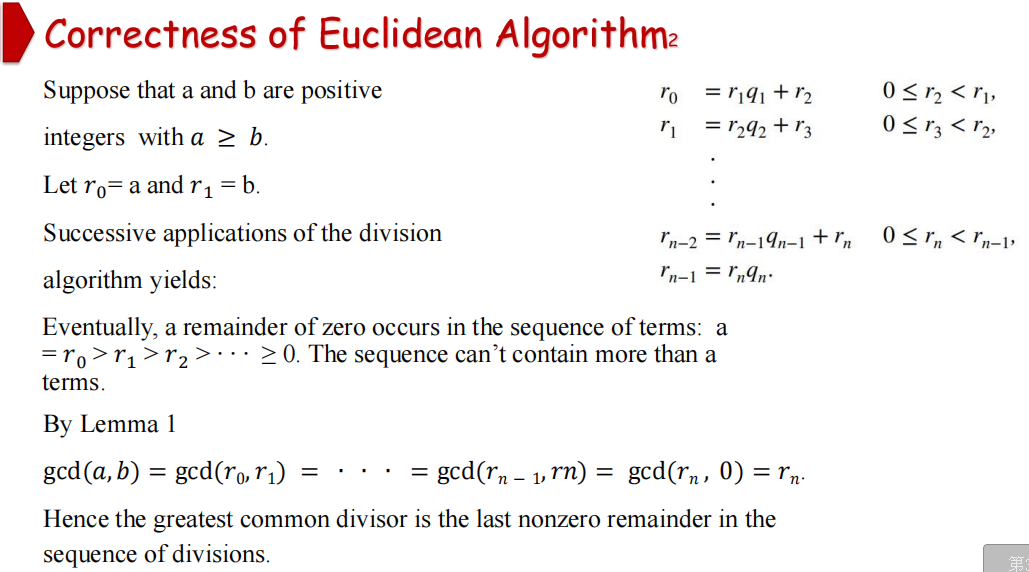


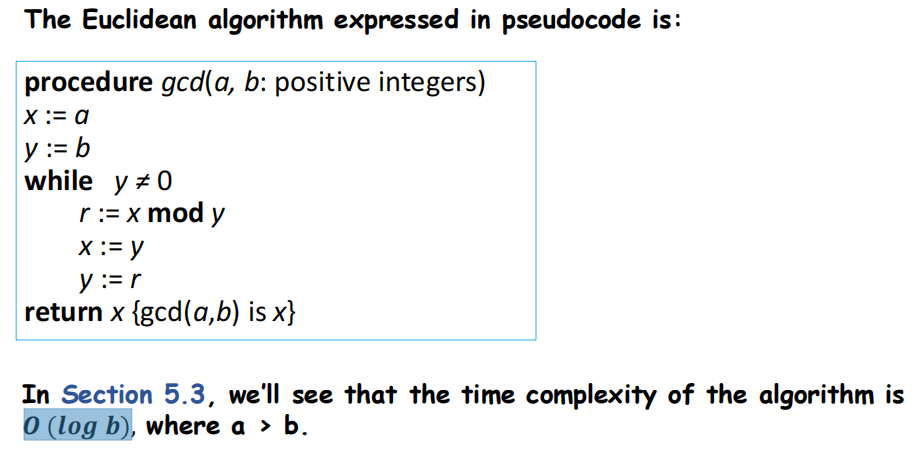


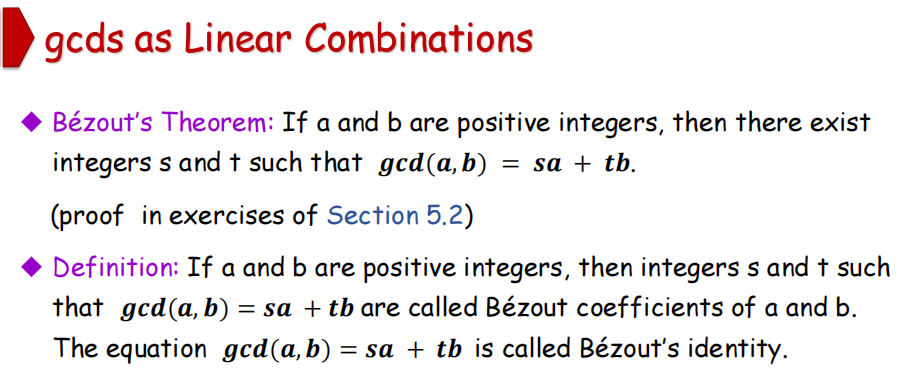


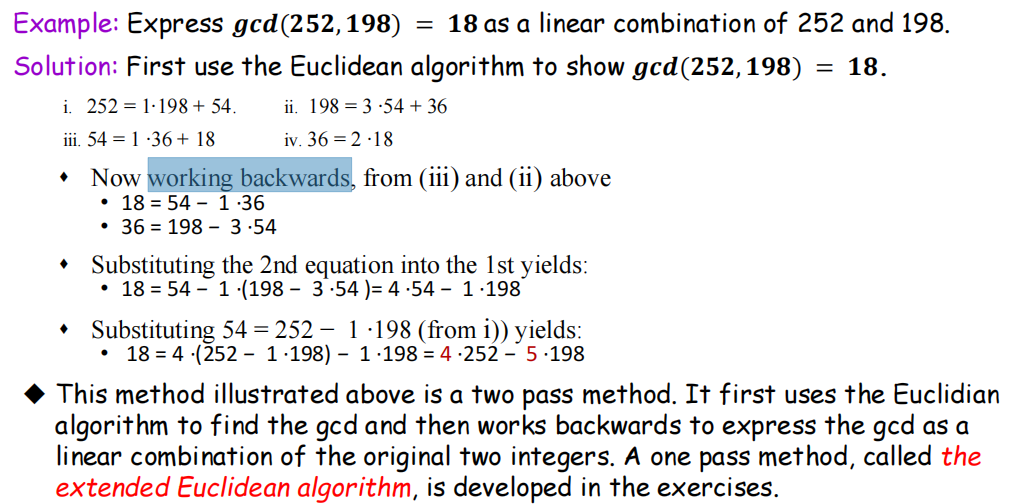


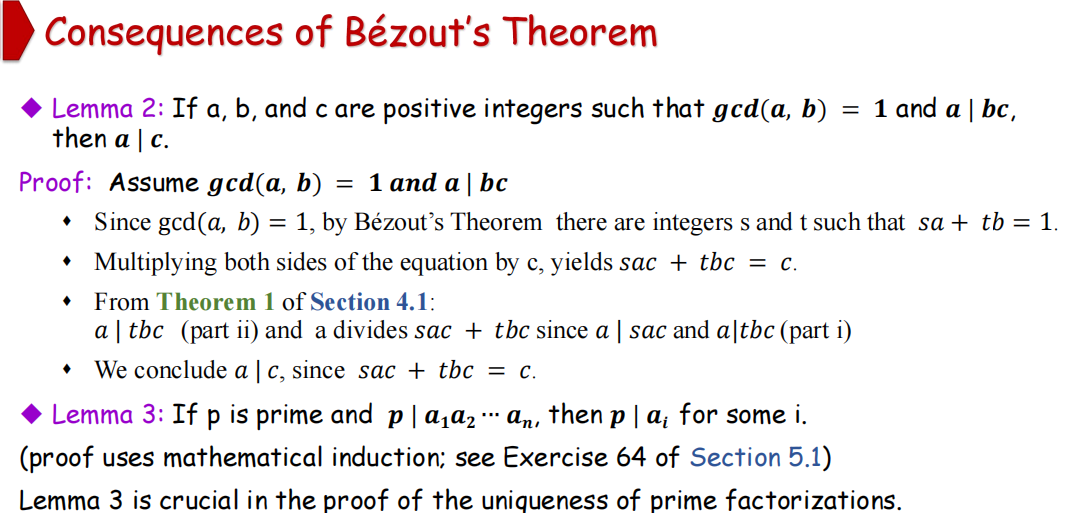






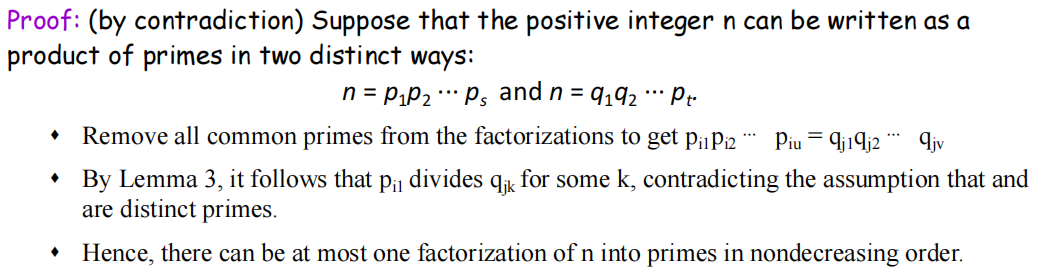








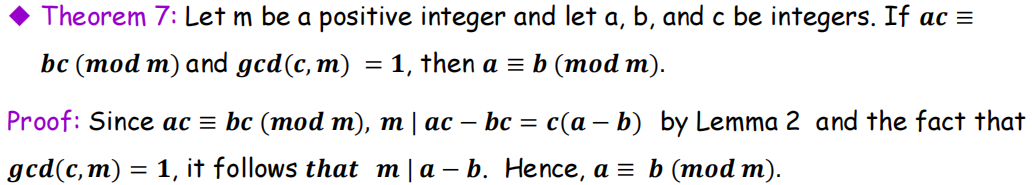
We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique.



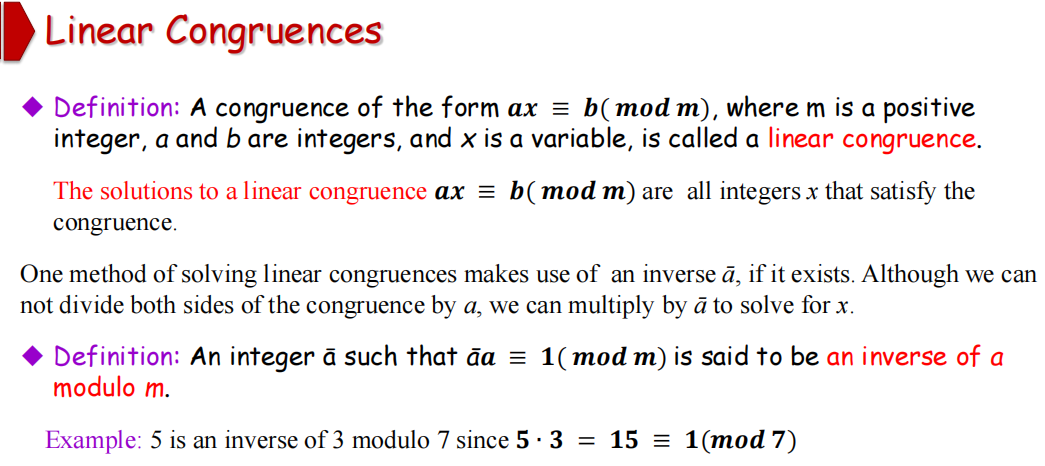


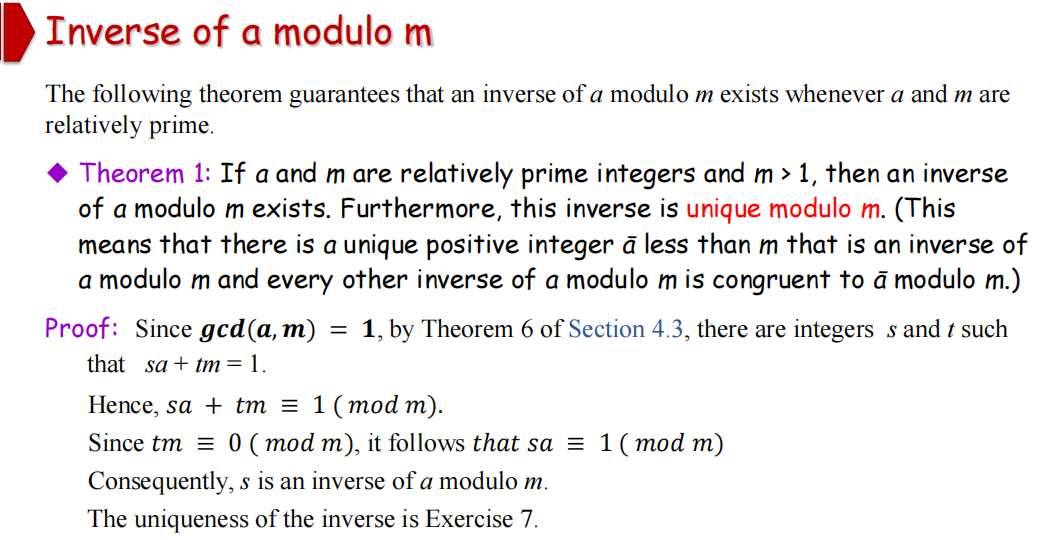
Dividing both sides of a valid congruence（同余） by an integer does not always produce a valid congruence (see Section 4.1).

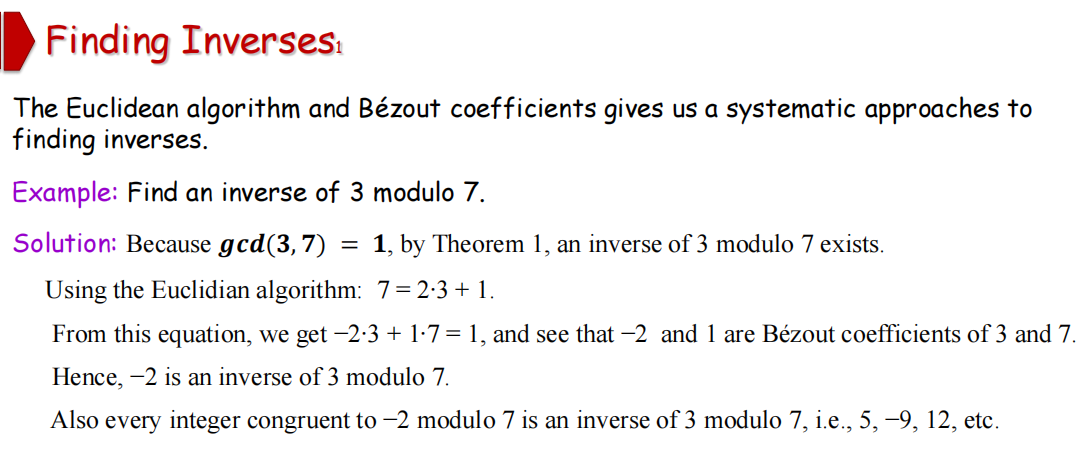
But dividing by an integer relatively prime to the modulus does produce a valid congruence:

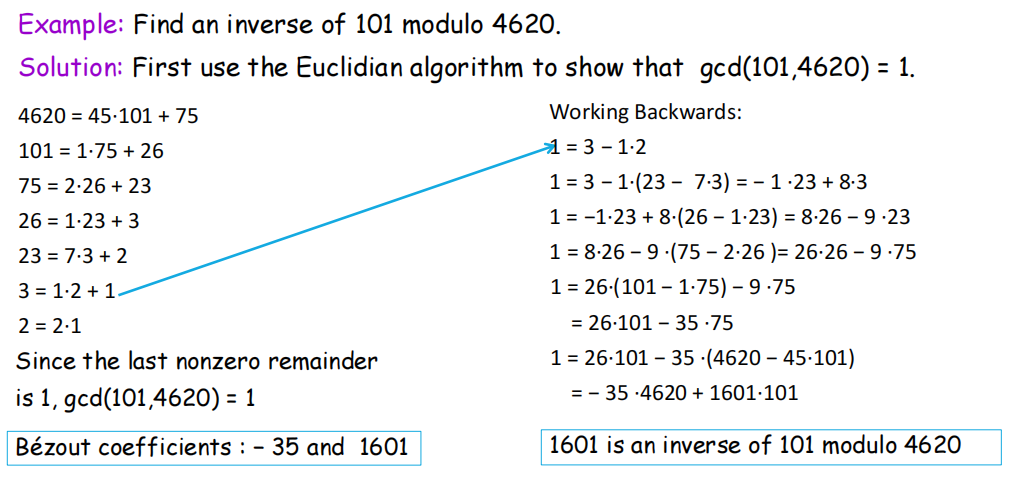


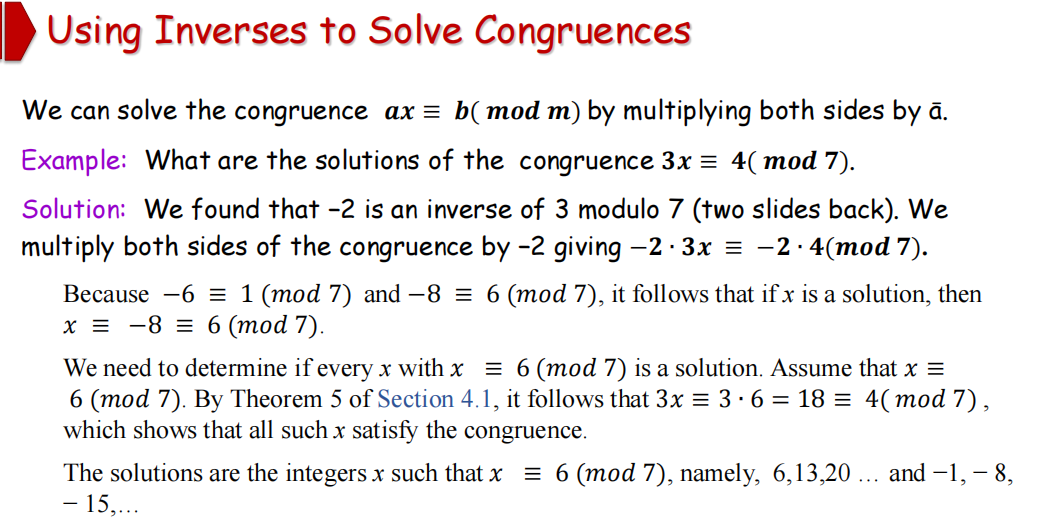
**（4.4）Solving Congruences（同余的求解）**



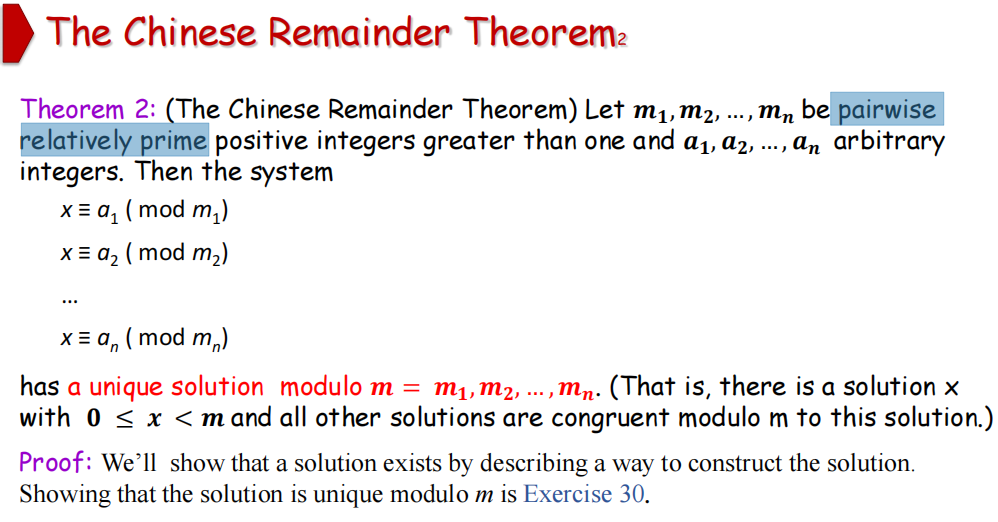




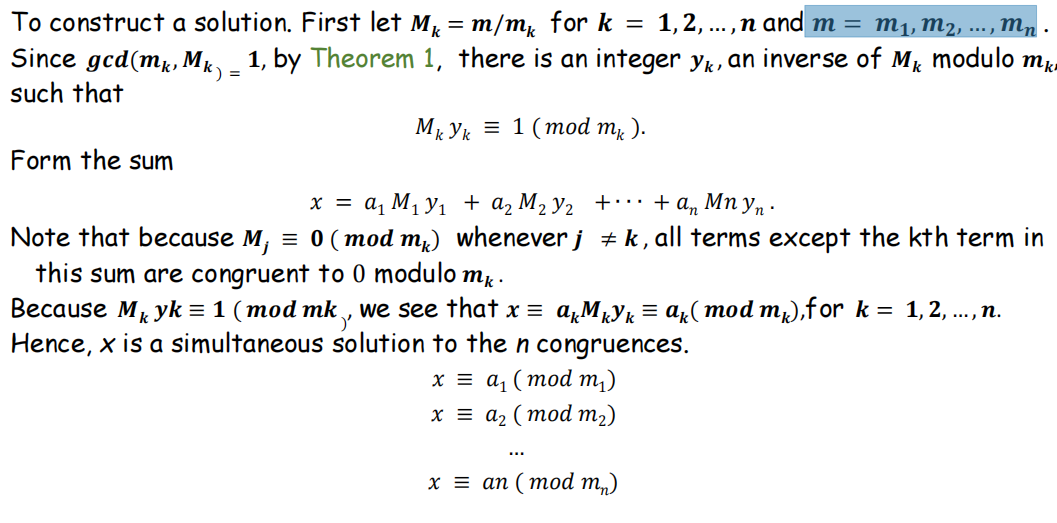


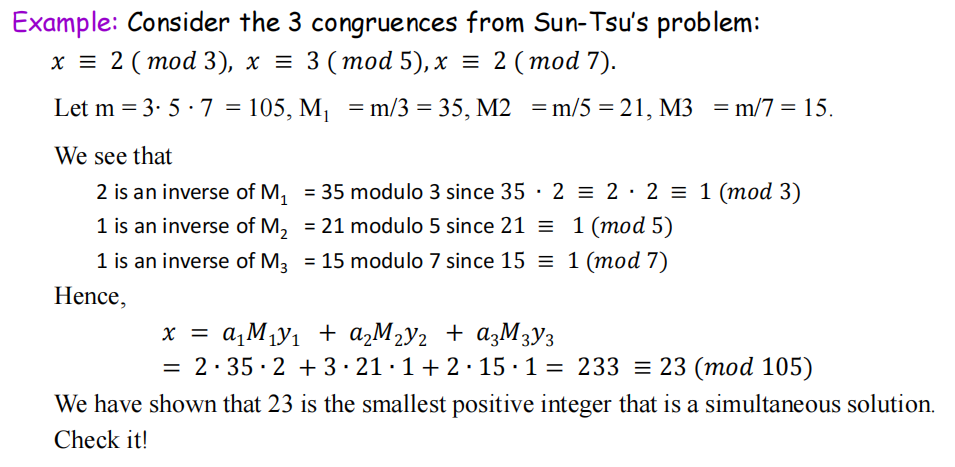


The Chinese Remainder Theorem（中国剩余定理）

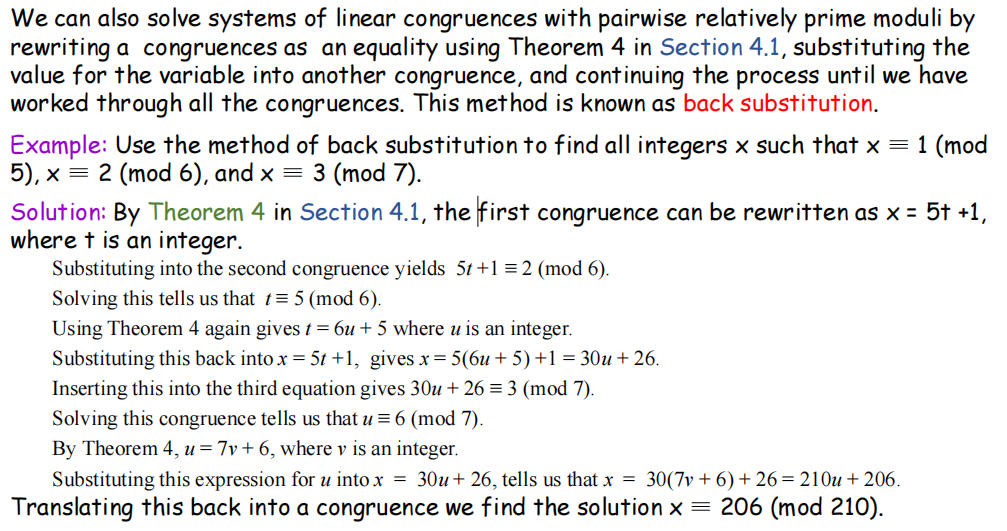


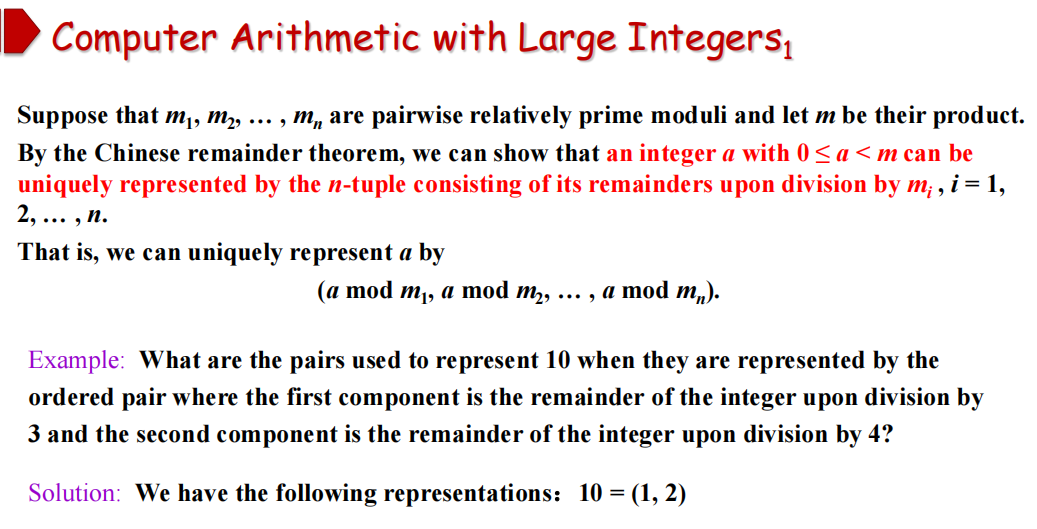
更正：m = m1 m2 ⋯ mn pairwise relatively prime(成对互为素数)

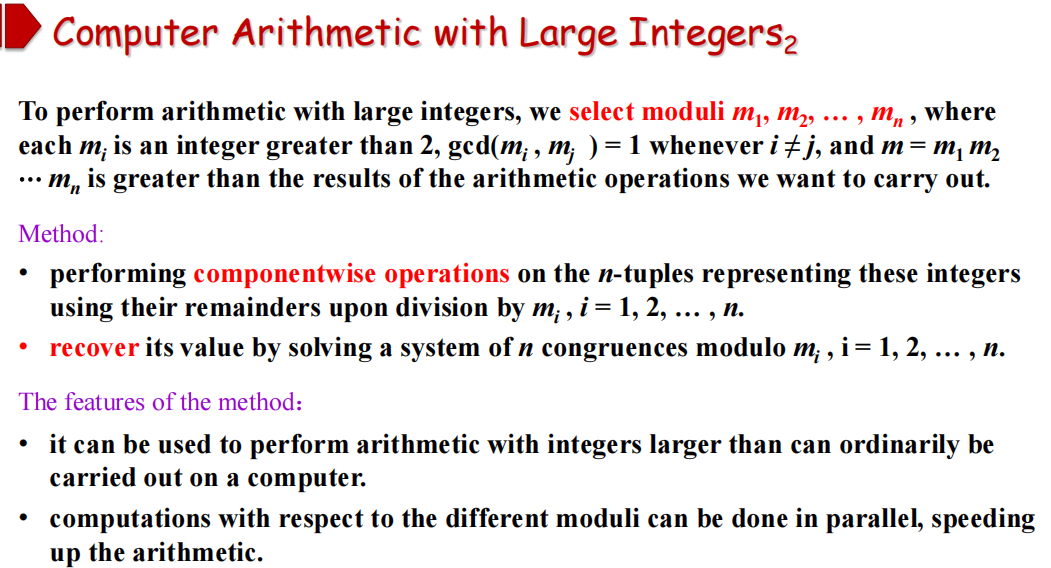


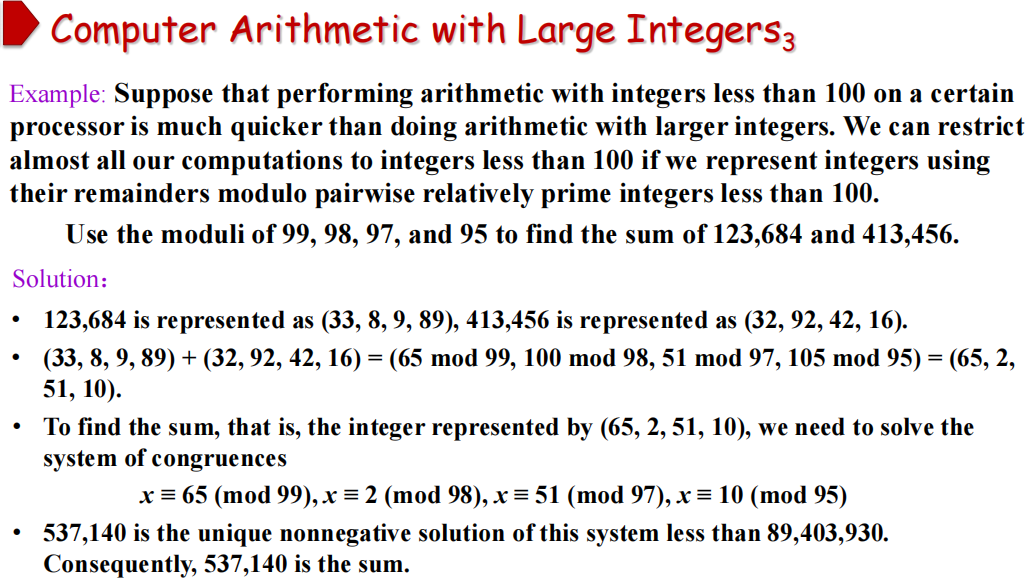


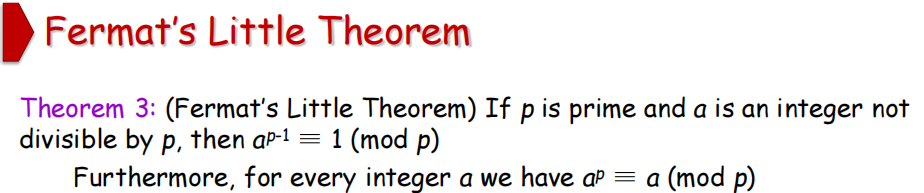
Back Substitution（回代）

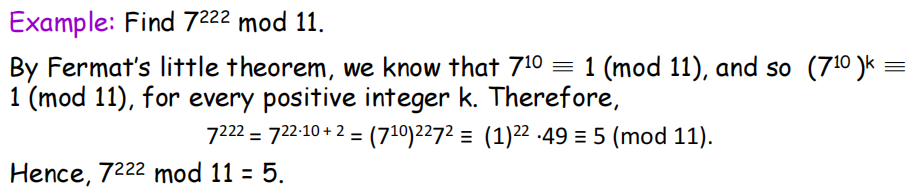






-





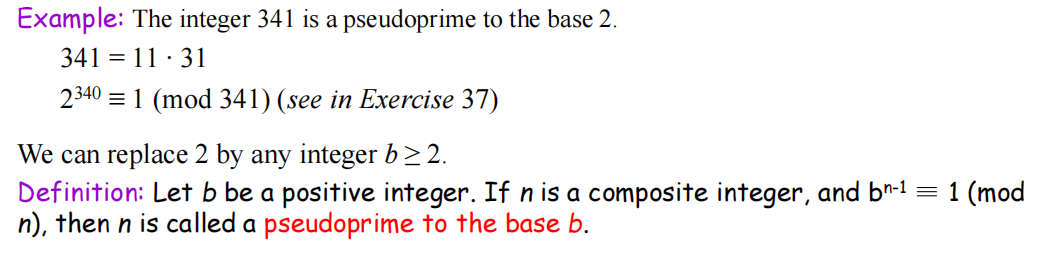
Pseudoprimes（伪素数）

By Fermat’s little theorem *n* > 2 is prime, where

2*n*-1 ≡ 1 (mod *n*).

But if this congruence holds, *n* may not be prime.

Composite integers *n（合数n）* such that 2n-1 ≡ 1 (mod *n*) are called pseudoprimes to the base 2.



Carmichael Numbers （卡迈克尔数）

