最大公因子与辗转相除法 ✅
剩余类、剩余系、缩系 ✅
欧拉函数 ✅
同余方程 ✅
乘法逆元、加法逆元 ✅
中国剩余定理 ✅
二次同余式 ✅
勒让德符号、雅可比符号、二次互反律 ✅
模一个整数的阶和原根 ✅
群、循环群、生成元 ✅
环、剩余类环 ✅
域、有限域 ✅

P140 strange

证明两整数a,b互质的充要条件是：存在两个整数s,t满足as+bt=1

匿名用户
2013-09-20

证明：1)充分性：因为as+bt=1,设c=(a,b),则c整除a和b,所以c整除as+bt,即c整除1,所以c=1,即a和b互质

2)必要性：因为a和b互质，所以(a,b)=1。

0是任何非零整数的倍数，1是任何整数的因子。任何非零整数是自身的因子和倍数。
设a,b,c是任意三个不为零的整数，且a = bq+c，q为整数，则 (a,b) = (b,c) 。
一个大于1的整数 p ，若它的因子只有两个，即1和它本身，则称该整数 p 为素数。
任意大于1的整数可以分解为素数幂形式的乘积。
1和0既非素数也非合数。
0与任何数都不互素　？
任意正整数a,b，存在整数s,t，使得 (a,b) = sa + tb 。
设a,b是两个正整数，则 [a,b] = ab/(a,b) 。
整数a,b模m同余的充要条件是 $m \mid a - b$ 。

P21 定理2.2

在与模 m 互素的所有剩余类中，各取一数所组成的集合叫做模 m 的一组缩系(也称为既约剩余系)。

欧拉函数 φ(m) 表示整数序列 0,1,2,...,m-1 (即整数模m的非负最小完全剩余系)中与 m 互素的数的个数，约定 φ(1) = 1，当 p 为素数时，显然有 φ(p) = p-1。

P25 定理2.8 欧拉定理

当 m 为合数时，如何求 φ(m)：利用欧拉函数 φ(m) 为积性函数、整数唯一分解定理

P26 定理2.13

当模 m 不大时，可以通过逐个验证 0,1,2,...,m-1 是否满足同余式，得到同余方程的解。

设 a,b 为任意整数，m 为任意正整数，(a,m) = d，则同余式 ax ≡ b (mod m) 有解的充要条件是 d | b 。若 d | b ，则同余式恰有 d 个解。

P29 定理2.18

P29 取 a' 为 s 除以 m 的余数

P31 定理2.20　?

P32 定理2.21 中国剩余定理

一次同余式组 x ≡ a1 (mod m1)，x ≡ a2 (mod m2)，可解的充要条件是 (m1,m2) | a1 - a2，且当同余式组可解时，对模 [m1,m2] 有唯一解。

RSA　?

若二次同余式 x^2 ≡ a (mod p)，(a,p) = 1 有解，则称 a 是模 p 的二次剩余

P40 定理3.2 欧拉判别法

P41 推论3.1

P42 推论3.2 定理3.4 勒让德符号

P43 定理3.5

P44 定理3.6 二次互反律 p,q 是互素的奇素数

计算勒让德符号，需要先将 a 进行标准分解，再根据勒让德符号的计算定理求得。

P46 定理3.7 雅可比符号

P48 定理3.10 m,n 为正奇数

P48 最后一段：雅可比符号与勒让德符号的计算法则相当。当m为素数时，n模m的雅可比符号为勒让德符号；当m为合数时，如果 n模m的雅可比符号 = -1，则 x^2 ≡ n (mod m) 一定无解；如果 n模m的雅可比符号 = 1，则 x^2 ≡ n (mod m) 不一定有解。

设 p 为奇素数，p 不能整除 n，二次同余式为 x^2 ≡ n (mod p)，如果 n 模 p 的勒让德符号 = -1，则同余式无解；如果 n 模 p 的勒让德符号 = 1，则同余式有两解。当 p 不大时，可将 x = 1,2,...,(p-1)/2 分别代入二次同余式中通过验证求解。

雅可比符号 m为正奇数

二次剩余 注意 P为奇素数

P58 定理4.1

设整数 g 满足 (g,m) = 1，如果 g 模 m 的阶为 φ(m)，则 g 称为模 m 的一个原根。

P60 定理4.6

如果非空集S上定义的二元运算满足封闭性、结合律($(ab)c = a(bc)$)，就称S关于该二元运算构成半群。

封闭性、结合律、单位元、逆元　　群

如果群G的二元运算满足交换律 ($ab = ba$)，则称G为交换群。

$H = \{e\}$ 和 $H = G$ 都是 G 的子群，叫做群 G 的平凡子群。

P87 定理6.2

P88 定义6.10 循环群 生成元

设G为群，若存在G中的一个元素 a，使得G中的任意元素均由 a 的幂组成，则称群G为循环群，元素 a 为循环群G的生成元，记为 $G = \langle a \rangle$。

设非空集合R有两个代数运算，其满足，加法交换群、乘法结合律、乘法对加法的分配律，则称R为环。

满足乘法交换的环称为交换环。

满足乘法单位元的环称为有单位元的环。

一个有单位元的无零因子交换环是整环。

除环没有零因子。

交换除环就是域。

P109 定义7.8 环同态

设R,R'是两个环，如果映射 $f: R \to R'$ 既是单同态又是满同态(即同态 f 是一一映射)，则称 f 为同构。

设 R (F) 是一个环 (域)，对任意的 $a \in R$ (F)，满足 $na = 0$ 成立的最小正整数 n，称为环 R (域 F) 的特征。如果不存在这样的正整数，则称环 R (域 F)的特征为 0。

如果一个环中的非零元集合构成乘法交换群，则该环就称为域。

域是可交换的、无零因子、每一个非零元都有逆元。

每个域包含且只包含一个素域。

不含真子域的域称为素域。

任意域 F 是自身的子域，称为 F 的平凡子域，若子域不是平凡子域，就称为真子域。

任何特征为 p 的域 F ，一定包含一个与 Z_p 同构的素域，因此 F 可以看成 Fp 的一个扩域。

剩余类环 Zp 是域的充要条件是 p 为素数。

有理数域和有限域都可以通过代数扩张得到新的域。

有限域 元素个数相同的域是同构的，元素的个数是素数的幂

不可约多项式，顾名思义即不能写成两个次数较低的多项式的乘积的多项式。