数论概论学习小结

第5章 整除性与最大公因数

定理 5.1 （欧几里得算法）

要计算两个整数 a 与 b 的最大公因数，先令 $r_{-1}=a$ 且 $r_{0}=b$ 然后计算相继的商和余数 $$ r_{i-1}=q_{i+1} \times r_i+r_{i+1} (i = 0,1,2,\dots) $$ 直到某余数 r_{n+1} 为 0. 最后的非零余数 r_n 就是 a 与 b 的最大公因数.

第6章 线性方程与最大公因数

定理 6.1 （线性方程定理）

设 a 与 b 是非零整数 $g=gcd(a,b).$ 方程 $$ax+by=g$$ 总是有一个整数解 (x_1,y_1)它可由前面叙述的欧几里得算法得到. 则方程的每一个解可由 $$(x_1+k\cdot\frac{b}{g},y_1-k\cdot\frac{a}{g})$$得到, 其中 k 可为任意整数.

第7章 因数分解与算术基本定理

断言 7.1

令 p 是素数, 假设 p 整除乘积 ab , 则 p 整除 a 或 p 整除 b (或者 p 既整除 a 也整除 b)

定理 7.2 (素数整除性质)

假设素数 p 整除乘积 $a_1a_2\dots a_r$, 则 p 整除 $a_1,a_2,\dots,a_r$ 中至少一个因数

定理 7.3 (算术基本定理)

每个整数 $n \ge 2$可唯一分解成素数乘积 $$ n=p_1p_2\dots p_r $$

第8章 同余式

如果 m 整除 $a-b$, 我们就说 a 与 b 模 m 同余并记之为 $$ a \equiv b \pmod{m} $$ 数 m 叫做同余式的模. 具有相同模的同余式在许多方面表现得很像通常的等式.如果 $$ a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m} $$ 则 $$ a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}, a_1a_2 \equiv b_1b_2 \pmod{m} $$ **提醒**: 用数除同余式并非总是可能的. 换句话说, 如果 $ac \equiv bc

\pmod{m}$, 则 $a \equiv b \pmod{m}$ 未必成立. 然而, 如果 $gcd(c,m)=1$, 则可从同余式 $ac \equiv bc \pmod{m}$ 两边消去 c.

定理 8.1 (线性同余式定理)

设 a, c 与 m 是整数, $m \ge 1$, 且设 $g=gcd(a,m)$. (a)如果 $g \nmid c$, 则同余式 $ax \equiv c \pmod{m}$ 没有解 (b)如果 $g \mid c$, 则同余式 $ax \equiv c \pmod{m}$ 恰好有 g 个不同的解. 要求这些解, 首先求线性方程 $$ au+mv=g $$ 的一个解 (u_0, v_0) (第6章叙述了解这个方程的方法). 则 $ x_0=cu_0/g $ 是 $ax \equiv c \pmod{m}$ 的解, 不同余解的完全集由 $$ x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m}, k=0,1,2,\dots,g-1 $$ 给出.

第9章 同余式、幂与费马小定理

定理 9.1 (费马小定理)

设 p 是素数, a 是任意整数且 $a \equiv\mkern-17mu/$ $0 \pmod{p}$, 则 $$ a^{p-1} \equiv 1 \pmod{p}. $$

断言 9.2

设 p 是素数, a 是任何整数且 $a \equiv\mkern-16mu/$ $0 \pmod{p}$, 则数 $$ a,2a,3a,\dots,(p-1)a \pmod{p} $$ 与数 $$ 1,2,3,\dots,(p-1) \pmod{p} $$ 相同, 尽管它们的次序不同.

第 10 章 同余式、幂与欧拉公式

在 0 与 m 之间且与 m 互素的整数个数是个重要的量, 我们赋予这个量一个名称: $$ \phi(m)=\#\{a:1\le a \le m, gcd(a,m)=1 \}. $$ 函数 ϕ 叫做欧拉函数.

定理 10.1 (欧拉公式)

如果 $gcd(a,m)=1$, 则 $$ a^{\phi (m)} \equiv 1 \pmod{m} $$

断言 10.2

如果 $gcd(a,m)=1$, 则数列 $$ b_1a,b_2a,b_3a, \dots , b_{\phi (m)}a \pmod{m} $$ 与数列 $$ b_1,b_2,b_3,\dots,b_{\phi (m)}\pmod{m} $$ 相同, 尽管它们可能次序不同

第 11 章 欧拉 ϕ 函数与中国剩余定理

定理 11.1 (ϕ 函数公式)

1. 如果 p 是素数且 $k\ge1$, 则 $$ \phi(p^k)=p^k-p^{k-1}. $$
2. 如果 $gcd(m, n)=1$, 则 $\phi(mn)=\phi(m)\phi(n)$.

定理 11.2 (中国剩余定理)

设 m 与 n 是整数, $gcd(m,n)=1$, b 与 c 是任意整数. 则同余式组 $$ x \equiv b\pmod{m} \ \ 与\ \ x \equiv c\pmod{n} $$ 恰有一个解 $0\le x\le mn.$

第 12 章 素数

定理 12.1 (无穷多素数定理)

存在无穷多个素数.

定理 12.2 (模 4 余 3 的素数定理)

存在无穷多个模 4 余 3 的素数.

定理 12.3 (算术级数的素数狄利克雷定理)

设 a 与 m 是整数, $gcd(a,m)=1.$ 则存在无穷多个素数模 m 余 a , 则存在无穷多个素数 p 满足 $$ p \equiv a \pmod{m} $$

第 13 章 素数计数

$$ \pi(x)=\#\{素数p|p \le x \}. $$

定理 13.1 (素数定理)

当 x 很大时, 小于 x 的素数个数近似等于 $x/\ln(x)$. 换句话说, $$ \lim_{x \rightarrow \infty}\frac{\pi(x)}{x/\ln(x)}=1 $$

第 14 章 梅森素数

命题 14.1

如果对整数 $a \ge 2$ 与 $n \ge 2$, a^n-1 是素数, 则 a 必等于 2 且 n 一定是素数

形如 2^p-1 的素数叫做*梅森素数*

第 15 章 梅森素数与完全数

*完全数*是等于其真因数之和的数

定理 15.1 (欧几里得完全数公式)

如果 2^p-1 是素数, 则 $2^{p-1}(2^p-1)$ 是完全数

定理 15.2 (欧拉完全数定理)

如果 n 是完全数, 则 n 是 $$ n=2^{p-1}(2^p-1) $$ 形式, 其中 2^p-1 是梅森素数

$$ \sigma(n)=n 的所有因数之和(包括 1 与 n). $$

定理 15.3 (σ函数公式)

1. 如果 p 是素数, $k \ge 1$, 则 $$ \sigma(p^k)=1+p+p^2+\dots+p^k=\frac{p^{k+1}-1}{p-1} $$
2. 如果 $gcd(m, n)=1$, 则 $$ \sigma(mn)=\sigma(m)\sigma(n). $$

第 16 章 幂模 m 与逐次平方法

算法 16.1 (逐次平方计算 $a^k \pmod{m}$)

用下述步骤计算 $a^k \pmod{m}$ 的值:

1. 将 k 表成 2 的幂次和:

$$ k=u_0+u_1\cdot2+u_2\cdot2^2+u_3\cdot2^3+\dots+u_r\cdot2^r $$

其中每个 u_i 是 0 或 1. (这种表示式叫做 k 的二进制展开.)

2. 使用逐次平方法制作模 m 的 a 的幂次表.

$$ a^1\equiv A_0 \pmod{m}\\ a^2\equiv (a^1)^2\equiv A_0^2\equiv A_1 \pmod{m}\\ a^4\equiv (a^2)^2\equiv A_1^2\equiv A_2 \pmod{m}\\ a^8\equiv (a^4)^4\equiv A_2^2\equiv A_3 \pmod{m}\\ \vdots \\ a^{2r}\equiv(a^{2r-1})^2\equiv A_{r-1}^2\equiv A_r \pmod{m} $$

注意要计算表的每一行, 仅需要取前一行最末的数, 平方它然后用模 m 简化. 也注意到表有 $r+1$ 行, 其中 r 是第 1 步中 k 的二进制展开式中 2 的最高指数.

3. 乘积

$$ A_0^{u_0}\cdot A_1^{u_1}\cdot A_2^{u_2}\cdots A_r^{u_r}\pmod{m} $$

同余于 $a^k \pmod{m}$. 注意到所有 u_i 是 0 或 1, 因此这个数实际上是 u_i 等于 1 的那些 A_i

的乘积.

第 17 章 计算模 m 的 k 次根

算法 17.1 (计算模 m 的 k 次根原理)

设 b, k, 与 m, 是已知整数, 满足 $$ gcd(b,m)=1 与 gcd(k,\phi(m))=1. $$ 下述步骤给出同余式 $$ x^k \equiv b \pmod{m} $$ 的解.

1. 计算 $\phi(m)$. (见第 11 章.)
2. 求满足 $ku-\phi(m)v=1$ 的正整数 u 与 v. (见第6章, 另一种叙述方法是 u 是为满足 $ku\equiv 1\pmod{\phi(m)}$ 的正整数, 所以 u 实际上是 $k\pmod{\phi(m)}$ 的逆)
3. 用逐次平方法计算 $b^u\pmod{m}$. (见第 16 章.)所得值给出解 x.

第 19 章 素性测试与卡米歇尔数

*卡米歇尔数*是这样的合数 n, 即对每个整数 $1 \le a\le n$, 都有 $$ a^n \equiv a\pmod{n} $$ 换句话说, 卡米歇尔数是可冒充素数的一种合数, 因为它没有合数特征的证据.

1. 每个卡米歇尔数是奇数.
2. 每个卡米歇尔数是不同素数的乘积.

定理 19.1 (卡米歇尔数的考塞特判别法)

设 n 是合数. 则 n 是卡米歇尔数当且仅当它是奇数, 且整除 n 的每个素数 p 满足下述两个条件:

1. p^2 不整除 n.
2. $p-1$ 整除 $n-1$.

定理 19.2 (素数的一个性质)

设 p 是奇素数, 记 $$ p-1=2^kq, q\ 是奇数. $$ 设 a 是不被 p 整除的任何数, 则下述两个条件之一成立:

1. a^q 模 p 余 1
2. 数 $a^q,a^{2q},a^{2^2q},\cdots,a^{2^{k-1}q}$ 之一模 p 余 -1

定理 19.3 (合数的拉宾-米勒测试)

设 n 是奇素数, 记 $n-1=2^kq$, q 是奇数. 对不被 n 整除的某个 a, 如果下述两个条件都成立, 则 n 是合数.

1. $a^q \equiv \mkern-17mu/ \ 1 \pmod{n}$,
2. 对所有 $i=0,1,2,\cdots,k-1,a^{2iq}\equiv\mkern-17mu/ -1 \pmod{n}$

如果 n 是奇合数, 则 1 与 $n-1$ 之间至少有 75% 的数可作为 n 的拉宾-米勒证据.

换句话说, 每个合数有许多拉宾-米勒证据来说明它的合数性, 所以, 不存在拉宾-米勒测试的任何 “ 卡米歇尔型数 ” .

第 20 章 欧拉 ϕ 函数与因数和

对任意整数 n, 定义函数 $F(n)$: $$ F(n)=\phi(d_1)+\phi(d_2)+\cdots+\phi(d_r), $$ 其中 $d_1,d_2,\cdots,d_r$ 是 n 的因数.

断言 20.1

如果 $gcd(m,n)=1$, 则 $F(mn)=F(m)F(n)$

定理 20.2 (欧拉 ϕ 函数求和公式)

设 $d_1,d_2,\cdots,d_r$ 是 n 的因数, 则 $$ \phi(d_1)+\phi(d_2)+\cdots+\phi(d_r)=n.(\sum_{d|n}\phi(d)=n) $$

第 21 章 幂模 p 与原根

如果 a 与 p 互素, 费马小定理(第 9 章)告诉我们 $$ a^{p-1}\equiv 1\pmod{p} $$ *a 模 p 的次数(或阶)指* $$ e_p(a)=(使得 a^e\equiv 1\pmod{p}的最小指数 e\ge 1) $$ (注意仅允许 a 与 p 互素.)

定理 21.1 (次数整除性质)

设 a 是不被素数 p 整除的整数, 假设 $a^n\equiv 1\pmod{p}$, 则次数 $e_p(a)$ 整除 n. 特别地, 次数 $e_p(a)$ 总整除 $p-1$.

具有最高次数 $e_p(g)=p-1$ 的数称为 模 p 的原根.

定理 21.2 (原根定理)

每个素数 p 都有原根. 更精确地, 有恰好 $\phi(p-1)$ 个模 p 的原根..

第 22 章 原根与指标

模素数 p 的原根 g 的优美体现在每个模 p 的非零数以 g 的幂次出现. 所以, 对任何 $1\le a<p$, 我们可选择幂 $$ g,g^2,g^3,g^4,\cdots,g^{p-3},g^{p-2},g^{p-1} $$ 中恰好一个与 a 模 p 同余. 相应的指数被称为以 g 为底的 a 模 p 的指标. 假设 p 与 g 已给出, 则记指标为 $I(a)$.

定理 22.1 (指标法则)

指标满足下述法则:

1. $I(ab)\equiv I(a)+I(b)\pmod{p-1}$ [乘积法则]
2. $I(a^k)\equiv kI(a)\pmod{p-1}$ [幂法则]

因为恰好与对数满足的法则 $$ log(ab)=log(a)+log(b) 与 log(a^k)=klog(a) $$ 相同. 由此, 指标也被称为 *离散对数*

第 23 章 模 p 平方剩余

与一个平方数模 p 同余的非零数称为模 p 的二次剩余. 不与任何一个平方数模 p 同余的数称为模 p 的(二次)非剩余. 我们将二次剩余简记为 QR, 而二次非剩余简记为 NR. 与 0 模 p 同余的数既不是二次剩余, 也不是二次非剩余.

定理 23.1

设 p 为一个奇素数, 则恰有 $\frac{p-1}{2}$ 个模 p 的二次剩余, 且恰有 $\frac{p-1}{2}$ 个模 p 的二次非剩余.

定理 23.2 (二次剩余乘法法则——版本 1)

设 p 为奇素数, 则

1. 两个模 p 的二次剩余的积是二次剩余.
2. 二次剩余与二次非剩余的积是二次非剩余.
3. 两个二次非剩余的积是二次剩余.

这三条法则可用符号表示如下: $$ QR\times QR=QR, QR\times NR=NR, NR\times NR=QR. $$

a 模 p 的勒让德符号是 $$ \left(\frac{a}{p}\right) = \left\{ \begin{array}{rl} 1 & 若 a 是模 p 的二次剩余,\\ -1 & 若 a 是模 p 的二次非剩余.\\ \end{array} \right. $$

定理 23.3 (二次剩余的乘法法则——版本 2)

设 p 为奇素数, 则 $$ \left(\frac a p\right)\left(\frac b p\right)=\left(\frac{ab}{p}\right) $$

第 24 章 -1 是模 p 平方剩余吗? 2 呢

定理 24.1 (欧拉准则)

设 p 为奇素数, 则 $$ a^{(p-1)/2}\equiv \left(\frac a p\right)\pmod{p}. $$

定理 24.2 (二次互反律——第 \rm {I} 部分)

设 p 为奇素数, 则 $$ -1 是模 p 的二次剩余, 若 p\equiv 1\pmod{4},\\ -1 是模 p 的二次非剩余, 若 p\equiv 3\pmod 4. $$ 换句话说, 用勒让德符号可以表示为 $$ \left(\frac{-1}{p}\right)=\left\{ \begin{array}{rl} 1 & 若 p\equiv 1\pmod{4},\\ -1 & 若 p\equiv3\pmod{4}.\\ \end{array} \right. $$

定理 24.3 (模 4 余 1 素数定理)

存在无穷多个素数与 1 模 4 同余

定理 24.4 (二次互反律——第 \rm {II} 部分)

设 p 为奇素数, 则当 p 模 8 余 1 或 7 时, 2 是模 p 的二次剩余; 当 p 模 8 余 3 或 5 时, 2 是模 p 的二次非剩余. 用勒让德符号表示为 $$ \left(\frac 2 p\right)=\left\{ \begin{array}{rl} 1 & 若 p\equiv 1 或 7\pmod{8}, \\ -1 & 若 p\equiv 3 或 5\pmod{8}. \end{array} \right. $$

第 25 章 二次互反律

定理 25.1 (二次互反律)

设 p, q 是不同的奇素数, 则 $$ ()={ .\ ()={ .\ ()={ . $$

定理 25.2 (广义二次互反律)

设 a, b 为正奇数, 则 $$ ()={ .\ ()={ .\ ()={ . $$