

目录

1 什么是数论	4
2 勾股数组	4
2.1 证明一: 本原勾股数组 (a,b,c) 中 a 和 b 奇偶性不同且 c 总是奇数	4
3 勾股数组和单位圆	5
4 费马大定理	5
5 整除性与最大公因数	5
5.1 整除性	5
5.2 最大公因数	5
5.3 欧几里得算法	5
5.3.1 欧几里得算法证明	6
6 线性方程与最大公因数	6
6.0.1 扩展欧几里得算法	6
7 因数分解与算术基本定理	7
7.1 素数整除性质	7
7.2 算术基本定理	7
8 同余式	8
8.1 线性同余式定理	8
9 同余式, 幂和费马小定理	9
9.1 费马小定理	9
10 同余式, 幂和欧拉公式	9
10.1 欧拉公式	10
11 欧拉函数与中国剩余定理	10
11.1 欧拉函数公式	10
11.2 中国剩余定理 (CRT)	11

11.2.1 使用中国剩余定理求解一元线性同余方程	11
12 素数	12
12.1 无穷多素数定理	12
12.2 模 4 余 3 的素数定理	13
13 素数计数	13
13.1 素数定理	13
13.2 哥德巴赫猜想	13
13.3 孪生素数猜想	13
13.4 $N^2 + 1$ 猜想	14
14 梅森素数	14
15 梅森素数与完全数	14
15.1 欧几里得完全数公式	14
15.2 σ 函数	14
15.2.1 σ 函数公式	14
15.3 欧拉完全数定理	15
16 幂模 m 和逐次平方法	16
17 计算模 m 的 k 次根	16
18 幂, 根与不可破密码	17
19 素性测试与卡米歇尔数	17
19.1 卡米歇尔数性质	18
19.2 卡米歇尔数的考塞特判别法	18
19.3 素数的一个性质	19
19.4 合数的拉宾-米勒测试	20
20 欧拉函数与因数和	20
20.1 欧拉函数求和公式	20

21 幂模 p 与原根	21
21.1 次数整除性质	21
21.2 原根定理	21
22 原根与指标	23
22.1 指标法则	23
22.2 指标与求解同余式	23
23 模 p 平方剩余	24
23.1 二次剩余乘法法则-版本 1	25
23.2 二次剩余乘法法则-版本 2	25
24 -1 是模 p 平方剩余吗?2 呢	26
24.1 欧拉准则	26
24.2 二次互反律-第 I 部分	26
24.3 模 4 余 1 素数定理	26
24.4 二次互反律-第 II 部分	27
25 二次互反律	27
25.1 广义二次互反律	28
26 哪些素数可表示成两个平方数之和	29
26.1 素数的两平方数之和定理	29
26.1.1 费马降阶法	29
27 习题	30
27.1 第一章	30
27.1.1 1.1	30

1 什么是数论

数论研究自然数集合 (正整数集合), 特别的, 数论研究不同类型数之间的关系.

数论的常用研究步骤.

1. 积累数据, 通常是数值数据, 也可能更抽象. 这一步是研究的事实基础.
2. 分析数据, 设法找出模式和关系. 例如平方数, 立方数.
3. 形成解释模式与关系的猜想 (即猜测), 通常借助公式来表达这些猜想.
4. 通过收集额外数据, 检查新信息是否符合猜想来验证自己的猜想.
5. 给出自己的猜想的论证即证明.

2 勾股数组

本原勾股数组是指一个三元组 (a,b,c) , 其中 a,b,c 没有公因数, 且满足

$$a^2 + b^2 = c^2$$

2.1 证明一: 本原勾股数组 (a,b,c) 中 a 和 b 奇偶性不同且 c 总是奇数

假设 a,b 都是奇数, 则 c 是偶数, 且则存在整数 x,y,z .

$$a = 2 * x + 1$$

$$b = 2 * y + 1$$

$$c = 2 * z$$

$$a^2 + b^2 = c^2$$

$$2 * (x^2 + y^2 + x + y) + 1 = 2 * z^2$$

最后的表达式明显不成立, 奇数不可能等于偶数, 所以 a,b 都是奇数不成立.

如果 a,b 都是偶数, 则 c 也就是偶数, a,b,c 之间存在公因数 2, 显然不成立.

所以 a 和 b 奇偶性不同, 则 c 是奇数.

3 勾股数组和单位圆

4 费马大定理

费马大定理

不可能将一个 3 次方分成两个 3 次方之和; 不可能将一个 4 次方分成两个 4 次方之和; 一般的, 任何高于 2 次的幂都不可能写成两个同次幂之和.

5 整除性与最大公因数

整除性和因数分解是数论的重要工具

5.1 整除性

假设 m, n 是整数, $m \neq 0$, m 整除 n 指 n 是 m 的倍数, 即存在整数 k 使得 $n = mk$, 记为 $m|n$, 类似的, 如果 m 不整除 n , 则记为 $m \nmid n$.

整除 n 的数称为 n 的因数.

5.2 最大公因数

对于两个整数, 它们的公因数是同时整除它们两个数的数.

对于两个数 a, b , 它们的最大公因数就是它们所有公因数中最大的数, 记为 $\gcd(a, b)$, 如果 $\gcd(a, b) = 1$, 称 a, b 互素.

5.3 欧几里得算法

求两个数最大公因数的最有效方法是欧几里得算法.

欧几里得算法步骤.

令 $r_{-1} = a$ 且 $r_0 = b$, 然后计算相继的商和余数

$$r_{i-1} = q_{i+1} * r_i + r_{i+1} \quad (i = 0, 1, 2, \dots)$$

直到某个余数 r_{n+1} 为 0, 最后的非零余数 r_n 就是 a, b 的最大公因数.
欧几里得算法总是会终止, 因为余数小于除数.

5.3.1 欧几里得算法证明

首先证明 r_n 是 a, b 的公因数.

$r_{n-1} = q_{n+1}r_n$ 说明 $r_n | r_{n-1}$.

$r_{n-2} = q_n r_{n-1} + r_n$ 说明 $r_n | r_{n-2}$.

同理可知, $r_n | r_{-1}, r_n | r_0$, 也就是 $r_n | a, r_n | b$.

然后证明 r_n 是 a, b 的最大公因数.

假设 d 是 a, b 的任意一个公因数.

由 $r_{-1} = q_1 * r_0 + r_1$ 也就是 $a = q_1 * b + r_1$, 可知 $d | r_1$, 因为 $d | a, d | b, d | a - q_1 b$.

同理可知 $d | r_2, d | r_3, \dots, d | r_n$. 所以 r_n 是 a, b 的最大公因数.

6 线性方程与最大公因数

形如 $ax + by$ 的最小正整数等于 $\gcd(a, b)$. 因为每一个正整数 $ax + by$ 都被 $\gcd(a, b)$ 整除.

这里对相等情况下 x, y 的值进行求解.

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

这里可以先求 $\gcd(a, b)$, 再通过配方法求 a 和 b .

6.0.1 扩展欧几里得算法

还有一种方法是利用欧几里得算法中的商和余数.

$$r_1 = a - q_1 b$$

$$r_2 = b - q_2 r_1, r_2 = b - q_2(a - q_1 b)$$

同理依次可以求出 $r_n = ax + by$, 也就是 $ax + by = \gcd(a, b)$. 通过加减 x, y 可以得出其他解. 同时这里也证明了方程 $ax + by = \gcd(a, b)$ 总是有解的.

7 因数分解与算术基本定理

素数: 一个整数 $p \geq 2$, 如果 p 的正因数仅有 1 与 p , 则 p 是素数. 不是素数的整数 $m \geq 2$ 叫做合数.

7.1 素数整除性质

令 p 是素数, 假设 p 整除乘积 ab , 则 p 整除 a 或者整除 b 或者同时整除 a 和 b .

证明:

如果 p 整除 a , 则已经证明.

如果 p 不整除 a , 则 $\gcd(p, a) = 1$, 即 $px + ay = 1$, 两边同乘 b .

$$pbx + aby = b$$

p 整除 pbx , 又因为 p 整除 ab , 所以 p 整除 aby , 所以 p 整除 b .

素数整除性质: 假设 p 整除乘积 $a_1 a_2 a_3 \dots a_n$, 则 p 整除 a_1, a_2, \dots, a_n 中至少一个因数. 该性质可以通过前面的证明结论证明.

7.2 算术基本定理

每个整数 $n \geq 2$ 可唯一分解成素数乘积 $n = p_1 p_2 \dots p_n$.

证明:

假设对于 $n \leq N$ 都可分解为素数乘积, 则现在考虑 $N + 1$.

如果 $N + 1$ 是素数, 则本身已经分解为素数乘积.

如果 $N + 1$ 不是素数, 则 $N + 1 = n_1 n_2$, $2 \leq n_1, n_2 \leq N$. 所以 n_1, n_2 可以分解为素数乘积, 所以 $N + 1$ 可分解为素数乘积.

通过数学证明可知每个整数 $n \geq 2$ 可分解成素数乘积.

现在证明分解的唯一性.

假设 $n = q_1 q_2 \dots q_n = p_1 p_2 \dots p_m$.

因为 $q_1 | n$, 所以 $q_1 | p_1 p_2 \dots p_m$, 由于素数整除性质, 所以 q_1 必整除 p_1, p_2, \dots, p_m 中的一个, 同时因为两者都是素数, 所以两者相等.

消去后可得 $q_2 \dots q_n = p_1 p_2 \dots p_{i-1} p_{i+1} \dots p_m$, 同理一直消去, 由于等式要一直成立, 所以两边素数数量相等, 同时每一个素数都一一对应, 则每个整数 $n \geq 2$ 可唯一分解成素数乘积 $n = p_1 p_2 \dots p_n$.

8 同余式

如果 m 整除 $a - b$, 则称为 a 与 b 模 m 同余并记之为 $a \equiv b \pmod{m}$, 数 m 称为同余式的模.

同余式的计算:

$$a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m}$$

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$$

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

如果 $\gcd(c, m) = 1$, 则可以从同余式 $ac \equiv bc \pmod{m}$ 消去 c 得到 $a \equiv b \pmod{m}$.

证明:

$$ac \equiv bc \pmod{m}, (ac - bc) = mk$$

$$(a - b)c = \frac{mk}{c}$$

因为 $\gcd(m, c) = 1$, 所以必存在 n 使得 $k = cn$.

$$a - b = mn$$

$$a \equiv b \pmod{m}$$

8.1 线性同余式定理

现在考虑求同余式 $ax \equiv c \pmod{m}$ 的解.

等价于求 $ax - c = my$, 也就是 $ax - my = c$,

利用第六章的结论: $ax - my$ 的每个数都是 $\gcd(a, m)$ 的倍数, 令 $g = \gcd(a, m)$.

如果 $\gcd(a, m)$ 不整除 c , 则同余式无解.

如果整除, 则首先存在 $ax - my = g$, 求解得 $ax_0 - my_0 = g$. 由于 g 整除 c , 等式两边同乘 $\frac{c}{g}$.

$$a \frac{cx_0}{g} + m \frac{cy_0}{g} = c$$

所以 $x = \frac{cx_0}{g} \pmod{m}$ 就是同余式的解.

设 x_1 是同余式的其他解, 则 $ax_1 \equiv ax_0 \pmod{m}$, 所以 $m | ax_1 - ax_0$, 即 $\frac{m}{g} | \frac{a(x_1 - x_0)}{g}$.

已知 m/g 和 a/g 没有公因数, 所以 m/g 必整除 $x_1 - x_0$. 即存在整数 k 使得 $x_1 = x_0 + k \frac{m}{g}$, 可知共有 g 个解, 通过取 $k = 0, 1, \dots, g-1$ 获得.

当 $g = \gcd(a, m) = 1$ 时, 恰好有一个解 $x \equiv \frac{c}{a} \pmod{m}$.

9 同余式, 幂和费马小定理

9.1 费马小定理

设 p 是素数, a 是任意整数且 $a \not\equiv 0 \pmod{p}$, 则

$$a^{p-1} \equiv 1 \pmod{p}$$

证明费马小定理之前, 先证明一个断言来推进定理的证明.

设 p 是素数, a 是任意整数且 $a \not\equiv 0 \pmod{p}$, 则数 $a, 2a, 3a, \dots, (p-1)a \pmod{p}$ 与数 $1, 2, 3, \dots, (p-1) \pmod{p}$ 相同, 尽管次序不同.

$a, 2a, 3a, \dots, (p-1)a$ 中存在 $p-1$ 个数, 同时都不被 p 整除, 假设取出 ma 和 na 并认为 $ma \equiv na \pmod{p}$.

则 $p|(j-k)a$, 由于 p 不整除 a , 所以 p 整除 $(j-k)$, 又因为 $1 \leq j, k \leq p-1$, 所以 $|j-k| \leq p-1$. 所以 $|j-k| = 0, m=n$.

所以 $a, 2a, 3a, \dots, (p-1)a$ 中每个乘积对模 p 不同余. 所以数 $a, 2a, 3a, \dots, (p-1)a \pmod{p}$ 与数 $1, 2, 3, \dots, (p-1) \pmod{p}$ 相同, 尽管次序不同.

开始证明费马小定理.

$$a(2a)(3a)\dots((p-1)a) \equiv 1 * 2 * 3 * \dots * (p-1) \pmod{p}.$$

$$a^{p-1} * (p-1)! \equiv (p-1)! \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

10 同余式, 幂和欧拉公式

假设存在 $a^k \equiv 1 \pmod{m}$, 即存在 $a^k - my = 1$, 则 $\gcd(a, m)$ 整除 $a^k - my$ 也就是 1.

说明如果 a 的某个幂模 m 余 1, 则必有 $\gcd(a, m) = 1$, 也就是说 a 和 m 互素.

在 0 与 m 之间且与 m 互素的整数个数是个重要量, 这个量为.

$$\phi(x) = \#\{a : 1 \leq a \leq m, \gcd(a, m) = 1\}.$$

$$\phi(1) = 1.$$

函数 $\phi(x)$ 叫做欧拉函数.

当 p 是素数时, $\phi(p) = p - 1$.

10.1 欧拉公式

如果 $\gcd(a, m) = 1$, 则

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

证明:

令 $1 < b_1 < b_2 < \dots < b_{\phi(m)} < m$ 是 0 与 m 之间且与 m 互素的 $\phi(m)$ 个整数.

首先证明断言: 如果 $\gcd(a, m) = 1$, 则数列 $b_1a, b_2a, \dots, b_{\phi(m)}a \pmod{m}$ 与数列 $b_1, b_2, \dots, b_{\phi(m)} \pmod{m}$ 相同, 尽管次序不同.

因为 b_n 与 m 互素, 所以 ab_n 也与 m 互素, 又因为 0 与 m 之间且与 m 互素的整数个数为 $\phi(m)$, 所以现在只需要证明前一个数列每个数对于模 m 不同即可证明断言.

取 $b_i a, b_j a$, 假设它们同余: $b_i a \equiv b_j a \pmod{m}$, 证明方式同之前证明费马小定理. 断言得证.

现在证明欧拉公式.

$$(b_1 a) * (b_2 a) * \dots * (b_{\phi(m)} a) \pmod{m} = b_1 * b_2 * \dots * b_{\phi(m)} \pmod{m}$$

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

11 欧拉函数与中国剩余定理

直接计算一个大合数的欧拉函数的值是困难的, 但是计算一个素数的欧拉函数的值是简单的.

11.1 欧拉函数公式

当一个数是素数的幂次时, 也就是 $m = p^k$ 时. 与 m 不互素的数就是 p 的倍数. 它们有 p^{k-1} 个.

$$\phi(m) = \phi(p^k) = p^k - p^{k-1}.$$

乘法公式: 如果 $\gcd(n, m) = 1$.

$$\phi(mn) = \phi(m)\phi(n).$$

乘法公式证明:

此处使用计数这个工具对该公式进行证明 (即用不同的方法计算数集中数的个数, 然后进行比较).

$\phi(mn)$ 对应 (指元素个数对应) 的集合为 $\{a : 1 \leq a \leq mn, \gcd(a, mn) = 1\}$.

$\phi(m)\phi(n)$ 对应的集合为 $\{(b, c) : 1 \leq b \leq m, \gcd(b, m) = 1, 1 \leq c \leq n, \gcd(c, n) = 1\}$.

定义一种关系: 取第一个集合的整数 a 并把它指派到序对 (b, c) 满足: $a \equiv b \pmod{m}, a \equiv c \pmod{n}$.

要证明两个集合元素个数相同, 即 $\phi(mn) = \phi(m)\phi(n)$, 需要证明:

1. 第一个集合中的不同数对应第二个集合的不同序对.
2. 第二个集合的每个序对适合第一个集合的某个数. 从而证明两个集合元素个数相同.

取第一个集合的数 a_1, a_2 , 假设它们在第二个集合有相同象, 即.

$$a_1 \equiv a_2 \pmod{m}, a_1 \equiv a_2 \pmod{n}$$

因为 m, n 互素, 所以 $a_1 - a_2$ 被 mn 整除. 即 $a_1 \equiv a_2 \pmod{mn}$, 所以 a_1, a_2 是第一个集合的相同元素, 第一个条件得证.

第二个条件的证明正好就是中国剩余定理, 所以乘法公式得证.

11.2 中国剩余定理 (CRT)

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

证明:

第一个同余式的解为 $x = my + b$, 带入第二个同余式: $my \equiv c - b \pmod{n}$.

已知 $\gcd(m, n) = 1$, 根据线性同余式定理可知 $my \equiv c - b \pmod{n}$ 恰好有一个解 $y_1, 0 \leq y_1 < n$.

则第一个同余式的解为: $x_1 = my_1 + b, 0 \leq x_1 \leq mn$.

得证.

11.2.1 使用中国剩余定理求解一元线性同余方程

对于如下这种一元线性同余方程, $n_1, n_2, n_3, \dots, n_k$ 两两互质, 可使用中国剩余定理求解.

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

$$x \equiv a_3 \pmod{n_3}$$

...

$$x \equiv a_k \pmod{n_k}$$

1. 计算所有模数的积 n ;
2. 对于第 i 个方程: 计算 $m_i = \frac{n}{n_i}$, 计算 m_i 在模 n_i 意义下的逆元 m_i^{-1} , 计算 $c_i = m_i m_i^{-1}$.

3. 方程组的唯一解为: $a = \sum_{i=1}^k a_i c_i$.

证明:

取 $i, j, i \neq j$.

则 $m_j \equiv 0 \pmod{n_i}, c_j \equiv m_j \equiv 0 \pmod{n_i}$.

又 $c_i \equiv m_i(m_i^{-1} \pmod{n_i}) \equiv 1 \pmod{n_i}$.

$$\begin{aligned} a &\equiv \sum_{i=1}^k a_i c_i \pmod{n_i} \\ &\equiv a_i c_i \pmod{n_i} \\ &\equiv a_i m_i (m_i^{-1} \pmod{n_i}) \pmod{n_i} \\ &\equiv a_i \pmod{n_i} \end{aligned}$$

得证.

12 素数

素数是数论的基本构件, 每个数由将素数乘在一起的唯一方式构成.

12.1 无穷多素数定理

欧几里得证明: 假设已列出有限的素数表, 如果能通过该表找出新的素数, 且加入表中后仍旧可以重复找新素数的过程, 就表明有无穷多素数.

证明:

假设已经列出 n 个素数 $p_1, p_2, p_3, \dots, p_n$, 给出 $A = p_1 p_2 p_3 \dots p_n + 1$.

如果 A 本身是素数, 则可以作为新素数加入表中.

如果 A 不是素数, 则存在一个素数 q 整除 A .

$q|p_1p_2p_3\cdots p_n + 1$, 如果 q 在 $p_1, p_2, p_3, \dots, p_n$ 中, 则 $q|1$, 所以 q 不在 $p_1, p_2, p_3, \dots, p_n$ 中. 所以 q 作为新素数加入表中.
得证.

12.2 模 4 余 3 的素数定理

存在无穷多个模 4 余 3 的素数.

证明:

假设已经列出模 4 余 3 的素数为: $3, p_1, p_2, p_3, \dots, p_n$, 给出 $A = 4p_1p_2p_3\cdots p_n + 3$.

A 能分解为素数乘积: $A = q_1q_2\cdots q_m$.

则 $q_1q_2\cdots q_m$ 中至少存在一个 q_i 模 4 余 3(根据同余式的乘法).

又因为 q_i 整除 A 且 $3, p_1, p_2, p_3, \dots, p_n$ 不整除 A , 所以 q_i 不存在 $3, p_1, p_2, p_3, \dots, p_n$ 中, 所以 q_i 是新的表元素.

得证.

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 , 即存在无穷多个素数 p 满足 $p \equiv a \pmod{m}$.

13 素数计数

素数计数函数: $\pi(x) = \#\{\text{素数 } p | p \leq x\}$.

13.1 素数定理

$$\lim_{n \rightarrow \infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

13.2 哥德巴赫猜想

每个偶数 $n \geq 4$ 可表示成两个素数之和.

13.3 孪生素数猜想

存在无穷多个素数 p 使得 $p+2$ 也是素数.

13.4 $N^2 + 1$ 猜想

存在无穷多个形如 $N^2 + 1$ 的素数.

14 梅森素数

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

证明:

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \dots + a^2 + a + 1)$$

所以 $a - 1$ 必须等于 1, 即 $a = 2$.

假设 n 能分解成 $n = mk$.

$$a^n - 1 = (a^m)^k - 1 = (2^m - 1)((2^m)^{k-1} + (2^m)^{k-2} + \dots + (2^m)^2 + (2^m) + 1).$$

所以 n 一定是素数.

得证.

形如 $2^p - 1$ 的素数叫做梅森素数.

15 梅森素数与完全数

完全数是等于其真因数之和的数.

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.

15.2 σ 函数

定义 $\sigma(n) = n$ 的所有因数之和 (包括 1 和 n).

15.2.1 σ 函数公式

对于素数 $p, \sigma(p) = p + 1$.

对于素数幂 $p^k, \sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}$.

如果 $\gcd(m, n) = 1$, 则 $\sigma(mn) = \sigma(m)\sigma(n)$.

证明:

如果 m 和 n 都是素数, $\sigma(mn) = 1 + m + n + mn = (1 + m)(1 + n) = \sigma(m)\sigma(n)$.

如果 m 可以分解为三个素数乘积, $m = q_1 q_2 q_3$.

$$\begin{aligned}\sigma(m) &= 1 + q_1 + q_2 + q_3 + q_1 q_2 + q_1 q_3 + q_2 q_3 + q_1 q_2 q_3 \\ &= (1 + q_1)(1 + q_2 + q_3 + q_2 q_3) \\ &= \sigma(q_1)\sigma(q_2 q_3) \\ &= \sigma(q_1)\sigma(q_2)\sigma(q_3)\end{aligned}$$

同理可证明如果 $\gcd(m, n) = 1$, 则 $\sigma(mn) = \sigma(m)\sigma(n)$.

当 $\sigma(n) = 2n$ 时, n 恰好是完全数.

15.3 欧拉完全数定理

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

证明:

假设 n 是偶完全数, n 是偶数说明可将它分解成 $n = 2^k m, k \geq 1, m \equiv 1 \pmod{2}$.

$$\begin{aligned}\sigma(n) &= \sigma(2^k m) \\ &= \sigma(2^k)\sigma(m) \\ &= (2^{k+1} - 1)\sigma(m)\end{aligned}$$

又因为 n 是完全数, 所以有: $(2^{k+1} - 1)\sigma(m) = 2^{k+1}m$.

由 $(2^{k+1} - 1)$ 是奇数可知: $2^{k+1} | \sigma(m)$.

所以 $\sigma(m) = 2^{k+1}c$, 带入得: $(2^{k+1} - 1)2^{k+1}c = 2^{k+1}m, m = (2^{k+1} - 1)c$.

假设 $c > 1, \sigma(m) \geq 1 + m + c \geq 1 + (2^{k+1} - 1)c + c \geq 1 + 2^{k+1}c \geq 1 + \sigma(m)$, 矛盾.

所以 $c = 1$, 即 $m = (2^{k+1} - 1), \sigma(m) = 2^{k+1} = m + 1$, 所以 m 为素数, $n = (2^{k+1} - 1)2^k$.

又由梅森素数的性质可知: 因为 $2^{k+1} - 1$ 为素数, 所以 $k + 1$ 为素数, 则 n 可以表示为: $2^{p-1}(2^p - 1)$, 其中 $2^p - 1$ 为梅森素数.

得证.

16 幂模 m 和逐次平方法

计算 $a^k \pmod{m}$ 的值.

1. 将 k 表示成 2 的幂次和: $k = u_0 + u_1 * 2 + u_2 * 2^2 + u_3 * 2^3 + \dots + u_r * 2^r$, 其中每个 u_i 是 0 或 1, 这种表达式叫做 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.

$$a^1 \equiv A_0 \pmod{m}$$

$$a^2 \equiv (a^1)^2 \equiv A_0^2 \equiv A_1 \pmod{m}$$

$$a^3 \equiv (a^2)^2 \equiv A_1^2 \equiv A_2 \pmod{m}$$

$$a^4 \equiv (a^3)^2 \equiv A_2^2 \equiv A_3 \pmod{m}$$

...

$$a^{2^r} \equiv (a^{2^{r-1}})^2 \equiv A_{r-1}^2 \equiv A_r \pmod{m}$$

3. 乘积 $A_0^{u_0} A_1^{u_1} A_2^{u_2} \dots A_r^{u_r} \pmod{m}$ 同余于 $a^k \pmod{m}$.

使用逐次平方法和费马小定理可以极为方便的证明一个数为合数.

取小于 m 的数 a, 如果 a 与 m 不互素, 则 a 是 m 的因数, m 是合数, 互素的话使用逐次平方法计算 $a^{m-1} \pmod{m}$, 如果答案不是 1 则 m 是合数. 注意, 答案是 1 不能确定 m 不是合数.

存在合数 m 对于所有与其互素的 a 满足 $a^{m-1} \equiv 1 \pmod{m}$, 这种数称为卡米歇尔数.

17 计算模 m 的 k 次根

设 b, k, m 是已知整数, 满足 $\gcd(b, m) = 1$, 与 $\gcd(k, \phi(m)) = 1$.

可以通过下列步骤求出同余式 $x^k \equiv b \pmod{m}$ 的解.

1. 计算 $\phi(m)$.
 2. 求满足 $ku - \phi(m)v = 1$ 的正整数 u 与 v. u 就是 k 在模 $\phi(m)$ 意义下的逆元.
 3. 用逐次平方法求 $b^u \pmod{m}$, 所得值给出解.
- 证明.

$$\begin{aligned}
x^k &= (b^u)^k \\
&= b^{uk} \\
&= b^{\phi(m)v+1} \\
&= b * (b^{\phi(m)})^v \\
&\equiv b \pmod{m}
\end{aligned}$$

18 幂, 根与不可破密码

RSA 加密与解密过程.

首先选取两个素数 p, q . 接下来将 p 和 q 相乘获得模 $m=pq$.

同时也就知道了: $\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$.

选取与 $\phi(m)$ 互素的整数 k , 此时可以将 m 和 k 作为公钥告诉别人, 别人可以利用 m 和 k 加密信息.

加密过程.

1. 先将信息数串分段成小于 m 的数, 从而获得一个数表 a_1, a_2, \dots, a_r .
2. 使用逐次平方法计算 $a_1^k \pmod{m}, a_2^k \pmod{m}, \dots, a_r^k \pmod{m}$, 获得一个新的数表 b_1, b_2, \dots, b_r , 也就是加密的信息.

解密过程.

1. 获取加密后的数表 b_1, b_2, \dots, b_r 后, 实际上就是解 $a_i^k \equiv b_i \pmod{m}$.
2. 由于自己拥有 p 和 q , 可以计算出 $\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$. 所以可以使用上一章的方法求出 a_i .

破解的难点: 由于只有 m , 所以无法直接求出 $\phi(m)$, 对于大素数来说, 这种破解在现有计算机算力的情况下是不现实的.

19 素性测试与卡米歇尔数

判断一个数是否是素数.

1. 对于较小的整数 n , 可以遍历检测从 2 到 \sqrt{n} 所有可能的 (素) 因数.
2. 通过费马小定理判断一个数是否一定是合数, 但这不能确定一个数是素数.

卡米歇尔数: 一个整数 n , 对于每个整数 $1 \leq a \leq n$, 都有 $a^n \equiv a \pmod{n}$. 即无法通过费马小定理确定卡米歇尔数一定是合数.

19.1 卡米歇尔数性质

A. 每个卡米歇尔数都是奇数.

B. 每个卡米歇尔数都是不同素数的乘积.

证明 A:

$$a^n \equiv a \pmod{n}, a = n - 1 \equiv -1 \pmod{n}.$$

$$(-1)^n \equiv -1 \pmod{n}.$$

这蕴含了 n 是奇数或者 2.

证明 B:

n 是卡米歇尔数, p 是整除 n 的一个素数, p^{e+1} 是整除 n 的 p 的最大次幂.

$$p^{ne} \equiv p^n \pmod{n}$$

所以 n 整除 $p^{ne} - p^n$, 又因为 p^{e+1} 整除 n , 所以 p^{e+1} 整除 $p^{ne} - p^n$.

所以 $\frac{p^{en} - p^e}{p^{e+1}} = \frac{p^{en-e}}{p}$ 的结果是一个整数. 易知 e 只能为 0.

19.2 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 满足下述条件:

(1) p^2 不整除 n .

(2) $p - 1$ 整除 $n - 1$.

证明:

将 n 分解成素数乘积, $n = p_1 p_2 p_3 \dots p_i$.

由 1 可知 p_1, p_2, \dots, p_i 互不相同, 由 2 可知 $n - 1 = (p_j - 1)k_j$.

现在任选一个整数 a , 计算 $a^n \equiv a \pmod{p_j}$.

如果 p_j 整除 a , 则: $a^n \equiv 0 = a \pmod{p_j}$.

如果 p_j 不整除 a .

$$\begin{aligned} a^n &= a^{(p_j-1)k_j+1} \\ &= (a^{p_j-1})^{k_j} * a \\ &\equiv 1^{k_j} * a \pmod{p_j} \\ &\equiv a \pmod{p_j} \end{aligned}$$

所以 $a^n - a$ 被每个素数 p_1, p_2, \dots, p_i 整除, 从而它被 $n = p_1 p_2 p_3 \dots p_i$ 整除 (p_1, p_2, \dots, p_i 互不相同).

所以 $a^n \equiv a \pmod{n}$.

此时已经证明满足条件的奇合数是卡米歇尔数.

在前面已经证明了每个卡米歇尔数都是不同素数的乘积.

现在证明对于卡米歇尔数 n , 整除 n 的每个素数 p 都有 $p-1$ 整除 $n-1$.

1.

这里要用到之后会证明的一个断言: 对每个素数 p , 至少存在一个数 g , 其幂 $g, g^2, g^3, \dots, g^{p-1}$ 都是模 p 不同余的 (g 被称为原根).

对每个 n 的素因数 p_x , 首先找到其原根 g .

$$g^n \equiv g \pmod{n}$$

也就是 $g^n - g$ 被 n 整除, 所以 $g^n - g$ 被 p_x 整除.

$$n = (p_x - 1)k + j$$

$$g^n \equiv g \pmod{p_x}$$

$$g^n = g^{(p_x-1)k+j} \equiv g^j \pmod{p_x}$$

$$g^j \equiv g \pmod{p_x}$$

又因为 $g, g^2, g^3, \dots, g^{p_x-1}$ 都是模 p_x 不同余的, 所以 $j=1$.

$n = (p_x - 1)k + 1, n - 1 = (p_x - 1)k, p_x - 1 | n - 1$, 考塞特判别法得证.

19.3 素数的一个性质

设 p 是一个奇素数, 记 $p-1 = 2^k q, q$ 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 $a^q, a^{2q}, a^{2^2q}, \dots, a^{2^{k-1}q}$ 之一模 p 余-1.

证明.

$$a^{p-1} \equiv 1 \pmod{p}$$

所以数表 $a^q, a^{2q}, a^{2^2q}, \dots, a^{2^{k-1}q}, a^{2^kq}$ 的最后一个数模 p 余 1.

因此下面两种可能之一必成立.

(1) 表中第一个数模 p 余 1. (2) 表中一些数模 p 不余 1, 但是平方后就模 p 余 1, 所以该数模 p 余-1.

得证.

19.4 合数的拉宾-米勒测试

设 n 是奇数, 设 $n-1 = 2^k q$, 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) $a^q \not\equiv 1 \pmod{n}$. (2) 对于所有 $i = 0, 1, 2, \dots, k-1, a^{2^i q} \not\equiv -1 \pmod{n}$.

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.

20 欧拉函数与因数和

定义函数 $F(n)$.

$F(n) = \phi(d_1) + \phi(d_2) + \dots + \phi(d_r)$, 其中 d_1, d_2, \dots, d_r 是 n 的因数.

20.1 欧拉函数求和公式

$F(n) = \phi(d_1) + \phi(d_2) + \dots + \phi(d_r) = n$, 其中 d_1, d_2, \dots, d_r 是 n 的因数.

证明:

对于素数 $p, F(p) = \phi(1) + \phi(p) = 1 + (p-1) = p$.

对于素数幂 $p^k, F(p^k) = \phi(1) + \phi(p) + \phi(p^2) + \dots + \phi(p^k) = 1 + (p-1) + (p^2 - p) + \dots + (p^k - p^{k-1}) = p^k$.

对于 $m = pq, p$ 和 q 都是素数, $F(m) = \phi(1) + \phi(p) + \phi(q) + \phi(pq) = \phi(1) + \phi(p) + \phi(q) + \phi(p)\phi(q) = (1 + \phi(p))(1 + \phi(q)) = F(p)F(q)$.

如果 $\gcd(m, n) = 1, m = d_1 d_2 d_3 \dots d_r, n = e_1 e_2 e_3 \dots e_s$.

由于 m 和 n 互素, 所以 mn 的因数为: $d_1 e_1, d_1 e_2, \dots, d_1 e_s, d_2 e_1, d_2 e_2, \dots, d_2 e_s, \dots, d_r e_1, d_r e_2, \dots, d_r e_s$.

$$\begin{aligned} F(mn) &= \phi(d_1 e_1) + \phi(d_1 e_2) + \dots + \phi(d_1 e_s) + \dots + \phi(d_r e_s) \\ &= \phi(d_1)\phi(e_1) + \phi(d_1)\phi(e_2) + \dots + \phi(d_1)\phi(e_s) + \dots + \phi(d_r)\phi(e_s) \\ &= (\phi(d_1) + \phi(d_2) + \dots + \phi(d_r))(\phi(e_1) + \phi(e_2) + \dots + \phi(e_s)) \\ &= F(m)F(n) \end{aligned}$$

对于任意自然数 n , 将 n 分解为素数幂的乘积.

$$\begin{aligned}
F(n) &= F(p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \\
&= F(p_1^{i_1}) F(p_2^{i_2}) \dots F(p_k^{i_k}) \\
&= p_1^{i_1} p_2^{i_2} \dots p_k^{i_k} \\
&= n
\end{aligned}$$

21 幂模 p 与原根

a 与 p 互素, 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 $e \geq 1$).

21.1 次数整除性质

设 a 与 p 互素. 假设 $a^n \equiv 1 \pmod{p}$, 则次数 $e_p(a)$ 整除 n, 特别的, 次数 $e_p(a)$ 总整除 p - 1.

证明:

$$a^{e_p(a)} \equiv 1 \pmod{p}.$$

假设 $a^n \equiv 1 \pmod{p}$, 设 $G = \gcd(e_p(a), n)$, 并设 (u, v) 是方程 $e_p(a)u - mv = G$ 的正整数解.

$$\begin{aligned}
a^{e_p(a)u} &= (a^{e_p(a)})^u \equiv 1^u \equiv 1 \pmod{p} \\
a^{e_p(a)u} &= a^{nv+G} = (a^n)^v * a^G \equiv 1^v * a^G \equiv a^G \pmod{p}
\end{aligned}$$

所以 $a^G \equiv 1 \pmod{p}$, 又 $G = \gcd(e_p(a), n)$, 所以 G 整除 $e_p(a)$ 和 n, $G \leq e_p(a)$.

又 $G \geq e_p(a)$ ($e_p(a)$ 定义), 所以 $G = e_p(a)$, $e_p(a)$ 整除 n. 因为 $a^{p-1} \equiv 1 \pmod{p}$, 所以 $e_p(a)$ 总整除 p - 1.

21.2 原根定理

具有最高次数 $e_p(g) = p-1$ 的数 g 称为模 p 的原根, 同时幂 $g, g^2, g^3, \dots, g^{p-1}$ 都是模 p 不同余的 (如果不是全不同余, 则存在 $1 \leq i < j \leq p-1, a^i \equiv a^j \pmod{p}$, 则 $a^{j-i} \equiv 1 \pmod{p}$, 其中 j - i 小于 p - 1).

原根定理: 每个素数 p 都有原根, 且恰好有 $\phi(p-1)$ 个.

证明:

首先定义一个函数: $\psi(d) = (\text{使得 } 1 \leq a < p \text{ 且 } e_p(a) = d \text{ 的 } a \text{ 的个数})$.

设 n 是整除 $p-1$ 的任何整数, 则 $p-1=nk$.

$$\begin{aligned} X^{p-1} - 1 &= X^{nk} - 1 \\ &= (X^n)^k - 1 \\ &= (X^n - 1)((X^n)^{k-1} + (X^n)^{k-2} + \cdots + (X^n)^2 + X^n + 1) \end{aligned}$$

根据费马小定理: $X^{p-1} - 1 \equiv 0 \pmod{p}$ 恰好有 $p-1$ 个解 $(0, \cdots, p-1)$.

而 $X^n - 1 \equiv 0 \pmod{p}$ 至多有 n 个解, $(X^n)^{k-1} + (X^n)^{k-2} + \cdots + (X^n)^2 + X^n + 1 \equiv 0 \pmod{p}$ 至多有 $nk - n$ 个解.(更一般的, $F(X)$ 是整数系 D 次多项式, 则同余式 $F(X) \equiv 0 \pmod{p}$ 至多有 D 个解)

由上可知: 对于 n 整除 $p-1$, 则同余式 $X^n - 1 \equiv 0 \pmod{p}$ 恰好有 n 个根满足 $0 \leq X < p$.

现在换一种方法计算 $X^n - 1 \equiv 0 \pmod{p}$ 的解的个数.

如果 $X=a$ 是解, 则 $a^n \equiv 1 \pmod{p}$, 由次数整除性质可知 $e_p(a)$ 整除 n , 如果观察 n 的因数, 且对 n 的每个因数 d , 取使得 $e_p(a) = d$ 的那些 a , 则可以得到 $X^n - 1 \equiv 0 \pmod{p}$ 的所有解.

即 $X^n - 1 \equiv 0 \pmod{p}$ 的解的个数为: $\psi(d_1) + \psi(d_2) + \psi(d_3) + \cdots + \psi(d_r)$.

此时可知. 对于 n 整除 $p-1$, 设 d_1, d_2, \cdots, d_r 是 n 的因数 (包括 1 和 n), 则

$$\psi(d_1) + \psi(d_2) + \psi(d_3) + \cdots + \psi(d_r) = n = \phi(d_1) + \phi(d_2) + \phi(d_3) + \cdots + \phi(d_r).$$

现在证明 $\psi(n) = \phi(n)$.

首先 $\psi(1) = 1 = \phi(1)$.

对于素数 q , $\psi(q) + \psi(1) = q = \phi(q) + \phi(1)$, $\psi(q) = \phi(q)$. 同理可证对于素数幂次, 不同素数乘积都满足 $\psi(n) = \phi(n)$.

归纳证明: 假设对于所有 $d < n$, 已经证明了 $\psi(d) = \phi(d)$. 设 d_1, d_2, \cdots, d_r 是 n 的因数 ($d_1 = n$).

$$\text{则: } \psi(n) + \psi(d_2) + \psi(d_3) + \cdots + \psi(d_r) = n = \phi(n) + \phi(d_2) + \phi(d_3) + \cdots + \phi(d_r). \psi(n) = \phi(n).$$

得证: 每个素数 p 都有原根, 且恰好有 $\phi(p-1)$ 个原根.

22 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. 所以对任何数 $1 \leq a < p$, 可选择幂 $g, g^2, g^3, g^4, \dots, g^{p-3}, g^{p-2}, g^{p-1}$ 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 和 g 给定, 则记指标为 $I(a), g^{I(a)} \equiv a \pmod{p}$.

$g=2, p=13$ 的指标表格.

a	1	2	3	4	5	6	7	8	9	10	11	12
$I(a)$	12	1	4	2	9	5	11	3	8	10	7	6

22.1 指标法则

指标法则:

$$(a) I(ab) \equiv I(a) + I(b) \pmod{p-1}. \quad (b) I(a^k) \equiv kI(a) \pmod{p-1}.$$

证明:

$$g^{I(ab)} \equiv ab \equiv g^{I(a)} g^{I(b)} \equiv g^{I(a)+I(b)} \pmod{p}.$$

即 $g^{I(ab)-I(a)-I(b)} \equiv 1 \pmod{p}$, 又 g 是原根, 所以 $p-1$ 整除 $I(ab) - I(a) - I(b)$, $I(ab) \equiv I(a) + I(b) \pmod{p-1}$ 得证.

$$I(a^k) \equiv kI(a) \pmod{p-1} \text{ 同理得证.}$$

注意: 总是通过模 $p-1$ 来简化指标.

22.2 指标与求解同余式

$$19x \equiv 23 \pmod{37}$$

$$I(19x) = I(23)$$

$$I(19) + I(x) \equiv I(23) \pmod{36}$$

$$35 + I(x) \equiv 15 \pmod{36}$$

$$I(x) \equiv 16 \pmod{36}$$

查表得 $x \equiv 9 \pmod{37}$.

$$3x^{30} \equiv 4 \pmod{37}$$

$$I(3x^{30}) = I(4)$$

$$I(3) + I(x^{30}) \equiv I(23) \pmod{36}$$

$$26 + 30I(x) \equiv 2 \pmod{36}$$

$$30I(x) \equiv 12 \pmod{36}$$

根据第八章得结论解 $I(x)$: 如果 $\gcd(a, m)$ 整除 c , 则同余式 $ax \equiv c \pmod{m}$ 有 $\gcd(a, m)$ 个解, 否则没有解.

求得 $I(x) \equiv 4, 10, 16, 22, 28, 34 \pmod{36}$.

即: $x \equiv 16, 25, 9, 21, 12, 28 \pmod{37}$.

指标也被称为离散对数. 给定一个大素数 p 以及模 p 得两个数 a 与 g . 离散对数问题 (DLP) 是求指数 k 使得: $g^k \equiv a \pmod{p}$, 即求以 g 为底的 a 模 p 的指标.

23 模 p 平方剩余

模 7 的平方剩余.

0	1	2	3	4	5	6
0	1	4	2	2	4	1

易知: 数 b 的平方剩余与数 $p-b$ 的平方剩余是模 p 相同的.

$$(p-b)^2 = p^2 - 2pb + b^2 \equiv b^2 \pmod{p}.$$

与一个平方数模 p 同余的非零数称为模 p 的二次剩余 (记为 QR). 不与任何一个平方数模 p 同余的非零数称为模 p 的 (二次) 非剩余 (记为 NR). 与 0 模 p 同余的数即不是 QR 也不是 NR.

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

证明:

二次剩余是非零数, 它们是模 p 平方剩余, 因此它们是这些数: $1^2, 2^2, \dots, (p-1)^2 \pmod{p}$.

由于其中有一半是重复的, 所以它们应该是: $1^2, 2^2, \dots, (\frac{p-1}{2})^2 \pmod{p}$.

此时只需要证明这些数是两两不相同的即可证明恰有 $\frac{p-1}{2}$ 个模 p 的二次剩余. 而总共为 $p-1$ 个数, 所以也就证明了恰有 $\frac{p-1}{2}$ 个模 p 的二次非剩余.

假设 b_1, b_2 都是 1 到 $\frac{p-1}{2}$ 之间的数, 且满足 $b_1^2 \equiv b_2^2 \pmod{p}$.

则 $p | b_1^2 - b_2^2 | (b_1 - b_2)(b_1 + b_2)$.

$b_1 + b_2$ 是 2 到 $p-1$ 之间的数, 因此不可能被 p 整除.

所以 p 整除 $b_1 - b_2$, 但是 $|b_1 - b_2| < \frac{p-1}{2}$, 所以 $b_1 = b_2$. 得证.

23.1 二次剩余乘法法则—版本 1

原根与二次剩余的关系.

设 g 是模 p 的一个原根. 那么 g 的幂: g^1, \dots, g^{p-1} 给出了模 p 的所有非零剩余. 其中一半为 QR, 一般为 QR.

显然 g^2, g^4, \dots, g^{p-1} 都是 QR 且刚好为 $\frac{p-1}{2}$ 个. 则另外 $\frac{p-1}{2}$ 个奇次幂就是 NR.

又因为 a 模 p 对原根 g 的指标是指满足 $a \equiv g^{I(a)} \pmod{p}$ 的幂 $I(a)$.

所以: QR 是指标 $I(a)$ 为偶数的那些数 a , NR 是指标 $I(a)$ 为奇数的那些数 a .

现在来描述二次剩余乘法法则—版本 1.

(1) 两个模 p 的二次剩余的积是二次剩余: $QR \times QR = QR$. (2) 二次剩余与二次非剩余的积是二次非剩余: $QR \times NR = NR$. (3) 两个二次非剩余的积是二次剩余: $NR \times NR = QR$.

证明: $I(ab) = I(a) + I(b)$. 则可由 $I(ab)$ 的奇偶性得证.

23.2 二次剩余乘法法则—版本 2

如果用数字替代 QR 和 NR, 则可以认为 $QR=1, NR=-1$.

勒让德引入了以下符号.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ 是模 } p \text{ 的 QR} \\ -1, & a \text{ 是模 } p \text{ 的 NR} \end{cases}$$

现在来描述二次剩余乘法法则—版本 2.

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

24 -1 是模 p 平方剩余吗?2 呢

24.1 欧拉准则

欧拉准则: 设 p 为素数, 则 $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

证明:

设 g 是模 p 的一个原根, 每个数 a 都与 g 的某个幂同余.

当 a 正好与 g 的偶次幂同余时 a 是二次剩余.

则 $a^{(p-1)/2} \equiv g^{k(p-1)} \equiv (g^{p-1})^k \equiv 1^k \equiv \left(\frac{a}{p}\right) \pmod{p}$.

当 a 正好与 g 的奇次幂同余时 a 是二次非剩余.

则 $a^{(p-1)/2} \equiv g^{k(p-1)} \cdot g^{(p-1)/2} \equiv (g^{p-1})^k \cdot g^{(p-1)/2} \pmod{p}$.

$g^{(p-1)/2}$ 必与 +1 或 -1 同余 (因为 $a^{p-1} \equiv 1 \pmod{p}$), 又因为 $e_p(g) = p-1$, 所以 $a^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}$.

24.2 二次互反律-第 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 $p \equiv 3 \pmod{4}$.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}$$

可以用欧拉准则证明:

$$(-1)^{(p-1)/2} \equiv (-1)^{(4k+1-1)/2} \equiv (-1)^{2k} \equiv 1 \pmod{p}.$$

$$(-1)^{(p-1)/2} \equiv (-1)^{(4k+3-1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}.$$

24.3 模 4 余 1 素数定理

定理: 存在无穷多个素数与 1 模 4 同余.

假设已存在一系列素数 p_1, p_2, \dots, p_r 都是模 4 余 1.

数 $A = (2p_1p_2 \cdots p_r)^2 + 1$ 可以分解为素数的乘积: $A = q_1q_2 \cdots q_s$.

显然 q_1, q_2, \dots, q_s 不在原来的素数列中. 由于 A 是奇数, 所以 q_1, q_2, \dots, q_s 都是奇数.

同时: $(2p_1p_2 \cdots p_r)^2 + 1 = A \equiv 0 \pmod{q_i}$. 也就是 $x = 2p_1p_2 \cdots p_r$ 是同余式 $x^2 \equiv -1 \pmod{q_i}$ 的解.

也就是-1 是模 q_i 的二次剩余. 由二次互反律可知 $q_i \equiv 1 \pmod{4}$.

24.4 二次互反律—第 II 部分

设 p 为奇素数, 则:

2 是模 p 的二次剩余, 若 $p \equiv 1$ 或 $7 \pmod{8}$.

2 是模 p 的二次非剩余, 若 $p \equiv 3$ 或 $5 \pmod{8}$.

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1 \text{ 或 } 7 \pmod{8} \\ -1, & p \equiv 3 \text{ 或 } 5 \pmod{8} \end{cases}$$

证明:

设 p 是一个奇素数, $P = \frac{p-1}{2}$. 从偶数 $2, 4, 6, \dots, p-1$ 开始将它们相乘. 并从每个数中提出因子 2, 可得 $2 \cdot 4 \cdot 6 \cdots (p-1) = 2^P P!$.

对 $2, 4, 6, \dots, p-1$ 进行模 p 简化, 使其全部落在 $-P$ 到 P 之间, 即 $-(p-1)/2$ 到 $(p-1)/2$ 之间. 前几个数不会改变, 而从数列中某一项开始所有数都大于 P , 这些大数需要减去 p .

$2^P P! = 2 \cdot 4 \cdot 6 \cdots (p-1) \equiv 2 \cdot 4 \cdot 6 \cdots (p-5) \cdot (p-3) \cdot (p-1) \equiv (-1)^{\text{大于 } P \text{ 的数的个数}} \cdot P! \pmod{p}$

约去 $P!$ 得到: $2^{\frac{p-1}{2}} \equiv (-1)^{\text{大于 } P \text{ 的数的个数}} \pmod{p}$.

通过欧拉准则可知大于 P 的数的个数为偶数是 2 是 p 的 QR.

这里给出 $p \equiv 3 \pmod{8}$ 的证明.

$p-1=8k+2, P=4k+1$, 大于 P 的数为 $4k+2, 4k+4, \dots, 8k+2$. 为奇数个, 说明 2 是 p 的 NR, $\left(\frac{2}{p}\right) = -1$.

25 二次互反律

设 p, q 是不同的奇素数, 则

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1 \text{ 或 } 7 \pmod{8} \\ -1, & p \equiv 3 \text{ 或 } 5 \pmod{8} \end{cases}$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & p \equiv 1 \pmod{4} \text{或} q \equiv 1 \pmod{4} \\ -\left(\frac{p}{q}\right), & p \equiv 3 \pmod{4} \text{且} q \equiv 3 \pmod{4} \end{cases}$$

一个二次互反律的利用示例.

$$\begin{aligned} \left(\frac{55}{179}\right) &= \left(\frac{5}{179}\right) \left(\frac{11}{179}\right) \\ &= \left(\frac{179}{5}\right) \times (-1) \times \left(\frac{179}{11}\right) \\ &= \left(\frac{4}{5}\right) \times (-1) \times \left(\frac{3}{11}\right) \\ &= 1 \times (-1) \times (-1) \times \left(\frac{11}{3}\right) \\ &= 1 \times (-1) \times (-1) \times \left(\frac{2}{3}\right) \\ &= 1 \times (-1) \times (-1) \times (-1) \\ &= -1 \end{aligned}$$

所以,55 是 179 的 NR.

25.1 广义二次互反律

设 a,b 为正奇数, 则

$$\begin{aligned} \left(\frac{-1}{b}\right) &= \begin{cases} 1, & b \equiv 1 \pmod{4} \\ -1, & b \equiv 3 \pmod{4} \end{cases} \\ \left(\frac{2}{b}\right) &= \begin{cases} 1, & b \equiv 1 \text{或} 7 \pmod{8} \\ -1, & b \equiv 3 \text{或} 5 \pmod{8} \end{cases} \\ \left(\frac{a}{b}\right) &= \begin{cases} \left(\frac{b}{a}\right), & a \equiv 1 \pmod{4} \text{或} b \equiv 1 \pmod{4} \\ -\left(\frac{b}{a}\right), & a \equiv 3 \pmod{4} \text{且} b \equiv 3 \pmod{4} \end{cases} \end{aligned}$$

26 哪些素数可表示成两个平方数之和

26.1 素数的两平方数之和定理

设 p 是素数, 则 p 是两平方数之和的充要条件是

$$p \equiv 1 \pmod{4} \text{ (或 } p=2)$$

首先证明: 如果 p 是两平方数之和, 则 $p \equiv 1 \pmod{4}$.

$$p = a^2 + b^2.$$

p 是奇数, 则 a, b 一奇数一偶数. 定奇数为 a , 偶数为 b .

$$a = 2n + 1, b = 2m, p = 4n^2 + 4n + 1 + 4m^2 \equiv 1 \pmod{4}$$

另外一种证明:

$$a^2 + b^2 \equiv 0 \pmod{p}, -a^2 \equiv b^2 \pmod{p}$$

$$\left(\frac{-a^2}{p}\right) = \left(\frac{b^2}{p}\right)$$

$$\left(\frac{-1}{p}\right) \left(\frac{a}{p}\right)^2 = \left(\frac{b}{p}\right)^2$$

$$\left(\frac{-1}{p}\right) = 1$$

-1 是模 p 的二次剩余, 所以 $p \equiv 1 \pmod{4}$.

然后要证明: $p \equiv 1 \pmod{4}$, 则 p 是两平方数之和.

首先介绍费马降阶法:

$p \equiv 1 \pmod{4}$, 由二次互反律可知 $x^2 \equiv -1 \pmod{p}$ 有一解.

设 $x=A$, 则 $A^2 + 1^2 = Mp$.

如果 $M = 1$, 则证明完成. 否则 $M \geq 2$.

对于 $M \geq 2$ 可以使用费马降阶法, 即使用 A, B, M 发现新的整数 a, b, m , 使得

$$a^2 + b^2 = mp, m \leq M - 1$$

如果 $m = 1$, 则证明完成. 否则重复这个过程直到 $m = 1$.

26.1.1 费马降阶法

先看一个恒等式: $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$

对于 $A^2 + 1^2 = Mp$.

选取数 $u, v, u \equiv A \pmod{M}, v \equiv B \pmod{M}, -\frac{1}{2}M \leq u, v \leq \frac{1}{2}M$.

观察到 $u^2 + v^2 \equiv A^2 + B^2 \equiv 0 \pmod{M}$

所以 $u^2 + v^2 = Mr(1 \leq r < M), A^2 + B^2 = Mp$.

$$(u^2 + v^2) * (A^2 + B^2) = M^2 rp.$$

利用 $u \equiv A \pmod{M}, v \equiv B \pmod{M}, -\frac{1}{2}M \leq u, v \leq \frac{1}{2}M$.

$$(uA + vB)^2 + (vA - uB)^2 = M^2 rp$$

得到一个新的式子 $(\frac{uA+vB}{M})^2 + (\frac{vA-uB}{M})^2 = rp$

证明费马降阶法一定会得到一个 $r = 1$ 的式子.

$$\text{最开始 } M = \frac{A^2+B^2}{p} \leq \frac{(p-1)^2+1^2}{p} = p - \frac{2p-2}{p} < p$$

$$vA - uB \equiv BA - AB \equiv 0 \pmod{M}. uA + vB \equiv AA - BB \equiv Mp \equiv 0$$

\pmod{M} . 所以 $vA - uB$ 和 $uA + vB$ 被 M 整除.

$$r = \frac{u^2+v^2}{M} \leq \frac{(M/2)^2+(M/2)^2}{M} = \frac{M}{2}.$$

现在还要证明 r 不会变成 0.

如果 $r=0$, 则 $u^2 + v^2 = 0$, 即 $u = v = 0$, 所以 $A^2 + B^2$ 能被 M^2 整除.

$A^2 + B^2 = Mp$, 所以 M 整除 p , 又 $M < p$, 所以 $M = 1$. 即 $A^2 + B^2 = p$.

则此时不需要降阶, 且上一步的 $r = 1$.

27 习题

27.1 第一章

27.1.1 1.1

给出求三角平方数的有效方法, 是否有无穷多个三角平方数?

思路:

如果 a 是三角数, 则存在 n 为正整数使得 $a = \frac{n(n+1)}{2}$.

如果 a 是平方数, 则 $a = m^2, m$ 为正整数.

如果 a 是三角平方数, 则存在正整数 n, m , 使得 $a = \frac{n(n+1)}{2} = m^2$.

n 为偶数, 上式可化为 $\frac{n}{2} * (n+1) = m^2$ ($\frac{n}{2}$ 和 $(n+1)$ 是两个整数).

易知 $\frac{n}{2} < n+1$, 所以此时 m 需要是一个合数, $m = j * k (j < k), \frac{n}{2} = j^2, n+1 = k^2$.

$$k^2 - j^2 = n+1 - \frac{n}{2} = \frac{n}{2} + 1 = (k+j)(k-j)$$

所以 $\frac{n}{2} + 1$ 被 $(k+j)$ 和 $(k-j)$ 整除.

n 为奇数同理, 上式可化为 $\frac{n+1}{2} * n = m^2(\frac{n+1}{2}$ 和 (n) 是两个整数).

除了 $n = 1$ 的情况, 易知 $\frac{n+1}{2} < n$, 所以此时 m 需要是一个合数, $m = j * k(j < k), \frac{n+1}{2} = j^2, n = k^2$.

到这里已经可以较为方便的寻找三角平方数.