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.

$$\begin{aligned} a &= 2*x+1 \\ b &= 2*y+1 \\ c &= 2*z \\ a^2+b^2 &= c^2 \\ 2*(x^2+y^2+x+y)+1 &= 2*z^2 \end{aligned}$$

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

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

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 $d | r_2$,$d | r_3$,...,$d | r_n$. 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), 再通过配方求 a 和 b.

还有一种方法是利用欧几里得算法中的商和余数.

$$\begin{aligned} & r_1 = a - q_1 b \\ & r_2 = b - q_2 r_1, r_2 = b - q_2(a - q_1 b) \end{aligned}$$

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 $a_1a_2a_3...a_n$, 则 p 整除 $a_1, a_2, ..., a_n$ 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 $n = p_1p_2...p_n$.

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 $N + 1 = n_1n_2$, $2 \leq n_1, n_2 \leq N$. 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 $n = q_1q_2...q_n = p_1p_2...p_m$.

因为 $q_1|n$, 所以 $q_1|p_1p_2...p_m$, 由于素数整除性质, 所以 q_1 必整除 $p_1, p_2, ..., p_m$ 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 $q_2...q_n = p_1p_2...p_{i-1}pi + 1...p_m$, 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 $n = p_1p_2...p_n$.

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:

$$\begin{aligned} a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m} \\ a_1 + a_2 \equiv b_1 + b_2 \pmod{m} \\ a_1 a_2 \equiv b_1 b_2 \pmod{m} \end{aligned}$$

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:

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

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

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 $k = 0, 1, ..., g-1$ 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 $a, 2a, 3a, ..., (p-1)a \pmod p$ 与数 $1, 2, 3, ..., (p-1) \pmod p$ 相同, 尽管次序不同.

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

开始证明费马小定理.

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

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

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

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.

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

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 $1 < b_1 < b_2 < ... < b_{\phi(m)} < m$ 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 $b_1a, b_2a, ..., b_{\phi(m)}a \pmod{m}$ 与数列 $b_1, b_2, ..., b_{\phi(m)} \pmod{m}$ 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_ia, b_ja, 假设它们同余:$b_ia \equiv b_ja \pmod{m}$, 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.

$(b_1a) * (b_2a) * ... * (b_{\phi(m)}a) \pmod{m} = b_1 * b_2 * ... * b_{\phi(m)} \pmod{m}$

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

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.

$\phi(mn)$ 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,$0 \leq y_1 < b$.

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

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,$n_1, n_2, n_3, ..., n_k$ 两两互质, 可使用中国剩余定理求解.

$$
\begin{aligned}
x &\equiv a_1 \pmod{n_1} \\
x &\equiv a_2 \pmod{n_2} \\
x &\equiv a_3 \pmod{n_3} \\
&... \\
x &\equiv a_k \pmod{n_k}
\end{aligned}
$$

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:$a = \Sigma_{i=1}^{k} a_i c_i$.

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

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

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 $p_1, p_2, p_3, ..., p_n$, 给出 $A = p_1 p_2 p_3 ... p_n + 1$.

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.

$q|p_1p_2p_3...p_n + 1$, 如果 q 在 $p_1, p_2, p_3, ..., p_n$ 中, 则 $q|1$, 所以 q 不在 $p_1, p_2, p_3, ..., p_n$ 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:$3, p_1, p_2, p_3, ..., p_n$, 给出 $A = 4p_1p_2p_3...p_n + 3$.

A 能分解为素数乘积:$A = q_1q_2...q_m$.

则 $q_1q_2...q_m$ 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 $3, p_1, p_2, p_3, ..., p_n$ 不整除 A, 所以 q_i 不存在 $3, p_1, p_2, p_3, ..., p_n$ 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:$\pi(x) = \#\{\ p|p \leq x\}$.

13.1 素数定理

$\lim\limits_{n\to\infty} \frac{\pi(x)}{x/ln(x)} = 1$

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:

$a^n-1=(a-1)(a^{n-1}+a^{n-2}+...+a^2+x+1)$

所以 a - 1 必须等于 1, 即 a = 2.

假设 n 能分解成 n = mk.

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

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,$\sigma(p^k)=1+p+p^2+...+p^k=\frac{p^{k+1}-1}{p-1}$.

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,$m = q_1q_2q_3$.

$$\begin{aligned}
\sigma(m) &= 1 + q_1 + q_2 + q_3 + q_1q_2 + q_1q_3 + q_2q_3 + q_1q_2q_3 \\
&= (1 + q_1)(1 + q_2 + q_3 + q_2q_3) \\
&= \sigma(q_1)\sigma(q_2q_3) \\
&= \sigma(q_1)\sigma(q_2)\sigma(q_3)
\end{aligned}$$

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:$k = u_0 + u_1 * 2 + u_2 * 2^2 + u_3 * 2^3 + ... + u_r * 2^r$, 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.

$$
\begin{aligned}
a^1 &\equiv A_0 \pmod{m} \\
a^2 &\equiv (a^1)^2 \equiv A_0^2 \equiv A_1 \pmod{m} \\
a^3 &\equiv (a^2)^2 \equiv A_1^2 \equiv A_2 \pmod{m} \\
a^3 &\equiv (a^4)^2 \equiv A_2^2 \equiv A_3 \pmod{m} \\
&... \\
a^{2r} &\equiv (a^{2r-1})^2 \equiv A_{r-1}^2 \equiv A_r \pmod{m}
\end{aligned}
$$

3. 乘积 $A_0^{u_0} A_1^{u_1} A_2^{u_2} ... A_r^{u_r} \pmod{m}$ 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 $a_1, a_2, ..., a_r$.

2. 使用逐次平方法计算 $a_1^k \pmod m$,$a_2^k \pmod m$,...,$a_r^k \pmod m$, 获得一个新的数表 $b_1, b_2, ..., b_r$, 也就是加密的信息.

解密过程.

1. 获取加密后的数表 $b_1, b_2, ..., b_r$ 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 $1 \le a \le n$, 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,$n = p_1 p_2 p_3 ... p_i$.

由 1 可知 $p_1, p_2, ..., p_i$ 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 $p_1, p_2, ..., p_i$ 整除, 从而它被 $n = p_1 p_2 p_3 ... p_i$ 整除 ($p_1, p_2, ..., p_i$ 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.

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 $g, g^2, g^3, ..., g^{p-1}$ 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.

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

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

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

20 习题

20.1 第一章

20.1.1 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.