

第六章 素数检验

6.1 伪素数

1. 伪素数 Fermat 素性检验

① 费马定理: n 为素数, $(b, n) = 1$ 有 $b^{n-1} \equiv 1 \pmod{n}$ ①

↓
找到一个整 b , $(b, n) = 1$, 使
 $b^{n-1} \not\equiv 1 \pmod{n}$, 则 n 为合数 ②

$$\textcircled{1}: \text{ord}_n(b) \mid (n-1)$$

②: 有整 b , $(b, n) = 1$, 使 $\text{ord}_n(b) \nmid (n-1)$

例: $2^{62} \equiv 4 \not\equiv 1 \pmod{63}$

$\therefore 63$ 是一个合数

或 $\text{ord}_{63}(2) = 6 \nmid 62 \therefore 63$ 是一个合数

② 伪素数

n 为合数, $(b, n) = 1$ 有 $b^{n-1} \equiv 1 \pmod{n}$

则 n 叫做基于 b 的 **伪素数**

(另一种定义见 Page 1)

例: 63 是基 $b=8$ 的伪素数

$$63 = 2 \times 3$$

$$8^{62} \equiv 1 \pmod{63}$$

③ 伪素数性质

n 为合数

① n 是基 b 的伪素数 当且仅当 $\text{ord}_n(b) \mid (n-1)$

② $\sim b$ 与 $b_2 \sim$, 则也是 $b_1 \cdot b_2$ 的

③ $\sim b \sim$, 则也是 b^{-1} 的

④ 存在 b 使 $b^{n-1} \equiv 1 \pmod{n}$ 不成立, 则 n 简化中至少一半也会让他不成立.

↙ 类心素数

证明: $\Rightarrow b_1^{n-1} \equiv 1, b_2^{n-1} \equiv 1 \pmod{n}$

$$\Rightarrow (b_1 \cdot b_2)^{n-1} \equiv 1 \pmod{n}$$

$$\Rightarrow b^{n-1} \equiv 1 \pmod{n}$$

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

例:

剩余系中至少有一半的数使得同余式 (6.1) 不成立.

例 6.1.5 设 $n = 63$, 求出所有整数 $b, 1 \leq b \leq n-1$ 使得 n 是对于基 b 的伪素数.

a	a^{n-1}	a	a^{n-1}	a	a^{n-1}	a	a^{n-1}	a	a^{n-1}
1	1	14	7	27	36	40	25	53	37
2	4	15	36	28	28	41	43	54	18
3	9	16	4	29	22	42	0	55	1
4	16	17	37	30	18	43	22	56	49
5	25	18	9	31	16	44	46	57	36
6	36	19	46	32	16	45	9	58	25
7	49	20	22	33	18	46	37	59	16
8	1	21	0	34	22	47	4	60	9
9	18	22	43	35	28	48	36	61	4
10	37	23	25	36	36	49	7	62	1
11	58	24	9	37	46	50	43		
12	18	25	58	38	58	51	18		
13	43	26	46	39	9	52	58		

定理 6.1.1 (iv) 告知我们: 对于大奇数, 如果有一个整数 $b, (b, n) = 1$, 使得同余式 (6.1) 不成立, 则模 n 的简化剩余系中至少有一半的数使得同余式 (6.1) 不成立. 这就是说, 对于随机选取的整数 $b, (b, n) = 1$, 有 50% 以上的机会来判断出 n 是合数, 或者说 n 是合数的可能性小于 50%.

④ Fermat 素性检验

给定奇整数 $n > 3$ 和安全参数 t

1) 随机选整 $b, (b, n) = 1, 2 \leq b \leq n-2$

2) 算 $r = b^{n-1} \pmod{n}$

3) 若 $r \neq 1$, 则 n 合

4) 上述过程重复 t 次.

一次出错概率为 $\frac{1}{2}$

t 次为 $\frac{1}{2^t}$

2. 无穷多伪素数

讨论伪素数的存在性.

引: d, n 为正整, 若 $d | n$, 则 $2^{d-1} | 2^n - 1$ ★ 经常用到

$$2^n - 1 = (2^d)^q - 1 = (2^d)^{q-1} + (2^d)^{q-2} + \dots + 2^d + 1 \quad (2^d - 1)$$

$$\therefore 2^{d-1} | 2^n - 1$$



$$\frac{a_1(1-q^n)}{1-q} = \frac{2^{dq}-1}{2^d-1}$$

定理: 存在无穷多个对于基2的伪素数.

证明: 若 n 是对于基2的伪素数, 有 $2^{n-1} \equiv 1 \pmod{n}$

则 $m = 2^n - 1$ 也是基2的伪素数.

证①: m 也是奇数

$$n = q \cdot d$$

$$\text{由引1得, } 2^d - 1 \mid 2^n - 1$$

$$\therefore m = 2^n - 1 \text{ 也是奇数}$$

证②: $2^{m-1} \equiv 1 \pmod{m}$

$$m-1 = 2^n - 2 = 2(2^{n-1} - 1)$$

$$\therefore 2^{n-1} \equiv 1 \pmod{n}$$

$$\therefore 2^{n-1} = kn + 1$$

$$\therefore m-1 = kn$$

$$\therefore \text{有 } 2^n - 1 \mid 2^{m-1} - 1$$

$$\therefore 2^{m-1} \equiv 1 \pmod{m}$$

3. 平方因子的判别

设 n 是一个有平方因子的整数, 则有 $(b, n) = 1$, 使 $b^{n-1} \not\equiv 1 \pmod{n}$. 大于1的平方数, 例如9是18的平方因子

$$b^{n-1} \not\equiv 1 \pmod{n}$$

4. Carmichael 数

讨论费马素性检验算法无效的整数

① 合数 n 称为 Carmichael 数 对所有 $(b, n) = 1$ 者都有 $b^{n-1} \equiv 1 \pmod{n}$ 成立

例: 整数 $561 = 3 \cdot 11 \cdot 17$ 是一个 Carmichael 数

证明: 若 $(b, 561) = 1$, 则 $\begin{cases} (b, 3) = 1 \\ (b, 11) = 1 \\ (b, 17) = 1 \end{cases}$

$$\therefore \text{有 } b^2 \equiv 1 \pmod{3}, b^{10} \equiv 1 \pmod{11}, b^{16} \equiv 1 \pmod{17}$$

$$\therefore \begin{cases} b^{560} = (b^2)^{280} \equiv 1 \pmod{3} \\ b^{560} \equiv 1 \pmod{11} \\ b^{560} \equiv 1 \pmod{17} \end{cases}$$

$$\therefore \text{有 } b^{560} \equiv 1 \pmod{561}$$

② 设 n 是一个奇合数

1) 如果 n 被一个大于 1 的平方数整除, 则 n 不是 Carmichael 数

2) 如果 $n = p_1 \cdots p_k$ 是一个无平方数, 则

$$n \text{ 是 Carmichael 数} \iff p_i - 1 \mid n - 1, 1 \leq i \leq k$$

证明书 P23-24

③ 每个 Carmichael 数至少是 3 个不同素数的乘积 (推论)

$$\text{考 } n = pq$$

$$\text{由 1) 得 } p-1 \mid (n-1) = n-1 = (n-1) - p(q-1) \equiv 0 \pmod{q-1}$$

不可能

6.2 Euler 伪素数

1. Euler 伪素数, Solovay-Strassen 素性检验

① 设 n 是奇素数, 有 $b^{\frac{n-1}{2}} \equiv (\frac{b}{n}) \pmod{n}$ 对任意整 b 成立.

第四章, P132 勒让德符号

因此若存在 $(b, n) = 1$ 使 $b^{\frac{n-1}{2}} \not\equiv (\frac{b}{n}) \pmod{n}$, 则 n 不是一个素数

例: $n = 341, b = 2$.

$$2^{\frac{341-1}{2}} \equiv 1 \pmod{341}$$

$$(\frac{2}{341}) = (-1)^{\frac{341-1}{2}} = -1 \neq 1 \therefore 341 \text{ 不是一个素数}$$

② 设 n 是一个正奇合数, $(b, n) = 1$.

$$\text{若 } b^{\frac{n-1}{2}} \equiv (\frac{b}{n}) \pmod{n}$$

则 n 叫做对于基 b 的 Euler 伪素数

例: $n=105, b=2$.

$$2^{\frac{105-1}{2}} \equiv 1 \pmod{105}$$

$$\left(\frac{2}{105}\right) = (-1)^{\frac{105-1}{8}} = 1 \quad \therefore 105 \text{ 是一个对于基 } 2 \text{ 的 Euler 伪素数}$$

③ Solovay-Strassen 素性检验

(书 [205-206 有一个大例子])

给定奇整数 $n \geq 3$ 和安全参数 t .

1) 随机取 $b, 2 \leq b \leq n-2$

2) 算 $r = b^{\frac{n-1}{2}} \pmod{n}$

3) 若 $r \neq 1$ 及 $r \neq -1$, 则 n 是合数

4) 算 $s = \left(\frac{b}{n}\right)$

5) 如果 $r \neq s$, 则 n 是合数

6) 重复 n 次.

2. 无穷多 Euler 伪素数

如果 n 是对于基 b 的 Euler 伪素数, 则 n 是对于基 b 的伪素数.

伪素数 $\not\leftarrow$ Euler 伪素数

证明:

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$$

$$\text{其中 } \left(\frac{b}{n}\right) = \pm 1 \pmod{n}$$

$$b^{n-1} \equiv \left(b^{\frac{n-1}{2}}\right)^2 \equiv \left(\frac{b}{n}\right)^2 \equiv 1 \pmod{n}$$

6.3 强伪素数

1. 强伪素数, Miller-Rabin 素性检验

n 为奇素数, 有 $n-1 = 2^s t$

比较常见的化简思想

$$\text{则 } b^{n-1} - 1 = \underbrace{(b^{2^{s-1}t} + 1)(b^{2^{s-2}t} + 1) \cdots (b^t + 1)(b^t - 1)}$$

书 Boy 说明该检验比费马素性检验效果好.

① $n-1=2^s t$ - 若有 $b^t \equiv 1 \pmod{n}$

$n-1=2^s t$ ↑ 验证

或存在 $b^{2^s t} \equiv -1 \pmod{n}$ ($0 < r < s$)

则 n 叫做对于基 b 的强伪素数

例: $n=2047=23 \cdot 89$ 是基 $b=2$ 的强伪素数

$$2^{2046/2} \equiv (2^n)^{93} \equiv (2048)^{93} \equiv 1 \pmod{2047}$$

② Miller-Rabin 素性检验

Miller-Rabin 素性检验

给定奇整数 $n \geq 3$ 和安全参数 k .

写 $n-1=2^s t$, 其中 t 为奇整数.

!!! 要掌握算法实现

(1) 随机选取整数 b , $2 \leq b \leq n-2$.

(2) 计算 $r_0 \equiv b^t \pmod{n}$.

$$\begin{aligned} r_0 &= b^t \pmod{n} \begin{cases} 1 & \checkmark \\ 0 & \times \end{cases} \\ r_{i+1} &= r_i^2 \pmod{n} \begin{cases} 1 & \checkmark \\ \neq 1 & \times \end{cases} \end{aligned}$$

(3) ① 如果 $r_0 = 1$ 或 $r_0 = n-1$, 则通过检验, 可能为素数. 回到 (1). 继续选取另一个随机整数 b , $2 \leq b \leq n-2$;

② 否则, 有 $r_0 \neq 1$ 以及 $r_0 \neq n-1$, 计算 $r_1 \equiv r_0^2 \pmod{n}$.

(4) ① 如果 $r_1 = n-1$, 则通过检验, 可能为素数, 回到 (1). 继续选取另一个随机整数 b , $2 \leq b \leq n-2$.

② 否则, 有 $r_1 \neq n-1$, 计算 $r_2 \equiv r_1^2 \pmod{n}$.

如此继续下去,

(s+2) ① 如果 $r_{s-1} = n-1$, 则通过检验, 可能为素数, 回到 (1). 继续选取另一个随机整数 b , $2 \leq b \leq n-2$.

② 否则, 有 $r_{s-1} \neq n-1$, n 为合数.

一次检验出错概率为 $\frac{1}{4}$

2. 无穷多强伪素数

① 存在无穷多个对于基 2 的强伪素数

同无穷多个伪素数的证明.

n 是基 2 的素数, 则 $m=2^n-1$ 是对于基 2 的强伪素数.

② n 是基 b 强伪 $\rightarrow n$ 是基 b Euler 伪 $\rightarrow$ 伪

③ n 为奇合数, 则 n 是对于基 b ($1 \leq b \leq n-1$) 的强伪素数的可能性至多 $\frac{1}{2}$.