在本章, 研究如何产生以及如何快速产生大素数, 特别是利用对于素数成立的定理 (Fermat 小定理、欧拉定理等) 的否定说法来产生大素数.

素性检验

伪素数

其实就是利用定理的逆否成立，判断不是，然后用算法多次迭代判断求出一个伪素数

Fermat 素性检验

根据 Fermat 小定理可知: 如果 n 是一个素数, 则对任意整数 b, $(b,n)=1$, 有

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

由此可得: 如果有一个整数 b, $(b,n)=1$ 使得

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

则 n 是一个合数.

将指数的运算用于上述的讨论, 并结合定理 5.1.1, 有: 如果 n 是一个素数, 则对任意整数 b, $(b,n)=1$, 有

$$\mathrm{ord}_n(b)\mid n-1.$$

由此可得: 如果有一个整数 b, $(b,n)=1$ 使得

$$\mathrm{ord}_n(b)\not\mid n-1.$$

费马小定理

则 n 是一个合数.

伪素数定义

定义 6.1.1 设 n 是一个奇合数. 如果整数 b, $(b,n)=1$ 使得同余式

$$b^{n-1}\equiv 1 \pmod n \tag{6.1}$$

成立, 则 n 叫做对于基 b 的**伪素数**.

性质

定理 6.1.1 设是一个奇合数, 则

(i) n 是对于基 b 的伪素数当且仅当 b 模 n 的阶整除 $n-1$.

(ii) 如果 n 是对于基 b_1 和基 b_2 的伪素数, 则 n 是对于基 $b_1\cdot b_2$ 的伪素数.

(iii) 如果 n 是对于基 b 的伪素数, 则 n 是对于基 b^{-1} 的伪素数.

(iv) 如果有一个整数 b 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.

无穷多伪素数

引理

引理 6.1.1 设 d, n 都是正整数. 如果 d 能整除 n, 则 2^d-1 能整除 2^n-1.

定理

定理 6.1.2 存在无穷多个对于基 2 的伪素数.

平方因子判断

定理 6.1.3 设 n 是一个有平方因子的整数, 则存在整数 b, $(b,n)=1$ 使得同余式 (6.1) 不成立, 即

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

Carmichael 数

定义 6.1.2 合数 n 称为 **Carmichael 数**, 如果对所有的正整数 b, $(b,n)=1$, 都有同余式

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

成立.

注 **Carmichael 数** n 也可解释为这样一个正合数 n, 它使得对所有的正整数 b, $(b,n)=1$, $n-1$ 都是序列 $u=\{u_k=b^k \mod n \mid k\geqslant 1\}$ 的周期.

判断

定理 6.1.4 设 n 是一个奇合数.

(i) **如果** n **被一个大于 1 平方数整除**, 则 n 不是 Carmichael 数.

(ii) **如果** $n=p_1\cdots p_k$ **是一个无平方数**, 则 n 是 Carmichael 数的充要条件是

$$p_i-1\mid n-1,\quad 1\leqslant i\leqslant k.$$

性质

定理 6.1.5 每个 Carmichael 数是至少三个不同素数的乘积.

注 (1) 存在无穷多个 Carmichael 数.

(2) 当 n 充分大时, 区间 $[2,n]$ 内的 Carmichael 数的个数 $\geqslant n^{2/7}$

Euler 伪素数

设 n 是奇素数. 根据定理 4.3.1, 有同余式

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

对任意整数 b 成立.

因此, 如果存在整数 b, $(b,n)=1$, 使得

$$b^{\frac{n-1}{2}}\not\equiv\left(\frac{b}{n}\right) \pmod n,$$

则 n 不是一个素数.

欧拉判别

定义 6.2.1 设 n 是一个正奇合数. 设整数 b 与 n 互素. 如果整数 n 和 b 满足条件

$$b^{\frac{n-1}{2}}\equiv\left(\frac{b}{n}\right) \pmod n, \tag{6.2}$$

定义

则 n 叫做对于基 b 的 **Euler 伪素数**.

Solovay-Stassen 素性检验

Solovay-Stassen 素性检验

给定奇整数 $n\geqslant 3$ 和安全参数 t.

(1) 随机选取整数 b, $2\leqslant b\leqslant n-2$.

(2) 计算 $r=b^{\frac{n-1}{2}} \pmod n$.

(3) 如果 $r\neq 1$ 以及 $r\neq n-1$, 则 n 是合数.

(4) 计算 Jacobi 符号 $s=\left(\frac{b}{n}\right)$.

(5) 如果 $r\neq s$, 则 n 是合数.

(6) 上述过程重复 t 次.

无穷多

定理 6.2.1 如果 n 是对于基 b 的 Euler 伪素数, 则 n 是对于基 b 的伪素数.

设 n 是奇素数, 并且有 $n-1=2^st$, 则有以下因数分解式:

$$b^{n-1}-1=\left(b^{2^{s-1}t}+1\right)\left(b^{2^{s-2}t}+1\right)\cdots\left(b^t+1\right)\left(b^t-1\right).$$

因此, 如果有同余式

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

则以下同余式至少有一个成立:

$$\begin{aligned} b^t &\equiv 1 \pmod n,\\ b^t &\equiv -1 \pmod n,\\ b^{2t} &\equiv -1 \pmod n,\\ &\vdots\\ b^{2^{s-1}t} &\equiv -1 \pmod n. \end{aligned}$$

由此得到: 如果有一个整数 b 使得

$$\begin{cases} b^t &\not\equiv 1 \pmod n,\\ b^t &\not\equiv -1 \pmod n,\\ b^{2t} &\not\equiv -1 \pmod n,\\ &\vdots\\ b^{2^{s-1}t} &\not\equiv -1 \pmod n, \end{cases}$$

则 n 是合数.

在计算 $b^{n-1} \pmod n$ 时, 通常要运用模重复平方法, 这时, 计算次序为

$$b^t \pmod n\to b^{2t} \pmod n\to(b^t)^2 \pmod n\to\cdots\to(b^t)^{2^{s-1}} \pmod n.$$

强伪素数

这意味着以下的素性检验方法比费马素性检验的效果要好一些.

验证定理

定义 6.3.1 设 n 是一个奇合数, 且有表示式 $n-1=2^st$, 其中 t 为奇数. 设整数 b 与 n 互素. 如果整数 n 和 b 满足条件

$$b^t\equiv 1 \pmod n,$$

或者存在一个整数 r, $0\leqslant r<s$ 使得

$$b^{2^rt}\equiv -1 \pmod n,$$

定义

则 n 叫做对于基 b 的 **强伪素数**.

Miller-Rabin 素性检验

Miller-Rabin 素性检验

给定奇整数 $n\geqslant 3$ 和安全参数 k.

写 $n-1=2^st$, 其中 t 为奇整数.

(1) 随机选取整数 b, $2\leqslant b\leqslant n-2$.

(2) 计算 $r_0\equiv b^t \pmod n$.

(3) ⓐ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, $2\leqslant b\leqslant n-2$;

ⓑ 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) ⓐ 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, $2\leqslant b\leqslant n-2$.

ⓑ 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) ⓐ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, $2\leqslant b\leqslant n-2$.

ⓑ 否则, 有 $r_{s-1}\neq n-1$, n 为合数.

无穷多

定理 6.3.1 存在无穷多个对于基 2 的强伪素数.

定理 6.3.2 如果 n 是对于基 b 的强伪素数, 则 n 就是对于基 b 的 Euler 伪素数.

定理 6.3.3 设是一个奇合数, 则 n 是对于基 b $(1\leqslant b\leqslant n-1)$ 的强伪素数的可能性至多为 25%.