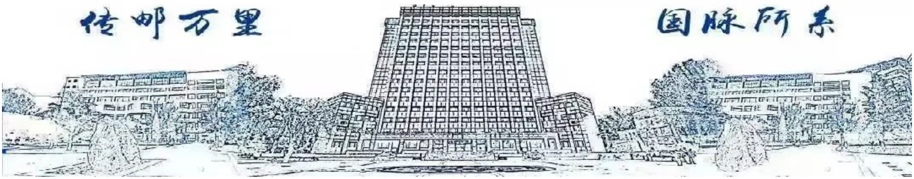
网络空间安全学院
School of Cyberspace Security, BUPT

信息安全数学基础

—— 素性检测

信数课题组

北京邮电大学



上次课回顾

阶

最小正整数 e，使得 $a^e \equiv 1 \mod m$

$\mathrm{ord}_m(a) = \varphi(m)$

基本性质

$a^d \equiv 1 \mod m \iff \mathrm{ord}_m(a) \mid d$

若 $b \equiv a \mod m$, 则 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

$\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$

$\mathrm{ord}_m(a) = \varphi(m)$ 时, $1 = a^0, a, \cdots, a^{\varphi(m)-1}$ 组成模 m 的简化剩余系.

$a^d = a^k \mod m \iff d \equiv k \mod \mathrm{ord}_m(a)$

$\mathrm{ord}_m(a^d) = \dfrac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))}$

模 m 有 $\varphi(\varphi(m))$ 个不同的原根.

模 m 原根的概率是 $\frac{\varphi(\varphi(m))}{\varphi(m)} = \prod_{i=1}^{s}(1-\frac{1}{p_i})$.

$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1, \iff \mathrm{ord}_m(a \cdot b) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$

若 $n \mid m$, 则 $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

若 $(m,n) = 1$, 则 $\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)]$.

$ord_{pq}(a) = [ord_p(a), ord_q(a)]$

$m = 2^n \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 时 $\mathrm{ord}_m(a) = [\mathrm{ord}_{2^n}(a), \mathrm{ord}_{p_1^{\alpha_1}}(a), \cdots, \mathrm{ord}_{p_k^{\alpha_k}}(a)]$.

$(m,n) = 1$ 对与 mn 互素的 a_1, a_2, 存在整数 a 使得 $\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)]$.

对与 m 互素的任意整数 a, b, 存在整数 c 使得 $\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$.

原根

存在性

模 p

模 p^α

g 或者 $g+p$ 是模 p^2 原根 $\Rightarrow$ 是模 p^α 的原根.

g 是模 p^α 原根, 则 g 与 $g+p^\alpha$ 中的奇数是模 $2p^\alpha$ 的原根.

模 2^α

$\alpha \geqslant 3$,

$a^{\frac{\varphi(2^\alpha)}{2}} \equiv a^{2^{\alpha-2}} \equiv 1 \mod 2^\alpha$

$\mathrm{ord}_{2^\alpha}(5) = \dfrac{\varphi(2^\alpha)}{2} = 2^{\alpha-2}$

模 m 的原根存在 $\iff m = 2, 4, p^\alpha, 2p^\alpha$

构造

$g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \mod m, \quad i = 1, \cdots, k.$

指标

n 次剩余

$x^n \equiv a \mod m$ 有解 $\iff (n, \varphi(m)) \mid \mathrm{ind}_g a$

目录

如何“快速”产生“大”素数？

如何“快速”产生“大”素数？

$\Downarrow$

Eratoshenes 筛法 ✘

如何“快速”产生“大”素数？

$\Downarrow$

Eratoshenes 筛法 ✗

$\Downarrow$

利用对于素数成立的定理 (如 Fermat 小定理、欧拉定理等) 的**逆否命题**进行“**素性检测**”.

如何“快速”产生“大”素数?

$\Downarrow$

Eratoshenes 筛法 ✘

$\Downarrow$

利用对于素数成立的定理 (如 Fermat 小定理、欧拉定理等) 的**逆否命题**

进行“**素性检测**”.

如果不满足 ** 定理的结论, 则一定不是素数; 否则, 如果满足 ** 定理的结论, 就称其通过对应的素性检测, 但其有可能是素数, 也有可能不是素数. 称通过某个素性检测但不是素数的整数为 ** **伪素数**.

根据 Fermat 小定理:

如果 n 是一个素数, 则对任意整数 b, $(b,n)=1$, 有 $b^{n-1}\equiv 1 \mod n$.

由此, 我们得到:

如果有一个整数 b, $(b,n)=1$ 使得 $b^{n-1}\not\equiv 1 \mod n$, 则 n 是合数.

根据 Fermat 小定理:

如果 n 是一个素数, 则对任意整数 b, $(b,n)=1$, 有 $b^{n-1}\equiv 1 \mod n$.

由此, 我们得到:

如果有一个整数 b, $(b,n)=1$ 使得 $b^{n-1}\not\equiv 1 \mod n$, 则 n 是合数.

例 5.1.1 因为 $2^{14}\equiv(2^4)^3\cdot 2^2\equiv 1^3\cdot 2^2\equiv 4\not\equiv 1 \mod 15$,

所以 15 是一个合数.

根据 Fermat 小定理:

如果 n 是一个素数, 则对任意整数 b, $(b,n)=1$, 有 $b^{n-1}\equiv 1 \mod n$.

由此, 我们得到:

如果有一个整数 b, $(b,n)=1$ 使得 $b^{n-1}\not\equiv 1 \mod n$, 则 n 是合数.

例 5.1.1 因为 $2^{14}\equiv (2^4)^3\cdot 2^2\equiv 1^3\cdot 2^2\equiv 4\not\equiv 1 \mod 15$,

所以 15 是一个合数.

注：上述说法的否命题不能成立. 事实上, 我们有

例 5.1.2 $4^{14}\equiv (4^2)^7\equiv 1 \mod 15$.

目录

定义 5.1.1

设 n 是一个奇合数. 如果整数 b, $(b,n)=1$ 使得同余方程

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

成立, 则 n 叫做对于基 b 的**伪素数**.

定义 5.1.1

设 n 是一个奇合数. 如果整数 b, $(b,n)=1$ 使得同余方程

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

成立, 则 n 叫做对于基 b 的**伪素数**.

例 5.1.3 整数 15 是对于基 $b=4$ 的伪素数.

定义 5.1.1

设 n 是一个奇合数. 如果整数 b, $(b,n)=1$ 使得同余方程

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

成立, 则 n 叫做对于基 b 的**伪素数**.

例 5.1.3 整数 15 是对于基 $b=4$ 的伪素数.

例 5.1.4 整数 $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, $645 = 3 \cdot 5 \cdot 43$ 都是对于基 $b=2$ 的伪素数, 因为

$$2^{340} \equiv 1 \mod 341,\ 2^{560} \equiv 1 \mod 561,\ 2^{644} \equiv 1 \mod 645.$$

定义 5.1.1

设 n 是一个奇合数. 如果整数 b, $(b,n)=1$ 使得同余方程

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

成立, 则 n 叫做对于基 b 的**伪素数**.

例 5.1.3 整数 15 是对于基 $b=4$ 的伪素数.

例 5.1.4 整数 $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, $645 = 3 \cdot 5 \cdot 43$ 都是对于基 $b=2$ 的伪素数, 因为

$$2^{340} \equiv 1 \mod 341,\ 2^{560} \equiv 1 \mod 561,\ 2^{644} \equiv 1 \mod 645.$$

引理 5.1.1

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

定义 5.1.1

设 n 是一个奇合数. 如果整数 b, $(b,n)=1$ 使得同余方程

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

成立, 则 n 叫做对于基 b 的**伪素数**.

例 5.1.3 整数 15 是对于基 $b=4$ 的伪素数.

例 5.1.4 整数 $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, $645 = 3 \cdot 5 \cdot 43$ 都是对于基 $b=2$ 的伪素数, 因为

$$2^{340} \equiv 1 \mod 341, \ 2^{560} \equiv 1 \mod 561, \ 2^{644} \equiv 1 \mod 645.$$

引理 5.1.1

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

证：因为 $d \mid n$, 所以存在一个整数 q 使得 $n = q \cdot d$. 因此, 我们有

$$2^n - 1 = (2^d)^q - 1 = (2^d - 1)((2^d)^{q-1} + (2^d)^{q-2} + \cdots + 2^d + 1).$$

故 $2^d - 1 \mid 2^n - 1$.

定理 5.1.1

存在无穷多个对于基 2 的伪素数.

定理 5.1.1

存在无穷多个对于基 2 的伪素数.

证： (i) 如果 n 是对于基 2 的伪素数, 则 $m = 2^n - 1$ 也是对于基 2 的伪素数.

定理 5.1.1

存在无穷多个对于基 2 的伪素数.

证： (i) 如果 n 是对于基 2 的伪素数, 则
$m = 2^n - 1$ 也是对于基 2 的伪素数.
事实上, 因为 n 是对于基 2 的伪素数, 所以 n 是奇合数, 并且

$$2^{n-1} \equiv 1 \mod n.$$

因为 n 是奇合数, 所以有因数分解式 $n = q \cdot d, 1 < q < n, 1 < d < n$,
根据引理 5.1.1, 我们得到 $2^d - 1 \mid 2^n - 1$, 因此 $2^n - 1$ 是合数.
现在验证：$2^{m-1} \equiv 1 \mod m$.
因为 $2^{n-1} \equiv 1 \mod n$, 所以我们可以将 $m - 1 = 2(2^{n-1} - 1)$ 写成

$$m - 1 = k \cdot n.$$

根据引理 5.1.1, 我们得到 $2^n - 1 \mid 2^{m-1} - 1$, 即 $m \mid 2^{m-1} - 1$.
因此, 同余方程 $2^{m-1} \equiv 1 \mod m$ 成立.
故 $m = 2^n - 1$ 是对于基 2 的伪素数.

(ii) 取 n_0 为对于基 2 的一个伪素数, 例如 $n_0 = 341$. 再令

$$n_i = 2^{n_{i-1}} - 1,\ i = 1, 2, \cdots,$$

根据结论 (i) 这些整数都是对于基 2 的伪素数.

(ii) 取 n_0 为对于基 2 的一个伪素数, 例如 $n_0 = 341$. 再令

$$n_i = 2^{n_{i-1}} - 1,\ i = 1, 2, \cdots ,$$

根据结论 (i) 这些整数都是对于基 2 的伪素数.

定理 5.1.2

设 n 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) 若 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) 若 n 是对于基 b 的伪素数, 则 n 是对于基 b^{-1} 的伪素数.

(iv) 若有一个整数 b 使得同余方程 $b^{n-1} \equiv 1 \mod n$ 不成立, 则模 n 的简化剩余系中至少有一半的数使得同余方程 $b^{n-1} \equiv 1 \mod n$ 不成立.

(ii) 取 n_0 为对于基 2 的一个伪素数, 例如 $n_0 = 341$. 再令

$$n_i = 2^{n_{i-1}} - 1,\ i = 1, 2, \cdots,$$

根据结论 (i) 这些整数都是对于基 2 的伪素数.

定理 5.1.2

设 n 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) 若 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) 若 n 是对于基 b 的伪素数, 则 n 是对于基 b^{-1} 的伪素数.

(iv) 若有一个整数 b 使得同余方程 $b^{n-1} \equiv 1 \mod n$ 不成立, 则模 n 的简化剩余系中至少有一半的数使得同余方程 $b^{n-1} \equiv 1 \mod n$ 不成立.

证：(i) 如果 n 是对于基 b 的伪素数, 则我们有 $b^{n-1} \equiv 1 \mod n$.

根据定理 4.1.1, 我们有 $\mathrm{ord}_n(b) \mid n-1$.

反过来, 如果 $\mathrm{ord}_n(b) \mid n-1$, 则存在整数 q 使得 $n-1 = q \cdot \mathrm{ord}_n(b)$. 因此, 有

$$b^{n-1} \equiv (b^{\mathrm{ord}_n(b)})^q \equiv 1 \mod n.$$

反过来, 如果 $\mathrm{ord}_n(b) \mid n-1$, 则存在整数 q 使得 $n-1 = q \cdot \mathrm{ord}_n(b)$. 因此, 有

$$b^{n-1} \equiv (b^{\mathrm{ord}_n(b)})^q \equiv 1 \mod n.$$

(ii) 因为 n 是对于基 b_1 和基 b_2 的伪素数, 所以我们有

$$b_1^{n-1} \equiv 1 \mod n, \ b_2^{n-1} \equiv 1 \mod n.$$

从而, $(b_1 \cdot b_2)^{n-1} \equiv b_1^{n-1} \cdot b_2^{n-1} \equiv 1 \mod n$.

故 n 是对于基 $b_1 \cdot b_2$ 的伪素数.

反过来, 如果 $\mathrm{ord}_n(b) \mid n-1$, 则存在整数 q 使得 $n-1 = q \cdot \mathrm{ord}_n(b)$. 因此, 有

$$b^{n-1} \equiv (b^{\mathrm{ord}_n(b)})^q \equiv 1 \mod n.$$

(ii) 因为 n 是对于基 b_1 和基 b_2 的伪素数, 所以我们有

$$b_1^{n-1} \equiv 1 \mod n, \ b_2^{n-1} \equiv 1 \mod n.$$

从而, $(b_1 \cdot b_2)^{n-1} \equiv b_1^{n-1} \cdot b_2^{n-1} \equiv 1 \mod n$.

故 n 是对于基 $b_1 \cdot b_2$ 的伪素数.

(iii) 因为 n 是对于基 b 的伪素数, 所以我们有 $b^{n-1} \equiv 1 \mod n$.

从而, $(b^{-1})^{n-1} \equiv (b^{n-1})^{-1} \equiv 1 \mod n$.

故 n 是对于基 b^{-1} 的伪素数.

反过来, 如果 $\mathrm{ord}_n(b) \mid n-1$, 则存在整数 q 使得 $n-1 = q \cdot \mathrm{ord}_n(b)$. 因此, 有

$$b^{n-1} \equiv (b^{\mathrm{ord}_n(b)})^q \equiv 1 \mod n.$$

(ii) 因为 n 是对于基 b_1 和基 b_2 的伪素数, 所以我们有

$$b_1^{n-1} \equiv 1 \mod n, \; b_2^{n-1} \equiv 1 \mod n.$$

从而, $(b_1 \cdot b_2)^{n-1} \equiv b_1^{n-1} \cdot b_2^{n-1} \equiv 1 \mod n$.
故 n 是对于基 $b_1 \cdot b_2$ 的伪素数.

(iii) 因为 n 是对于基 b 的伪素数, 所以我们有 $b^{n-1} \equiv 1 \mod n$.
从而, $(b^{-1})^{n-1} \equiv (b^{n-1})^{-1} \equiv 1 \mod n$.
故 n 是对于基 b^{-1} 的伪素数.

(iv) 设 $b_1, \cdots, b_s, b_{s+1}, \cdots, b_{\varphi(n)}$ 是模 n 的简化剩余系, 其中前 s 个数使得同余方程 $b^{n-1} \equiv 1 \mod n$ 成立, 后 $\varphi(n) - s$ 个数使得同余方程 $b^{n-1} \equiv 1 \mod n$ 不成立.

根据假设条件, 存在一个整数 b, $(b,n)=1$, 使得同余方程

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

不成立, 再根据结论 (ii) 和 (iii), 我们有 s 个模 n 的简化剩余 $b\cdot b_1, \cdots, b\cdot b_s$ 使得同余方程 $b^{n-1}\equiv 1 \mod n$ 不成立.

根据假设条件, 存在一个整数 b, $(b,n)=1$, 使得同余方程

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

不成立, 再根据结论 (ii) 和 (iii), 我们有 s 个模 n 的简化剩余 $b \cdot b_1, \cdots, b \cdot b_s$ 使得同余方程 $b^{n-1} \equiv 1 \mod n$ 不成立.

因此, $s \leqslant \varphi(n) - s$, 即 $\varphi(n) - s \geqslant \frac{\varphi(n)}{2}$.

这就是说, 模 n 的简化剩余系中至少有一半的数使得同余方程

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

不成立.

根据假设条件, 存在一个整数 b, $(b,n)=1$, 使得同余方程

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

不成立, 再根据结论 (ii) 和 (iii), 我们有 s 个模 n 的简化剩余 $b \cdot b_1, \cdots,$ $b \cdot b_s$ 使得同余方程 $b^{n-1} \equiv 1 \mod n$ 不成立.

因此, $s \leqslant \varphi(n) - s$, 即 $\varphi(n) - s \geqslant \frac{\varphi(n)}{2}$.

这就是说, 模 n 的简化剩余系中至少有一半的数使得同余方程

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

不成立.

注: 定理 5.1.2 (iv) 告诉我们, 对于大奇数 n, 随机选取整数 b, $(b,n)=1$, 有 50% 以上的机会能判断出 n 是合数.

或者说, 满足同余方程 $b^{n-1} \equiv 1 \mod n$ 的 n 是合数的可能性小于 50%.

目录

现在, 我们给出判断一个大奇整数 n 为素数的方法.

随机选取整数 $b_1, 0 < b_1 < n$, 利用广义欧几里德除法计算 b_1 和 n 的最大公因数 $d_1 = (b_1, n)$. 如果 $d_1 > 1$, 则 n 不是素数. 如果 $d_1 = 1$, 则计算 $b_1^{n-1} \mod n$, 看看同余方程 $b_1^{n-1} \equiv 1 \mod n$ 是否成立.

如果 $b_1^{n-1} \equiv 1 \mod n$ 不成立, 则 n 不是素数; 如果 $b_1^{n-1} \equiv 1 \mod n$ 成立, 则 n 是合数的可能性小于 $1/2$, 或者说 n 是素数的可能性大于 $1-(1/2)$.

现在, 我们给出判断一个大奇整数 n 为素数的方法.

随机选取整数 $b_1, 0 < b_1 < n$, 利用广义欧几里德除法计算 b_1 和 n 的最大公因数 $d_1 = (b_1, n)$. 如果 $d_1 > 1$, 则 n 不是素数. 如果 $d_1 = 1$, 则计算 $b_1^{n-1} \mod n$, 看看同余方程 $b_1^{n-1} \equiv 1 \mod n$ 是否成立.

如果 $b_1^{n-1} \equiv 1 \mod n$ 不成立, 则 n 不是素数; 如果 $b_1^{n-1} \equiv 1 \mod n$ 成立, 则 n 是合数的可能性小于 $1/2$, 或者说 n 是素数的可能性大于 $1-(1/2)$.

重复上面的步骤.

再随机选取整数 $b_2, 0 < b_2 < n$, 利用广义欧几里德除法计算 b_2 和 n 的最大公因数 $d_2 = (b_2, n)$. 如果 $d_2 > 1$, 则 n 不是素数. 如果 $d_2 = 1$, 则计算 $b_2^{n-1} \mod n$, 看看同余方程 $b_2^{n-1} \equiv 1 \mod n$ 是否成立.

如果不成立, 则 n 不是素数; 如果成立, 则 n 是合数的可能性小于 $1/2^2$, 或者说 n 是素数的可能性大于 $1-(1/2^2)$.

继续重复上述步骤, $\cdots\cdots$, 直至第 t 步.

随机选取整数 $b_t, 0 < b_t < n$, 利用广义欧几里德除法计算 b_t 和 n 的最大公因数 $d_t = (b_t, n)$. 如果 $d_t > 1$, 则 n 不是素数. 如果 $d_t = 1$, 则计算 $b_t^{n-1} \mod n$, 看看同余方程 $b_t^{n-1} \equiv 1 \mod n$ 是否成立.

如果不成立, 则 n 不是素数；如果成立, 则 n 是合数的可能性小于 $1/2^t$, 或者说 n 是素数的可能性大于 $1-(1/2^t)$.

继续重复上述步骤, $\cdots\cdots$, 直至第 t 步.

随机选取整数 $b_t, 0 < b_t < n$, 利用广义欧几里德除法计算 b_t 和 n 的最大公因数 $d_t = (b_t, n)$. 如果 $d_t > 1$, 则 n 不是素数. 如果 $d_t = 1$, 则计算 $b_t^{n-1} \mod n$, 看看同余方程 $b_t^{n-1} \equiv 1 \mod n$ 是否成立.

如果不成立, 则 n 不是素数；如果成立, 则 n 是合数的可能性小于 $1/2^t$, 或者说 n 是素数的可能性大于 $1-(1/2^t)$.

上述过程也可以简单归纳为：

素性检测 1 (Fermat 素性检测)

给定奇整数 $n \geqslant 3$ 和安全参数 t.

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

(2) 计算 $r = b^{n-1} \mod n$.

(3) 如果 $r \neq 1$, 则 n 是合数.

(4) 上述过程重复 t 次.

目录

对于 Fermat 素性检测算法无效的整数？

对于 Fermat 素性检测算法无效的整数？

定义 5.1.2

设 n 为合数，如果对所有的正整数 b，$(b,n)=1$，都有同余方程 $b^{n-1}\equiv 1 \mod n$ 成立，则称 n 为 Carmichael 数.

对于 Fermat 素性检测算法无效的整数？

定义 5.1.2

设 n 为合数，如果对所有的正整数 b, $(b,n)=1$, 都有同余方程 $b^{n-1} \equiv 1 \mod n$ 成立，则称 n 为 Carmichael **数**.

例 5.1.5 整数 $561 = 3 \cdot 11 \cdot 17$ 是一个 Carmichael 数.

对于 Fermat 素性检测算法无效的整数？

定义 5.1.2

设 n 为合数, 如果对所有的正整数 b, $(b,n)=1$, 都有同余方程 $b^{n-1}\equiv 1 \mod n$ 成立, 则称 n 为 Carmichael **数**.

例 5.1.5　整数 $561=3\cdot 11\cdot 17$ 是一个 Carmichael 数.

证：如果 $(b,561)=1$, 则 $(b,3)=(b,11)=(b,17)=1$.

根据 Fermat 小定理, 我们有

$$b^2\equiv 1 \mod 3,\ b^{10}\equiv 1 \mod 11,\ b^{16}\equiv 1 \mod 17.$$

从而, 我们有

$$\begin{cases} b^{560}\equiv (b^2)^{280}\equiv 1 \mod 3,\\ b^{560}\equiv (b^{10})^{56}\equiv 1 \mod 11,\\ b^{560}\equiv (b^{16})^{35}\equiv 1 \mod 17.\end{cases}$$

因此, 有 $b^{560}\equiv 1 \mod 561$.

定理 5.1.3

设 n 是一个奇合数.

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

(ii) 如果 $n = p_1 \cdots p_k$ 是一个无平方因数的整数，则 n 是 Carmichael 数的充要条件是 $p_i - 1 \mid n - 1$, $1 \leqslant i \leqslant k$.

定理 5.1.3

设 n 是一个奇合数.

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

(ii) 如果 $n = p_1 \cdots p_k$ 是一个无平方因数的整数，则 n 是 Carmichael 数的充要条件是 $p_i - 1 \mid n - 1,\ 1 \leqslant i \leqslant k$.

定理 5.1.4

每个 Carmichael 数是至少三个不同素数的乘积.

定理 5.1.3

设 n 是一个奇合数.

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

(ii) 如果 $n = p_1 \cdots p_k$ 是一个无平方因数的整数, 则 n 是 Carmichael 数的充要条件是 $p_i - 1 \mid n - 1,\ 1 \leqslant i \leqslant k$.

定理 5.1.4

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 $\geqslant n^{\frac{2}{7}}$.

设 n 是奇素数, 根据欧拉判别法则 (定理 3.3.3), 我们有同余方程

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

对任意整数 b 成立. 因此, 如果存在整数 b, $\gcd(b, n) = 1$, 使得

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

则 n 不是一个素数.

设 n 是奇素数, 根据欧拉判别法则 (定理 3.3.3), 我们有同余方程

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

对任意整数 b 成立. 因此, 如果存在整数 b, $\gcd(b,n)=1$, 使得

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

则 n 不是一个素数.

例 5.2.1　设 $n=341$, $b=2$. 我们分别计算得到

$$2^{\frac{341-1}{2}} \equiv 1 \mod 341 \text{ 以及 } \left(\frac{2}{341}\right) = (-1)^{\frac{341^2-1}{8}} = -1.$$

因为 $2^{\frac{341-1}{2}} \not\equiv \left(\frac{2}{341}\right) \mod 341$, 所以 341 不是一个素数.

目录

定义 5.2.1

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

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

则 n 叫做对于基 b 的 Euler **伪素数**.

定义 5.2.1

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

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

则 n 叫做对于基 b 的 Euler **伪素数**.

例 5.2.2　设 $n = 561$, $b = 2$, 则 561 是一个对于基 2 的 Euler 伪素数.

解：我们分别计算得到

$$2^{\frac{561-1}{2}} \equiv 1 \mod 561 \text{ 以及 } \left(\frac{2}{561}\right) = (-1)^{\frac{561^2-1}{8}} = 1.$$

则 $2^{\frac{561-1}{2}} \equiv \left(\frac{2}{561}\right) \mod 561$, 所以 561 是对于基 2 的 Euler 伪素数.

定理 5.2.1

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

定理 5.2.1

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

证：设 n 是对于基 b 的 Euler 伪素数，则我们有

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

上式两端平方，并注意到 $\left(\frac{b}{n}\right) = \pm 1 \mod n$，我们有

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

因此，n 是对于基 b 的伪素数.

定理 5.2.1

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

证：设 n 是对于基 b 的 Euler 伪素数, 则我们有

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

上式两端平方, 并注意到 $\left(\frac{b}{n}\right) = \pm 1 \mod n$, 我们有

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

因此, n 是对于基 b 的伪素数.

注：定理 5.2.1 的逆命题不成立, 即不是每个伪素数都是 Euler 伪素数.

定理 5.2.1

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

证：设 n 是对于基 b 的 Euler 伪素数，则我们有

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

上式两端平方，并注意到 $\left(\frac{b}{n}\right) = \pm 1 \mod n$，我们有

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

因此，n 是对于基 b 的伪素数.

注：定理 5.2.1 的逆命题不成立，即不是每个伪素数都是 Euler 伪素数.

例 5.2.3　341 是对于基 2 的伪素数，但不是对于基 2 的 Euler 伪素数.

目录

现在，给出判断大奇整数 n 为素数的 Solovay-Stassen (S-S) 素性检测方法.

素性检测 2 （S-S 素性检测）

给定奇整数 $n \geqslant 3$ 和安全参数 t.

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

(2) 计算 $r = b^{\frac{n-1}{2}} \mod n$.

(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.

现在, 给出判断大奇整数 n 为素数的 Solovay-Stassen (S-S) 素性检测方法.

素性检测 2 （S-S 素性检测）

给定奇整数 $n \geqslant 3$ 和安全参数 t.

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

(2) 计算 $r = b^{\frac{n-1}{2}} \mod n$.

(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.

注：通过 S-S 素性检测的整数 n, 其是合数的可能性小于 $\frac{1}{2^t}$, 或者说, 其是素数的可能性大于 $1-\frac{1}{2^t}$.

目录

设 n 是奇素数, 并且有 $n-1=2^s t$, 则我们有如下因数分解式:

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

因此, 如果有同余方程 $b^{n-1}\equiv 1 \mod n$,

则以下同余方程至少有一个成立:

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

定义 5.3.1

设 n 是一个奇合数, 且有表达式 $n-1=2^s t$, 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

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

或者存在一个整数 r, $0 \leqslant r < s$ 使得

$$b^{2^r t} \equiv -1 \mod n,$$

则 n 叫做对于基 b 的**强伪素数**.

定义 5.3.1

设 n 是一个奇合数，且有表达式 $n-1=2^s t$，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

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

或者存在一个整数 r, $0 \leqslant r < s$ 使得

$$b^{2^r t} \equiv -1 \mod n,$$

则 n 叫做对于基 b 的**强伪素数**.

例 5.3.1 整数 $n = 2047 = 23 \cdot 89$ 是对于基 $b=2$ 的强伪素数.

定义 5.3.1

设 n 是一个奇合数，且有表达式 $n-1=2^s t$，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

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

或者存在一个整数 r，$0 \leqslant r < s$ 使得

$$b^{2^r t} \equiv -1 \mod n,$$

则 n 叫做对于基 b 的**强伪素数**.

例 5.3.1 整数 $n=2047=23 \cdot 89$ 是对于基 $b=2$ 的强伪素数.

解: 因为 $2^{2046/2} \equiv (2^{11})^{93} \equiv (2048)^{93} \equiv 1 \mod 2047$,

所以整数 2047 是对于基 $b=2$ 的强伪素数.

定理 5.3.1

存在无穷多个对于基 2 的强伪素数.

定理 5.3.1

存在无穷多个对于基 2 的强伪素数.

证：如果 n 是对于基 2 的伪素数, 则 $m = 2^n - 1$ 是对于基 2 的强伪素数.

定理 5.3.1

存在无穷多个对于基 2 的强伪素数.

证：如果 n 是对于基 2 的伪素数, 则 $m = 2^n - 1$ 是对于基 2 的强伪素数.

事实上, 因为 n 是对于基 2 的伪素数, 所以 n 是奇合数, 并且 $2^{n-1} \equiv 1 \mod n$. 由此得到, $2^{n-1} - 1 = nk$, 其中 k 是整数. 进一步, k 是奇数. 我们有 $m - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2^1 nk$, 这是 $m - 1$ 分解成 2 的方幂和奇数乘积的表达式.

定理 5.3.1

存在无穷多个对于基 2 的强伪素数.

证：如果 n 是对于基 2 的伪素数, 则 $m = 2^n - 1$ 是对于基 2 的强伪素数.

事实上, 因为 n 是对于基 2 的伪素数, 所以 n 是奇合数, 并且 $2^{n-1} \equiv 1 \mod n$. 由此得到, $2^{n-1} - 1 = nk$, 其中 k 是整数. 进一步, k 是奇数. 我们有 $m - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2^1 nk$, 这是 $m - 1$ 分解成 2 的方幂和奇数乘积的表达式.

注意到 $2^n = (2^n - 1) + 1 = m + 1 \equiv 1 \mod m$, 我们有

$$2^{(m-1)/2} \equiv 2^{nk} \equiv (2^n)^k \equiv 1 \mod m.$$

此外, 我们知道, n 是合数时, m 也是合数. 故 $m = 2^n - 1$ 是对于基 2 的强伪素数.

定理 5.3.1

存在无穷多个对于基 2 的强伪素数.

证：如果 n 是对于基 2 的伪素数, 则 $m = 2^n - 1$ 是对于基 2 的强伪素数.

事实上, 因为 n 是对于基 2 的伪素数, 所以 n 是奇合数, 并且 $2^{n-1} \equiv 1 \mod n$. 由此得到, $2^{n-1} - 1 = nk$, 其中 k 是整数. 进一步, k 是奇数. 我们有 $m - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2^1 nk$, 这是 $m - 1$ 分解成 2 的方幂和奇数乘积的表达式.

注意到 $2^n = (2^n - 1) + 1 = m + 1 \equiv 1 \mod m$, 我们有

$$2^{(m-1)/2} \equiv 2^{nk} \equiv (2^n)^k \equiv 1 \mod m.$$

此外, 我们知道, n 是合数时, m 也是合数. 故 $m = 2^n - 1$ 是对于基 2 的强伪素数.

因为对于每个对于基 2 的伪素数 n 产生一个对于基 2 的强伪素数 $2^n - 1$ 且两两互不相同, 而且存在无穷多个对于基 2 的伪素数, 所以存在无穷多个对于基 2 的强伪素数.

定理 5.3.2

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

定理 5.3.2

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

定理 5.3.3

设 n 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最多是 25%.

目录

给出判断大奇整数 n 为素数的 Miller-Rabin（M-R）素性检测方法.

素性检测 3（M-R 素性检测）

给定奇整数 $n \geqslant 3$ 和安全参数 k. 写出 $n-1=2^s t$, 其中 t 为奇整数.

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

(2) 计算 $i=0$, $r=b^t \mod n$.

(3) 如果 $r=1$ 或者 $r=n-1$, 则通过检测, n 可能是素数;

否则, $r \neq 1$ 或者 $r \neq n-1$, 计算 $i=i+1$, $r=r^2 \mod n$.

(4) 重复执行步骤 (3), 直到 $i=s-1$.

(5) 如果 $r=n-1$, 则通过检测, n 可能是素数;

否则, $r \neq n-1$, n 为合数.

(6) 上述过程重复 k 次.

给出判断大奇整数 n 为素数的 Miller-Rabin（M-R）素性检测方法.

素性检测 3 （M-R 素性检测）

给定奇整数 $n \geqslant 3$ 和安全参数 k. 写出 $n-1=2^s t$, 其中 t 为奇整数.

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

(2) 计算 $i=0$, $r=b^t \mod n$.

(3) 如果 $r=1$ 或者 $r=n-1$, 则通过检测, n 可能是素数;

否则, $r\neq 1$ 或者 $r\neq n-1$, 计算 $i=i+1$, $r=r^2 \mod n$.

(4) 重复执行步骤 (3), 直到 $i=s-1$.

(5) 如果 $r=n-1$, 则通过检测, n 可能是素数;

否则, $r\neq n-1$, n 为合数.

(6) 上述过程重复 k 次.

注：通过 M-R 素性检测的整数 n, 其是合数的可能性小于 $\frac{1}{4^k}$, 或者说, 其是素数的可能性大于 $1-\frac{1}{4^k}$.

从上述结论可知, 随着 k 的选取和增加, 通过 M-R 素性检测的整数 n 几乎可以确定是一个素数, 但 M-R 素性检测仍是一个概率性算法. 如何使其变成确定性的算法?

从上述结论可知, 随着 k 的选取和增加, 通过 M-R 素性检测的整数 n 几乎可以确定是一个素数, 但 M-R 素性检测仍是一个概率性算法. 如何使其变成确定性的算法?

以 ψ_m 表示对于前 m 个最小素数 $2, 3, \cdots, p_m$ 为基的最小强伪素数, 那么对于任意的整数 $n < \psi_m$, 只需要分别以前 m 个最小素数为基对 n 进行 M-R 素性检测, 就可以确定性得出 n 是否是素数.

从上述结论可知, 随着 k 的选取和增加, 通过 M-R 素性检测的整数 n 几乎可以确定是一个素数, 但 M-R 素性检测仍是一个概率性算法. 如何使其变成确定性的算法?

以 ψ_m 表示对于前 m 个最小素数 $2, 3, \cdots, p_m$ 为基的最小强伪素数, 那么对于任意的整数 $n < \psi_m$, 只需要分别以前 m 个最小素数为基对 n 进行 M-R 素性检测, 就可以确定性得出 n 是否是素数.

C. Pomerance 和 G. Jaeschke 等人给出 ψ_m, $1 \leqslant m \leqslant 8$ 的具体值和 $\psi_9, \psi_{10}, \psi_{11}$ 的对应上界. Z. Zhang 进一步降低 $\psi_9, \psi_{10}, \psi_{11}$ 的上界并猜想其就是 $\psi_9, \psi_{10}, \psi_{11}$ 的确值, 还给出 ψ_m, $12 \leqslant m \leqslant 20$ 的猜想. 后来, 2014 年, Y. Jiang 和 Y. Deng 给出 $\psi_9, \psi_{10}, \psi_{11}$ 猜想的证明, 2017 年 J. Sorenson 和 J. Webster 给出 ψ_{12}, ψ_{13} 猜想的证明.

关于 $\psi_m, 1 \leqslant m \leqslant 13$ 的结果

$$
\begin{aligned}
\psi_1 &= 2047 = 23 \cdot 89; \\
\psi_2 &= 13\ 73653 = 829 \cdot 1657; \\
\psi_3 &= 253\ 26001 = 2251 \cdot 11251; \\
\psi_4 &= 32150\ 31751 = 151 \cdot 751 \cdot 28351; \\
\psi_5 &= 215\ 23028\ 98747 = 6763 \cdot 10627 \cdot 29947; \\
\psi_6 &= 347\ 47496\ 60383 = 1303 \cdot 16927 \cdot 157543; \\
\psi_7 &= \psi_8 = 34155\ 00717\ 28321 = 10670053 \cdot 32010157; \\
\psi_9 &= \psi_{10} = \psi_{11} = 3825\ 12305\ 65464\ 13051 = 149491 \cdot 747451 \cdot 34233211; \\
\psi_{12} &= 3186\ 65857\ 83403\ 11511\ 67461 \\
&= 399165290221 \cdot 798330580441; \\
\psi_{13} &= 33170\ 44064\ 67988\ 73859\ 61981 \\
&= 1287836182261 \cdot 2575672364521;
\end{aligned}
$$

关于 $\psi_m, 14 \leqslant m \leqslant 20$ 的猜想

$$
\begin{aligned}
\psi_{14} &= 600\ 30942\ 89670\ 10580\ 03125\ 96501 \\
&= 54786377365501 \cdot 109572754731001; \\
\psi_{15} &= 5927\ 63610\ 75595\ 57326\ 34463\ 30101 \\
&= 172157429516701 \cdot 344314859033401; \\
\psi_{16} = \psi_{17} &= 56413\ 29280\ 21909\ 22101\ 40875\ 01701 \\
&= 531099297693901 \cdot 1062198595387801; \\
\psi_{18} = \psi_{19} &= 1543\ 26786\ 44434\ 20616\ 87767\ 76407\ 51301 \\
&= 2777829966397710 1 \cdot 5555659932795420 1; \\
\psi_{20} &> 10^{36}.
\end{aligned}
$$

2002 年, Agrawal, Kayal 和 Saxena 给出了一个素性检测的确定性算法, 简称 A-K-S 素性检测算法, 并给出了证明. 该算法及证明涉及后续抽象代数的相关知识, 这里仅给出简单的理论表述.

定理 5.4.1

设 a 是与 p 互素的整数，则 p 是素数的充要条件是

$$(x-a)^p \equiv x^p - a \mod p.$$

定理 5.4.1

设 a 是与 p 互素的整数，则 p 是素数的充要条件是

$$(x-a)^p \equiv x^p - a \mod p.$$

定理 5.4.2

设 n 是一个正整数，q 和 r 是素数，S 是有限整数集合，其元素个数为 s. 若

(i) q 整除 $r-1$;

(ii) $n^{(r-1)/q} \mod r \notin \{0,1\}$;

(iii) 对所有不同的 $b, b' \in S$ 有 $(n, b-b') = 1$;

(iv) $\binom{q+s-1}{s} \geq n^{2[\sqrt{r}]}$;

(v) 对所有的 $b \in S$ 都有 $(x+b)^n \equiv x^n + b \mod (n, x^r - 1)$,

则 n 是一个素数的方幂.

本课作业

1. 证明：91 是对于基 3 的伪素数.
2. 证明：$2821 = 7 \cdot 13 \cdot 31$ 是 Carmichael 数.
3. 设 $b = 2$, 判断 $n = 1105$ 是否为 Euler 伪素数.
4. 证明：25 是对于基 7 的强伪素数.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn