

素性检验 在本章, 我们研究如何产生以及如何快速产生大素数.

伪素数

Fermat 素性检验

1 伪素数

根据Fermat 小定理: 如果 n 是素数, 则对任意整数 b , $(b, n) = 1$, 有

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

由此: 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.

例1 因为 $2^{62} \equiv 2^{60} \cdot 2^2 \equiv (2^6)^{10} \cdot 2^2 \equiv 64^{10} \cdot 2^2 \equiv 4 \not\equiv 1 \pmod{63}$,
所以63 一个是合数.

上述说法的否定说法不能成立. 事实上, 我们有

例2 $8^{62} \equiv (2^6)^{31} \equiv 1 \pmod{63}$.

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

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

成立, 则 n 叫做对于基 b 的**伪素数**.

例3 整数63 都是对于基 $b = 8$ 的伪素数,

例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

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

要证明：存在无穷多个对于基2 的伪素数.

引理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 $n = dq$. 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1 存在无穷多个对于基2 的伪素数.

证 (I) 要证: 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

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

由于 n 是奇合数, 所以有因数分解

$$n = dq, \quad 1 < d < n, 1 < q < n.$$

根据引理, $2^d - 1 \mid 2^n - 1$. 因此 $m = 2^n - 1$ 是合数.

现在验证: $2^{m-1} \equiv 1 \pmod{m}$.

因为 $2^{n-1} \equiv 1 \pmod{n}$, 所以 $m - 1 = 2(2^{n-1} - 1) = kn$.

根据引理, $2^n - 1 \mid 2^{m-1} - 1$. 因此, 同余式

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

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 $n_0 = 341$ 是一个对于基2 的伪素数. 再令

$$n_1 = 2^{n_0} - 1, \quad n_2 = 2^{n_1} - 1, \quad n_3 = 2^{n_2} - 1, \quad \dots$$

根据结论(I), 这些整数都是对于基2 的伪素数.

定理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) 如果 n 是对于基 b_1 和基 b_2 的伪素数, 则 n 是对于基 $b_1 b_2$ 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.

定理2 设 n 是奇合数. 则

(iv) 如果有一个整数 b , $(b, n) = 1$, 使(1) 不成立, 则模 n 的简化剩余系中至少有一半的数使(1) 不成立.

证(iv) 设 $b_1, \dots, b_s, b_{s+1}, \dots, b_{\varphi(n)}$ 是模的简化剩余系, 其中前 s 个数使得(1) 成立, 后 $\varphi(n) - s$ 个数使得(1) 不成立. 根据假设条件, 存在一个整数 b , $(b, n) = 1$, 使得(1) 不成立, 再根据结论(ii) 和(iii), 有 s 个模 n 不同简化剩余

$$bb_1, \dots, bb_s$$

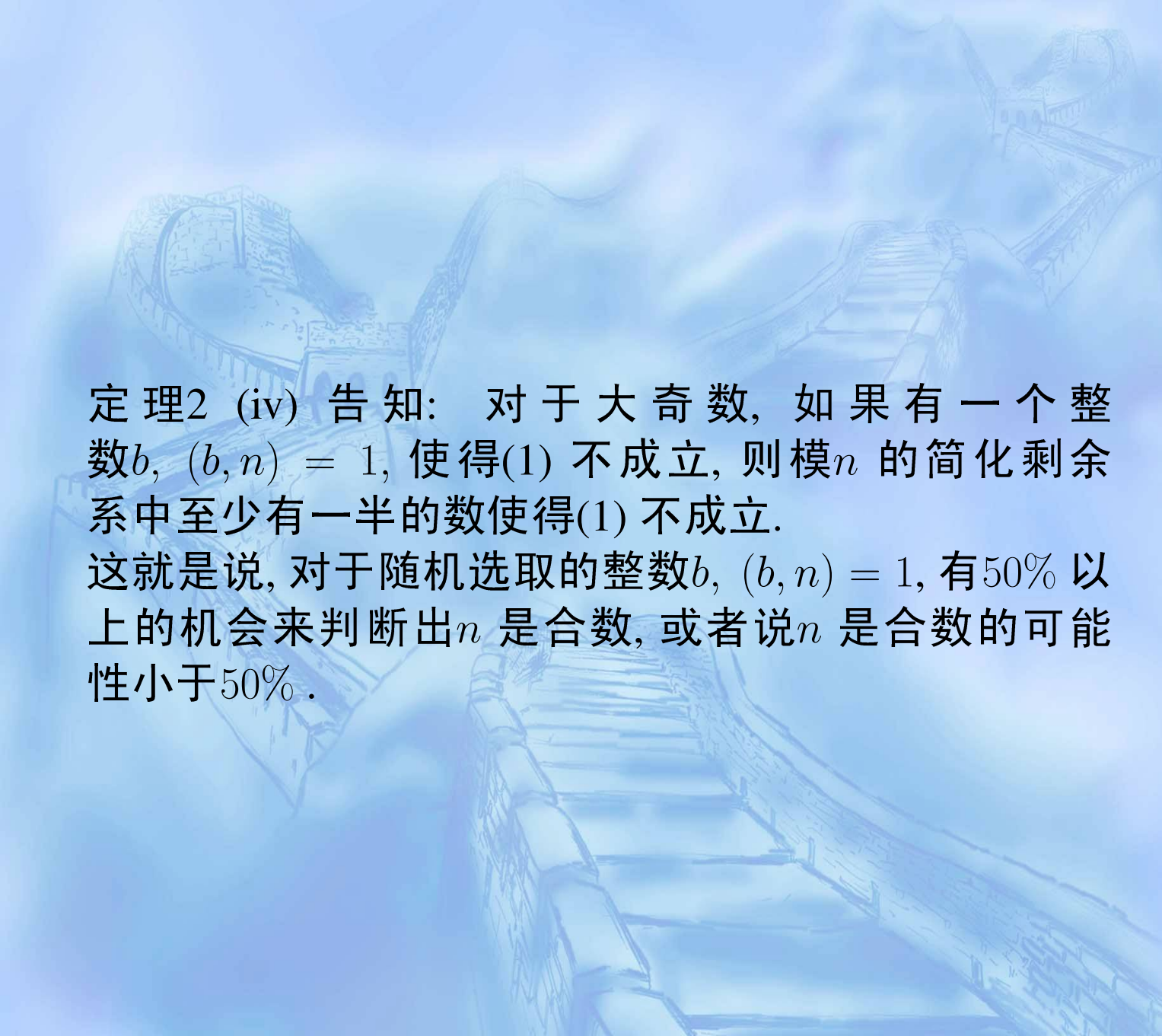
使得(1) 不成立. 因此,

$$s \leq \varphi(n) - s, \text{ 或者 } \varphi(n) - s \geq \frac{\varphi(n)}{2}.$$

这就是说, 模 n 的简化剩余系中至少有一半的数使得(1) 不成立.

例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.

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



定理2 (iv) 告知: 对于大奇数, 如果有一个整数 b , $(b, n) = 1$, 使得(1) 不成立, 则模 n 的简化剩余系中至少有一半的数使得(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%.

现在, 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 , $0 < b_1 < n$, 计算

$$d_1 = (b_1, n).$$

如果 $d_1 > 1$, 则 n 不是素数.

如果 $d_1 = 1$, 则计算 $b_1^{n-1} \pmod{n}$, 看看同余式(1)

$$b_1^{n-1} \equiv 1 \pmod{n} \quad (1)$$

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 $\frac{1}{2}$ 或者说 n 是素数可能性大于 $1 - \frac{1}{2}$.

重复上述步骤.

再随机选取整数 b_2 , $0 < b_2 < n$, 计算

$$d_2 = (b_2, n).$$

如果 $d_2 > 1$, 则 n 不是素数.

如果 $d_2 = 1$, 则计算 $b_2^{n-1} \pmod{n}$, 看看同余式(1)

$$b_2^{n-1} \equiv 1 \pmod{n} \quad (1)$$

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 $\frac{1}{2^2}$ 或者说 n 是素数可能性大于 $1 - \frac{1}{2^2}$.

继续重复上述步骤, ..., 直至第 t 步.

随机选取整数 b_t , $0 < b_t < n$, 计算

$$d_t = (b_t, n).$$

如果 $d_t > 1$, 则 n 不是素数.

如果 $d_t = 1$, 则计算 $b_t^{n-1} \pmod{n}$, 看看同余式(1)

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

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 $\frac{1}{2^t}$ 或者说 n 是素数可能性大于 $1 - \frac{1}{2^t}$.



上述过程也可简单归纳为:

Fermat 素性检验

给定奇整数 $n \geq 3$ 和安全参数 t .

1. 随即选取整数 b , $2 \leq b \leq n - 2$;
2. 计算 $r = b^{n-1} \pmod{n}$;
3. 如果 $r \neq 1$, 则 n 是合数.
4. 上述过程重复 t 次.

定义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.

例6 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,

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

从而,

$$b^{560} \equiv (b^2)^{280} \equiv 1 \pmod{3}, \quad b^{560} \equiv (b^{10})^{56} \equiv 1 \pmod{11},$$

$$b^{560} \equiv (b^{16})^{35} \equiv 1 \pmod{17}.$$

因此,

$$b^{560} \equiv 1 \pmod{561}.$$

定理3 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

$$p_i - 1 \mid n - 1, 1 \leq i \leq k.$$

证 (i) 反证法. 设对所有的正整数 b , $(b, n) = 1$, 都有同余式

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

成立. 根据定理假设, 存在一个素数幂 p^α , $\alpha \geq 2$, 使得 $n = p^\alpha \cdot n'$, $(n', p) = 1$. 根据§5.2 定理3, 存在 g 使得 g 是模 p^α 原根, 即

$$\text{ord}_{p^\alpha}(g) = p^{\alpha-1}(p-1).$$

现在运用§3.2 定理1 (中国剩余定理), 可求得 $x \equiv b \pmod{n}$ 满足:

$$x \equiv g \pmod{p^\alpha}, \quad x \equiv 1 \pmod{n'}.$$

这时, 我们有 $(b, n) = 1$ 以及

$$\text{ord}_{p^\alpha}(b) = \text{ord}_{p^\alpha}(g) = p^{\alpha-1}(p-1).$$

因为 $b^{n-1} \equiv 1 \pmod{n}$, 所以 $b^{n-1} \equiv 1 \pmod{p^\alpha}$. 根据§5.1 定理1, 得

$$\text{ord}_{p^\alpha}(b) | n-1 \quad \text{或} \quad p^{\alpha-1}(p-1) | n-1.$$

因此, $p | n-1$. 这不可能.

(ii) 设 $n = p_1 \cdots p_k$ 是一个无平方数.
充分性. 设有正整数 b , $(b, n) = 1$, 则

$$(b, p_i) = 1, \quad 1 \leq i \leq k.$$

我们有

$$b^{p_i-1} \equiv 1 \pmod{p_i}, \quad 1 \leq i \leq k.$$

进而

$$b^{n-1} \equiv (b^{p_i-1})^{(n-1)/(p_i-1)} \equiv 1 \pmod{p_i}, \quad 1 \leq i \leq k.$$

这说明 n 是 Carmichael 数.

必要性. 设 n 是Carmichael 数. 则对所有的正整数 b , $(b, n) = 1$, 都有同余式

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

固定 i , $1 \leq i \leq k$, 设 g_i 是模 p_i 原根, 则存在整数 b_i 满足

$$x \equiv g_i \pmod{p_i}, \quad x \equiv 1 \pmod{n/p_i}.$$

这时, $(b_i, n) = 1$, 且

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

进而,

$$b_i^{n-1} \equiv 1 \pmod{p_i}.$$

这意味着

$$\text{ord}_{p_i}(b_i) | n - 1 \quad \text{或} \quad p_i - 1 | n - 1.$$

定理4 每个Carmichael 数是至少三个不同素数的乘积.

证 (i) 反证法. 假设有一个Carmichael 数 n , 其可以表示为两个素数的乘积. 不妨设 $n = pq$, $p < q$. 根据定理3 (ii), 我们有 $n - 1 \equiv 0 \pmod{q - 1}$. 从而,

$$p - 1 = n - 1 - p(q - 1) \equiv 0 \pmod{q - 1}.$$

这不可能. 因此, 每个Carmichael 数是至少三个不同素数的乘积. 证毕.

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 $\geq n^{2/7}$.

2 Euler 伪素数

设 n 是奇素数. 根据定理, 有同余式

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

对任意整数 b 成立.

因此, 如果存在整数 b , $(b, n) = 1$, 使得

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

则 n 不是一个素数.

例1 设 $n = 341$, $b = 2$. 分别计算得到:

$2^{170} \equiv 1 \pmod{341}$ 以及 $\left(\frac{2}{341}\right) = (-1)^{(341^2-1)/8} = -1$,

因为 $2^{170} \not\equiv \left(\frac{2}{341}\right) \pmod{341}$. 所以341 不是一个素数.

定义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:

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

则 n 叫做对于基 b 的**Euler 伪素数**.

例2 设 $n = 1105$, $b = 2$. 分别计算得到:

$$2^{552} \equiv 1 \pmod{1105} \text{ 以及 } \left(\frac{2}{1105}\right) = (-1)^{(1105^2-1)/8} = 1.$$

因为 $2^{552} \equiv \left(\frac{2}{1105}\right) \pmod{1105}$, 所以1105 是一个对于基2 的Euler 伪素数.

定理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2 的Euler 伪素数, 则

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

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

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

因此, n 是对于基 b 的伪素数.

定理1的逆不成立, 即不是每个伪素数都是Euler 伪素数. 例如: 341 是对于基2 的伪素数, 但不是对于基2 的Euler 伪素数.

Solovay-Stassen 素性检验

给定奇整数 $n \geq 3$ 和安全参数 t .

1. 随即选取整数 b , $2 \leq b \leq n - 2$;
2. 计算 $r = b^{(n-1)/2} \pmod{n}$;
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.

3 强伪素数

设 n 是正奇整数, 并且有 $n - 1 = 2^s t$, 则有如下因数分解式:

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

因此, 如果 $b^{n-1} \equiv 1 \pmod{n}$, 则如下同余式至少有一个成立:

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

定义1 设 n 是一个奇合数, 且有表示式 $n - 1 = 2^s t$, 其中 t 为奇数. 设 $(b, n) = 1$. 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 , $0 \leq r < s$ 使得

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

则 n 叫做对于基 b 的**强伪素数**.

例1 整数 $n = 2047 = 23 \cdot 89$ 是对于基 $b = 2$ 的强伪素数.

解 因为 $2^{2046/2} \equiv (2^{11})^{93} \equiv (2048)^{93} \equiv 1 \pmod{2046}$.

定理1 存在无穷多个对于基2 的强伪素数.

证 (I) 要证: 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, 且

$$2^{n-1} \equiv 1 \pmod{n}, \quad 2^{n-1} - 1 = nk$$

对某整数 k , 进一步, k 是奇数,

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

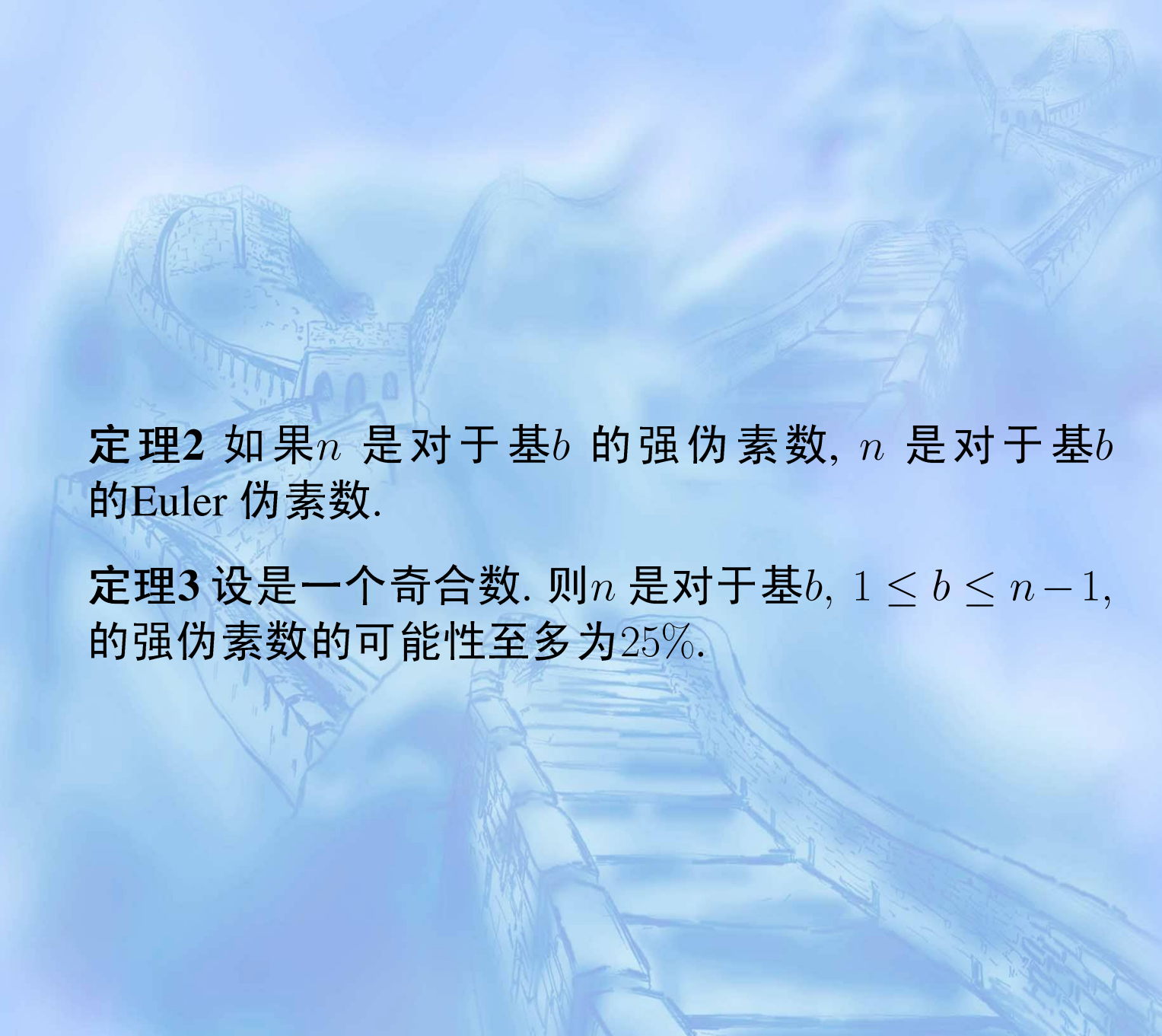
这是 $m - 1$ 分解为2 的幂和奇数乘积的表达式.

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

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

此外, 在定理1的证明中, 我们知道: n 是合数时, m 也是合数. 故 m 是对于2的强伪素数.

因为对于基2的伪素数 n 产生一个对于基的强伪素数 $2^n - 1$, 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的伪素数.



定理2 如果 n 是对于基 b 的强伪素数, n 是对于基 b 的Euler 伪素数.

定理3 设 n 是一个奇合数. 则 n 是对于基 b , $1 \leq b \leq n-1$, 的强伪素数的可能性至多为25%.

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.

1. 随机选取整数 b , $2 \leq b \leq n - 2$;
2. 计算 $r_0 \equiv b^t \pmod{n}$;
3. a) 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 , $2 \leq b \leq n - 2$;

- b) 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. a) 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 , $2 \leq b \leq n - 2$;

- b) 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. a) 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 , $2 \leq b \leq n - 2$;

- b) 否则, 有 $r_{s-1} \neq n - 1$, n 为合数.