2022-2023学年秋季学期

课程名称: 信息安全数学基础

英文名称: Mathematical Foundations for Information Security

授课团队：胡磊、许军、王丽萍

助　　教：郭一

信息安全数学基础

Mathematical Foundations for Information Security

[第 7 次课] 素性检验

授课教师：许军

授课时间：2022年10月26日

概 要

- Fermat拟素数
- Euler拟素数
- Miller-Rabin强拟素数

Fermat拟素数

研究如何产生以及如何快速产生大素数.

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.

反过来不一定成立

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, $\boldsymbol{(b, n)=1}$ 使得同余式 $b^{n-1} \equiv 1 \pmod{n}$ (1) 成立, 则 n 叫做对于基 b 的 **拟素数**.

也称b 是使得 n 为素数的一个 **证据** （witness）

- 若 n 的确是素数，则任意与 n 互素的b 都是使得 n 为素数的证据。素数 n 一定被判定为素数（没有**漏判**）
- 若 n 不是素数，则证据 b 将非素数 n 判定为素数（有**误判**）

例 3 整数 63 都是对于基 $b=8$ 的拟素数,

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 $b=2$ 的拟素数, 因为

$\boldsymbol{2^{340}=1(\mathrm{mod}341)}$，$2^{560} \equiv 1 \pmod{561}$, $2^{644} \equiv 1 \pmod{645}$

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 $r = b^{n-1} \bmod n$
3. 如果 $r \neq 1$, 则 n 是合数.
4. 上述过程重复 t 次.

- 若 n 的确是素数，则任意与 n 互素的b 都是使得 n 为素数的证据。素数 n 一定被判定为素数（没有**漏判**）
- 若 n 不是素数，则证据 b 将非素数 n 判定为素数（这是一次误判），试图**通过多次判断减少误判的几率**

- 漏判和误判在统计学上称为**第一类错误和第二类错误**

误判的几率？先看证据的性质：

定理 2 设 n 是一个奇合数．则

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

(ii) 如果 n 是对于基 b_1 和基 b_2 的拟素数，则 n 是对于基 b_1b_2 的拟素数.

(iii) 若 n 是对于基 b 的拟素数，则 n 是对于基 b^{-1} 的拟素数.

证 (ii) 因为 n 是对于基 b_1 和基 b_2 的拟素数，所以 $b_1^{n-1} \equiv 1,\quad b_2^{n-1} \equiv 1 \pmod{n}$. 从而，$(b_1b_2)^{n-1} \equiv b_1^{n-1}b_2^{n-1} \equiv 1 \pmod{n}$. 故 n 是对于基 b_1b_2 的拟素数.

(iii) 因为 n 是对于基 b 的拟素数，$b^{n-1} \equiv 1 \pmod{n}$. 从而，$(b^{-1})^{n-1} \equiv (b^{n-1})^{-1} \equiv 1 \pmod{n}$. 故 n 是对于基 b^{-1} 的拟素数.

设n是奇数，模n既约剩余系中，使得n为Fermat伪素数的证据为$b_1,\cdots,b_k$，其余元素$b_{k+1},\cdots,b_{k+l}$ 不是使得n为伪素数的证据。

性质：若 $l\geqq 1$，则 $k\leqq l$，且一次Fermat判断将合数误判为素数的概率 $\leqq 1/2$.

证明：$b_1b_{k+1},\cdots,b_kb_{k+1}$不是使得n为伪素数的证据，且两两模n不同余。所以 $k\leqq l$。

但是，若 $l=0$，则 Fermat判断总是将合数n判为素数.

（不幸的是，这样的n存在）

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

$$b^{560} \equiv (b^2)^{280} \equiv 1 \pmod{3}, \quad b^{560} \equiv (b^{10})^{56} \equiv 1 \pmod{11}, \quad b^{560} \equiv (b^{16})^{35} \equiv 1 \pmod{17}.$$

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

定理 3 设 n 是一个奇合数.

(i) 如果 n 被一个大于 1 平方数，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 $p_i - 1 \mid n - 1,\ 1 \leq i \leq k$.

定理 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 $\geq n^{2/7}$.

给出判断一个大奇整数 n 为素数的方法:（对**Carmichael**数失效）

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) 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) 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, $\ldots$, 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) 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 $1 - \frac{1}{2^t}$.

Euler拟素数

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 拟素数**.

例 2 设 $n=1105$, $b=2$. 分别计算得到： $2^{552}\equiv 1 \pmod{1105}$ 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 拟素数.

定理 1 如果 n 是对于基 b 的 Euler 拟素数, 则 n 是对于基 b 的拟素数.

证 设 n 是对于基 2 的 Euler 拟素数, 则 $b^{(n-1)/2}\equiv\left(\frac{b}{n}\right) \pmod{n}$. 上式两端平方, 并注意到 $\left(\frac{b}{n}\right)=\pm1 \pmod{n}$,

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

因此, n 是对于基 b 的拟素数.

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

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.

设n是奇数，模n既约剩余系中，使得n为Euler伪素数的证据一定是使得n为Fermat伪素数的证据,其个数k’小于等于使得n为Fermat伪素数的证据的个数k，所以Solovay-Strassen测试的误判率小于等于Fermat测试的误判率。

欧拉测试不能总是出错

对于非素数的奇数，一定有欧拉测试的非证据，即

l≧1。

则 k≦l，一次欧拉判断将合数判为素数的概率 ≦ 1/2.

Claim: Euler测试不能总是错.

即对奇数n, 若n不是素数, 则一定存在

$a\in\mathbb{Z}_n^*$, s.t. $a^{\frac{n-1}{2}}\not\equiv\left(\frac{a}{n}\right) \pmod n$

证明: 反证法, 设 $\forall a\in\mathbb{Z}_n^*$, 均有

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

令 $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. 因为 $a^{n-1}\equiv 1 \pmod n$,

$$a^{n-1}\equiv 1\pmod{p_i^{\alpha_i}}$$

所以 $p_i^{\alpha_i-1}(p_i-1) \mid n-1 \Longrightarrow \alpha_i=1$.

即 $n=p_1\cdots p_r$, $a^{\frac{p_1\cdots p_r-1}{2}}\equiv\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\pmod{p_1\cdots p_r}$

若 $r\ge 2$. 设 $1\le i\le p_1$, $a_i\in\mathbb{Z}_n^*$, s.t.

$$\begin{cases} a_i\equiv i \pmod{p_1} \\ a_i\equiv 1 \pmod{p_j} \quad 对\forall j\ge 2 \end{cases}$$

以 a_i 为 a 代入上式有 (只考虑 mod p_2)

$$1\equiv\left(\frac{i}{p_1}\right)\pmod{p_2}$$

因为 $p_2\ge 3$, 所以 $1=\left(\frac{i}{p_1}\right)$, 此式对 $i=1,2,\cdots,p_1-1$ 不可能都成立, 矛盾.

Miller-Rabin强拟素数

设 n 是正奇整数，并且有 $n-1=2^s t$

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

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

$$b^t\equiv 1,\quad b^t\equiv -1,\quad b^{2t}\equiv -1,\ldots,\quad b^{2^{s-1}t}\equiv -1 \pmod{n}.$$

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, $0\le r<s$ 使得 $b^{2^r t}\equiv -1 \pmod{n}$, 则 n 叫做对于基 b 的 **强拟素数**.

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

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 的强拟素数.

证 (I) 要证：如果 n 是对于基 2 的拟素数，则 $m=2^n-1$ 是对于基 2 的强拟素数.

事实上，因为 n 是对于基 2 的拟素数，所以

n 是奇合数，且 $2^{n-1}\equiv 1 \pmod{n}$, $2^{n-1}-1=nk$ 对某整数 k, 进一步，k 是奇数，$m-1=2^n-2=2(2^{n-1}-1)=2^1nk$,

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 的强拟素数.

因为对于基 2 的拟素数 n 产生一个对于基的强拟素数 2^n-1, 而且存在无穷多个对于基 2 的拟素数，所以存在无穷多个对于基 2 的拟素数.

定理 2 如果 n 是对于基 b 的强拟素数， n 是对于基 b 的 Euler 拟素数.

定理 3 设是一个奇合数. 则 n 是对于基 b, $1 \le b \le n-1$, 的强拟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.

一次测试将合数判为素数的概率

1或者	$\leqq 1/2$	（Fermat）
$\leqq 1/2$		（Euler）
$\leqq 1/4$		（Miller-Rabin）

上述概率严格递减。