网络安全数学基础(一)

沈佳辰
jcshen@sei.ecnu.edu.cn

网络安全数学基础

第五章 素性检验

華東師範大學
EAST CHINA NORMAL UNIVERSITY

§5.1 拟素数

- 由费马小定理，我们知道对于大于1的正整数n，如果存在整数$b, (b, n) = 1$，使得$b^{n-1} \not\equiv 1 \ (mod\ n)$，则$n$是合数。

§5.1 拟素数

- 由费马小定理，我们知道对于大于1的正整数n，如果存在整数$b, (b, n) = 1$，使得$b^{n-1} \not\equiv 1 \ (mod\ n)$，则$n$是合数。

- 例 判断$n = 63$是否为素数

§5.1 拟素数

- 由费马小定理，我们知道对于大于1的正整数n，如果存在整数$b,(b,n)=1$，使得$b^{n-1}\not\equiv 1\ (mod\ n)$，则$n$是合数。

- 例 判断$n=63$是否为素数

因为$2^{63-1}=2^{6\cdot 10+2}=64^{10}\cdot 4\equiv 1\cdot 4\not\equiv 1\ (mod\ 63)$，因此63不是素数。

- 那么给定大于1的正整数n和整数b，$(b,n)=1$，如果$b^{n-1}\equiv 1\ (mod\ n)$，那么能判定$n$是素数吗？

- 那么给定大于1的正整数n和整数b，$(b, n) = 1$，如果$b^{n-1} \equiv 1 \ (mod\ n)$，能判定$n$是素数吗？

- n不一定是素数。事实上$8^{63-1} = 8^{2\cdot 31} = 64^{31} \equiv 1 \ (mod\ 63)$。

- 定义5.1.1 设$n > 1$为奇合数，若存在整数b，使得$b^{n-1} \equiv 1 \ (mod\ n)$，则$n$称为对于基$b$的拟素数。

- 定义5.1.1 设$n > 1$为奇合数，若存在整数b，使得$b^{n-1} \equiv 1 \ (mod\ n)$，则$n$称为对于基$b$的拟素数。

- 由前例可知63为对于基8的拟素数。

- 定义5.1.1 设$n > 1$为奇合数，若存在整数b，使得$b^{n-1} \equiv 1 \ (mod\ n)$，则$n$称为对于基$b$的拟素数。

- 由前例可知63为对于基8的拟素数。

- 例由$2^{340} = (2^{10})^{34} \equiv 1^{34} = 1 \ (mod\ 341)$可知$341 = 11 \cdot 31$是对于基2的拟素数；由$2^{560} = (2^{40})^{14} \equiv 1^{14} = 1 \ (mod\ 561)$可知$561 = 3 \cdot 11 \cdot 17$是对于基2的拟素数。

- 定理5.1.1 设$n, d \in Z^+$，若$d|n$，那么$\left(2^d - 1\right)|(2^n - 1)$。

华东师范大学 EAST CHINA NORMAL UNIVERSITY

- 定理5.1.1 设$n, d \in Z^{+}$，若$d|n$，那么$\left(2^{d}-1\right)|(2^{n}-1)$。

证明：因为$d|n$，因此存在$q \in Z^{+}$，使得$n = dq$，则$2^{n}-1 = 2^{dq}-1 = (2^{d}-1)(2^{d(q-1)}+2^{d(q-2)}+\cdots+1)$，得证。

- 定理5.1.2 存在无穷多个对于基2的拟素数。

- 定理5.1.2 存在无穷多个对于基2的拟素数。

证明：令$n_0 = 341$，对于$i \in Z^+$，令$n_i = 2^{n_{i-1}} - 1$，如果能证明对于所有i，n_i都是对于基2的拟素数，则定理得证。

事实上，由前例可知$n_0 = 341$为对于基2的拟素数。

设n_i是对于基2的拟素数，则存在$q, d \in Z, q, d > 1$，使得$n_i = dq$，由定理5.1.1可知，$1 < \left(2^d - 1\right) | (2^{n_i} - 1) = n_{i+1}$，因此$n_{i+1}$为奇合数。另一方面由于$n_i$是对于基2的拟素数，因此$2^{n_i - 1} \equiv 1 \ (mod\ n_i)$，所以$n_i | 2(2^{n_i - 1} - 1) = n_{i+1} - 1$，由定理5.1.1可知$n_{i+1} = (2^{n_i} - 1) | (2^{n_{i+1} - 1} - 1)$，即$2^{n_{i+1} - 1} \equiv 1 \ (mod\ n_{i+1})$，所以$n_{i+1}$是对于基2的拟素数，得证。

- 定理5.1.3 设n是一个奇合数， b, b_1, b_2为与n互素的整数，则

(i) n是对于基b的拟素数当且仅当b模n的次数整除$n-1$；

(ii) 若n是对于基b_1和b_2的拟素数，则n也是对于基$b_1 b_2$的拟素数；

(iii) 若n是对于基b的拟素数，则n也是对于基$b^{-1}\ (mod\ n)$的拟素数；

(iv) 若$b^{n-1} \equiv 1\ (mod\ n)$不成立，那么模$n$的简化剩余系中至少有一半的数不满足同余式$x^{n-1} \equiv 1\ (mod\ n)$。

(iv)的证明：设$a_1,\cdots,a_{\varphi(n)}$是模$n$的一组简化剩余系，其中$a_1,\cdots,a_k$满足同余式$x^{n-1}\equiv 1\ (mod\ n)$，$a_{k+1},\cdots,a_{\varphi(n)}$不满足同余式$x^{n-1}\equiv 1\ (mod\ n)$，则$ba_1,\cdots,ba_{\varphi(n)}$也构成模$n$的一组简化剩余系，且$ba_1,\cdots,ba_k$不满足同余式$x^{n-1}\equiv 1\ (mod\ n)$，因此存在$a'_{k+1},\cdots,a'_{\varphi(n)}$，使得$a_{k+1}\equiv a'_{k+1},\cdots,a_{\varphi(n)}\equiv a'_{\varphi(n)}\ (mod\ n)$，且$ba_1,\cdots,ba_k\in\{a'_{k+1},\cdots,a'_{\varphi(n)}\}$，故$k\leq\varphi(n)-k$，即$\varphi(n)-k\geq\frac{\varphi(n)}{2}$，得证。

(iv)的证明：设$a_1,\cdots,a_{\varphi(n)}$是模$n$的一组简化剩余系，其中$a_1,\cdots,a_k$满足同余式$x^{n-1}\equiv 1\ (mod\ n)$，$a_{k+1},\cdots,a_{\varphi(n)}$不满足同余式$x^{n-1}\equiv 1\ (mod\ n)$，则$ba_1,\cdots,ba_{\varphi(n)}$也构成模$n$的一组简化剩余系，且$ba_1,\cdots,ba_k$不满足同余式$x^{n-1}\equiv 1\ (mod\ n)$，因此存在$a'_{k+1},\cdots,a'_{\varphi(n)}$，使得$a_{k+1}\equiv a'_{k+1},\cdots,a_{\varphi(n)}\equiv a'_{\varphi(n)}\ (mod\ n)$，且$ba_1,\cdots,ba_k\in\{a'_{k+1},\cdots,a'_{\varphi(n)}\}$，故$k\leq\varphi(n)-k$，即$\varphi(n)-k\geq\frac{\varphi(n)}{2}$，得证。

- 此时对于随机选取的与n互素的整数a_i，至少有$\frac{1}{2}$的概率可判断出n是合数。

- 算法5.1.1（费马素性检验）给定正奇数n 和参数$t \in Z^+$，

(i) 随机选取小于n的正整数b，如果$(n, b) \neq 1$，则n是合数，算法终止；

(ii) 计算$b^{n-1}\ (mod\ n)$，若$b^{n-1} \equiv 1\ (mod\ n)$不成立，则$n$是合数，算法终止；

(iii) 若选过t个b，则判断n是素数，否则返回至(i)。

- 算法5.1.1（费马素性检验）给定正奇数n 和参数$t \in Z^+$，

(i) 随机选取小于n的正整数b，如果$(n, b) \neq 1$，则n是合数，算法终止；

(ii) 计算$b^{n-1}\ (mod\ n)$，若$b^{n-1} \equiv 1\ (mod\ n)$不成立，则$n$是合数，算法终止；

(iii) 若选过t个b，则判断n是素数，否则返回至(i)。此时对于每一个随机选取的b，都有$(n, b) = 1$且$b^{n-1} \equiv 1\ (mod\ n)$，故$n$是合数的可能性不超过$\frac{1}{2}$，因此$t$轮之后，$n$是合数的可能性不超过$\frac{1}{2^t}$，即误判$n$是素数的概率不超过$\frac{1}{2^t}$。

- 定义5.1.2 设$n > 1$为奇合数，若对于所有整数$b, (b, n) = 1$，都有$b^{n-1} \equiv 1 \ (mod\ n)$，则$n$称为Carmichael数。

- 定义5.1.2 设$n > 1$为奇合数，若对于所有整数$b, (b, n) = 1$，都有$b^{n-1} \equiv 1\ (mod\ n)$，则$n$称为Carmichael数。

- $561 = 3 \cdot 11 \cdot 17$是一个Carmichael数。

- 定义5.1.2 设$n > 1$为奇合数，若对于所有整数$b, (b, n) = 1$，都有$b^{n-1} \equiv 1 \ (mod\ n)$，则$n$称为Carmichael数。

- $561 = 3 \cdot 11 \cdot 17$是一个Carmichael数。

事实上，对于所有整数$b, (b, n) = 1$，都有$(b, 3) = 1, (b, 11) = 1, (b, 17) = 1$，因此有$b^2 \equiv 1 \ (mod\ 3), b^{10} \equiv 1 \ (mod\ 11), b^{16} \equiv 1 \ (mod\ 17)$，故$b^{560} = (b^2)^{280} \equiv 1 \ (mod\ 3), b^{560} = (b^{10})^{56} \equiv 1 \ (mod\ 11), b^{560} = (b^{16})^{35} \equiv 1 \ (mod\ 17)$，由孙子定理可知$b^{560} \equiv 1 \ (mod\ 561)$，因此561是Carmichael数。

- 定理5.1.4 设$n > 1$为奇合数，则

(i) 若n能被一个大于1的平方数整除，则n不是Carmichael数；

(ii) 若$n = p_1 \cdots p_s$不含大于1的平方因子，则n是Carmichael数的充要条件是对任意$i, 1 \le i \le s$，都有$(p_i - 1)|(n - 1)$。

- 定理5.1.5

(i) 所有Carmichael数都至少是3个不同素数的乘积；

(ii) 存在无穷个Carmichael数。

- 定理5.1.5

(i) 所有Carmichael数都至少是3个不同素数的乘积；
(ii) 存在无穷个Carmichael数。

- 若n是Carmichael数，则费马素性检验必将产生误判。

§5.2 欧拉拟素数

- 由欧拉判别法则，对正奇数n和整数b，若n是素数，则有$b^{\frac{n-1}{2}} \equiv (\frac{b}{n}) \ (mod\ n)$。

- 如果存在与n互素的整数b，使得$b^{\frac{n-1}{2}} \equiv (\frac{b}{n}) \ (mod\ n)$不成立，则$n$是合数。

- 例 对$n=341$，我们计算$2^{\frac{341-1}{2}}=(2^{10})^{17}\equiv 1\ (mod\ 341)$，另一方面，$\left(\frac{2}{341}\right)\equiv(-1)^{\frac{341^2-1}{8}}=(-1)^{14535}=-1\ (mod\ 341)$，因此$2^{\frac{341-1}{2}}\not\equiv\left(\frac{2}{341}\right)\ (mod\ 341)$，故341是合数。

- 定义5.1.3 设$n > 1$为奇合数，若对于整数$b, (b, n) = 1$，有$b^{\frac{n-1}{2}} \equiv (\frac{b}{n}) \ (mod\ n)$，则$n$称为对于基$b$的欧拉拟素数。

- 例 对$1105=5\cdot 221$，计算$2^{\frac{1105-1}{2}}=2^{552}\equiv 1\ (mod\ 1105)$，另一方面，$\left(\frac{2}{1105}\right)\equiv(-1)^{\frac{1105^2-1}{8}}=(-1)^{152628}=1\ (mod\ 1105)$，因此$2^{\frac{1105-1}{2}}\equiv\left(\frac{2}{1105}\right)\ (mod\ 1105)$，所以1105是对于基2的欧拉拟素数。

- 定理5.1.6 如果奇合数n是对于基b的欧拉拟素数，那么它也是对于基b的拟素数。

华东师范大学 EAST CHINA NORMAL UNIVERSITY

- 定理5.1.6 如果奇合数n是对于基b的欧拉拟素数，那么它也是对于基b的拟素数。

证明：因为n是对于基b的欧拉拟素数，所以$b^{\frac{n-1}{2}} \equiv (\frac{b}{n}) \ (mod\ n)$，两边平方可得$b^{n-1} \equiv \left(\frac{b}{n}\right)^2 = 1 \ (mod\ n)$，故$n$是对于基$b$的拟素数。

- 定理5.1.6的逆命题不成立，即并非所有对于基b的拟素数n都是对于基b的欧拉拟素数。

- 定理5.1.6的逆命题不成立，即并非所有对于基b的拟素数n都是对于基b的欧拉拟素数。

- 341是对于基2的拟素数，但不是对于基2的欧拉拟素数。

- 算法5.1.2（Solovay-Stassen素性检验）给定正奇数n 和参数$t \in Z^+$，

(i) 随机选取小于n的正整数b，计算$b^{\frac{n-1}{2}}\ (mod\ n)$，如果$b^{\frac{n-1}{2}} \not\equiv \pm 1\ \ (mod\ n)$，则$n$是合数，算法终止；

(ii) 计算$(\frac{b}{n})$，如果$b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right)(mod\ n)$，则$n$是合数，算法终止；

(iii) 若选过t个b，则判断n是素数，否则返回至(i)。此时对于每一个随机选取的b，都有$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right)(mod\ n)$，设$n$是合数但一轮检验通过的概率为$\epsilon$，则$t$轮之后，$n$是合数的可能性不超过$\epsilon^t$，即误判$n$是素数的概率不超过$\epsilon^t$。由定理5.1.6可知$\epsilon \le \frac{1}{2}$。

§5.3 强拟素数

- 设n为正奇数，$b \in Z, b > 1,$ 令$n = t2^s + 1$，其中$t, s \in Z^+, 2 \nmid t$，则$b^{n-1} - 1 = (b^{2^0 t} - 1)(b^{2^0 t} + 1)(b^{2^1 t} + 1) \cdots (b^{2^{s-1} t} + 1)$，因此若$n$为素数，则$b^{n-1} \equiv 1\ (mod\ n)$且$Z_n$无零因子，所以
  $b^{2^0 t} \equiv 1, b^{2^0 t} \equiv -1, b^{2^1 t} \equiv -1, \ldots, b^{2^{s-1} t} \equiv -1\ (mod\ n)$
  中必有一个成立。

§5.3 强拟素数

- 设n为正奇数，$b \in Z, b > 1$, 令$n = t2^s + 1$，其中$t, s \in Z^+, 2 \nmid t$，则$b^{n-1} - 1 = (b^{2^0 t} - 1)(b^{2^0 t} + 1)(b^{2^1 t} + 1) \cdots (b^{2^{s-1} t} + 1)$，因此若$n$为素数，则$b^{n-1} \equiv 1\ (mod\ n)$且$Z_n$无零因子，所以
$$b^{2^0 t} \equiv 1, b^{2^0 t} \equiv -1, b^{2^1 t} \equiv -1, \ldots, b^{2^{s-1} t} \equiv -1\ (mod\ n)$$
中必有一个成立。

- 定义5.1.4 设$n > 1$为奇合数， $b \in Z, (b, n) = 1$，令$n = 2^s t + 1$，其中t为奇数，若$b^t \equiv 1\ (mod\ n)$或存在$r \in Z, 0 \le r < s$，使得$b^{2^r t} \equiv -1\ (mod\ n)$，则$n$称为对于基$b$的强拟素数。

- 例$2047=23\cdot 89$是对于基2的强拟素数。

  事实上，$2047-1=2\cdot 1023$，而$2^{1023}=(2^{11})^{93}\equiv 1^{93}=1\ (mod\ 2047)$，因此2047是对于基2的强拟素数。

- 定理5.1.7 存在无穷多个对于基2的强拟素数。

- 定理5.1.7 存在无穷多个对于基2的强拟素数。

证明：首先我们证明若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$2^{n-1} \equiv 1\ (mod\ n)$，此时$m - 1 = 2(2^{n-1} - 1) = 2nk$，其中$k$为奇数，计算$2^{nk} = (2^n)^k \equiv (1)^k = 1\ (mod\ m = 2^n - 1)$。再由定理5.1.2，因为$n$是对于基2的拟素数，所以$m = 2^n - 1$是对于基2的拟素数，因此$m$是对于基2的强拟素数。

- 定理5.1.8 如果n是对于基2的强拟素数，那么它也是对于基2的欧拉拟素数。

- 定理5.1.8 如果n是对于基2的强拟素数，那么它也是对于基2的欧拉拟素数。

- 定理5.1.9 设n是奇合数，$b \in Z, 1 \leq b < n$，那么n是对于基b的强拟素数的概率不超过$\frac{1}{4}$。

- 算法5.1.3（Miller-Rabin素性检验）给定正奇数n 和参数 $t \in Z^+$，令$n = 2^s k + 1$，其中k为正奇数，

(i) 若已选过t个b，则判断n是素数，算法终止；

(ii) 随机选取整数$b, 2 \le b \le n-2$，令$i = 0$，计算$r_i = b^k \ (mod\ n)$，如果$r_i = 1$或$n-1$，则返回至(i)；

(iii) 若$i < s-1$，令$i = i+1$，计算$r_i = r_{i-1}^2\ (mod\ n)$，如果$r_i = n-1$，则返回至$(i)$ ；

(iv) 判断n是合数，算法终止。

- 算法5.1.3（Miller-Rabin素性检验）给定正奇数n 和参数$t \in Z^+$，令$n = 2^s k + 1$，其中k为正奇数，

(i) 若已选过t个b，则判断n是素数，算法终止；

(ii) 随机选取整数$b, 2 \le b \le n-2$，令$i = 0$，计算$r_i = b^k \pmod n$，如果$r_i = 1$或$n-1$，则返回至(i)；

(iii) 若$i < s-1$，令$i = i+1$，计算$r_i = r_{i-1}^2 \pmod n$，如果$r_i = n-1$，则返回至(i)；

(iv) 判断n是合数，算法终止。

显然n是合数的可能性不超过$\frac{1}{4^t}$，即误判n是素数的概率不超过$\frac{1}{4^t}$。

实验4

- 实现Miller-Rabin素性检验算法，随机生成一个奇数n，判断它是素数还是合数，其中t取10。
- 要求输出中间结果，包括$s, k,$ 每一轮选择的随机数b, r_i,和跳出循环的位置(ii),(iii)或(iv)，算法结束时的总轮数。
- 语言：C/C++或Python
- 使用头歌平台搭建环境并提交作业