密码学数学基础 - 初等数论

Lecture Notes

作者：黄征 & Huang Zheng

组织：上海交通大学网络空间安全学院

时间：秋季学期, 2020

版本：0.1

自定义：Lecture Notes

希望数学书如东坡肉肥而不腻。肥：营养好，高能量。不腻：看了不容易晕。——hz

目录

初等数论研究整数的性质。

初等数论是各种中小学数学竞赛的重要内容之一，所以很多同学从小学开始就接触过初等数论的相关内容。本文可以让学生" 温故而知新"。

笔记 本书是为了配合密码学数学基础课程教学而写的课程注记。作者水平有限，成书仓促，如有错误之处，敬请指正。

第一章 整除

定义 1.1 (整除)

定义 | 为整除的符号，整除定义如下：

$a \neq 0, a \mid b \iff \exists l, s.t.\ \ b = al$

我们称作 a 整除 b。如果 a 整除 b，那么 a 是 b 的因数。

性质 整除有如下性质：

1. $a|b, b|c \Rightarrow a|c$
2. $a|b, a|c \Rightarrow a|(bs+ct)$
3. (带余除法) $\forall a, b(b>0), \exists q, r, s.t.\ a = bq + r\ (0 \leq r < b)$

定义 1.2 (最大公因数)

给定 $a_1, a_2, ...a_n$ 不全为 0，集合 $\{d|d>0, d|a_1, d|a_2, ..., d|a_n\}$ 为有限集合，则其极大元存在且唯一，称为 $a_1, a_2, ...a_n$ 的最大公因数（GCD），记为 $(a_1, a_2, ...a_n)$，或者记为 $GCD(a_1, a_2, ...a_n)$ 。

最常用的是求两个数 a 和 b 的最大公因子，记作 (a, b)。

1.1 Euclid 算法 (辗转相除法)

例 1.1

回顾一下小学就学过的辗转相除法。

命题 1.1 (Euclid)

在带余除法中，$\forall a, b(b>0), \exists q, r, s.t. a = bq + r(0 \leq r < b)$ ，于是可得：$(a, b) = (b, r)$。

证明：记 S_1 为 a 与 b 所有公因子组成的集合，S_2 为 b 与 r 所有公因子组成的集合。显然这两个集合都是有限集合。对任意一个 $d \in S_1$，$d|a, d|b \Rightarrow d|r \Rightarrow d \in R_2$(整除性质1)。同理，对任意一个 $d \in S_2$，$d|b, d|r \Rightarrow d|a \Rightarrow d \in R_1$(整除性质1)。所以，$S_1 = S_2$，两个集合的极大元也相同，于是可得 $(a, b) = (b, r)$。

例 1.2 求最大公因数 输入 a, b，求 (a, b)。

用带余除法求 $a = bq_1 + r_1$。

用带余除法求 $b = r_1 q_2 + r_2$。

用带余除法求 $r_1 = r_2 q_3 + r_3$。

....

直到 $r_{n-1} = r_n q_n + 0$ 终止，则 $r_n = (a, b)$ 。

性质 关于最大公因数有几个基本的性质，对于整数 a, b, n:

1. $(a, b) = (a \pm b, b)$
2. $(na, nb) = n(a, b)$

定义 1.3

给定整数 a, b。如果 $(a, b) = 1$，那么我们称 a 和 b 互素。♣

和最大公因数相对应的有最小公倍数，我们常常用 $lcm(a, b)$ 或者 $[a, b]$ 表示两个数 a 和 b 的最小公倍数。显然，$[a, b] = \frac{ab}{(a,b)}$

第二章 连分数

定义 2.1 (连分数定义)

$a \in \mathbb{R}$，a 的连分数形式可以使用如下的步骤进行计算：

令 q_1 为小于 a 的最大正整数，即 $0 < a - q_1 < 1$。于是存在 $a_2 = \frac{1}{a-q_1}$，$a_2 > 1$，使得 $a = q_1 + \frac{1}{a_2}$。

如果 a_2 不是整数，那么 a_2 也可以写成 $a_2 = q_2 + \frac{1}{a_3}$ 的形式，其中 $0 < a_2 - q_2 < 1$，$a_3 = \frac{1}{a_2-q_2}$，$a_3 > 1$。所以：

$$a = q_1 + \cfrac{1}{q_2 + \cfrac{1}{a_3}}$$

当 a_n 为整数的时候，过程终止，得到的结果就是 a 的连分数形式。(注意，这个过程有可能不终止。) ♣

例 2.1

$$\frac{10}{7} = 1 + \frac{1}{2 + \frac{1}{3}}$$

例 2.2 求黄金分割数 $\phi = \frac{\sqrt{5}-1}{2}$ 的连分数。

显然有 $\frac{\sqrt{5}+1}{2} = \phi + 1$。

因为 $(\sqrt{5}-1)(\sqrt{5}+1) = 4$ 所以 $\frac{\sqrt{5}-1}{2} \cdot \frac{\sqrt{5}+1}{2} = 1$，即 ϕ 与 $\phi + 1$ 互为乘法逆元。

$$\phi = \frac{\sqrt{5}-1}{2} = \frac{1}{\frac{\sqrt{5}+1}{2}} = \frac{1}{\phi + 1}$$

于是可得：

$$\phi = \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \dots}}}$$

根据上式可以用程序写出黄金分割数的近似计算代码，小数点后 7 位的值为：0.6180340。

例 2.3 和" 连分数比较相似" 的一个例子 (不符合连分数定义) 类似连分数的方法有很强的表示能力。

$$e - 1 = 1 + \cfrac{2}{2 + \cfrac{3}{3 + \cfrac{4}{4 + \cfrac{5}{5 + \ddots}}}}$$

命题 2.1 (连分数和有理数)

$$\alpha \in \mathbb{Q} \Leftrightarrow \exists q_1, ..., q_n \in \mathbb{Z}, s.t.\ \alpha = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + ... + \frac{1}{q_n}}}$$

证明：根据有理数的定义，必要性（$\Leftarrow$）是显然的。下面仅证明充分性。

由条件 $\alpha \in \mathbb{Q}$，那么不妨假设 $\alpha = \frac{a}{b}$，其中 $a > b$。使用 Euclid 算法，$a = bq_1 + r_1$，所以 $\frac{a}{b} = q_1 + \frac{r_1}{b}$，其中 $0 \leq \frac{r_1}{b} < 1$。

同理，$\frac{b}{r_1} = q_2 + \frac{r_2}{r_1}$，其中 $0 \leq \frac{r_2}{r_1} < 1$。于是

$$\alpha = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}}$$

由于 Euclid 算法会在有限步之后终止，所以 a 可以用有限连分数的形式表示。任何一个正的有理数写成连分数的形式，也有与之对应的一串正整数 $(q_1, q_2, ..., q_n)$，这些正整数正好是 Euclid 算法得到的商。♠

性质 有理数对应的正整数串是有限的。无理数对应的正整数串是无限的。

例 2.4 $\frac{105}{38}$ 对应的正整数串是 $(2, 1, 3, 4, 2)$

第三章 素数 (Prime Number)

定义 3.1

只能被 1 和自身整除的正整数为素数。素数又称为质数。不是素数的整数是合数。

命题 3.1

p 是一个素数，对于任意整数 a，有 $p|a$ 或者 $(p,a)=1$。

引理 3.1 (Euclid lemma)

If a prime p divides the product ab of two integers a and b, then p must divide at least one of those integers a and b. 即：$p \mid ab \Rightarrow p \mid a \;\; or \;\; p \mid b$

注 Not to be confused with Euclid's theorem or Euclidean algorithm.

命题 3.2 (Euclid lemma 推广)

如果 $p|a_1a_2...a_n$，那么 $\exists a_i$，$p|a_i$。

定理 3.1 (定理)

[Euclid's theorem] 素数有无穷多个。

证明：反证法。

注 另一类证明方法 [P. G. Lejeune-Dirichlet]：证明有无限个形如 $4k+1$ 或者 $4k-1$ 的素数。更一般的，有无限个形如 $ak+b$ 的素数，其中 $(a,b)=1$。

因为素数有无穷多，所以大家比较关心目前人类已知的最大素数。梅森素数是指形如 2^n-1 的素数，记为 $M(n)$。目前几个已知最大素数都是梅森素数。这些素数是由互联网梅森素数大搜索分布式计算项目（GIMPS）找到的。

搜索梅森素数的历史记录：

- December 7, 2018 Prime M(82,589,933) discovered!
- December 26, 2017 Prime M(77,232,917) discovered!
- January 7, 2016 Prime M(74,207,281) discovered!

命题 3.3 (代数基本定理，Unique factorization theorem)

任意一个大于 1 的正整数 n 都能表示成 $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ 的形式，其中 $\alpha_1,\alpha_2...\alpha_k>0$，$p_1<p_2<...<p_k$ 均为素数，且这种表示方法是唯一的。

例 3.1 $663=17*13*3$，这个分解是唯一的。

素数对于数论与其他数学的重要性来自于“代数基本定理”。素数可被认为是自然数的“基本建材”。

你可能已经猜到素数和密码是有关系的，素数是密钥的构成部分。全世界每个人都需要密钥，每个人的密钥应该是不一样的，这样我们应该需要很多不同的素数。尽管素数是无穷多的，然而现实中的计算机都是有限状态机，不能处理无限大的数。从实践的角度，我们更关心的问题是在“计算方便且安全”的范围内是否有足够的素数满足人民的需求。目前（2020 年）我们认为“计算方便且安全”的范围大概是从 2048 比特到 4096 比特的整数。这就涉及到素数密度的问题，素数定理回答了这个问题。在数论中，素数定理描述素数在自然数中分布的渐进情况，给出随着数字的增大，素数的密度逐渐降低的形式化描述。

注 我们的直觉是素数分布是不规则的。有两个比较极端的观察结果：一方面可以证明两个素数之间的距离可以无限大；
考虑一个整数序列：

$$k!+2, k!+3, ..., k!+k$$

这个整数序列的长度是 $k-1$ 个，序列中的每个数都是合数 (显然 $i|k!+i$)。于是可以找到两个素数，他们的间隔大于任意的 $k-1$。

另一方面有些素数之间非常接近，如 $5, 7$，又如 $17, 19$。如果 $p, p+2$ 都是素数，我们称之为称为" 孪生素数对"，目前还不知道是否有无限个孪生素数对。

" 庾信平生最萧瑟，暮年诗赋动江关"--杜甫。张益唐，浙江平湖人，2013 年 4 月 17 日在《数学年刊》发表《质数间的有界间隔》，首次证明了存在无穷多对间隙为有限的质数（具体间隙小于 7000 万），从而在孪生素数猜想这一数论难题上取得质的突破。张益唐坎坷而传奇的数学历程激励了广大莘莘学子。

定义 3.2

对正实数 x，定义 $\pi(x)$ 为素数计数函数，即不大于 x 的素数个数。

$\pi(x)=\sum_{p\leq x}1=\#\{p\leq x \mid p\ is\ prime.\}$ ♣

素数定理是由 Jacques Hadamard 和 Charles de la Vallée Poussin 在 1896 年证明的。此前最接近的结论是 1850 年 Pavnutii Lvovich Chebyshev 给出的。

定理 3.2 (素数定理)

$\lim\limits_{x\to\infty}\pi(x)\cdot\frac{ln(x)}{x}=1$ ♡

从素数基本定理可知 $\pi(x)\approx\frac{x}{ln(x)}$。

第四章 同余

定义 4.1

给定一个正整数 n，如果两个整数 a 和 b 满足 $a-b$ 能够被 n 整除，即 $(a-b)/n$ 得到一个整数，那么就称整数 a 与 b 模 n 同余，记作 $a=b \mod n$。

模 n 同余定义了整数的一个等价关系。

性质

1. 自反性：$a=a \mod n$；
2. 对称性：若 $a=b \mod n$，则 $b=a \mod n$；
3. 传递性：若 $a=b \mod n$，$b=c \mod n$，则 $a=c \mod n$；
4. 同余式相加：若 $a=b \mod n$，$c=d \mod n$，则 $ac=bd \mod n$；
5. 同余式相乘：若 $a=b \mod n$，$c=d \mod n$，则 $ac=bd \mod n$。

定义 4.2 (同余类, Residue class)

通过计算整数模 n 的余数，我们可以把所有整数分成 n 类，记

$$\bar{r}_n=\{mn+r|m\in F\}$$

为模 n 余 r 的同余类（也称剩余类）。

例 4.1 $\bar{3}_10=\{...,-7,3,13,23,...\}$ 为模 10 余 3 的同余类。

在模 n 的上下文比较清楚的情况下，我们常常省略下标 n。在上下文清楚的情况下，我把同余符合直接写成等号。

定义 4.3 (完全剩余系，Complete residue system)

从 $\bar{0},\bar{1},...,n\bar{-}1$ 中各挑一个元素就组成了一个模 n 的完全剩余系 R_n。

$R_n=\{r_0,r_1,...,r_{n-1}\}$

其中，$r_0\in\bar{0},r_1\in\bar{1},...,r_{n-1}\in n\bar{-}1$。

挑出的这个元素称为该同余类的代表元。一个同余类中的元素都可以作为代表元，我们常用的代表元是最小非负的那一个，称为模 n 的最小非负完全剩余系。例如 $R_n=\{0,1,...,n-1\}$，最小非负完全剩余系是我们常用的剩余系。

定义 4.4 (简化最小非负完全剩余系，Reduced residue system)

取一个模 n 的完全剩余系 R_n，取所有和 n 互素的代表元，这些代表元组成一个模 n 的简化剩余系，记为 Φ_n。

在简化剩余系中，代表元取最小的非负的，那么就形成了简化最小非负剩余系。

例 4.2

$\Phi_9 = \{1, 2, 4, 5, 7, 8\}$ 为模 9 的简化最小非负剩余系。

4.1 扩展欧几里得除法

扩展欧几里得除法是在辗转相除法之上的扩展应用，可以解决这样的问题：存在整数 s, t 使得 $(ab) = sa + tb$。

4.2 中国剩余定理

中国剩余定理 (Chinese remainder theorem, CRT)《九章算术》中曾经提到过一个经典的“物不知数”问题:

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何?”

写成数学语言就是求解包括 3 个方程的同余方程组:

$$\begin{cases} x = 2 \mod 3 \\ x = 3 \mod 5 \\ x = 2 \mod 7 \end{cases}$$

先考虑更简单的 2 个同余方程的情况:

命题 4.1 (同余方程个数为 2 的情况)

整数 p 和 q 互素。如下同余方程组:

$$\begin{cases} x = a \mod p \\ x = b \mod q \end{cases}$$

在 $0 \le x < pq$ 范围内有唯一解。

证明:(存在性)由于 p 和 q 互素,所以存在 p_1 和 q_1 满足 $p_1 = p^{-1} \mod q$, $q_1 = q^{-1} \mod p$。令 $y = aqq_1 + bpp_1$，容易验证 y 满足同余方程组。

(唯一性) 假设另一个整数 z 也满足同余方程组。因为 $z = a \mod p$，所以 $y - z$ 是 p 的整数倍。同理，$y - z$ 也是 q 的整数倍。再由于 p 和 q 互素，所以 $y - z$ 是 pq 的整数倍，于是 $z = y \mod pq$。所以在 $0 \le xpq$ 范围内只能 $y = z$，所以解是唯一的。

理解了 2 个同余方程“物不知数”问题之后，我们可以把这个问题推广到多个同余方程的情况，这就是中国剩余定理。

定理 4.1 (中国剩余定理)

正整数 $n_1, n_2, ..., n_k > 1$，并且两两互素。定义 $N = \sum_{i=1}^{k} n_i$。给定正整数 $a_1, ...a_k$，那么同余方程组：

$$\begin{cases} x = a_1 \mod n_1 \\ x = a_2 \mod n_2 \\ \dots \\ x = a_k \mod n_k \end{cases}$$

在 $0 \le x < N$ 范围内有唯一解。

证明：证明过程可以参考 2 个同余方程组的情况。我们可以直接把解写出来。定义 定义 $b_i = \frac{N}{n_i}$。b_i 是除了 n_i 之外的乘积，由于 n_i 两两互素，所以 $c_i = b_i^{-1} \mod n_i$ 存在。

于是定义：$x = \sum_{i=1}^{k} a_i b_i c_i \mod N$ 容易检验，x 就是方程的唯一解。 ♡

命题 4.2

给定正整数 a, b, m, n。如果 $a = b \mod m$，$a = b \mod n$，并且 $(m, n) = 1$，那么 $a = b \mod mn$。 ♠

4.3 欧拉定理

定义 4.5 (欧拉函数)

给定 n 是正整数，欧拉函数 $\phi(n)$ 表示"小于 n 的正整数中和 n 互素的数的个数"。并且：

$$\phi(n) = n \cdot \prod_{2 \le p \le n,\ p \mid n} (1 - \frac{1}{p})$$

♣

知道 n 的素数分解，计算 n 是很容易的。

例 4.3 $\phi(9) = \phi(3 * 3) = 9 * (1 - \frac{1}{3}) = 6$。

例 4.4 模 9 的简化最小非负剩余系中元素个数为 $\phi(9) = 6$

例 4.5 $\phi(100) = \phi(2^2 \cdot 5^2) = 100 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 40$

为了说明欧拉函数是如何计算的，我们先考虑 $n = p^e$ 的情况，其中 p 是素数，e 是正整数。首先求小于等于 n 的正整数个数：在 $1 \le k \le p^e$ 范围内, 如果 $(k, p^e) \ne 1$，只能 k 等于中 p 的倍数。p 的倍数有 $1 \cdot p, 2 \cdot p, ..., (p^{e-1}) \cdot p$，总共 p^{e-1} 个倍数。如果只考

虑小于 $n = p^e$ 的情况，总共 $p^{e-1} - 1$ 个倍数。所以

$$\phi(p^e) = (p^e - 1) - (p^{e-1} - 1) = p^e(1 - \frac{1}{p})$$

对于 n 是一般情况，我们先考虑如下一个引理：

引理 4.1

假设 m 和 n 是两个正整数，并且 $(m, n) = 1$。那么 $\phi(mn) = \phi(m)\phi(n)$。

证明：我们首先构造两个集合，第一个集合是模 mn 的简化最小非负剩余系 Φ_{mn}，第二个集合定义为

$$S = \{(a, b) | a \in \Phi_m, b \in \Phi_n\}$$

其中 Φ_m, Φ_n 分别是模 m, n 的简化最小非负剩余系，S 中的元素是二元组。显然 $|\ \Phi_{mn}\ | = \phi(mn)$，并且显然 $|S| = \phi(m)\phi(n)$。如果我们能证明两个集合之间存在一一映射，那么这两个集合的元素个数也是相同的。于是我们来构造一个映射：

$$f : \Phi_{mn} \to S, f(a) = (a \mod m, a \mod n)$$

证明映射是单射：（反证法）假设 $a, b \in \Phi_{mn}$ 满足 $a \neq b$ 且 $f(a) = f(b)$ 那么 $a = b \mod m, a = b \mod n$。因为 $(m, n) = 1$，所以 $a = b \mod mn$。于是 a, b 是 Φ_{mn} 中的同一个元素，与假设矛盾。

证明映射是满射：给定 $(a, b) \in S$，通过中国剩余定理我们能够证明有唯一解，并且这个唯一解在简化最小非负剩余系 Φ_{mn} 中，所以映射是满射。由此 f 是一一映射，于是 $|\Phi_{mn}| = |S|$。 ♡

定理 4.2 (欧拉定理)

给定正整数 a 和 n 互素，那么就有

$$a^{\phi(n)} = 1 \mod n$$

其中 $\phi(n)$ 是欧拉函数。

证明：考虑简化最小非负剩余系 Φ_n：

$$\Phi_n = \{b_1, b_2, ..., b_{\phi(n)}\}$$

令 $a\Phi_n = \{ab_1, ab_2, ..., ab_{\phi(n)}\}$，即是把 Φ_n 中的每个元素都乘以 a。(我们考虑最小非负剩余系，乘法结果需要 $\mod n$ 取最小非负余数)

观察 $a\Phi_n$ 中的元素，我们有 2 个结论：

1. $a\Phi_n$ 中的每个元素与 n 互素。$(b_i, n) = 1, (a, n) = 1 \Rightarrow (ab_i, n) = 1$。
2. 如果 $i \neq j$，那么 $ab_i \neq ab_j$。（反证法）因为 $(a, n) = 1$，所以 a 逆元存在（在 $\mod n$ 的情况下）。如果 $ab_i = ab_j$，那么等式两端同乘 a^{-1}，可得 $b_i = b_j$，这与集合的定义矛盾。

由此可知 $a\Phi_n$ 就是简化最小非负剩余系，$a\Phi_n = \Phi_n$。

$$\prod_{i=1}^{\phi(n)} b_i = \prod_{i=1}^{\phi(n)} ab_i = a^{\phi(n)} \prod_{i=1}^{\phi(n)} b_i$$

由于 $(b_i, n) = 1$，所以 b_i 逆元存在（在 $\mod n$ 的情况下）。我们可以在同乘逆元，消去 b_i，于是可得：

$$a^{\phi(n)} = 1 \mod n$$

♡

从欧拉定理可以很容易推出费马小定理：

定理 4.3 (费马小定理)

假如 a 是一个整数，p 是一个素数，那么 $a^p - a$ 是 p 的倍数。即是：

$$a^p = a \mod p$$

♡

第五章 素数判定

判断一个数是否为素数，最直观的想法是寻找该数的因子，然而目前尚无有效的分解整数的算法。所以我们需要检测一个整数是否为素数的算法。

5.1 朴素判断素数算法

遍历 N 能否能被从 2 到 $\sqrt{(N)}$ 之间的素数整除。若不能则为素数。

例 5.1 判断 101 是不是素数，只需要判断 101 是否能被 $[2, 10]$ 之间的素数整除，即 101 是否能被 2、3、5、7 整除即可，如果不能，则 101 就是素数。

5.2 费马素性测试

回想一下费马小定理：如果一个数 n 是素数，任取整数 $a \in [2, n-1]$，有 $a^{n-1} = 1 \mod n$ 。

由此，我们可以做费马素性测试：任取整数 $a \in [2, n-1]$，计算并判断 $a^{n-1} \mod n$ 是否为 1。如果不是，那么 n 一定是合数。

当 $a^{n-1} = 1 \mod n$ 的时候，n 一定是素数吗？显然不一定。

例 5.2 例如 $n = 561 = 3 * 11 * 17$。任取 $a \in \Phi_n$，可以通过中国剩余定理证明：$a^{561-1} = 1 \mod 561$。也就是说最小简化剩余系中的每个元素都能通过费马素性测试，然而 561 是一个合数。

这样的合数称为 Carmichael numbers。Carmichael numbers 有无限多。

费马素性测试显然是一个概率性的方法。

5.3 Miller-Rabin

Miller-Rabin 也是概率性的素数检测方法。相对于费马素性测试，大部分人更倾向于使用 Miller-Rabin 方法。

引理 5.1

n 是素数当且仅当 $x^2 = 1 \mod n$ 的根是 ± 1。

注 域上的 2 次多项式最多 2 个根。

如果奇数 n 通过了费马素性测试，即 $a^{p-1}=1$。因为 $a^{(p-1)/2}$ 是平方根，我们进一步检验 $a^{(p-1)/2=\pm 1}$ 是否成立。不过还是有一些数（如 1729）还是能欺骗进一步检验。于是我们可以再加强检验，考虑到 n 是偶数，不妨假设 n 有 s 个为 2 的因子，即 $n=2^s q$，其中 q 是奇数。我们写出一个数的序列：

$$\{a^{2^s q}=a^{n-1}, a^{2^{(s-1)}q}, a^{2^{(s-2)}q}, ..., a^{2^0 q}=a^q\}$$

该序列的每一个数都是前一个数的平方根。如果 n 是一个素数，那么有如下观察结论：

1. 该序列从 1 开始；
2. 要么所有的数字都是 1，要么第一个不为 1 的数字是 -1。

Miller-Rabin 算法随机挑选 $a \in \mathbb{Z}_n$，如果得到的序列不满足以上观察结论，则 n 不是素数。

如果得到的序列满足观察结论，n 也还是有可能是合数，Miller-Rabin 算法就会出错。可以证明，如果 n 是合数，Miller-Rabin 算法出错的概率最多是 $1/4$。如果迭代运行 Miller-Rabin 算法的 k 次，出错的概率小于 $(1/4)^k$。

5.4 AKS

AKS 素数测试（又被称为 Agrawal–Kayal–Saxena 素数测试和 Cyclotomic AKS test）是一个决定型素数测试算法，由三个来自 Indian Institute of Technology Kanpur 的计算机科学家，Manindra Agrawal、Neeraj Kayal 和 Nitin Saxena，在 2002 年 8 月 6 日发表于一篇题为 PRIMES is in P（素数属于 P）的论文。作者们因此获得了许多奖项，包含了 2006 年的哥德尔奖和 2006 年的 Fulkerson Prize。这个算法可以在多项式时间之内，决定一个给定整数是素数或者合数。

5.5 Openssl 如何生成大素数

OpenSSL 使用多种测试来检查素数。首先，他们对数字进行确定性检查，尝试将候选数除以多个小素数，然后进行费马和 Miller-Rabin 素数检验。最初的素数测试会丢弃绝大多数候选素数。每一步测试都增加了它是素数的确定性。

分析一下 openssl 的代码，可见 openssl 素数生成的步骤大致如下：

1. 产生一个指定长度的随机数。
2. 将最低为设为 1，使之为奇数。(大于 2 的素数都是奇数)
3. Do a real quick test to see if it is divisible by small primes (一般是小于 5000 的素数).
4. If it fails here, add 2 and repeat at step 3.
5. Do Fermat's little theorem on it. If it fails, go back to step 1.

6. Do a Miller-Rabin probability test on it (relatively expensive), iterating the number of times suggested for the length of prime in question (like 5 is typically enough).

显然 OpenSSL 的素数测试也是一个概率性的方法。还有较慢的方法可以完全确定测试一个素数，例如 Agrawal–Kayal–Saxena 素性测试。不过从应用的角度来看，openssl 的方法已经非常可靠，因此确定性的素数测试方法很少使用。

例 5.3 利用 openssl 命令行产生一个随机数，判断是否为素数：

```
> openssl rand -hex 256 | xargs openssl prime -hex
```

例 5.4 利用 openssl 命令行产生一个素数：

```
> openssl prime -generate -bits 2048 -hex
```

第 六 章 Sage for Basic Number Theory

例 6.1 判断 $2^(8) + 1$ 是否一个素数。

```
2^(8)+1 in Primes()
```

例 6.2 判断 $2^(2^15) + 1$ 是否一个素数。(非常慢)

```
2^(2^15)+1 in Primes()
```

例 6.3 计算 $51^(2006) \mod 97$。

```
R = Integers(97)
a = R(51)
a^2006
```

例 6.4 得到 2005 之后的下一个素数。

```
next_prime(2005)
```

例 6.5 得到 10 到 20 之间的素数。

```
list(primes(10, 20))
```

参考文献

[1] GEEKSFORGEEKS. Primality Test | Set 3 (Miller–Rabin)[J/OL]. 2018, 0(0):1-1. https://www.geeksforgeeks.org/primality-test-set-3-miller-rabin/.

[2] ZHIHU. 切比雪夫不等式[J/OL]. 2019, 0(0):1-1. https://zhuanlan.zhihu.com/p/41337006.

[3] ZHIHU. Euler theorem[J/OL]. 2020, 0(0):1-1. https://zhuanlan.zhihu.com/p/35060143.

[4] ZHIHU. 中国剩余定理[J/OL]. 2020, 0(0):1-1. https://crypto.stanford.edu/pbc/notes/numbertheory/crt.html.

[5] SAGE. sage for number theory[J/OL]. 2020, 0(0):1-1. https://doc.sagemath.org/html/en/constructions/number_theory.html.