第 5 章　素性检测

在数论及其应用领域，素性检测占据着举足轻重的地位。不仅是数学本身研究的基础，更在加密等安全技术中扮演着核心角色，如 RSA 算法的安全性高度依赖于大素数的生成。因此，高效且准确的素性检测方法对于保障信息安全具有重要意义。

前书中我们已介绍试除法等初等的素性检测算法，本章我们将在此基础上进一步介绍著名的 Fermat 素性检测、Solovay-Stassen 素性检测、Miller-Rabin 素性检测和 Agrawal-Kayal-Saxena 素性检测.

由此我们可以看到，素性检测不仅是数学研究的重要课题，更是现代信息安全体系的基础。从 Fermat 素性检测到 Agrawal-Kayal-Saxena 素性检测，每一种方法的提出都推动了素性检测技术的发展，为实际应用提供了更加高效、准确的解决方案。

本章的知识要点：

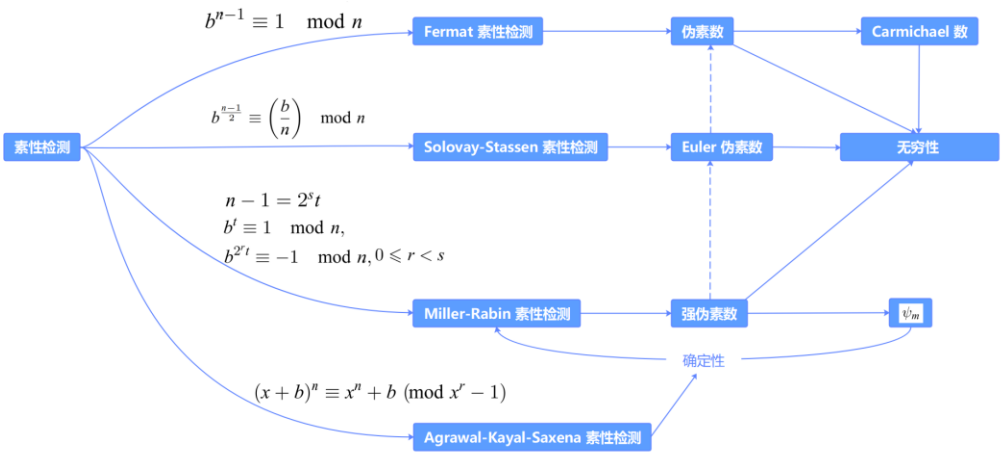

图 5-1 素性检测知识点图谱

5.1 Fermat (费马)素性检测

根据 Fermat 小定理，我们知道：如果 n 是一个素数，则对任意整数 b，（b，n）=1，有

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

由此，我们得到：如果有一个整数 b，（b，n）=1 使得 $b^{n-1} \not\equiv 1 (\mathrm{mod}\, n)$，则 n 是一个合数.

例 5.1.1 因为$2^{14} \equiv (2^4)^3 \cdot 2^2 \equiv 1^3 \cdot 2^2 \equiv 4 \not\equiv 1 \pmod{15}$, 所以 15 是一个合数.

上述说法的否命题不能成立. 事实上，我们有

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

5.1.1 伪素数

定义 5.1.1 设 n 是一个奇合数，如果整数 b，（b，n）=1 使同余方程 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 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 $341=11\cdot 31,\quad 561=3\cdot 11\cdot 17,\quad 645=3\cdot 5\cdot 43$ 都是对于基 b=2 的伪素数，

因为 $2^{340}\equiv 1(\mathrm{mod}\, 341),\quad 2^{560}\equiv 1(\mathrm{mod}\, 561),\quad 2^{644}\equiv 1(\mathrm{mod}\, 645)$.

接下来讨论伪素数的存在性.

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 $n=dq$，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 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 $2^{n-1}\equiv 1(\mathrm{mod}\, n)$.

由于 n 是奇合数，所以我们有因数分解式 $n=dq,\quad 1<d<n,\quad 1<q<n$，

根据引理 5.1.1，我们得到 $2^d-1\mid 2^n-1$，因此 $m=2^n-1$ 是合数.

现在验证：$2^{m-1}\equiv 1(\mathrm{mod}\, m)$.

因为 $2^{n-1}\equiv 1(\mathrm{mod}\, n)$，所以我们可以将 $m-1=2(2^{n-1}-1)$ 写成 $m-1=kn$，

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

$$2^{m-1}\equiv 1(\mathrm{mod}\, m)$$

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 是一个对于基 2 的伪素数，再令

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

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，（（b，n）=1）的伪素数当且仅当 b 模 n 的指数整除 n-1.

(*ii*) 如果 n 是对于基 b_1（（b_1，n）=1）和基 b_2（（b_2，n）=1）的伪素数，则 n 是对于基 b_1b_2 的伪素数.

(*iii*) 如果 n 是对于基 b，（（b，n）=1）的伪素数，则 n 是对于基 b^{-1} 的伪素数.

(*iv*) 如果有一个整数 b，（b，n）=1，使得同余方程 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 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 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 不成立.

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

根据定理 4.1.1，我们有 $ord_n(b)\,|\,n-1$.

反过来，如果 $ord_n(b)\,|\,n-1$，则存在整数 q 使得 $n-1=ord_n(b)q$.

因此，我们有 $b^{n-1}\equiv (b^{ord_n(b)})^q\equiv 1(\mathrm{mod}\, n)$.

（*ii*）因为 n 是对于基 b_1 和基 b_2 的伪素数，所以我们有

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

从而，$(b_1b_2)^{n-1}\equiv b_1^{\,n-1}b_2^{\,n-1}\equiv 1(\mathrm{mod}\, n)$.

故 n 是对于基 b_1b_2 的伪素数.

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

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

故 n 是对于基 b^{-1} 的伪素数.

（*iv*）设 $b_1,\cdots,b_s,b_{s+1},\cdots,b_{\varphi(n)}$ 是模的简化剩余系，其中前 s 个数使得同余方程 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 成立，后 $\varphi(n)-s$ 个数使得同余方程 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 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 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 不成立. 再根据结论（*ii*）和（*iii*），我们有 s 个模 n 不同简化剩余 $bb_1,\cdots,bb_s$ 使得同余方程 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 不成立.

因此，$s\le\varphi(n)-s$，或者 $\varphi(n)-s\ge\dfrac{\varphi(n)}{2}$. 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 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 不成立.

注：定理 5.1.2（*iv*）告诉我们，对于大奇数，如果有一个整数 b，（b，n）=1 使得同余方程 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 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 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 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,满足同余方程 $b^{n-1} \equiv 1 (\mathrm{mod}\, n)$ 的 n 是合数的可能性小于 50%.

5.1.2 Fermat 素性检测方法

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，$0 < b_1 < n$，利用广义欧几里得除法计算 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 $b_1^{n-1} (\mathrm{mod}\, n)$，看看同余方程 $b_1^{n-1} \equiv 1 \pmod{n}$是否成立.

如果 $b_1^{n-1} \equiv 1 \pmod{n}$不成立，则 n 不是素数；

如果 $b_1^{n-1} \equiv 1 (\mathrm{mod}\, n)$ 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, $0 < b_2 < n$，利用广义欧几里得除法计算 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 $b_2^{n-1} (\mathrm{mod}\, n)$，看看同余方程 $b_2^{n-1} \equiv 1 (\mathrm{mod}\, n)$ 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，…，直至第 t 步.

随机选取整数 b_t, $0 < b_t < n$，利用广义欧几里得除法计算 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 $b_t^{n-1} (\mathrm{mod}\, n)$，看看同余方程 $b_t^{n-1} \equiv 1 (\mathrm{mod}\, n)$ 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）：

给定奇数 $n \geq 3$ 和安全参数 t

1. 随机选取整数 $b, 2 \leq b \leq n-2$;
2. 计算 $r = b^{n-1} (\mathrm{mod}\, n)$；
3. 如果 $r \neq 1$，则 n 是合数;
4. 重复上述步骤 t 次

5.1.3 Carmichael 数

本节讨论使得 Fermat 素性检测算法无效的整数.

定义 5.1.2 合数 n 为 **Carmichael** 数，如果对所有的正整数 $b,(b,n)=1$ 都有同余方程 $b^{n-1}\equiv 1(\mathrm{mod}\, n)$ 成立.

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

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

从而

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

因此，我们有

$$b^{560}\equiv 1(\mathrm{mod}\, 561).$$

定理 5.1.3 设 n 是一个奇合数.

(*i*) 如果 n 被一个大于 1 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

$$p_i-1\,|\,n-1, 1\le i\le k.$$

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 数的个数大于等于 $n^{2/7}$.

5.2 Solovay-Stassen (S-S)素性检测

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

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

对任意整数 b 成立.

因此，如果存在整数 $b,(b,n)=1$，使得

$$b^{(n-1)/2} \neq (\frac{b}{n}) (\mathrm{mod}\, n),$$

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：

$$2^{170} \equiv 1 (\mathrm{mod}\, 341)$$

以及

$$(\frac{2}{341}) = (-1)^{(341^2-1)/8} = -1$$

因为

$$2^{170} \not\equiv (\frac{2}{341}) (\mathrm{mod}\, 341)$$

所以 341 不是一个素数.

5.2.1 Euler 伪素数

定义 5.2.1 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：

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

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：$2^{280} \equiv 1 \pmod{561}$以及$\left(\frac{2}{561}\right)=(-1)^{(561^2-1)/8}=1$.

因为 $2^{280} \equiv \left(\frac{2}{561}\right) \pmod{561}$,

所以 561 是一个对于基 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.

证 设 n 是对于基 b 的 Euler 伪素数，则我们有

$$b^{(n-1)/2} \equiv (\frac{b}{n}) (\mathrm{mod}\, n).$$

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

$$b^{n-1} \equiv (b^{(n-1)/2})^2 \equiv (\frac{b}{n})^2 \equiv 1 (\mathrm{mod}\, n).$$

因此，n 是对于基 b 的伪素数.

定理 5.2.1 的逆不成立，即不是每个伪素数都是 Euler 伪素数.

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

5.2.2 S-S 素性检测方法

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 $n \geq 3$ 和安全参数 t.

1. 随机选取整数 $b, 2 \leq b \leq n-2$；
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 $s = (\frac{b}{n})$；
5. 如果 $r \neq s$，则 n 是合数；
6. 上述过程重复 t 次.

5.3 Miller-Rabin (M-R)素性检测

5.3.1 强伪素数

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

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

因此，如果有同余方程

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

则如下同余方程至少有一个成立：

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

定义 5.3.1 设 n 是一个奇合数，且有表示式 $n-1 = 2^s t$，其中 t 为奇数. 设整数 b 与

n 互素. 如果整数 n 和 b 满足条件 $b^t \equiv 1(\mathrm{mod}\, n)$,或者存在一个整数 $r, 0 \le r < s$ 使得 $b^{2^r t} \equiv -1(\mathrm{mod}\, n)$，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 $2^{2046/2} \equiv (2^{11})^{93} \equiv (2048)^{93} \equiv 1(\mathrm{mod}\, 2047)$

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.

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 $2^{n-1} \equiv 1(\mathrm{mod}\, n)$.

由此得到 $2^{n-1} - 1 = nk$，对某整数 k，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 $2^n = (2^n - 1) + 1 = m + 1 \equiv 1(\mathrm{mod}\, m)$，我们有

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

此外，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 2 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 的强伪素数.

定理 5.3.2 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 5.3.3 设 n 是一个奇合数，则 n 是对于基 $b,\ \ 1 \le b \le n-1$ 的强伪素数的可能性至多为 25%.

5.3.2 M-R 素性检测方法

现在，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 $n \ge 3$ 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 $b,\ \ 2 \le b \le n-2$；

2. 计算 $i = 0, r \equiv b^t \pmod{n}$；

3. 如果 $r = 1$ 或 $r = n-1$，则通过检测，n 可能为素数;

   否则，有 $r \neq 1$ 以及 $r \neq n-1$，我们计算 $i = i+1, r = r^2 \pmod{n}$；

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 可能为素数;

   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？

以ψ_m表示对于前 m 个最小素数 2, 3, … , 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.

Pomerance 和 Jaeschke 等人给出了ψ_m，$1 \leq m \leq 8$ 的具体值和ψ_m，$9 \leq m \leq 11$ 的对应上界. Zhang 进一步降低ψ_m，$9 \leq m \leq 11$ 的上界并猜想这些新上界就是其确值, 还给出了ψ_m，$12 \leq m \leq 20$ 的猜想. 后来, 2014 年, Jiang 和 Deng 给出了ψ_m，$9 \leq m \leq 11$ 猜想的证明, 2017 年 Sorenson 和 Webster 给出了ψ_m，$12 \leq m \leq 13$ 猜想的证明.

关于ψ_m，$1 \leq m \leq 13$ 的确定值.

ψ_1=2047=23·89;

ψ_2=1373653=829·1657;

ψ_3=25326001=2251·11251;

ψ_4=3215031751=151·751·28351;

ψ_5=2152302898747=6763·10627·29947;

ψ_6=3474749660383=1303·16927·157543;

ψ_7=ψ_8=341550071728321=10670053·32010157;

ψ_9=ψ_{10}=ψ_{11}=3825123056546413051=149491·747451·34233211;

ψ_{12}=318665857834031151167461=399165290221·798330580441;

ψ_{13}=3317044064679887385961981=1287836182261·2575672364521.

关于ψ_m，$14 \leq m \leq 20$ 的猜想.

ψ_{14}=6003094289670105800312596501=54786377365501·109572754731001;

ψ_{15}=592763610755955732634463301 01=172157429516701·344314859033401;

ψ_{16}=ψ_{17}=564132928021909221014087501701=531099297693901·1062198595387801;

ψ_{18}=ψ_{19}=154326786444342061687677640751301=27778299663977101·55556599327954201;

ψ_{20}> 10^{36}.

5.4 Agrawal–Kayal–Saxena (A-K-S)素性检测

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

$$(x-a)^p \equiv (x^p - a) \pmod{p}.$$

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

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

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

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

则 n 是一个素数的方幂.