第 4 章：公钥密码学

4.1 数论基础

赵俊舟

junzhou.zhao@xjtu.edu.cn

2025 年 3 月 22 日

目录

目录

数论简介

- 数论主要研究整数集合 $\mathbb{Z}$ 的性质，尤其关注正整数集合 $\mathbb{Z}^+$

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \qquad \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$$

- 按数的可分性，一个正整数总能分为以下三类：
  - 单位元：1
  - 素数：$2, 3, 5, 7, 11, 13, 17, 19, \ldots$
  - 合数：$4, 6, 8, 9, 10, 12, 14, 15, \ldots$
- 一个正整数 $p > 1$ 是素数当且仅当它只有因子 1 和 p。
- 素数是数论的核心，因为所有整数 $n > 1$ 都可以进行素因子分解：

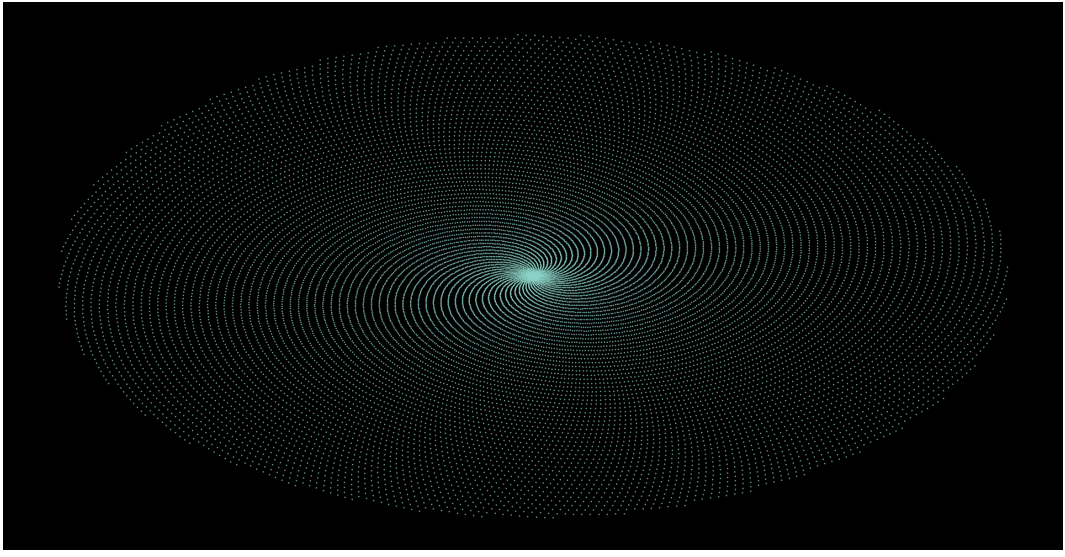
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

其中 $p_1 < p_2 < \cdots < p_k$ 为素数，$\alpha_1, \alpha_2, \ldots, \alpha_k$ 为正整数。

关于素数的研究问题

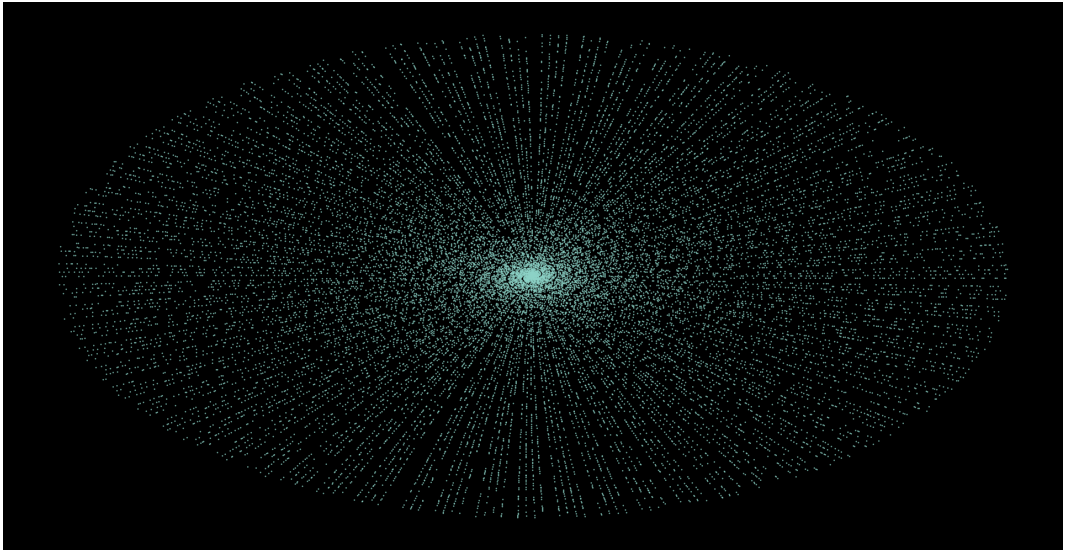
- 数论已经被研究了 2000 多年，关于素数仍有许多问题悬而未决，例如
  - Q1: 素数的分布情况
    做出关键贡献的学者：欧几里得（300BC）、黎曼（1859）、阿达马和普桑（1896）等
  - Q2: 孪生素数的分布情况
    做出关键贡献的学者：哥德巴赫（1742）、陈景润（1966）、张益唐（2013）等
  - Q3: 等差素数列的分布情况
    做出关键贡献的学者：陶哲轩（2007）等
- 数论中的问题通常很容易表述，但这些问题往往很难解决。

Q1: 素数的分布（前 2 万个整数的分布）



$x \to (x\cos(x), x\sin(x))$

Q1: 素数的分布（前 2 万个素数的分布情况）



$x \to (x\cos(x), x\sin(x))$

Q1: 素数的分布

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Q1: 素数的分布

- 欧几里得在其著作《几何原本》中证明有无穷多个素数。
- 最小的素数是 2，目前发现的最大素数是 $2^{136,279,841}-1$（发现于 2024 年 10 月 21 日），共 $41,024,320$ 位数，比上一个发现的最大素数（2018 年）多 $1,600$ 位。
- 用 $\pi(x)$ 表示不超过 x 的素数个数，欧几里得定理其实说明

$$\pi(x) \to \infty \quad \text{as} \quad x \to \infty$$

- 更准确的结论是素数定理，由阿达马（1896）等人证明

$$\pi(x) \sim \frac{x}{\ln x}$$

- 可以近似认为，在区间 $[1, x]$ 碰到一个素数的概率为 $1/\ln x$；或者说，在 x 附近，每 $\ln x$ 个整数中有一个素数。

Q1: 素数的分布

- 如果黎曼猜想为真，那么素数定理可以进一步精确为

$$\pi(x) = \int_2^x \frac{\mathrm{d}t}{\ln t} + O(xe^{-c\sqrt{\ln x}})$$

- 黎曼猜想是复分析中的一个著名猜想：复平面上 ζ 函数

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s = \sigma + it, \sigma, t \in \mathbb{R}$$

  满足 $0 < Re(s) < 1$ 的所有非平凡零点都位于 $Re(s) = 1/2$ 上，即满足 $\zeta(\rho) = 0$ 的点 ρ 具有形式 $\rho = 1/2 + it$。

- 黎曼猜想是克雷数学研究所于 2000 年提出的 7 个千禧年大奖难题之一，每个难题奖金 100 万美元。

Q2: 孪生素数的分布

- 孪生素数指相差为 2 的素数对，例如 $(3,5),(5,7),(11,13)$ 等。目前发现的最大孪生素数为（发现于 2016 年）：
$$2,996,863,034,895 \times 2^{1,290,000} \pm 1$$
- 用 $\pi_2(x)$ 表示不超过 x 的孪生素数数量，孪生素数猜想说明
$$\pi_2(x) \to \infty \quad \text{as} \quad x \to \infty$$
- 如果素数分布服从独立同分布，那么
$$\pi_2(x) \sim \frac{x}{(\ln x)^2}$$
- 素数分布显然不独立，哈代和利特尔伍德猜想：
$$\pi_2(x) = 2\prod_{p\geq 3}\frac{p(p-2)}{(p-1)^2}\int_2^x \frac{\mathrm{d}t}{(\ln t)^2} \approx 1.320323632\int_2^x \frac{\mathrm{d}t}{(\ln t)^2}$$

Q2: 孪生素数的分布

- 陈景润利用筛法证明：有无穷多个整数对 $(p, p+2)$ 其中 p 为素数，$p+2$ 是不超过 2 个素数的乘积（1966–1973）。
- 张益唐证明：间距小于 7000 万的素数对有无穷多个（2013）。
- 仅仅过了几个月，素数对之差被缩小为 246。
- 差是 2 的素数对为孪生素数对，差是 4 的素数对为表亲素数对，差是 6 的素数对为性感素数对……。
- 波里尼亚克猜想（也称为弱孪生素数猜想，1849）：存在无穷多个素数对 $(p, p+2k), k = 1, 2, 3, \ldots$。

Q3: 等差素数列的分布

- 等差素数列是如下形式的素数数列

$$p, p+d, p+2d, \ldots, p+kd$$

其中 p 是首项，d 是公差，$p+kd$ 是尾项。例如 $(3,5,7)$，$(5,11,17,23,29)$。

- 目前发现的最长等差素数列为（记为 AP27，2009）

$$224,584,605,939,537,911 + 81292139 \cdot 23\# \cdot k \quad k = 0, \ldots, 26$$

其中 $23\#$ 是不超过 23 的素数的乘积。

- 格林-陶定理（2004）：存在任意长的等差素数列。
- 陶哲轩等人于 2006 年获菲尔兹奖，等同于数学诺贝尔奖。
- 目前仍不清楚怎样去发现任意长等差素数列，也不清楚等差连续素数列的存在情况。

关于素数的参考资料

- Great Internet Mersenne Prime Search:
  `https://www.mersenne.org`
- The largest known simultaneous primes:
  `http://primerecords.dk/simultprime.htm`
- 目前发现的最长等差素数列:
  `http://primerecords.dk/aprecords.htm`
- 目前发现的最长等差连续素数列:
  `http://primerecords.dk/cpap.htm`

目录

目录

费马定理

定理 (费马定理 Fermat's Little Theorem)

若 p 是素数，a 是正整数且不能被 p 整除，则有

$$a^{p-1} \equiv 1 \pmod{p}$$

证明.

- 考虑小于 p 的正整数集合 $R \triangleq \{1, \ldots, p-1\}$。用 a 乘所有元素并对 p 取模，得到 $X \triangleq \{a \bmod p, \ldots, a(p-1) \bmod p\}$。
- $\gcd(a, p) = 1 \Rightarrow X$ 的元素都不为 0 且互不相等 $\Rightarrow R = X$。
- 将两个集合中所有元素相乘并对 p 取模，得到

$$a \times 2a \times \cdots \times a(p-1) \equiv 1 \times 2 \times \cdots \times (p-1) \pmod{p}$$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

因为 $(p-1)!$ 和 p 互素，可以消去，从而得到费马定理。 □

费马定理

例 ($a = 7, p = 19$)

$a^{p-1} \bmod p = 7^{18} \bmod 19$

$7^2 = 49 \equiv 11 \pmod{19}$, $7^4 = 121 \equiv 7 \pmod{19}$

$7^8 = 49 \equiv 11 \pmod{19}$, $7^{16} = 121 \equiv 7 \pmod{19}$

$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$

推论 (费马定理等价形式)

若 p 是素数且 a 是任意正整数，则 $a^p \equiv a \pmod{p}$。

注意，这里不要求 a 与 p 互素。

例 ($a = 10, p = 5$)

$a^p = 10^5 \equiv 0 \pmod{5} = a \pmod{p}$

目录

欧拉函数（Euler's Totient Function）

定义 (欧拉函数)

欧拉函数，记作 $\phi(n)$，是比 n 小且与 n 互素的正整数的个数。

习惯上约定 $\phi(1) = 1$。

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

欧拉函数

性质

p, q 是素数且 $p \neq q$，则 $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$。

证明.

- 考虑集合 $\{1, \ldots, pq-1\}$，其中不与 pq 互素的数的集合为 $\{p, 2p, \ldots, (q-1)p\}$ 和 $\{q, 2q, \ldots, (p-1)q\}$。
- 因为 p 和 q 互素，所以这两个集合无交集：假设存在 $1 \leq i \leq q-1$ 和 $1 \leq j \leq p-1$，满足 $ip = jq$，两边模 p 得 $jq \bmod p = 0$，因为 p, q 为素数，故 $jq \bmod p \neq 0$，所以这两个集合不可能有交集。
- 两个集合共有 $p-1+q-1$ 个整数，所以

$$\phi(n) = (pq-1) - (p-1+q-1) = (p-1)(q-1) = \phi(p)\phi(q)$$

□

欧拉函数

性质

p 是素数，则 $\phi(p^k) = p^{k-1}(p-1)$。

性质

正整数 n 的素因子分解为 $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$，则

$$\phi(n) = \prod_{i=1}^{t} p_i^{k_i - 1}(p_i - 1)$$

- 对一个正整数 n 进行素因子分解是很困难的事情，因此目前尚不存在通用的计算 $\phi(n)$ 的高效算法。
- 数论中可以证明，计算一个正整数 n 的欧拉函数 $\phi(n)$ 等同于对 n 进行素因子分解。

欧拉定理（Euler's Theorem）

定理 (欧拉定理)

对于任意互素的正整数 a 和 n，有 $a^{\phi(n)} \equiv 1 \pmod{n}$。

证明.

- 令小于 n 且与 n 互素的正整数构成集合 $R \triangleq \{x_1, \ldots, x_{\phi(n)}\}$，然后将 a 与 R 中的每个元素相乘然后模 n，得到集合 $X \triangleq \{ax_1 \bmod n, \ldots, ax_{\phi(n)} \bmod n\}$。
- 由于

1. $\gcd(a, n) = 1 \wedge \gcd(x_i, n) = 1 \Rightarrow \gcd(ax_i, n) = 1 \Rightarrow \gcd(ax_i \bmod n, n) = 1$，即 X 中的每个元素与 n 互素；
2. X 中没有重复元素：若 $ax_i \bmod n = ax_j \bmod n$，则 $x_i = x_j$。

- 所以，X 其实是 R 的一个排列，$X = R$。

欧拉定理（Euler's Theorem）

- 把两个集合中的元素乘起来

$$\prod_{i=1}^{\phi(n)}(ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)}(ax_i \bmod n) \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

因为 $\gcd(\prod_{i=1}^{\phi(n)} x_i, n) = 1$，所以利用模运算的性质得到

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

从而得到欧拉定理。 □

欧拉定理（Euler's Theorem）

- 费马定理是欧拉定理当 n 为素数时的一个特殊情况。
- 例如，$a = 3, n = 10, \phi(n) = 4, a^{\phi(n)} = 3^4 \equiv 1 \pmod{10}$

推论

n 是素数，对任意正整数 a，有 $a^{\phi(n)+1} \equiv a \pmod{n}$。

注意

上述推论要求 n 是素数，如果 n 不为素数，考虑下例

- $a = 2, n = 4$，此时 $\phi(n) = 2$。
- $2^3 \bmod 4 = 8 \bmod 4 = 0$，而 $2 \bmod 4 = 2$，两者不相等。

目录

目录

素性测试

- 密码学中常常需要寻找大素数。
- 传统的方法是用试除法，即依次除小于该数平方根的所有整数，这种方法只对较小的数有用。
- 可以采用基于素数特性的统计素性测试方法：
  - 其中所有的素数都满足素数特性。
  - 但是有一些被称为伪素数的合数也满足素数特性。
- 也可使用一种较慢的确定性素性测试方法。

奇整数的表示

奇整数的表示

$n \geq 3$ 的奇整数可表示为 $n-1=2^k q$，其中 $k>0$，q 是奇数。

证明.

注意到 $n-1$ 是偶数，可以用 2 去除 $n-1$，直到所得结果为奇数，此处共做了 k 次除法。 □

例

$n=7: n-1=2\times 3$
$n=9: n-1=2^3\times 1$
$n=13: n-1=2^2\times 3$

素数的两个性质

性质 (性质一)

若 p 是素数，a 是小于 p 的正整数，则 $a^2 \bmod p = 1$ 当且仅当 $a \bmod p = 1$ 或 $a \bmod p = p - 1$。

证明.

- $\Rightarrow$: 由 $a^2 \bmod p = 1$ 知 $p|(a^2 - 1)$ 即 $p|(a+1)(a-1)$。由于 p 是素数，故只能是 $p|(a+1)$ 或 $p|(a-1)$，得 $a \bmod p = 1$ 或 $a \bmod p = -1 \bmod p = p - 1$。
- $\Leftarrow$: 当 $a \bmod p = 1$ 或 $a \bmod p = p - 1$ 时，有 $p|(a-1)$ 或 $p|(a+1)$，所以 $p|(a+1)(a-1)$，即 $p|(a^2 - 1)$，从而得到 $a^2 \bmod p = 1$。

某些合数也可能成立。$p = 4$，当 $a = 1$ 或 3 时，$a^2 \bmod p = 1$

素数的两个性质

性质 (性质二)

设 p 是大于 2 的素数，有 $p-1=2^k q$，$k>0$，q 是奇数。设 a 是小于 p 的整数，则以下两个结论必然有一个成立：

- $a^q \bmod p = 1$。
- 在整数 $a^q \bmod p, a^{2q} \bmod p, \ldots, a^{2^{k-1}q} \bmod p$ 中存在一个数为 $p-1$。即存在 $0 \le j \le k-1$，满足 $a^{2^j q} \bmod p = p-1$。

例

例如 $p=29$ 为素数，$29-1=2^2\times 7$。取 $a=2$，则 $a^q \bmod p = 2^7 \bmod 29 = 12$，$a^{2q} \bmod p = 2^{14} \bmod 29 = 28$，满足第二个结论，故该性质对素数 29 成立。

素数的两个性质

证明.

- 因为 p 是素数，则由费马定理可知 $a^{p-1} \equiv 1 \pmod{p}$。由于 $p-1 = 2^k q$，则 $a^{2^k q} \bmod p = 1$。
- 观察下述数列：

$$a^q \bmod p, a^{2q} \bmod p, \ldots, a^{2^{k-1}q} \bmod p, a^{2^k q} \bmod p = 1$$

这个数列最后一个数为 1，而且每个数为前一个数的平方。

- 最后一个数为 1，那么前一个数只能为 1 或 $p-1$。如果倒数第二个数为 1，则它前一个数只能为 1 或 $p-1$；依次类推。
- 所以，这个数列要么全是 1，即第一个数为 1；要么数列中某个数为 $p-1$，从这个数之后全为 1。

从而证明了性质二。 □

目录

Miller-Rabin 素性测试

Miller-Rabin 素性测试

- 若 n 为素数，$n-1=2^k q$，$a \in \{1,\ldots,n-1\}$，那么数列

$$a^q \bmod n, a^{2q} \bmod n, \ldots, a^{2^{k-1}q} \bmod n$$

要么第一个数为 1，要么数列中某个数为 $n-1$。

- 如果不满足上一条，那么 n 必为合数。
- 注意，如果上述条件满足，也不一定推出 n 一定为素数。

例

例如，$n=2047=23\times 89$，则 $n-1=2\times 1023$。计算 $2^{1023} \bmod 2047=1$，所以虽然 $n=2047$ 满足条件，但不是素数。

Miller-Rabin 素性测试

算法 1: PrimeTest(n)

输入: 奇整数 n
输出: n 是不是素数

1 找出整数 k, q，其中 $k > 0$，q 是奇数，使 $n - 1 = 2^k q$。
2 随机选取整数 $a \in \{1, \ldots, n-1\}$。
3 **if** $a^q \bmod n = 1$ **then**
4 **return** 可能是素数。
5 **for** $j = 0$ to $k - 1$ **do**
6 **if** $a^{2^j q} \bmod n = n - 1$ **then**
7 **return** 可能是素数。
8 **return** 是合数。

重复使用 Miller-Rabin 算法

- 如果返回 ‘‘合数’’，则这个数必为合数。否则可能为素数。
- 有结论：给定一个非素奇数 n 和一个随机整数 $a, 1 < a < n-1$，程序 PrimeTest 误报的概率小于 $1/4$（即当程序返回 “n 可能是素数” 时，误报的概率小于 $1/4$）。
- 因此，如果选择 t 个不同 a 进行测试，则它们都能通过测试并产生误报的概率小于 $(1/4)^t$。
- 对随机选取的 a，重复调用 PrimeTest(n)，如果某时刻 PrimeTest 返回 ‘‘合数’’，则 n 一定不是素数。
- 若 PrimeTest 连续 t 次返回 ‘‘可能是素数’’，当 t 足够大时，可以相信 n 是素数。

Miller-Rabin 素性测试举例

例 (考虑素数 $n = 29$)

- $n - 1 = 28 = 2^2 \times 7 = 2^k q$
- 选取 $a = 2$
  - $a^q \bmod n = 12$，$a^{2q} \bmod n = 28$，返回 “有可能是素数”
- 选取 $a = 10$
  - $a^q \bmod n = 17$，$a^{2q} \bmod n = 28$，返回 “有可能是素数”

例 (考虑合数 $n = 13 \times 17 = 221$)

- $n - 1 = 220 = 2^2 \times 55 = 2^k q$
- 选取 $a = 5$
  - $a^q \bmod n = 112$
  - $a^{2q} \bmod n = 168$。返回 “合数”

目录

确定性素性判定方法 AKS

- 2002 年以前，没有高效的方法证明一个大数的素性，包括 Miller-Rabin 算法在内，所有在用算法给出的都是概率性结果。
- 2002 年 Agrawal, Kayal 和 Saxena 给出了一个相对简单的确定性算法 AKS，可以有效判定一个大数是否为素数，但是看上去没有 Miller-Rabin 算法快，因此没有代替古老的概率算法。

素数的分布

- 由数论中的素数定理可知，n 附近的素数分布情况为平均每 $\ln n$ 个整数中有一个素数。平均而言，在找到一个素数之前必须测试约 $\ln n$ 个整数。
- 偶数肯定不是素数，因此需要测试 $0.5 \ln n$ 个整数。例如，若要找 2200 左右的素数，则约需要 $0.5 \ln 2200 = 69$ 次测试。
- 这只是个平均值，在数轴上的某些位置，素数非常密集，而在其他有些位置，素数非常稀疏。
  - 两个相邻的奇数 $1,000,000,000,061$ 和 $1,000,000,000,063$ 都是素数。
  - 而 $1001! + 2, 1001! + 3, \ldots, 1001! + 1000, 1001! + 1001$ 这 1000 个连续的整数都是合数。

目录

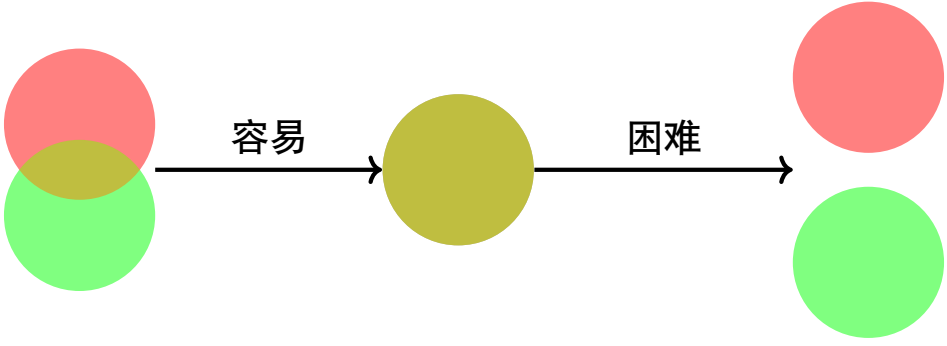
目录

单向函数

单向函数（One-way Function）

函数 f 若满足下列条件，则称 f 为单向函数：

1. 对于所有属于 f 定义域的任一 x，容易计算 $y = f(x)$；
2. 对于几乎所有属于 f 值域的任一 y，求得 x 使 $y = f(x)$，在计算上不可行。



离散对数问题（Discrete Logarithm Problem, DLP）

- 给定素数 p 和整数 $a \in \{1, 2, \ldots, p-1\}$。
- 若给定整数 x，求 $y = a^x \bmod p$ 很容易。
- 但是若给定 y 求 x，则为离散对数问题。
- 目前最快方法需要

$$L(p) = \exp\{(\ln p)^{1/3}(\ln \ln p)^{2/3}\}$$

次运算。

- 例如，当 $p = 512$ 位时，$L(p) \approx 2^{256} \approx 10^{77}$，计算上不可行。
- The discrete logarithm problem is belived to be extremely hard, and no efficient solution is known at this point.

因数分解问题（Factoring Problem, FAC）

- 给定大素数 p 和 q，求 $n = p \times q$，只要一次乘法。
- 给定 n，求 p 和 q，即为因数分解问题，最快方法需要 $\exp\{c\sqrt{\ln n \ln\ln n}\}$ 次运算，其中 c 为大于 1 的正整数。
- The problem of computing $\phi(n)$ is equivalent to factoring n, in that an efficient algorithm for one problem implies an efficient algorithm for the other.
- It remains an interesting open problem to relate (in either direction) the hardness of the discrete logarithm problem to that of the factoring problem.

目录

指数函数

- 令 $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$，$p$ 为素数，则 $\mathbb{Z}_p^*$ 及其上面的模 p 乘法运算构成有限群 $G = (\mathbb{Z}_p^*, \times_p)$。
- 令 $g \in \mathbb{Z}_p^*$ 为群中任意元素，$g^x \bmod p$ 称为**指数函数**。
- 称序列 $\langle g \rangle \triangleq \{g^0, g^1, g^2, \ldots\}$ 为 g **产生的序列**。
- 因为 $\mathbb{Z}_p^*$ 是有限群，$\langle g \rangle$ 必重复，为周期序列。
- 当存在最小正整数 T，使得 $g^T \equiv 1 \pmod{p}$ 时，称 T 为 g 在 $\mathbb{Z}_p^*$ 中的**阶**（也称为**序**或**周期**），记为 $order(g) = T$。
- 根据 Lagrange 定理，循环群中子群的阶必定整除群的阶。
- 因此，$\mathbb{Z}_p^*$ 中元素 g 的阶必定整除 $p-1$，即 $order(g) | order(G)$

指数函数的特性：周期性（$a^x \bmod 19$）

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

指数函数的特性：本原元

定义 (本原元)

若 $g \in \mathbb{Z}_p^*$ 的阶为 $order(g) = p - 1$，则称 g 为模 p 的本原元。

- 本原元也称为素根或原根。
- 当 g 为模 p 运算的本原元时，由 g 产生的序列 $\langle g \rangle$ 具有最大周期（安全性高）。
- 对于所有素数 p，其本原元必定存在。
- 当 g 为模 p 的本原元且 a 与 $p - 1$ 互素，则 $g^a \bmod p$ 也为模 p 本原元。
- 模 p 的本原元个数为 $\phi(p - 1)$。

指数函数的特性：本原元

例 (本原元)

- $p = 11, g = 2, \phi(p-1) = \phi(10) = 4$, 即存在 4 个模 11 本原元。
- 若 $g = 2$ 为模 p 本原元，则 $2^1 \bmod 11 = 2$，$2^3 \bmod 11 = 8$，$2^7 \bmod 11 = 7$，$2^9 \bmod 11 = 6$ 均为模 11 本原元。
- 找到一个本原元后可以很容易找到所有本原元，问题是如何找到第一个本原元。

快速指数运算

- 如果 x 是一个大整数，如何快速计算 g^x？需 $x-1$ 次乘法。
- 将 x 写为二进制形式：

$$x = (x_{n-1} \cdots x_0) = \sum_{i=0}^{n-1} x_i 2^i = \sum_{i:x_i=1} 2^i$$

所以

$$g^x = g^{\sum_{i:x_i=1} 2^i} = \prod_{i:x_i=1} g^{2^i}$$

- $g^{11} = g^{(1011)} = g^8 \cdot g^2 \cdot g$, $g^{23} = g^{(10111)} = g^{16} \cdot g^4 \cdot g^2 \cdot g$
- 需要 $n-1$ 次平方及 $w(x)-1$ 次乘法，$w(x)$ 为 x 二进制串中 1 的个数。
- 平均而言，$w(x) = n/2$，因此平均需要 $1.5n-2$ 次乘法。

快速指数运算

```
long FastExp(long g,long n){
  long base = g;
  long result = 1;
  while(n!=0){
    if((n&1) == 1) result *= base;
    base *= base;
    n >>= 1;
  }
  return result;
}
```

目录

计算乘法逆元

- 如果 $ax \bmod n = 1$，那么 $x = a^{-1} \bmod n = ?$
- 根据欧拉定理：若 $\gcd(a, n) = 1$，则 $a^{\phi(n)} \bmod n = 1$。
- 因此，$a^{-1} = a^{\phi(n)-1} \bmod n$。
- 如果 $\phi(n)$ 已知，则 a 的逆元可以用快速指数运算法求得。
- 如果 n 是素数，则 $\phi(n) = n - 1$，所以 $x = a^{n-2} \bmod n$。
- 如果 $\phi(n)$ 未知，可以用扩展 Euclid 算法来求逆。

在 $\mathrm{GF}(2^n)$ 中求逆元

- 因为除了 0，$\mathrm{GF}(2^n)$ 中每个元素都与素多项式 $p(x)$ 互素，所以 $\phi(p(x)) = 2^n - 1$。
- 所以 $a^{-1} = a^{\phi(p(x))-1} \bmod p(x) = a^{2^n-2} \bmod p(x)$。

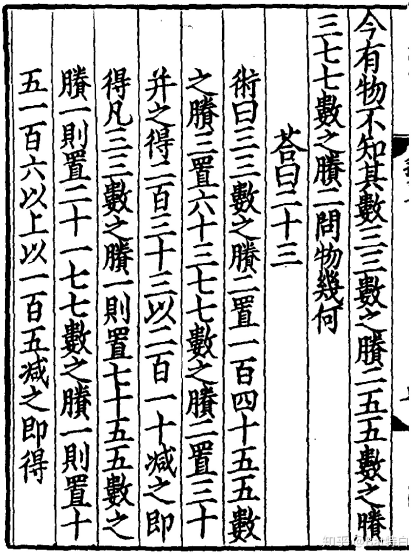
例

在 $\mathrm{GF}(2^3)$ 中，$a = 100$，$p(x) = 1011$，则 $a^{-1} = a^{\phi(x)-1} \bmod p(x) = a^{2^3-2} \bmod p(x) = 100^6 \bmod 1011 = 111$。

目录

中国余数定理 Chinese Remainder Theorem (CRT)

- 也称为“孙子定理”。
- 一元线性同余问题最早可见于中国南北朝时期（公元 5 世纪）的数学著作《孙子算经》中的“物不知其数”问题。
- 中国余数定理说明某一范围内的整数可通过它对两两互素的整数取模所得的余数来重构。


今有物不知其數三三數之賸二五五數之賸
三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五數
之賸三置六十三七七數之賸二置三十
并之得二百三十三以二百一十減之即
得凡三三數之賸一則置七十五五數之
賸一則置二十一七七數之賸一則置十
五一百六以上以一百五減之即得

举例：如何由余数重构整数

例

- $\mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$ 中的 10 个整数可通过它们对 2 和 5（10 的素因子）取模所得的两个余数来重构。
- 假设数 x 的余数 $r_2 = 0$ 且 $r_5 = 3$，即 $x \bmod 2 = 0$，$x \bmod 5 = 3$
- 则 x 是 $\mathbb{Z}_{10}$ 中的偶数且被 5 除余 3，唯一解 $x = 8$。

CRT 的几种表述形式

令 $n_1, \ldots, n_k$ 两两互素，$n = \prod_{i=1}^{k} n_i$，则以下两种表述等价：

表述一

$\mathbb{Z}_n$ 中的任一整数 $a \in \mathbb{Z}_n$ 都对应一个 k 元组 $(x_1, \ldots, x_k)$，其中 $x_i = a \bmod n_i$，$i = 1, \ldots, k$。

表述二

一元线性同余方程组

$$\begin{cases} x \equiv x_1 \pmod{n_1} \\ x \equiv x_2 \pmod{n_2} \\ \cdots \\ x \equiv x_k \pmod{n_k} \end{cases}$$

在 $\mathbb{Z}_n$ 中有一个公共解 x。

CRT 的作用

- 模数 n 很大时，模 n 的运算可以转换为模较小的数 n_i 上的运算，事先需分解 $n = n_1 \times \cdots \times n_k$。
- $\mathbb{Z}_n$ 中的算术运算可以转换为 k 元组上的算术运算。若

$$A \leftrightarrow (a_1, \ldots, a_k)$$
$$B \leftrightarrow (b_1, \ldots, b_k)$$

则

$$(A + B) \bmod n \leftrightarrow ((a_1 + b_1) \bmod n_1, \ldots, (a_k + b_k) \bmod n_k)$$
$$(A \times B) \bmod n \leftrightarrow ((a_1 \times b_1) \bmod n_1, \ldots, (a_k \times b_k) \bmod n_k)$$

因为

$$(A \cdot B) \bmod n_i = (A \bmod n_i \cdot B \bmod n_i) \bmod n_i = (a_i \cdot b_i) \bmod n_i$$

其中 $\cdot \in \{+, \times\}$。

CRT 的证明

当 $k = 2$ 时

已知

$$\begin{cases} x \equiv x_1 \pmod{n_1} \\ x \equiv x_2 \pmod{n_2} \end{cases}$$

其中 n_1 和 n_2 互素且 $n = n_1 n_2$，求 $x \in \mathbb{Z}_n$。

- 由扩展欧几里得算法可得整数 m_1, m_2 且 $m_1 n_1 + m_2 n_2 = 1$
- 一元线性同余方程组的解为 $x = (x_1 m_2 n_2 + x_2 m_1 n_1) \bmod n$
- 因为

$$x \bmod n_1 = x_1 m_2 n_2 \bmod n_1 = x_1$$
$$x \bmod n_2 = x_2 m_1 n_1 \bmod n_2 = x_2$$

CRT 的证明

推论

如果

$$\begin{cases} x \equiv y \pmod{p} \\ x \equiv y \pmod{q} \end{cases}$$

其中 p 和 q 互素，那么

$$x \equiv y \pmod{pq}$$

CRT 的证明

当 $k = 3$ 时

已知

$$\begin{cases} x \equiv x_1 & (\mathrm{mod}\ n_1) \\ x \equiv x_2 & (\mathrm{mod}\ n_2) \\ x \equiv x_3 & (\mathrm{mod}\ n_3) \end{cases}$$

其中 n_1, n_2, n_3 两两互素且 $n = n_1 n_2 n_3$，求 $x \in \mathbb{Z}_n$。

- $k > 2$ 时的情况可以归约为 $k = 2$ 时的情况。
- 由前两个等式可以确定 $x \equiv x_{12} \pmod{n_1 n_2}$。
- 再与第三个等式可以确定 $x \equiv x_{123} \pmod{n_1 n_2 n_3}$。

CRT 的证明

完整证明.

- $\forall i$， n/n_i 与 n_i 互素 $\Rightarrow \exists y_i, (n/n_i)y_i \bmod n_i = 1$。
- $\forall i \neq j$， n/n_i 有因子 $n_j \Rightarrow (n/n_i)y_i \bmod n_j = 0$。
- 令

$$x \triangleq \sum_{i=1}^{k} \frac{n}{n_i} y_i x_i \bmod n$$

因为

$$x \bmod n_j = \frac{n}{n_j} y_j x_j \bmod n_j = x_j$$

所以 x 是 $x \bmod n_j = x_j, j = 1, \ldots, k$ 的公共解。

“物不知其数”问题求解

$x \bmod 3 = 2,\ x \bmod 5 = 3,\ x \bmod 7 = 2$

$n_1 = 3, n_2 = 5, n_3 = 7$

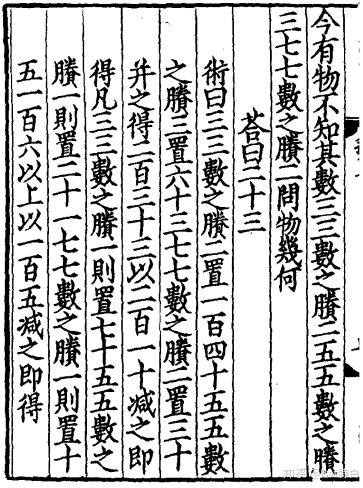
$x_1 = 2, x_2 = 3, x_3 = 2$

$n = 3 \times 5 \times 7 = 105$

- 求 $y_i = (n/n_i)^{-1} \bmod n_i$，得
  $y_1 = 2, y_2 = 1, y_3 = 1$
- 代入前面得到的公式中

$$
\begin{aligned}
x &= \sum_i \frac{n}{n_i} y_i x_i \bmod n \\
&= (70 \times 2 + 21 \times 3 + 15 \times 2) \bmod 105 \\
&= 23
\end{aligned}
$$

从而得到结果 23。


今有物不知其數三三數之賸二五五數之賸二七七數之賸二問物幾何
答曰二十三
術曰三三數之賸二置一百四十五五數之賸三置六十三七七數之賸二置三十并之得二百三十三以二百一十減之即得凡三三數之賸一則置七十五五數之賸一則置二十一七七數之賸一則置十五一百六以上以一百五減之即得

‘‘物不知其数’’问题求解

《孙子歌诀》

三人同行七十希，
五树梅花廿一支，
七子团圆正半月，
除百零五便得知。

明朝数学家程大位《算法统宗》

小结

1. 数论简介
2. 费马定理和欧拉定理
3. 素性测试
4. 单向函数与指数函数
5. 计算乘法逆元
6. 中国余数定理