数论初窥

谢兴宇

计算机科学与技术系，清华大学

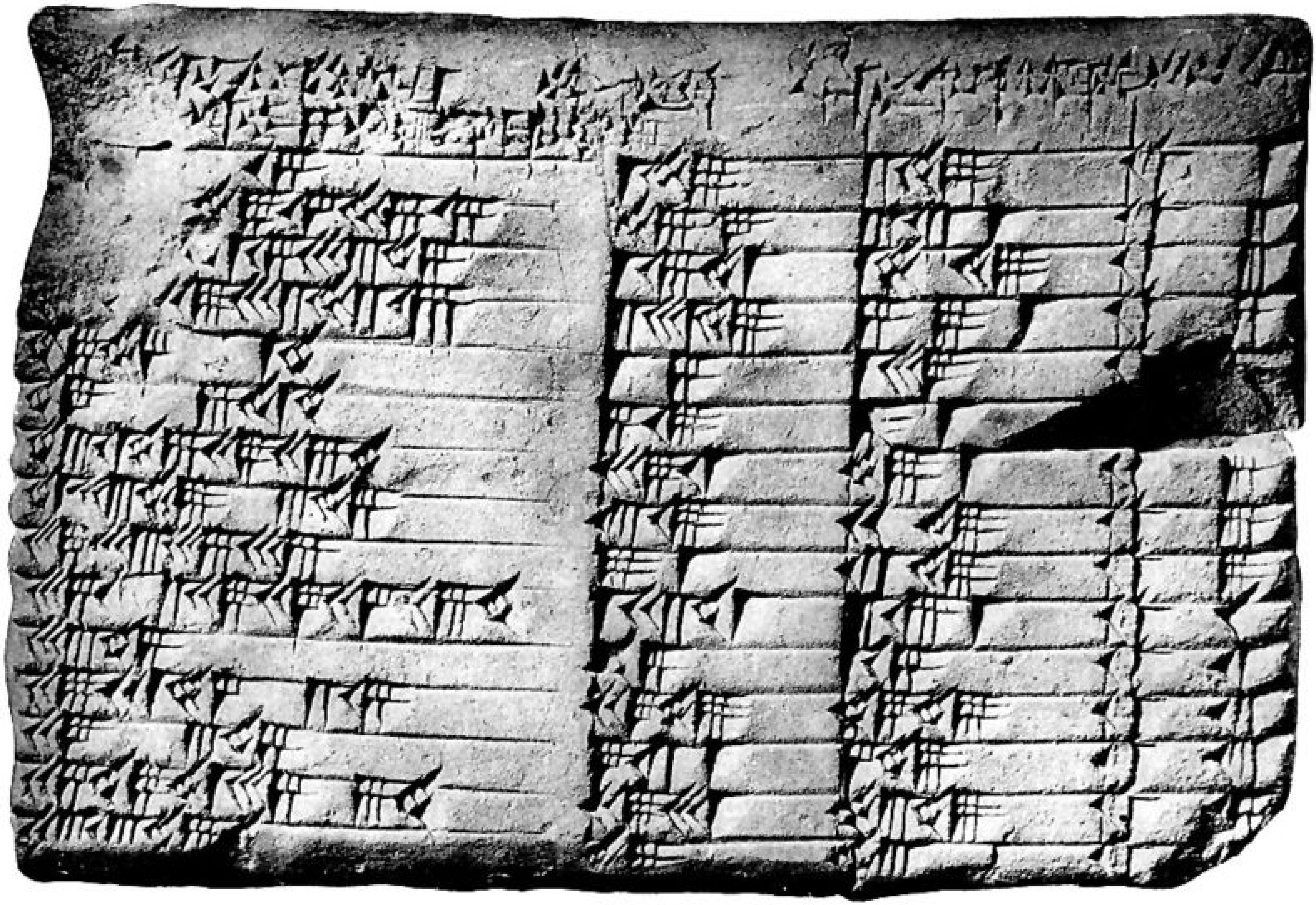
数论简介

数论主要研究整数的性质。如不特殊说明，此章中所有数均为整数。

> 数学是科学的皇后，数论是数学的皇后。
> ——卡尔·弗里德里希·高斯

在20世纪之前，数论(Number Theory)被称为算术(Arithmetic)，后来“算术”一词的含义逐渐演变为“对数字或元素的运算”。

起源



毕达哥拉斯学派

> 毕达哥拉斯忙于学习各国智慧，访问巴比伦、埃及和波斯，受到占星家、牧师和婆罗门的指导，他习得占星术、几何、算术和音乐，以及种种不同的技能和知识、从完全不同的人那里——唯独除却希腊的智者。当毕达哥拉斯回到希腊，他让希腊人第一次接触到那些来自世界各地的奇妙思想。
> ——尤比修斯

毕达哥拉斯学派相信“万物皆数”。

第一次数学危机：希帕索斯发现$\sqrt{2}$不是有理数。

整除

定义

若$\exists k, s.t. b = ak$, 则称$a|b$。此时， a是b的因子，b是a的倍数。

性质

传递性：$a|b, b|c$，则$a|c$。

线性：$c|a, c|b$，则$c|(ma+nb)$。

带余除法：$b>0, \exists! q, r, a=bq+r$

素数

定义

若$n(n>1)$除了1和它本身外不能被任何正整数整除，则称n为素数（质数），否则称n为合数。

性质

- 每个大于1的正整数都有一个素因子。
- 素数是无穷多的。
    - 现存最早的证明出自欧几里得（Ευκλειδης）于公元前300年所著的《几何原本》（Στοιχεῖα Stoicheia）（卷4，命题20），这也是现存最古老的对素数的研究。[17]
- 素数定理：$\lim_{x\to\infty}\pi(x)/(x/\log x)=1$
    - Proved by Jacques Hadamard and Charles Jean de la Vallée Poussin in 1896

关于素数的猜想

- 伯特兰猜想：$\forall n > 1, \exists p, n < p < 2n$且$p$为素数。
  - 1852年（猜想被提出7年后），切比雪夫给出了第一个证明。
- 孪生素数猜想：存在无穷多的形如p和$p+2$的素数对。
- 哥德巴赫猜想：每个大于2的正偶数可以写成两个素数的和。
- 弱哥德巴赫猜想：任一大于7的奇数都可表示为三个奇素数之和。
  - 2012和2013年，Harald Helfgott在arXiv上发表了两篇论文，声称证明了弱哥德巴赫猜想。[2][3]
- n^2+1猜想：存在无穷多个形如n^2+1的素数，其中n是正整数。

素性测试

- Simple primality test: 枚举所有不超过$\sqrt{n}$的数，对n试除。
  - 若n为合数，则必有不超过$\sqrt{n}$的（质）因子。
  - 时间复杂度：$O(\sqrt{n})$
  - 若只枚举不超过$\sqrt{n}$的质数，时间复杂度降为$O(\sqrt{n}/\log n)$
- Miller-Rabin primality test：随机算法，需要选取k个随机种子。
  - 时间复杂度：$O(k\log^3 n)$
  - 借助FFT，可加速至$\tilde{O}(k\log^2 n)$
- AKS primality test: 第一个可被证明的、通用的、多项式的、确定的素性测试算法。
  - 2006 Gödel Prize, 2006 Fulkerson Prize
  - $\tilde{O}(\log^6 n)$

筛法

求出$1 \sim n$中所有的质数。

- 埃拉托斯特尼筛法：从小到大枚举所有质数，并以之筛去它的倍数。
  - 原载于尼科马库斯所著《算术入门》。
  - Erdős–Kac theorem: $\frac{\omega(n)-\log\log n}{\sqrt{\log\log n}}$服从标准正态分布，其中$\omega(n)$ = the number of distinct prime factors of n。
  - 时间复杂度：$O(n\log\log n)$[4]
- 欧拉筛法：从$1 \sim n$枚举i，再从小到大枚举质数p_j，筛去ip_j，直到$i \bmod p_j = 0$。
  - 最早Euler由欧拉提出，1978年被Gries和Misra再次发现。[5]
  - 时间复杂度：$O(n)$

最大公因子

定义

所有能同时整除a和b的整数中最大者，记为(a, b)。

若$(a, b) = 1$，我们称a与b互素。

性质

- 若$(a, b) = d$，则$(a/d, b/d) = 1$
- $(a, b) = \min_{x, y \in \mathbb{Z}} ax + by$
- $\{k(a, b) | k \in \mathbb{Z}\} = \{ax + by | x, y \in \mathbb{Z}\}$
- $d = (a, b)$当且仅当$d|a, d|b$且如果$c|a, c|b$则$c|d$
- $(a + cb, b) = (a, b)$
- 若$(a, b) = 1$且$a|bc$，则$a|c$

求解：欧几里得算法

载于欧几里得《几何原本》。

```
int euclidean(int a, int b) {
        return b ? euclidean(b, a % b): a;
}
```

时间复杂度：$O(\log n)$

WLOG, $a > b$, 若 `euclidean(a, b)` 的递归次数为n，则 $a \geq fi_n, b \geq fi_{n-1}$。亦即，欧几里得算法在相邻两项斐波那契数处取得最坏情况。

欧几里得算法的时间复杂度在1844年被Gabriel Lamé证明，这被视为计算复杂性理论之滥觞。

目前最快的求最大公约数的算法的时间复杂度为：$O(\log n(\log\log n)^2\log\log\log n)$

丢番图方程

亚历山大港的丢番图（Διόφαντος ὁ Ἀλεξανδρεύς），生于公元前3世纪，有"代数之父"之称，著有巨著《算术》。丢番图是第一个承认分数的数学家，也是第一个将符号引入代数的数学家。

> 丢番图的一生，幼年占去1/6，又过了1/12的青春期，又过了1/7才结婚，五年后生儿子，子先父四年而卒，寿为其父一半。
> ——《希腊诗选》

丢番图方程是形如$\sum_{i=1}^{n} a_i x_i^{k_i} = c$的方程，其中所有数均为整数。

双变量一次线性丢番图方程

$$ax + by = c$$

裴蜀定理（Bézout's lemma）：若$d = (a, b) \nmid c$，方程无解；若$d | c$，方程有无穷多解。若方程有特解x_0, y_0，则其所有解可表示为：

$$x = x_0 + (b/d)n, y = y_0 - (a/d)n$$

上述定理在历史上由Claude Gaspard Bachet de Méziriac于著作《有关整数的令人快乐与惬意的问题集》（Problèmes plaisants et délectables qui se font par les nombres）中首次发表证明[9]，Étienne Bézoutj将之推广至多项式[8]。

求解：扩展欧几里得算法

```
void ex_euclidean(int a, int b, int &x, int &y) {
	if (b) {
		ex_euclidean(b, a % b, y, x);
		y -= a / b * x;
	}
	else x = 1, y = 0;
}
```

若$bx' + (a \bmod b)y' = (a, b)$，则
$ay' + b(x' - y'\lfloor \frac{a}{b} \rfloor) = (a, b)$.

故可令$x = y', y = x' - y'\lfloor \frac{a}{b} \rfloor$，便有$ax + by = (a, b)$。

定理：扩展欧几里得算法求出的(x, y)是所有使得
$ax + by = (a, b)$的(x, y)中$|x|$最小的，也是$|y|$最小的。[7]

多变量一次线性丢番图方程

$\sum_{i=1}^{n} a_i x_i = b$

有解当且仅当$(a_1, a_2, \cdots, a_n) | b$

时间复杂度：$O(n + \log \min_{i=1}^{n} a_i)$

算术基本定理

引理：若素数p整除$a_1, a_2, \cdots, a_n$，则$\exists i, 1 \leq i \leq n, p|a_i$

算术基本定理：任一正整数可被唯一地写成素数次幂的乘积。

出自欧几里得《几何原本》卷9定理14.

算术基本定理的应用

通过素数定理，我们在一个整数与一个无穷维向量之间建立双射。

$a=\prod_i p_i^{\alpha_i}, b=\prod_i p_i^{\beta_i}$

$(a,b)=\prod_i p_i^{\min(\alpha_i,\beta_i)}, [a,b]=\prod_i p_i^{\max(\alpha_i,\beta_i)}$

$(a,b)[a,b]=ab$

分解质因式

```
for (int i = 2; i * i <= n; ++i)
        for (;n % i == 0; n /= i)
                output(i);
if (n != 1) output(n);
```

若n是合数，则n必有一个不超过$\sqrt{n}$的素因子，至多有一个超过$\sqrt{n}$的素因子。

时间复杂度：$O(\sqrt{n}/\log n)$

也可用筛法在$O(n)$时间内预处理出每个数的最小质因子或最小素幂。

同余

1801年，卡尔·弗里德里希·高斯在介绍中国剩余定理时首次引入同余符号。[19]

若$m|(a-b)$，则称a与b模m同余，记作$a\equiv b \pmod m$。

同余是等价关系。

- 自反性：$a\equiv a \pmod m$
- 对称性：若$a\equiv b \pmod m$，则$b\equiv a \pmod m$。
- 传递性：若$a\equiv b \pmod m$，$b\equiv c \pmod m$，则$a\equiv c \pmod m$。

因此，我们可以定义模m完全剩余系为一个整数的集合，使每个整数恰和此集合中的一个元素模m同余。

同余的性质

若$a \equiv b \pmod m, c \equiv d \pmod m$，则：

- $a + c \equiv b + d \pmod m$
- $a - c \equiv b - d \pmod m$
- $ac \equiv bd \pmod m$

若$ac \equiv bc \pmod m, a \equiv b \pmod {m/(c, m)}$。

线性同余方程

$ax \equiv b (\bmod m)$

若$(a, m) \nmid b$，无解；若$(a, m) | b$，则恰有(a, m)个模m不同余的解。

特别地，若(a, m)互质，线性同余方程必有唯一解。

逆元

若$ax \equiv 1 \pmod m$，则称x为a在模m意义下的逆元，记作a^{-1}。

$a \equiv a^{-1} \pmod m$当且仅当$a \equiv 1 \pmod m$或
$a \equiv -1 \pmod m$。

中国剩余定理

> 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？ ——《孙子算经》

若$m_1, m_2, \cdots, m_r$两两互素，则线性同余方程组

$$\begin{cases} x \equiv a_1 (\bmod m_1) \\ x \equiv a_2 (\bmod m_2) \\ \cdots \\ x \equiv a_r (\bmod m_r) \end{cases}$$

在模$M = \prod_{i=1}^{r} m_i$意义下有唯一解

$x \equiv \sum_{i=1}^{r} a_i M_i y_i (\bmod M)$，

其中$M_i = M / m_i$，y_i是M_i模m_i的逆元。

扩展中国剩余定理

在不保证$m_1, m_2, \cdots, m_r$两两互素的前提时，如何求线性同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$
的解？

利用扩展欧几里得合并方程/判断是否有解。

威尔逊定理

威尔逊定理：$(n-1)! \equiv -1(\bmod n)$当且仅当$n$是质数。

历史：最早的版本由海什木(c. 1000 AD)给出[10]；莱布尼茨在17世纪再度发现，但并未发表[11]；1770年，Edward Waring在发表的著作*Meditationes Algebraicae*中声称他的学生John Wilson给出了这一猜想[12]；1771年，拉格朗日给出了第一个证明[13]。

证明：

- 充分性：除了1和$n-1$之外的所有数必有一个不等于自身的逆元。
- 必要性：若n不为质数且$n>4$，则$(n-1)! \equiv 0(\bmod n)$；若$n=4$，$(n-1)! \equiv 2(mathrmmod\, n)$

费马小定理

费马小定理：若p为质数，$a^p \equiv a(\bmod p)$。

等价的，若$p \nmid a$，$a^{p-1} \equiv 1(\bmod p)$。

历史：1640年10月18日，在写给知己Frénicle de Bessy的信中，费马第一次阐述了这个定理[14]。莱布尼茨于1683年之前在未发表的手稿中给出了证明[14]；1736年，欧拉发表了第一个证明（基本与莱布尼茨相同）[15]。

证明：利用
$\{1, 2, \cdots, p-1\} \equiv \{a, 2a, \cdots, (p-1)a\}(\bmod p)$。

欧拉定理

欧拉函数：$\phi(m)$为不超过m且与m互素的正整数个数。
$\phi(m) = m\prod_{p|m}(1-1/p)$

模m的既约剩余系：模m的完全剩余系中与m互素的数组成的集合。

欧拉定理：若$(a,m)=1$，则$a^{\phi(m)}\equiv 1 (\bmod m)$。

证明：

- 从群论的角度来看，欧拉定理是拉格朗日定理的推论。
- 从初等数论的角度来看，欧拉定理是费马小定理的推广。

欧拉定理的逆定理：若$a^{\phi(m)}\equiv 1 (\bmod m)$，则$(a,m)=1$。

欧拉定理的推广：Carmichael's Theorem最终给出了最小通用指数的形式。

逆元的求解

求n的逆元

- 扩展欧几里得算法
- 欧拉定理
- $n^{-1} \equiv -(p \bmod n)^{-1}\lfloor \frac{p}{n} \rfloor \pmod p$
  - 关于其时间复杂度，目前最好的界为$O(n^{1/3}+\epsilon)$的上界和$\Omega(\frac{\ln n}{\ln\ln n})$的下界[16]。
  - Jeffrey Shallit offers US $200 for any significant improvement on MO.

求$1 \sim n$的逆元

- 利用$n^{-1} \equiv -(p \bmod n)^{-1}\lfloor \frac{p}{n} \rfloor \pmod p$递推。
- 利用$n!^{-1} = (n+1)^{-1}(n+1)$求出所有阶乘的逆，再利用$n^{-1} \equiv n!^{-1}(n-1)!$求出所有数的逆。

总结

- 基本概念：整除、取模、同余……
- 素数：素数定理、素性测试、埃拉托斯特尼筛法、欧拉筛法……
- 最大公因子：欧几里得算法、最小公倍数……
- 素幂式：算术基本定理、质因子分解……
- 线性同余方程（组）：扩展欧几里得算法、裴蜀定理、中国剩余定理……
- 逆元：费马小定理、欧拉定理……

参考资料

[1] Rosen, K. (2011). *Elementary number theory and its applications*. 6th ed. Boston, Mass.: Pearson.

[2] Helfgott, Harald A. (2013). "Major arcs for Goldbach's theorem". arXiv: 1305.2897

[3] Helfgott, Harald A. (2012). "Minor arcs for Goldbach's problem". arXiv: 1205.5252

[4]Jonathan Sorenson, *An Introduction to Prime Number Sieves*, Computer Sciences Technical Report #909, Department of Computer Sciences University of Wisconsin-Madison, January 2, 1990

[5] Gries, David; Misra, Jayadev (December 1978), "A linear sieve algorithm for finding prime numbers", Communications of the ACM, 21 (12): 999–1003, doi:10.1145/359657.359660.

参考资料

[6] LeVeque, W. J. (1996). *Fundamentals of Number Theory*. New York: Dover. ISBN 0-486-68906-9.

[7] David. (2014). Does the Extended Euclidean Algorithm always return the smallest coefficients of Bézout's identity? . Mathematics Stack Exchange.

[8] Bézout, É. (1779). Théorie générale des équations algébriques. Paris, France: Ph.-D. Pierres.

[9] Bachet, Claude-Gaspard. (2015) Problèmes plaisants et délectables qui se font par les nombres. Paris: Cinquième édition revue, simplifiée et augmentée.

[10] O'Connor, John J.; Robertson, Edmund F., "Abu Ali al-Hasan ibn al-Haytham", *MacTutor History of Mathematics archive*, University of St Andrews.

参考资料

[11] Giovanni Vacca. (1899). "Sui manoscritti inediti di Leibniz" (On unpublished manuscripts of Leibniz), *Bollettino di bibliografia e storia delle scienze matematiche* (Bulletin of the bibliography and history of mathematics)

[12] Edward Waring. (1770). *Meditationes Algebraicae*. Cambridge, England.

[13] Joseph Louis Lagrange. (1771). "Demonstration d'un théorème nouveau concernant les nombres premiers". *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres*. Berlin.

[14] Burton, David M. (2011). *The History of Mathematics / An Introduction* (7th ed.), McGraw-Hill, ISBN 978-0-07-338315-6

[15] Ore, Oystein. (1988). *Number Theory and Its History*, Dover, ISBN 978-0-486-65620-5

参考资料

[16] Vlado Keselj. (1996). Length of Finite Pierce Series: Theoretical Analysis and Numerical Computations. Ontario, Canada.

[17] Stillwell, John (2010). *Mathematics and Its History*. Undergraduate Texts in Mathematics (3rd ed.). Springer.

[18] Nicomachus. *Introduction to Arithmetic*.

[19] Ireland, Kenneth; Rosen, Michael. (1990). *A Classical Introduction to Modern Number Theory* (2nd ed.). Springer-Verlag, ISBN 0-387-97329-X