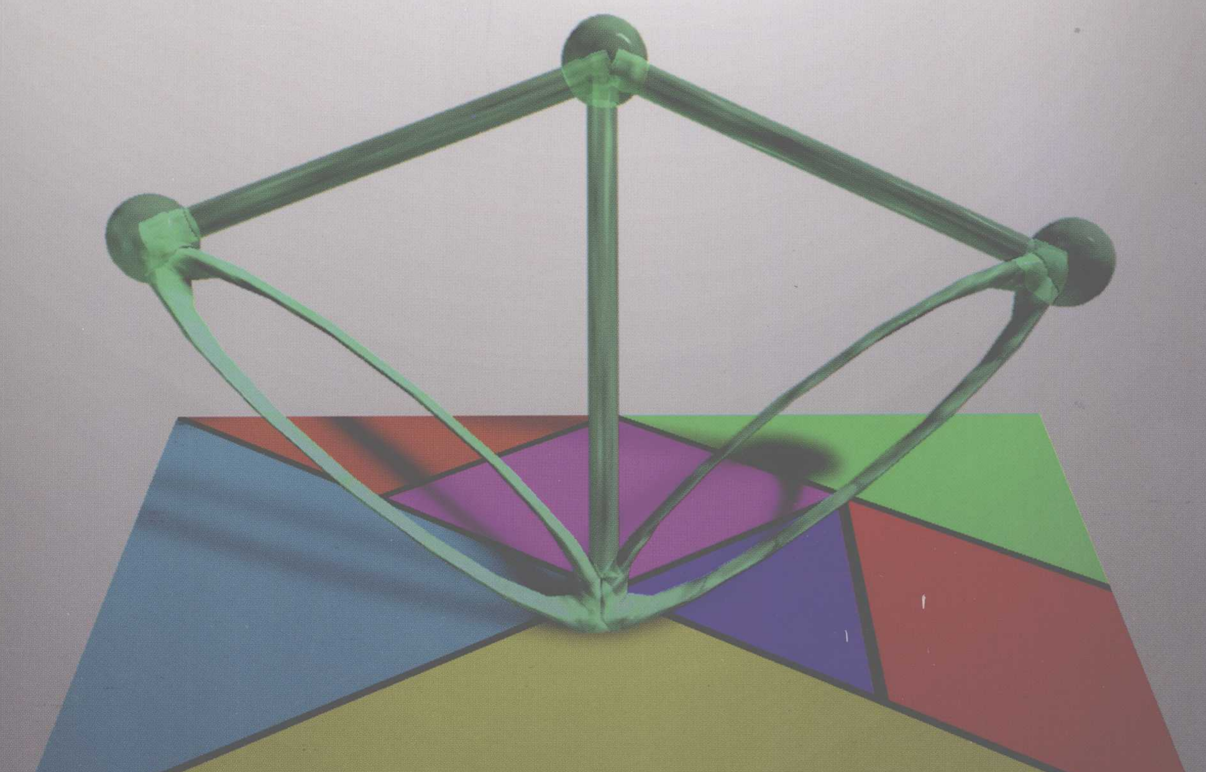
计算机科学组合学丛书

椭圆曲线密码算法导引

卢开澄 卢华明 编著



清华大学出版社

内 容 简 介

本书分为两个部分，共6章。第一部分是数学基础，介绍与椭圆曲线算法有关的数论、群论与有限域理论；第二部分是椭圆曲线有效算法，讨论椭圆曲线公钥密码及其实用算法。

本书语言精练，结构合理，内容丰富，立论严谨，适合作为计算机专业高年级学生和研究生的教材，也可供科技工作者参考。

图书在版编目（CIP）数据

椭圆曲线密码算法导引/卢开澄，卢华明编著．—北京：清华大学出版社，2008.5
（计算机科学组合学丛书）
ISBN 978-7-302-16988-8

Ⅰ．椭…　Ⅱ．①卢…②卢…　Ⅲ．椭圆曲线—密码—算法　Ⅳ．TN918.1

中国版本图书馆CIP数据核字(2008)第017152号

责任编辑：张　民　徐跃进
责任校对：焦丽丽
责任印制：杨　艳

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印　装　者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×260　　**印　张**：8　　**字　数**：182千字
版　　次：2008年5月第1版　　**印　次**：2008年5月第1次印刷
印　　数：1～3000
定　　价：19.00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177转3103　　产品编号：027249-01

计算机科学组合学丛书序

电子计算机的出现是20世纪的大事，它改变了我们这个世界的面貌。可以毫不夸张地说，它的影响遍及所有角落，几乎无处不感觉到它的存在。数学更不例外。严格地说，电子计算机本身就是近代数学的辉煌成就。将计算机与数学割裂开来，既不合理也不可能。组合学也就是在计算机科学蓬勃发展的刺激下而崛起的，从而成为近若干年来最活跃的数学分支。它研究的问题有的可追溯到 Euler 和 Hamiltan 等 18 世纪的数学家，但它成为新的分支还是近若干年的事。它从与计算机科学相结合中获得了广阔的发展空间，从而也为计算机科学奠定了理论基础。

什么是计算机科学呢？有的学者将它定义为研究算法的一门学科。研究算法无疑是计算机科学的重要领域，也是本丛书的核心内容，贯穿始终。组合学家在20世纪70年代初建立的算法复杂性“NP理论”，至今仍然令无数计算机科学工作者与数学工作者为之折腰。

计算机科学里的组合学内容十分广泛。本丛书涉及组合分析、图论、组合算法、近代密码学、组合优化、编码理论及算法复杂性等7部分。

组合分析是算法的理论基础。组合分析之与组合算法犹如数学分析之与计算数学，众所周知，前者是后者的理论根基。

图论原本是组合数学这个“家族”的主要成员，只因它已成长壮大，故自立门户独立出去。

算法复杂性的NP理论是近三十年的一大成就。研究表明对于一类叫做NPC类的困难问题，至今都没找到有效算法，但它们难度相当，只要其中任何一个找到多项式解法，则全体都获得解决；或证明它们根本不存在有效办法。不论是前者还是后者都还看不见露到海平面上的桅杆塔，它吸引了众多的有志之士。密码学是其中十分引人入胜的分支。如若设计好的密码，对它的破译等价于某一NPC类困难问题，无疑这样的密码将是牢不可破的。

在计算机网络深入普及的信息时代，信息本身就是时间，就是财富。信息的传输通过的是脆弱的公共信道，信息储存于“不设防”的计算机系统中，如何保护信息的安全使之不被窃取及不至于被篡改或破坏，已成为当今被普遍关注的重大问题。密码是有效而且可行的办法。在计算机网络的刺激下，近代密码学便在算法复杂性理论的基础上建立起来了。密码作为一种技术，自从人类有了战争，不久便有了它。但作为一门学科则是近二十多年的事。甚至于它已成为其他学科的基础。密码也从此走出“军营”，进入百姓家。

实际中的“优化”问题是大量的，半个多世纪以来它曾经几度辉煌。近来在计算机科学的影响下，又出现了若干闪光点，十分耀眼，引人注目。

实际上密码也是一种编码。如果说密码学研究的编码是保证通信的保密与安全，则

编码理论研究的是通信中如何纠错与检错。计算机纠错码是既实用、理论上又饶有趣味的分支。

本丛书是作者在清华大学计算机科学与技术系长期工作的总结。它不是一部“长篇”记述，而是互相关联又彼此相对独立，因此难免有少量交叉。它们涉及的面如此之广，囿于作者的水平，缺点和错误在所难免，敬请读者不吝指正。谢谢。

作　　者

本 书 序

椭圆曲线原属抽象数学“代数几何学”的一个分支，自从 Koblitz 等人提出用来构造公钥密码以来，获得了快速发展。事实证明它比 RSA 更有效，密钥更短而抗击能力更强，从而给密码研究提供了新工具、新方法，也给椭圆曲线研究注入了活力。椭圆曲线密码已成为密码学的重要内容之一。椭圆曲线密码算法作为“计算机密码学”的续篇，可以为非数学专业的人士在椭圆曲线与“密码”之间搭起一座桥梁。全书分两部分：数学基础和椭圆曲线有效算法。无疑第一部分是桥墩，是基础；第二部分是桥本身。第一部分由卢华明执笔，第二部分由卢开澄完成。

编　　者

2007 年 11 月

目　录

第一部分　数学基础

第二部分 椭圆曲线密码有效算法

第一部分　数学基础

第1章　数论简介

1.1　基本概念

(1) 设 a、b 是两个整数，$b\neq 0$。若存在整数 c，得

$$a = bc$$

则称 b 是 a 的约数，a 是 b 的倍数。b 可整除 a，表示为 $b|a$；$b\nmid a$ 则表示 b 不能整除 a。

(2) 一个大于 1 的整数 p，若只有 1 和 p 两个约数，此外再也没有其他约数时，这样的数 p 称为素数。例如

$$2,3,5,7,11,17,19,23,29,\cdots$$

都是素数。

(3) 一个大于 1 的数 n 总可以分解为若干素数的乘积。例如 $n=34\,300$ 有

$$\begin{aligned}34\,300 &= 2\times 17\,150 = 2^2\times 8575 = 2^2\times 5\times 1715\\ &= 2^2\times 5^2\times 343 = 2^2\times 5^2\times 7\times 49 = 2^3\times 5^2\times 7^3\end{aligned}$$

即 34 300 是由两个 2、两个 5 和 3 个 7 的连乘积。

一般令

$$n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k},\quad a_i\geqslant 1,\quad i=1,2,\cdots,k$$

其中 $p_1,p_2,\cdots,p_k$ 是 k 个素数，即数 n 分解为 a_i 个 p_i，$i=1,2,\cdots,k$，的乘积。

(4) 若正整数 n 不被小于或等于 $\sqrt{n}$ 的所有素数除尽，则 n 便是素数。例如 $n=119$，$\sqrt{119}<\sqrt{121}=11$。

小于 11 的素数有 2,3,5,7。119 不是 2,3,5,7 的倍数，所以 119 本身也是素数。

上面的讨论实际上已提供了一个判定素数的方法。

以 $n=60$ 为例，$\sqrt{60}<\sqrt{64}=8$，小于 8 的素数为 2,3,5,7。

$2,\ 3,\ \cancel{4},\ 5,\ \cancel{6},\ 7,\ \cancel{8},\ \bcancel{9},\ \cancel{10},\ 11,\ \cancel{12},\ 13,\ \cancel{14},\ \bcancel{15},\ \cancel{16},\ 17,$
$\cancel{18},\ 19,\ \cancel{20},\ \bcancel{21},\ \cancel{22},\ 23,\ \cancel{24},\ \sout{25},\ \cancel{26},\ \bcancel{27},\ \cancel{28},\ 29,\ \cancel{30},\ 31,\ \cancel{32},\ \bcancel{33},$
$\cancel{34},\ \sout{35},\ \cancel{36},\ 37,\ \cancel{38},\ 39,\ \cancel{40},\ 41,\ \cancel{42},\ 43,\ \cancel{44},\ \cancel{45},\ \cancel{46},\ 47,\ \cancel{48},\ \bcancel{49},$
$\cancel{50},\ \bcancel{51},\ \cancel{52},\ 53,\ \cancel{54},\ \sout{55},\ \cancel{56},\ \bcancel{57},\ \cancel{58},\ 59,\ \cancel{60}$

即 2 是素数，从上面数列排除 2 的倍数的数(4,6,8,…,60)，被排除的数用“/”表示。

3 是 2 以后的第一个素数，从余下的数列中再排除 3 的倍数的数(9,15,21,27,33,51,57)，被排除的数记以“\”。

下一个素数 5，再从余下的数中排除 25,35,55，“—”表示被排除的数。

最后一个是 7，被排除的 7 的倍数为“|”式标的 49。剩下的数：

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59$$

都是素数。

(5) 最大公约数

设 a 和 b 是整数，若存在整数 d，使得 $d|a$，又 $d|b$，则称 d 为 a 和 b 的公约数。公约数中的最大者，称为最大公约数，用 $\gcd(a,b)$ 表示，有时就简记为 (a,b)。

求 $\gcd(a,b)$ 的方法，不妨令 $a>b$，

$$a = qb + r$$

即用 b 去除 a，得商数 q，余数 r，$r<b$。

定理 $\gcd(a,b)=\gcd(b,r)$。

证 设 $d=\gcd(a,b)$， $d_1=\gcd(b,r)$，由 $a=qb+r$， $a-qb=r$，已知 $d|r$，由 $d|b$ 及 $d|r$，故 $d|d_1$。

反过来，$d_1=\gcd(b,r)$，$a=qb+r$，故 $d_1|a$，由 $d_1|a$，及 $d_1|b$，故 $d_1|d$，

从 $d|d_1$ 得 $d_1|d$，即 $d=d_1$，所以

$$\gcd(a,b) = \gcd(b,r)$$

假定

$$a = qb + r, \quad b = q_1 r + r_1, \quad r_1 = q_2 r_1 + r_2, \cdots$$
$$(a,b) = (b,r) = (r_1,r_1) = (r_1,r_2) = \cdots$$
$$r < b, \quad r_1 < r, \quad r_2 < r_1, \cdots$$

例如求 $\gcd(3468,595)$

因

$$3468 = 5 \times 595 + 493$$
$$d = (3468,595) = (595,493)$$
$$595 = 493 + 102$$

故

$$d=(595,493)=(493,102)$$

又

$$493=4\times 102+85$$

故

$$d=(493,102)=(102,85)$$
$$102=85+17$$

故

$$d=(102,85)=(85,17)$$
$$85=17\times 5, \quad d=(85,17)=17$$

故

$$\gcd(3468,595)=17$$

(6) 若 $d=\gcd(a,b)$，则存在整数 l,m，使

$$d = la + mb$$

还是通过前面讨论的例子来说明，一般的道理也在其中了。

$3468=5\times595+493$

$493=3468-5\times595$

$595=493+102$

$102=595-493$

$493=4\times102+85$

$85=493-4\times102$

$102=85+17$

$17=102-85$

$85=5\times17$

$17=\gcd(3468,595)$

从 $17=102+85$ 回溯，过程如下

$$
\begin{aligned}
17 &= 102-85=102-(493-4\times102)\\
&=5\times102-493=5(595-493)-493\\
&=5\times595-6\times493=5\times595-6(3468-5\times595)\\
&=-6\times3468+35\times595
\end{aligned}
$$

即

$$17=-6\times3468+35\times595$$

(7) 若 a 与 b 互素，则存在整数 l 和 m，使

$$la+mb=1$$

a 与 b 互素，即 $(a,b)=1$，这个结论实际上是前面例子 $d=\gcd(a,b)=1$ 的特例，但它具有非常重要的意义，故单独提出来。

以 $a=493,b=139$ 为例：

$493=3\times139+76$

$76=493-3\times139$

$139=76+63$

$63=139-76$

$76=63+13$

$13=76-63$

$63=4\times13+11$

$11=63-4\times13$

$13=11+2$

$2=13-11$

$11=5\times2+1$

$1=11-5\times2$

$1=(11,2)=(13,11)=(63,13)=(76,63)=(139,76)=(493,139)$

$$
\begin{aligned}
1&=11-5\times2=11-5(13-11)=6\times11-5\times13\\
&=6(63-4\times13)-5\times13=6\times63-29\times13\\
&=6\times63-29(76-63)=35\times63-29\times76\\
&=35(139-76)-29\times76=35\times139-64\times76
\end{aligned}
$$

$$=35\times 135-64(495-3\times 139)$$

故

$$1=-64\times 495-227\times 139$$

1.2 同 余 式

设 m 是一正整数，任意一整数 a，除以 m 的余数设为 r，即

$$a=qm+r,\quad 0\leqslant r<m$$

最小的非负余数有 m 个：

$$0,1,2,\cdots,m-1$$

定义 如果整数 a 和 b，用 m 除所得的最小非负余数相同，则称 a 和 b 模 m 同余，用

$$a\equiv b \bmod m$$

来表示。

若 $a\equiv b \bmod m$，即 $a-b$ 是 m 的倍数

$$m\mid a-b$$

例如 $a=15,b=22,m=7$，15 和 22 除以 7 余数都是 1，即 $15\equiv 1 \bmod 7$，$22\equiv 1 \bmod 7$，$22-5\equiv 0 \bmod 7$。

同理 $-6\equiv 1 \bmod 7$，故 $-6,15,22$ 都是 mod 7 和 1 同余。

同余式的基本性质：

(1) $a\equiv a \bmod m$

(2) 若 $a\equiv b \bmod m$，$b\equiv c \bmod m$，则

$$a\equiv c \bmod m$$

(3) 若 $a\equiv b \bmod m$，$c\equiv d \bmod m$，则

$$a\pm c\equiv b\pm d \bmod m$$
$$ac\equiv bd \bmod m$$

(4) $(ab)c\equiv a(bc) \bmod m$

定理 若 $ab\equiv ac \bmod m$，$(a,m)=1$，则

$$b\equiv c \bmod m$$

成立。

证 即证明 $(a,m)=1$ 是 $b\equiv c \bmod m$ 的充分条件。

$(a,m)=1$，根据 1.1 节的(7)，存在整数 p 和 q，使

$$1=pa+qm$$
$$qa-1=-qm$$

根据同余式的定义

$$pa\equiv 1 \bmod m$$

或

$$p\equiv a^{-1} \bmod m$$

即 $(a,m)=1$，则存在 $a^{-1} \bmod m$，使 $aa^{-1}\equiv a^{-1}a\equiv 1 \bmod m$，用 a^{-1} 乘同余式：

$$ab\equiv ac \bmod m$$

两端，可得

$$(a^{-1}a)b \equiv (a^{-1}a)c \bmod m$$

即

$$b \equiv c \bmod m$$

例 1.2.1 求解同余方程 $4x \equiv 11 \bmod 13$，

$$13 = 4 \times 3 + 1$$
$$1 = (-3) \times 4 + 13$$

故

$$(-3) \times 4 \equiv 1 \bmod 13$$
$$4^{-1} \equiv -3 \bmod 13$$
$$-3 \equiv 13 - 3 \equiv 10 \bmod 13$$

即

$$4^{-1} \equiv 10 \bmod 13$$

用 10 乘 $4x \equiv 11 \bmod 13$ 得

$$40x \equiv 110 \bmod 13$$
$$x \equiv 6 \bmod 13$$

例 1.2.2 十进制数 $a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$，若

$$\left(\sum_{i=0}^{m} a_i 10^i\right)\left(\sum_{j=0}^{n} b_j 10^j\right) = \sum_{k=0}^{l} c_k 10^k \tag{1.2.1}$$

则

$$\left(\sum_{i=0}^{m} a_i\right)\left(\sum_{j=0}^{n} b_j\right) = \sum_{k=0}^{l} c_k \bmod 9$$

或

$$\left(\sum_{i=0}^{m} a_i \bmod 9\right)\left(\sum_{j=0}^{n} b_j \bmod, 9\right) \equiv \sum_{k=0}^{l} c_k \bmod 9 \bmod 9 \tag{1.2.2}$$

即式(1.2.2)成立是式(1.2.1)成立的必要条件。式(1.2.2)式不成立则式(1.2.1)式必然出错，当然式(1.2.2)式成立，并不能保证式(1.2.1)式正确但式(1.2.2)成立，而式(1.2.1)出错的概率比较小。所以可用式(1.2.2)作验证式(1.2.1)的正确性。从上例可知式(1.2.2)的验证要容易得多。

证明用到

$$10 \equiv 1 \bmod 9, \quad 10^i \equiv 1 \bmod 9, \quad i = 0,1,2,\cdots$$

$$\sum_{i=0}^{m} a_i 10^m \equiv \sum_{i=0}^{m} a_i \bmod 9$$

证明由读者来完成。但这个结果可以用来检验算术乘法的结果是否正确，例如

$$\begin{array}{r} 564 \\ \times 253 \\ \hline 1692 \\ 2820 \\ +)\ 1128 \\ \hline 142692 \end{array} \quad \Rightarrow \quad \begin{array}{r} 5+6+4 \equiv 6 \bmod 9 \\ \times)\ 2+5+3 \equiv 1 \\ \hline 6 \end{array}$$

$1+4+2+6+9+2\equiv 24\equiv 6 \mod 9$

$6=6$

1.3 Euler 函数

定义 设不大于正整数 n，而与 n 互素的函数为 $\phi(n)$，称 $\phi(n)$ 为 Euler(欧拉)函数。例如 $\phi(1)=1$，$\phi(2)=1$，$\phi(3)=2$，1 与任何数互素。若 p 是素数，则 $\phi(p)=p-1$。

定理 1.3.1 若 $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$，$a_i\geqslant 1$，$p_i$ 是素数，$i=1,2,\cdots,k$，则

$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

证 证明上面公式的方法颇多，下面利用一种比较直观的结果：

$$|A\cup B|=|A|+|B|-|A\cap B|$$

即具有性质 A 与性质 B 的元素数目 $|A\cup B|$ 等于具有性质 A 的元素数目 $|A|$ 与具有性质 B 的元素数目 $|B|$ 之和，减去同时具有性质 A 与性质 B 的数目 $|A\cap B|$（见图 1.3.1）。

这个公式还可以推广为

$$\begin{aligned}&|A\cup B\cup C|\\=&|A|+|B|+|C|-(|A\cap B|+|A\cap C|+|B\cap C|)+|A\cap B\cap C|\end{aligned}$$

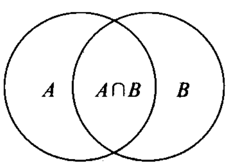


图 1.3.1

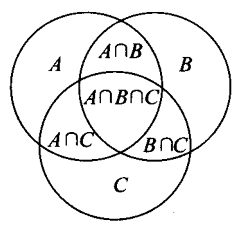


图 1.3.2

这个公式也很直观。无非加多了，减去加多了的部分；减多了，再补上减多了的部分，如图 1.3.2 所示。从 $|A\cup B|=|A|+|B|-|A\cap B|$ 也可以推出后一公式，中间用到

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$$

这一公式本身也十分直观，请读者从图 1.3.3 来识别这个公式所指的部分，哪一部分是 $A\cap(B\cup C)$，哪一部分是 $A\cap B$，$A\cap C$。依此类推，通过数学归纳法可得一般的公式：

$$\begin{aligned}|A\cup A_2\cup\cdots\cup A_n|=&|A_1|+|A_2|+\cdots\\&+|A_n|-(|A_1\cap A_2|+|A_1\cap A_3|+\cdots\\&+|A_{n-1}\cap A_n|)+(|A_1\cap A_2\cap A_3|+\cdots\\&+|A_{n-2}\cap A_{n-1}\cap A_n|)-\cdots\\&\pm|A_1\cap A_2\cap\cdots\cap A_n|\end{aligned}$$

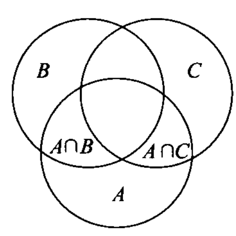


图 1.3.3

或

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{i=1}^{n}\sum_{j>i} |A_i \cap A_j|$$

$$+ \sum_{i=1}^{n}\sum_{j>i}\sum_{k>j} |A_i \cap A_j \cap A_k| - \cdots \pm |A_1 \cap A_2 \cap \cdots \cap A_n|$$

公式的证明留作思考。

还有一个比较直观的公式

$$(\overline{A \cup B}) = \overline{A} \cap \overline{B}$$

如图 1.3.4 影线所示的区域即$(\overline{A \cup B})$。更一般的公式有

$$(\overline{\bigcup_{i=1}^{n} A_i}) = \bigcap_{i=1}^{n} \overline{A_i}$$

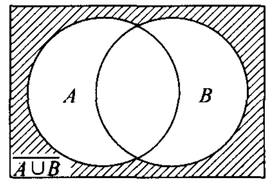


图 1.3.4

所以有另一个公式：

$$|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| = \left|\overline{\bigcup_{i=1}^{n} A_i}\right| = N - |A_1 \cup A_2 \cup \cdots \cup A_n|$$

$$= N - \left(\sum_{i=1}^{n} |A_i| - \sum_{i=1}^{n}\sum_{j>i} |A_i \cap A_j| + \cdots \pm |A_1 \cap A_2 \cap \cdots \cap A_n|\right)$$

其中 N 是全体元素的个数。

在利用后面这一公式证明欧拉函数计算公式之前，我们先看一个例子，求比 105 小与 105 互素的整数的个数。

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

令 A_1 为比 105 小并且是 3 的倍数的整数集合；

令 A_2 为比 105 小并且是 5 的倍数的整数集合；

令 A_3 为比 105 小并且是 7 的倍数的整数集合。

问题导致求

$$|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}| = 105 - (|A_1| + |A_2| + |A_3|) + (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) - |A_1 \cap A_2 \cap A_3|$$

$$A_1 = \frac{105}{3} = 35, \quad |A_2| = \frac{105}{5} = 21, \quad |A_3| = \frac{105}{7} = 15$$

$$|A_1 \cap A_2| = \frac{105}{15} = 7, \quad |A_1 \cap A_3| = \frac{105}{21} = 5$$

$$|A_2 \cap A_3| = \frac{105}{35} = 3, \quad |A_1 \cap A_2 \wedge A_3| = \frac{105}{105} = 1$$

故

$$|\overline{A_1} \wedge \overline{A_2} \wedge \overline{A_3}| = 105 - (35 + 25 + 15) + (7 + 5 + 3) - 1$$
$$= 105 - 71 + 15 - 1 = 48$$

这 48 个数是：

1,2,4,8,11,13,16,17,19,22,23,26,29,31,32,34,37,38,41,43,44,46,47,52,53,58,59,61,62,64,67,68,71,73,74,76,79,82,83,86,88,89,92,94,97,101,103,104。

现在来证明公式

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad a_i \geqslant 1, \quad i = 1,2,\cdots,k$$

令 A_i 为比 n 小并为 p_i 倍数的整数集合，$i=1,2,\cdots,k$，

$$|A_i| = \frac{n}{p_i}, \quad i = 1,2,\cdots,k$$

$$|A_i \cap A_j| = \frac{n}{p_i p_j}, \quad i,j = 1,2,\cdots,k$$

$$|A_1 \cap A_2 \cap \cdots \cap A_k| = \frac{n}{p_1 p_2 \cdots p_k}$$

所以有

$$\begin{aligned}
\phi(n) &= |\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_k}| \\
&= N - \left(\sum_{i=1}^{k} |A_i| - \sum_{i=1}^{k}\sum_{j>i} |A_i \cap A_j| + \cdots \pm |A_1 \cap A_2 \cap \cdots \cap A_k|\right) \\
&= N - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k}\right) + \left(\frac{n}{p_1 p_2} + \frac{n}{p_2 p_3} + \cdots + \frac{n}{p_{k-1} p_k}\right) - \cdots \pm \frac{n}{p_1 p_1 p_2 \cdots p_k} \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

推论 若 n_1, n_2 是两个互素的正整数，则

$$\phi(n_1 n_1) = \phi(n_1)\phi(n_2)$$

定理 1.3.2 若 n 是正整数，则

$$\sum_{d|n} \phi(d) = n$$

设将除尽 n 的因数 d 从小到大排列

$$1 = d_1 < d_2 < \cdots < d_r = n$$

则

$$n = d_1 d_r = d_2 d_{r-1} = \cdots = d_{r-1} d_2 = d_r d_1$$

现在先讨论 $n = d_1 d_r$，与 n 以 d_1 为最大公约数的数有 $\phi(d_r)$ 个，不大于 n 与 n 有公约数 d_1 的数为

$$d_1, 2d_1, \cdots, d_r d_1$$

若 $(sd_1, n) = d_1$，即 $(sd_1, d_r d_1) = d_1$，必要条件是 $(s, d_r) = 1$，这样的 s 共 $\phi(d_r)$ 个，所以不大于 n 与 n 有最大公约数的数共 $\phi(d_r)$ 个。

同样的道理，不大于 n 以 d_2 为最大公约数的数有 $\phi(d_{r-1})$ 个……不大于 n 与 n 有最大公约数 d_r 的数有 $\phi(d_1)$ 个，任何一个不大于 n 与 n 有一个最大公约数，或为 d_1 或为 d_2 或为 d_r，所以

$$n = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_r) = \sum_{i=1}^{r} \phi(d_i)$$

1.4 Euler 定理、Fermat 定理

Euler 定理：若 $(a, m) = 1$，则

$$a^{\phi(m)} \equiv 1 \bmod m$$

证 设 $r_1,r_2,\cdots,r_{\phi(m)}$ 是 $\phi(m)$ 个小于 m 与 m 互素的数，则序列

$$ar_1, ar_2, \cdots, ar_{\phi(m)} \bmod m$$

是 $r_1,r_2,\cdots,r_{\phi(m)}$ 的某一种排列，即不存在 $r_i,r_j(\neq r_i)$ 使

$$ar_i \equiv ar_j \bmod m$$

因 $(a,m)=1$，故存在 $a^{-1} \bmod m$，使 $aa^{-1}\equiv a^{-1}a\equiv 1 \bmod m$，用 a^{-1} 乘 $ar_i\equiv ar_j \bmod m$ 导致

$$r_i \equiv r_j \bmod m$$

与假定相矛盾。故存在 $r_j\in\{r_1,r_2,\cdots,r_{\phi(m)}\}$，使

$$ar_i \equiv r_j \bmod m,$$

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)}, \quad \bmod m$$

由于 $r_1r_2\cdots r_{\phi(m)}$ 与 m 互素，故得

$$a^{\phi(m)} \equiv 1 \bmod m$$

Fermat 定理：p 是素数，$p\nmid a$ 则

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

Fermat 定理是 Euler 定理的 $m=p$ 时的特殊情况，p 是素数，$p\nmid a$，$(p,a)=1$，$\phi(p)=p-1$，故

$$a^{p-1} \equiv 1 \bmod m$$

例 1.4.1 $m=15$， $a=4$， $(a,m)=(4,15)=1$， $15=3\times 5$

$$\phi(m)=15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=15\times\frac{2}{3}\times\frac{4}{5}=8$$

小于 15 而与 15 互素的数共 8 个：1,2,4,7,8,11,13,14

有：

$$ar_1 \equiv 4, \quad ar_4 \equiv 8, \quad ar_3 \equiv 16 \equiv 1, \quad ar_4 = 28 \equiv 13$$

$$ar_5 \equiv 32 \equiv 2, \quad ar_6 = 44 \equiv 14, \quad ar_7 = 52 \equiv 7$$

$$ar_8 = 56 \equiv 11$$

由 Euler 定理，若 $(a,m)=1$，mod m 存在 a^{-1}，而且

$$a^{-1} \bmod m = a^{\phi(m)-1} \bmod m$$

$(a,p)=1$，p 是素数时，$a^{-1} \bmod p\equiv a^{p-2} \bmod p$。还可以利用 Euler 公式或 Fermat 定理来简化某些模幂运算。

例 1.4.2 求 $13^{2180} \bmod 58$，$\phi(58)=58\left(1-\frac{1}{2}\right)\left(1-\frac{1}{29}\right)=28$

$(13,58)=1$，根据 Euler 定理

$$13^{28} \equiv 1 \bmod 58$$

又 $2180=77\times 28+24$

$$13^{2180} = 13^{28\times 77+24} = (13^{28})^{77} \times 13^{24}$$

故

$$13^{2180} \bmod 58 \equiv (13^{28})^{77} \times 13^{24} \bmod 58$$

$$\equiv 13^{24} \bmod 58 = (13^2)^{12} \bmod 58$$