EVANGELOS KRANANIS

数论与密码学

PRIMALITY AND CRYPTOGRAPHY

中国人民解放军 总参谋部第五十一研究所

数论与密码学

Primality and Cryptography

作者：Evangelos Kranakis

译者：何良生

校对：黄浩

总参第五十一研究所翻译
总参机要局第六处 印刷

1988年12月

译者序

自1976年迪菲－-赫尔曼发表了著名的<< New Directions in Cryptography >>和1977年美国联帮标准局公布了DES以来，密码学已经引起了世界上许多密码学专家、大学教授、学者和其它业余爱好者的广泛重视和研究，使密码学冲破了视为禁区的军事、外交领域而开始走向民间，并逐步渗入了数学、计算机科学、信息论、通信等科学领域。于是各国的民间密码学术讨论会以至世界性的密码学术讨论会应运而生.社会领域的各个部门包括政府、商业界、金融贸易界、甚至一些企图保密某些信息的个人均对此产生了浓厚的兴趣，有些应用已为社会带来了效益。

近几年来，各种密码学专著和优秀论文不断涌现。对传统的报密、话加密以及计算机数据库，计算机网络通信领域的数据加密作了许多介绍和探讨，对各种密码体制作了许多分析和阐述。但是，迄今为止，在我们国内能系统地代表研究方向的数论密码基础理论专著尚不足，而随着计算机与通信事业的发展，对数论密码的研究显得愈来愈重要和迫切。我们翻译了这本数论密码试图弥补其不足以满足社会各界的研究及应用要求。

本书是计算机科学系列出版物之一，这些出版物包括<<Fundamentals of the average case analysis of particular algorithme>> <<The foundations of program verification>><<Primaty and Cryptography>><<Telecommunication-security measures>> Computers-Access contral>><<Cryptography>> 出版这些书的编辑委员会成员是：德国的萨尔大学数学和信息论科学系教授古力特贺滋（Günter.Hotz),美国的新哈芬康乃狄各州耶鲁大学计算机科学系教授米卡尔.J.费斯克尔(Michael J.Fischer)，法国的巴黎大学数学和信息科学系教授迈雷尔尼瓦特（Maurice Nivat)，英国的南普屯大学计算机研究系教授戴维W.巴伦(Divid W.Barron)。我们选译了<<Primatity and Cryptography>>，该书是耶鲁大学教授 Evangelos KranakiS撰写的，于1986年出版。我们认为该书是目前信息保密研究和应用中一部很有价值的书。它系统地把数论和密码学紧密地联系在一起，自成一个体系。所列参考资料齐全，读者阅读时可以不翻阅其它任何书籍即可通盘了解，观其全貌。根据该书的内容和深度，它可供从事密码学、数学、计算机科学、信息论以及通信等学科的研究人员、大学教师、工程师、技术人员阅读和参考，亦可供上述有关学科的研究生和大学本科高年级学生阅读。

该书已分别受到美国、英国、法国、联帮德国、加拿大、澳大利亚、新加坡等国的有关专家学者的关注。

我们翻译这本书以忠实于原文的意义为宗旨，在翻译过程中，尽量考虑中国读者的语言习惯以便读者阅读时感到轻松愉快.原文有明显错误的地方，译者作了改正并加了译者注。

该书由何良生同志翻译，黄浩同志校阅，郭远福同志作了大量的文字整理工作。由于时间仓促，译校水平有限，错误和不当之处难免，望读者批评指正，以便再版时修正。

译．校．者

88,10.

原版前言

有史以来，人们为了使得所传递的消息的意义对非法的用户是不可理解的，因此，在军事和外交通信领域，密码术已经获得了广泛的应用和发展。根据 Francis Bacon 的观念，在密码体制的所有优点之间，下面的几条是必须的：

- 对合法用户来说，密码的读和写是容易的，
- 对非法的用户来说，解密是不可能的，
- 对合法用户来说，解密是没有疑义的。

在今天，上面所列的 Bacon 的三条基本原理仍然是正确的，而且，引用迪菲(Diffie)和赫尔曼(Hellman)的一段论述：

> 控制通讯网络的计算机的发展，可以保证使得处于世界上不同地点的人或计算机之间的接触变得不费力而又廉价，而且可以用远程通信来代替大部分邮政和信使。对许多应用来说，这些联系都必须保证安全，既要防止窃听又要防止一些不合法的消息渗入线路。但是目前安全问题的解决还大大落后于通讯技术的其它一些领域，现时的密码已不能满足需要了。这种密码强加给这种体制的用户这样严重的不便，以致于抵消了使用远程数据处理新技术所带来的许多好处。

在许多用户之间经由电子媒介安全传输信息这种要求使得密码学从古老的绝对安全性观念中解脱出来而接受新的相对安全性关念成为必然。这样一来，在前一种安全性观念下，设计者使密码体制的安全性基于绝对的标准(例如仙侬信息理论)，在后一种安全性观念下，人们只是在以某个问题(通常是数论）是难解性的问题的假定下来证明所设计的体制是安全的。这种新的思想已经使得构造公开密钥密码体制成为可能，在这方面，迪菲和赫尔曼这样写道：

> 通信双方只使用公开的信道而且仅仅利用公开的已知技术即可进行一次安全的通信联系。

本书是1984年春季耶鲁大学密码学术讨论会上一系列报告的概括。它的目的是离析和分析从现代的有关素性检测、伪随机生成器和公开密钥密码体制方面的文献中所提出的一些最重要的数学观念。在做这项工作时，我已经

尽力使得本书尽可能地自包含。

第一章发展了计算数论的技术，这些技术对理解有关伪随机生成器和公开密钥密码体制方面的现代文献是必要的。同时基于数论概念，本书给出了下面一些观念和算法：阀方案，重复平方和乘法模数指数法，艾德尔曼、蔓得斯、米勒关于计算平方根的算法和佛里格、赫尔曼关于计算指标的算法。

第二章给出了一些到目前已知的最重要的素性检测。为完整性起见，开始于恩拉托森斯筛，接下来是Williams[4]，素性检测可以被分成三种类型：利用特殊函数的检测(例如：鲁卡斯-勒黑姆检测)，未被证明的假设检测(即它的有效性依赖于扩展黎曼假设)和蒙特卡罗检测(例如斯洛娃-斯嘲森，拉宾)。另外还给出了布拉特检测；这个检测可以被用来确定素数的二元表示所形成的集合的复杂度。这一章以非常快的鲁米尼-艾德尔曼检测而告结束。

第三章是对在伪随机生成器和公开密钥密码体制的发展中所需要的基本的概率论观念的一个导引。精采部分包括弱大数定律和伯恩斯坦大数定律。

第四章和第五章不打算对文献中所有存在的伪随机生成器和可用的公开密钥密码体制给出其详尽的研究。我们的意图是通过仅仅给出一些基本的生成器和密码体制来清楚了解数论和现代公开密钥密码学之间的联系。同时，我们完全省略了对非公开密钥密码学的讨论。但是读者在后面所列的这本书可以找到您心满意足的资料：David Shulman's, An Annotated Bibliography of Cryptography, 在本书的参考文献中也列入了这篇资料。

最后，第六章略述了伪随机生成器和公开密钥密码体制的主要理论。所给出的材料包括：下一比特检测和Yao's统计检测的等价，基于伪随机函数以及异或定理的不可逼近谓词和单向函数的构造。

读者可能会注意到因式分解算法没有被写进本书，M.Voorhoeve在文章“指数阶的因子分解算法”中和C. Pomerance在文章“某些整数因子分解算法的分析和比较”中都把这个专题讨论得很漂亮。

在本书中，我已经尽最大的努力以最直接的方式给出这些材料并保证其数学上的严谨性。正如大卫.希尔伯特所说的：

> ... 认为证明中的严谨性是简单性的敌人是一个错误。相反，我们通过大量的例子可以证实严谨的方法同时也是更简单和更容易被理解的方法。对证明的严谨性所作的巨大努力迫使我们找到更简单的证明方法。它也频繁地引导这种方法到比具有更少严谨性的老方法更具发展能力的方法。

在每一章末尾的文献附注中，给出了著作目录指南。读者对文献中所引文章中给出的许多不同的观点应有所了解，当然，并不是所有都能够被包括在本书中。另外，省略的专题包括：信息论，数据加密标准，数字签名，表决方案和验证技术。我希望，如果您渴望获得有关这方面一个更详细的陈述，您可求助于所列的参考文献。

本书给出的结果预先假定读者具有理论计算机科学或数学专业的大学生应该具有的数学修养。基本代数观念方面的某些知识(例如：群、环、同态)将是有用的。由于读者的背景可能是各种各样的，因此，我难以准确说明具体读这本书时所应该采用的合适次序。然而，图1能给出各章相互依赖的一种看法。因而，第一章和第二章可以独立于其它章而一起读；只在2.16节(概率素性检测)和第四、第五、第六章用到第三章的内容.另外，如果读者已经熟悉了有关伪随机生成器和公开密钥密码体制的基础知识，那么他可直接学习第六章。

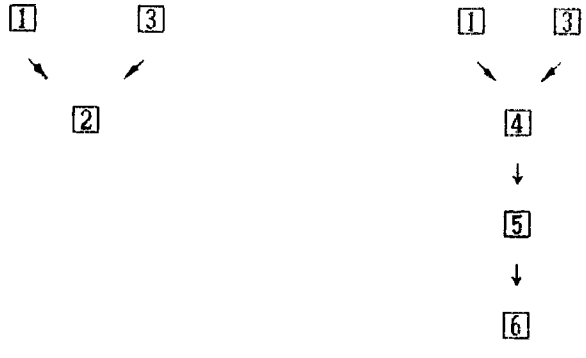

图1：各章之间的依赖性

在大多数节的末尾给出了一些练习，这些练习包括三种类型：对在主要正文中已经被证明的结果给出其另一种不同的证明；给出一些附加的结果以及提醒读者他必须完成主要正文中所给出证明的详细陈述。在任何情形下，练习将能检验和加深读者对材料的了解，读者应该试做所有的练习。

在本书中广泛使用了“有效算法”的概念，读者应认为“有效算法”的概念是等同于概率多项式时间算法的。

对正文中所给出的结果，我已经尽最大的努力使读者知道它们的原始发明人，如果有时我没有这样做，那是由于我不知而不是故意。同时对本书可

能包含的缺陷和错误我负全部责任，而且我非常乐意收到能改进本介绍的任何批评和建议。

我非常感激我的许多同事，他们对本书的初稿提出了许多意见和改进。另外，我要特别地感谢在最初报告期间研讨会的成员对我所提出的启发性意见。他们是：Dana Angluin, Josh Cohen, Mike Fischer, Dan Gusfield, Neil Immerman, Ming Kao, Philip Laird, Susan Landau, Jerry Leichter, Jingke Li, Angus Macintyre, Lenny Pitt, Philip Scowcroft, David Wittenberg And Carol Wood. 我特别要感谢Dan Gusfield和Silvio Micali, Dan Gusfield激发我研究素性检测，和Silvio Micali对最后三章的组织和注释提出了大量的改进。我也衷心感谢 Mike Fischer的大力支持和鼓励以及大量的有远见卓识的讨论，这些讨论帮助我改进了第六章的介绍。

排印工作是由作者在耶鲁大学计算机科学系利用TEX的一个译本LATEX完成的。

伊万季诺斯　克雷勒基斯
耶鲁大学
1985.8.

第一章 数 论

1.1 引言

首先，这一章是想向读者引进一些基本的数论概念。其次，是想向读者提供数论中某些问题研究的有效步骤。这里所引进的概念和结果对素性检测，伪随机生成器和公开密钥密码体制的讨论是必要的。

这一章所引进的概念包括：费波拉契数，欧拉函数，本原根，凯米丘尔函数，勒根爵－雅柯比符号，指标和连分数。另外，对以下几个定理给出了完备的证明：关于乘法群Z_m^*具有循环群特性的那些m的特征的高斯定理(定理1.9)，二次互反律(定理1.13)，素数定理的一个更弱说明的车贝谢夫证明(定理1.20)，丢番图近似定理(定理1.24)。定理1.7给出了中国剩余定理对阀方案的一个应用。

这一章描述了以下一些算法：重复平方和相乘的指数方法(定理1.8)，埃得尔曼、曼得斯和米勒关于模素数平方根的计算方法(定理1.15)，富里格(Pholig)和赫尔曼计算指标的方法(定理1.18)。

确实，这一章中所给出的某些定理的详细证明(即定理1.9，1.13和1.20)对理解这几章中所包含的有关伪随机生成器和公开密钥密码体制的概念可能不是十分必要的，但是，对这些证明和每节后面的练习的致深学习和研究，将无可怀疑地会提高读者对所包含的数论理论的修养。

1.2 同态论

设H，G是两个阿贝尔群，$H\subseteq G$。对$a\in G$，我们考虑陪集$H+a=\{h+a, h\in H\}$，这里“+”是G的群运算。G／H是G模H的商群。它包含所有H+a陪集，这里a取遍G。G／H的群运算“$\oplus$”定义为$(H+a)\oplus(H+b)=H+(a+b)$，不难证明具有这个群运算的G／H也是一个阿贝尔群。显然，陪集的集合$\{H+a: a\in G\}$是G的一个划分，并且每个集合的大小为|H|，容易推出|H|整除|G|。

设f是群G到群H的一个满同态(也就是说f是一个到上的群同态)，f的核$K=\ker(f)$是使f(a)等于H中的单位元素的所有那些a的集合，这里$a\in G$，不难证明群G／K是同构于H的阿贝尔群。所要求的同构映射为$F(k+a)=f(a)$，

回忆下述定理的证明已经被略述：

定理1.1 (Lagrange)

(i) 如果$H\subseteq G$，则$|H|$整除$|G|$。

(ii) 如果f是阿贝尔群G到阿贝尔群H的一个闵同态，并且K是f的核，那么，群G/K同构于群H。此外，$|G|=|K|\cdot|H|$。

(iii) 对所有的$a\in G$, $f^{-1}(a)$是G/K中的一个元素且$|f^{-1}(a)|=|K|$。

练习

1、设G是一个有限阿贝尔群，证明具有形式$x^2=a(a\in G)$的所有方程在G中具有完全相同个数的解。提示：考虑阿贝尔群$H=\{a^2, a\in G\}$，并且让f是一个同态$f(x)=x^2$。然后利用定理1.1。

2、扩充练习1到形式为$x^n=a$的方程，这里$a\in G, n\geqslant 1$。

3、证明运算“$\oplus$”的定义是独立于陪集首的选择的。

在下面的两个练习中$H\subseteq G$，通过证明练习1和练习5来完成定理1.1的证明。

4、对所有$a\in G$, $|H+a|=|H|$。

5、$\{H+a, a\in G\}$形成G的一个划分。

1.3 费波拉契数

由归纳法，费波拉契数序列$f_0, f_1, \ldots, f_n, \ldots$被定义如下：

$f_0=0$ 如果$n=0$

$f_1=1$ 如果$n=1$

$f_n=f_{n-1}+f_{n-2}$ 如果$n\geqslant 2$

了解n阶费波拉契数的数量级别大小是有用的。我们很容易用下述方法来确定它。我们知道二次方程x^2+x+1有两个平方根$(1+\sqrt{5})/2$和$(1-\sqrt{5})/2$。其中正的平方根$(1+\sqrt{5})/2$被称为黄金比率(golden ratio)，简记为R。通过对n进行归纳，容易验证对所有的$n>1$, $f_n\geqslant R^{n-2}$。的确，假定$f_m\geqslant R^{n-2}$对所有$m\leqslant n$成立，那么，$f_{n+1}=f_n+f_{n-1}\geqslant R^{n-2}+R^{n-3}=R^{n-3}(R+1)=R^{n-3}\cdot R^2=R^{n-1}$。

很自然，对经由欧几里德算法对两个整数的最大公因数估计的步骤数的研究，费波拉契数是有用的。的确，假定a>b>0是两个给定的整数，引用欧几里德算法定义序列

$0<r_n<r_{n-1}<\ldots<r_1<r_0=b<r_{-1}=a,\ d_1, d_2, \ldots, d_n, d_{n+1}$

满足$r_{i-2}=d_i r_{i-1}+r_i$, $i=1, 2, \ldots, n$，且$r_{n-1}=d_{n+1}r_n$。很清楚，$r_n=\gcd(a, b)$（看下面的练习1）。通过对$i=n, n-1, \ldots, 0, -1$进行逆归纳有$r_i \geqslant f_{n+1-i}$，特别，$a \geqslant f_{n+2}$，且$b \geqslant f_{n+1}$. 而事实上，经由欧几里德算法来计算$\gcd(f_{n+2}, f_{n+1})$所需要的除法步数仅为$n+2$，它也是计算$\gcd(a, b)$所需要的步除法数，由于$a \geqslant f_{n+2} \geqslant R^n$，我们有$\log_R a \geqslant n$，因此，下面定理已经被证明：

定理1.2（G.Lame） 如果N是一个大于0的整数，那么，对任何小于或等于N的两个正整数a、b，经由欧几里德算法来计算$\gcd(a, b)$所需要的除法步数至多为$-2+[\log_R N]$。

练习

1、利用上述记号证明$r_n=\gcd(a, b)$。

2、证明由欧几里德算法可导出一个计算下面问题的有效算法：给定任何整数a、b，计算α、β使得$\gcd(a, b)=a\alpha+b\beta$。并把它推广到n个整数的最大公因数。

3、对n个整数的最大公因数验证类似于定理1.2的结果。

4、对n个整数的最小公倍数验证类似的结果。提示：利用等式$\mathrm{lcm}(a_1, a_2, \ldots, a_n)=(a_1 a_2, \ldots, a_n)/\gcd(a_1, \ldots, a_n)$。

5、证明单位圆的内切正十边形的边长为R，这里R是黄金中值。

1.4 同余

设a, b是整数，符号a|b表示a整除b，也就是对某个整数k有b=ka。称整数a, b是模整数m同余的（记为$a \equiv b \bmod m$）如果m|(a-b)，否则称a, b是模m非同余的（记为$a \not\equiv b \bmod m$）。很清楚，对每一个固定的m，关系“$\equiv \bmod m$”具有反身性、对称性和传递性，因此它是所有整数构成的集合Z上的一个

等价关系，对每一个整数a，用$\bar{a}$表示a的等价类，也就是说，$\bar{a}=\{x, x\equiv a \bmod m, x\in Z\}$。对每一个m，仅仅存在m个模m的等价类，也就是说$\bar{0}, \bar{1}, \ldots, \overline{m-1}$。$Z_m=\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$是模m的所有等价类的集合，$Z_m^*=\{\bar{a}\in Z_m, \gcd(a, m)=1\}$。

在集合Z_m上，我们能象下面一样定义两种运算，加法(用“+”表示)，乘法(用“·”表示)：$\bar{a}+\bar{b}$(相对应地$\bar{a}\cdot\bar{b}$)=a+b的等价类(相对应地a·b的等价类)。赋于这两种运算的集合Z_m形成一个有单位元的交换环，但不一定是一个域，因为它可能有零因子。然而$<Z_m, +>$和$<Z_m^*, \cdot>$都是阿贝尔群。

例1.1　图1给出了Z_{11}^*的乘法表

·	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

图1：Z_{11}^*的乘法表

如果$\gcd(a, m)=1$，则存在整数b，c，满足$ab+cm=1$，因此$\bar{a}\cdot\bar{b}=\bar{1}$，也就是说$\bar{a}$在$Z_m^*$中是可逆的。群$Z_m^*$的阶用$\phi(m)$表示，这里$\phi$是欧拉示性函数(Eulertotint function)或简称为欧函数。

由上面的讨论可得到一个重要的推论：

定理1.3 (Euler－Fermat) 对所有$a\in Z_m^*$,有$a^{\phi(m)}\equiv 1 \bmod m$

证明： 设a如上，让$\mu_1,\ldots,\mu_{\phi(m)}$是$Z_m^*$中的所有元素。很清楚，$a\cdot\mu_1,\ldots,a\cdot\mu_{\phi(m)}$也是$Z_m^*$中的所有元素。相应地$a\cdot\mu_1\cdot\ldots\cdot a\mu_{\phi(m)}=\mu_1\cdot\ldots\cdot\mu_{\phi(m)}$,因此$a^{\phi(m)}\cdot\mu_1\cdot\ldots\cdot\mu_{\phi(m)}=\mu_1\cdot\ldots\cdot\mu_{\phi(m)}$。但是从上面可观察到$\mu_1\cdot\ldots\cdot\mu_{\phi(m)}$在$Z_m$中是可逆的。从而有$a^{\phi(m)}\equiv 1 \bmod m$。

为了避免记号上的不必要的复杂性，从现在起我们将用同样的符号来代表一个整数a和它的等价类$\overline{a}$(模整数m)。由于两个符号所代表的内容是很清楚的，因此上述记法不会引起混乱。

定理1.4 (Euler) $\sum_{d|m}\phi(d)=m$

证明 设$\phi_d(m)=|\{x\in Z_m;\gcd(x,m)=d\}|$,那么，$\sum_{d|m}\phi_d(m)=m$.然而，只要$d|m$，$\phi_d(m)=\phi(m/d)$。从而推出

$$m=\sum_{d|m}\phi_d(m)=^{*}\sum_{d|m}\phi(m/d)=\sum_{d|m}\phi(d)$$

这就完成了定理的证明。

(*原文中为$\phi(d/m)$,有错－译者注)

具有形式$f(x)\equiv 0 \bmod m$的任何同余称为模m多项式同余，这里f(x)是系数在Z_m中变量为x的多项式。如果存在$x\in Z_m$使$f(x)\equiv 0 \bmod m$，则称这个同余是可解的；$\{x;f(x)\equiv 0 \bmod m, x\in Z_m\}$称为这个同余的解集合。探讨解$f(x)\equiv 0 \bmod m$的同余是数论中最重要的问题之一，这里f(x)是系数在Z_m中变量为x的多项式。具有一个未知数的线性同余解在下述定理中得到了回答。

定理1.5 线性同余$ax\equiv b \bmod m$是可解的当且仅当$g=\gcd(a,m)$整除b。事实上，如果x_0是$ax\equiv b \bmod m$的任何解，那么

$$x_i=x_0+im/g,\qquad i=0,1,\ldots,g-1$$

形成了它模m的不同解的完全集合。

证明 如果$ax\equiv b \bmod m$是可解的，那么m必须整除ax-b。由于$g|m$且$g|a$，因此$g|b$。相反地，假定$g|b$,则有$b=kg$,对某个整数k,利用最大公因数的基本性质，我们知道存在整数λ、μ使得

$$g=\lambda a+\mu m$$

从而

$$b=kg=k\lambda a+k\mu m=(k\lambda)a+(k\mu)m$$

因此$k\lambda$是同余方程$ax\equiv b \bmod m$的一个解。

由上不难看到，如果x_0是上述同余方程的任何解，则定理中定义的任何x_i也是上述同余方程的解。此外，解x_i还是模m不同的。剩下只需证明$ax\equiv b \bmod m$的任意解c都等于某个x_i即可。的确，由于$ac\equiv ax_0\equiv \bmod m$，从而有$m|a(c-x_0)$，但是$g=\gcd(a, m)$，因此$(m/g)|(c-x_0)$，到此完成了定理的证明。

练习

1、证明对所有$n\geqslant 1$，n是素数当且仅当$\phi(n)=n-1$。

2、证明对所有$t\geqslant 1$和所有素数p，$\phi(p^t)=(p-1)p^t$。利用它来计算$\phi(n)$，这里n为大于0的任意整数。

1.5 中国剩余定理

即使每一个同余方程有解，整个线性同余方程组也不一定有解。

例1.2 $x\equiv 0 \bmod 3$和$x\equiv 1 \bmod 6$每一个都有解，但整个系统没有解。

但是如果模数是两两互素的，则这个系统总是有解的。

例1.3 23是下面的同余系统的一个解：

$$x\equiv 2 \bmod 3 \quad x\equiv 3 \bmod 5 \text{ 和 } x\equiv 2 \bmod 7$$

下面的定理给出了一般的线性同余系统的结构。

定理1.6 (Chinese Remainder Theorem) 只要$m_1, m_2, \ldots, m_k$是两两互素的并且$\gcd(a_1, m_1)=\ldots=\gcd(a_k, m_k)=1$，那么系统$a_ix=b_i \bmod m_i (i=1, 2, \ldots, k)$恰好有一个解(模$m=m_1m_2\ldots m_k$)。

证明 从定理的假设我们很容易推出解的唯一性。为了证明存在性，可找整数c_i满足$a_ic_i\equiv 1 \bmod m_i$，这里$i=1, 2, \ldots, k$。如果$m=m_1\ldots m_k$并且$n_i=m/m_i$，那么，$\gcd(n_1, \ldots, n_k)=1$。因此，从最大公因数的基本性质可推出，存在整数$t_1, t_2, \ldots, t_k$使得

$$t_1n_1+t_2n_2+\ldots+t_kn_k=1$$

令$e_i=t_in_i$，那么，我们很容易验证

$$e_i\equiv\delta_{i,j}\bmod m_j$$

这里当i=j时，$\delta_{i,j}=1$；当$i\neq j$时，$\delta_{i,j}=0$。选择

$$c=e_1c_1b_1+\ldots+e_kc_kb_k$$

只要证明c是前叙同余系统的解即可。事实上，对每个i

$$a_ic\equiv a_ib_1c_1e_1+\ldots+a_ib_kc_ke_k\equiv a_ib_ic_ie_i\equiv b_i\bmod m_i$$

到此完成了证明。

不假定模数是两两互素的中国剩余定理的进一步推广可以在[L13]的定理3-12中找到(参看练习2)。

关系到消息传输的安全性，涉及(k,n)阈方案的构造，中国剩余定理有一个有趣的应用。一个阈方案由n个人$P_1,P_2,\ldots,P_n$组成，并且他们共享一个秘密S，且共享的方式满足下述性质：

(1) $k\leqslant n$.

(2) 每个P_i有某些信息I_i。

(3) 知道$\{I_1,I_2,\ldots,I_n\}$中的任何k个消息能使人很容易地发现S.

(3) 知道$\{I_1,I_2,\ldots,I_n\}$中任何l(l<k)个消息不能使人很容易地发现S.

定理1.7 对所有$2\leqslant k\leqslant n$，存在一个(k,n)阈方案。

证明 (k,n)阈方案的构造是基于(k,n)阈序列的构造，米格罗特(Mignotte)如下定义了阈序列：一个(k,n)阈序列是一个递增的序列$m_1<m_2<\ldots<m_n$，$m_1,m_2,\ldots,m_n$是两两互素的正整数且满足

$$m_1m_2\ldots m_k>m_nm_{n-1}\ldots m_{n-k+2}\qquad(1)$$

假定一个阈序列$m_1<m_2<\ldots<m_n$已经被构造，让$M=m_1m_2\ldots m_k$，$N=m_nm_{n-1}\ldots m_{n-k+2}$。设秘密S是满足$N<S<M$的任何整数，并且设消息$I_i$如下定义：

$$I_i\equiv S\bmod m_i,\quad i=1,2,\ldots,n$$

下面我们将证明如上定义的秘密S和信息$\{I_1,I_2,\ldots,I_n\}$形成一个(k,n)阈方案。事实上，我们设$\{I_{i1},I_{i2},\ldots,I_{ik}\}$被给定，由中国剩余定理，系统

$$x\equiv I_i\bmod m_i,\quad i\in\{i_1,i_2,\ldots,i_k\}$$

好有一个解。定理1.6的证明表明这个解是S，并且给出为

$$S \equiv e_{i1} \cdot I_{i1} + \ldots + e_{ik} \cdot I_{ik} \bmod (m_{i1} \ldots m_{ik})$$

这里$e_i \equiv \delta_{i,j} \bmod m_j$。从(1)可以推出$S < m_{i1} \ldots m_{ik}$，因此

$$S = e_{i1} \cdot I_{i1} + \ldots + e_{ik} \cdot I_{ik}$$

另一方面，要是$\{I_{i1}, \ldots, I_{ik-1}\}$被给定，那么，从中国剩余定理推出

$$S \equiv e_{i1} \cdot I_{i1} + \ldots + e_{ik-1} \cdot I_{ik-1} \bmod (m_{i1} \ldots m_{ik}) \qquad (2)$$

很清楚，为了计算S，由(2)仅仅只能得到S的模$m_{i1} \ldots m_{ik}$的值。因此为了发现满足(2)的秘密S，人们至少需要在$(M-N)/N$个可能的值中进行搜索。

为了结束定理的证明，我们只需构造满足数量$(M-N)/N$是大的(k, n)阈方案。这将会使得当$\{I_1, I_2, \ldots, I_n\}$中$l(l<k)$个消息被知道时，人们难于计算S。这个可利用1.15节练习3中的主要不等式来作。事实上，可找到t使前面被提到的不等式保持，可推出在区间$(P_t(k^t-1)/k^t, P_t]$至少存在n个素数。设$m_1, m_2, \ldots, m_n$是这个区间内的后n个素数，也就是说$m_i = P_{t-n+i}(i=1, 2, \ldots, n)$。剩下来只需证明这是一个阈序列。事实上，

$$M = m_1 m_2 \ldots m_k \geqslant P_t^{k-1/k} > P_t^{k-1} \geqslant m_n m_{n-1} \ldots m_{n-k+2} = N$$

由于

$$(M-N)/N \geqslant (P_t^{k-1/k} - P_t^{k-1}) / P_t^{k-1} = P_t^{1-1/k} - 1$$

到此完成了定理的证明。

练习

1、如果r是$m(>1)$的不同素因数的个数，那么，$x^2 \equiv x \bmod m$恰好有2^r个不同的模m解。提示：利用中国剩余定理。

2、中国剩余定理的下述推广没有预先假定模数是两两互素的。更精确地证明下述表达是等价的：

(1) 系统$x \equiv b_i \bmod m_i \quad (i=1, 2, \ldots, n)$有一个解。

(2) 任何指标对$1 \leqslant i, j \leqslant n$，

$$b_i \equiv b_j \bmod (\gcd(m_i, m_j))$$

此外，如果这个解存在，那么，它是模$\mathrm{lcm}(m_1, \ldots, m_n)$唯一的。

1.6 模指数

给定一个固定的模数m和一个指数e，及任意的x，存在$x^e \bmod m$的计算问题。下面描述了解这问题的方法，我们称这种方法为重复平方和乘法指数法。

定理1.8 存在一个有效的算法A使得：当其输入为给定的m、e、x时，它的输出$A(m,e,x)=x^e \bmod m$，算法A至多需要$[\log_1 e]$次平方、$[\log_2 e]$次乘法和$[\log_2 e]$次除法。

证明 如上所述，设m、e、x是整数，考虑e的二元系统表示，即$e=2^n e_n+2^{n-1}e_{n-1}+\ldots+2e_1+e_0$，这里$n=[\log_2 e]$。那么，$X^e \equiv X^{2^n e_n+\ldots+2e_1+e_0} \bmod m$。通过逆归纳，如下定义序列$x_0, x_1, \ldots, x_n$和$y_1, y_2, \ldots, y_n$：$x_n=x^{e_n}$，$y_n=X_n^2 \bmod m$，对$i \geqslant 1$，定义$x_{n-i} \equiv y_{n+1-i} X^{e_{n-i}} \bmod m$，$y_{n-i} \equiv x_{n-i}^2 \bmod m$。容易推出$x_0 \equiv X^e \bmod m$。

下面的算法表述了上面的递归构造：

输入：e，m，x

步骤1：计算n和$e_0, e_1, \ldots, e_n$各比特使得

$e=2^n e_n+2^{n-1}e_{n-1}+\ldots+2e_1+e_0$，这里$e_n \neq 0$

步骤2：让y = 1

步骤3：对$i=n, n-1, \ldots, 0$重复作$y \equiv y^2 X^{e_i} \bmod m$。

输出：y

例1.4 利用前面的算法，例1.1的表，$13=2^3 \cdot 1+2^2 \cdot 1+2^1 \cdot 0+2^0 \cdot 1$这个事实和图2的表可证明$7^{13} \equiv 3 \bmod 11$。

i	ei	y≡Y	输出
3	1	a · A	7
2	1	b · B	2
1	0	c · C	4
0	1	d · D	2

Y：$y^2 7^{e_i} \bmod 11$；$a=1^2$；$b=7^2$；$c=2^2$；$d=4^2$；$A=7^{e_3}$；$B=7^{e_2}$；$C=7^{e_1}$；$D=7^{e_0}$

图2 $7^{13} \bmod 11$的计算