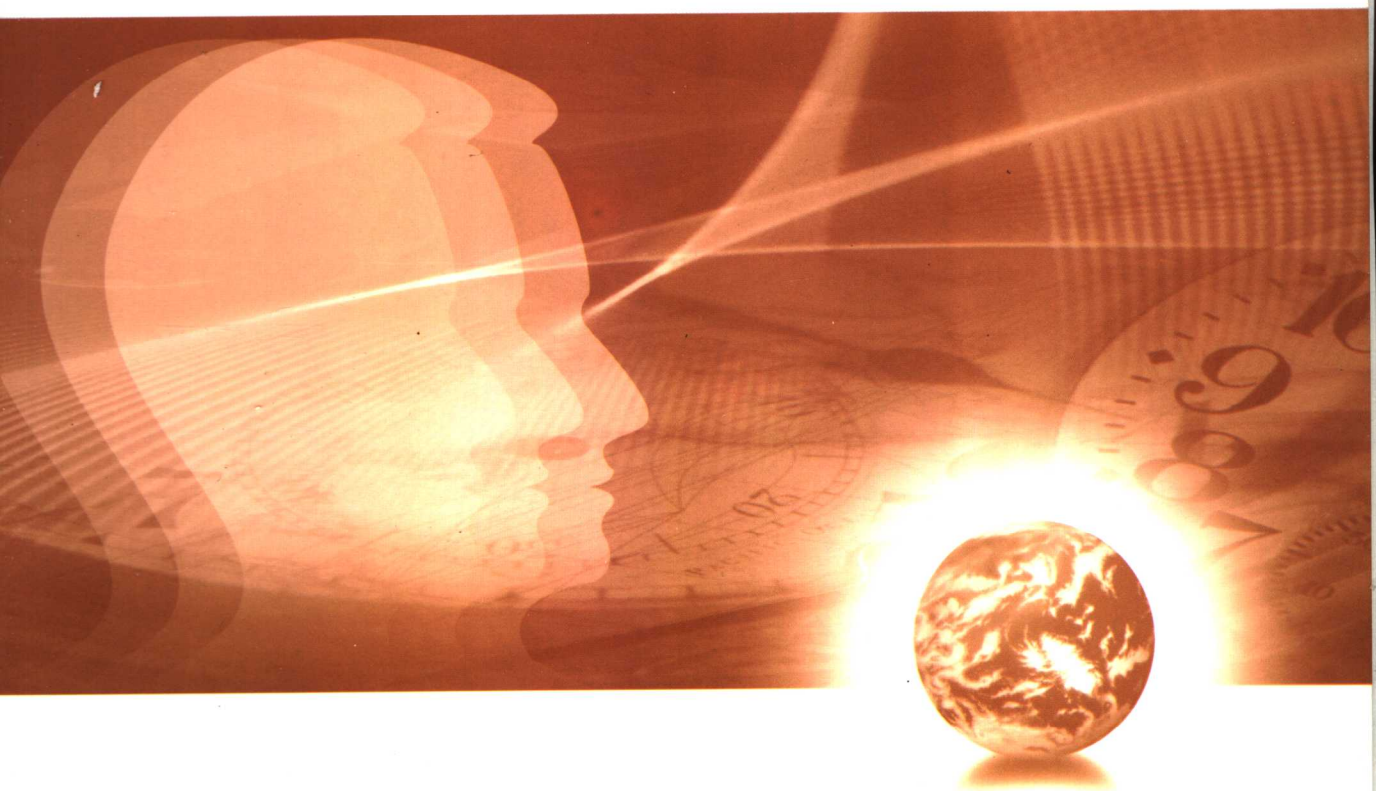
高等院校计算机科学与技术
“十五”规划教材

应用密码学



王衍波 薛通 编著

机械工业出版社
CHINA MACHINE PRESS

高等院校计算机科学与技术“十五”规划教材

应用密码学

王衍波　薛　通　编著

机械工业出版社

本书讲解了现代密码学的数学基础知识和基本概念，DES、IDEA、AES等对称密码算法，RSA、NTRU 等公钥密码算法，ElGamal、DSS 等数字签名算法及序列密码学的基础。还讲解了现代密码学的三个新的重要研究方向：椭圆曲线密码学、混沌密码学、量子密码学的基本原理和方法。最后讲解了几个典型的密码协议。

本书可用作信息安全专业本科生的教材，也可作为其他信息技术专业的研究生、科技工作者的参考用书。

图书在版编目（CIP）数据

应用密码学/王衍波，薛通编著. —北京：机械工业出版社，2003.8
高等院校计算机科学与技术“十五”规划教材
ISBN 7-111-12781-1

Ⅰ. 应… Ⅱ. ①王…②薛… Ⅲ. 密码—理论—高等学校—教材
Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字（2003）第 066342 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策　　划：胡毓坚
责任编辑：车　忱
责任印制：路　琳

北京大地印刷厂印刷 · 新华书店北京发行所发行

2003 年 8 月第 1 版 · 第 1 次印刷
787mm×1092mm 1/16 · 14 印张 · 345 千字
0001－5000 册
定价：20.00 元

出 版 说 明

信息技术高度普及的今天，具备一定层次的信息技术素养成为社会素质教育的一个重要目标，由此对高等院校的计算机专业教育提出了更高更新的要求。教育水平提高的关键是教学质量，那么对教学质量有直接影响的教材建设就成为了计算机专业教育的根本，为重中之重。

适逢高等院校计算机专业教育改革的关键时期，为配合相关的教材建设，机械工业出版社会同全国在该领域内享誉盛名、具备雄厚师资和技术力量的高等院校，包括清华大学、上海交通大学、南京大学、成都电子科技大学、东南大学、西安电子科技大学、解放军理工大学、北京科技大学等重点名校，组织了多位长期从事教学工作的骨干教师，集思广益，对当前高等院校的教学现状开展了广泛而深入的研讨，继而紧密结合当前技术发展需要并针对教学改革所提出的问题，精心编写了这套面向普通高等院校计算机专业的系列教材，并陆续出版。

本套教材内容覆盖了普通高等院校计算机专业学生的必修课程，另外还恰如其分地添加了一些选修课程，总体上分为基础、软件、硬件、网络和多媒体五大类。在编写过程中，对教学改革力度比较大、内容新颖以及各院校急需的并且适应社会经济发展的新教材，优先选择出版。

本套教材注重系统性、普及性和实用性，力求达到专业基础课教材概念清晰、深度合理的标准，并且注意与专业课教学的衔接；专业课教材覆盖面广、深浅适中，在体现相关领域最新发展的同时注重理论联系实际。全套教材体现了教育改革的最新思想，可作为高等院校计算机科学与技术专业的教学用书，同时也是培训班和自学使用的最佳教材。

机械工业出版社

前　言

随着计算机网络的普及，大量的电子数据通过网络传输到世界各地成为可能。但在具有重大的经济价值或关系国家、军队的命运等重要数据的传输过程中，任何一点泄露和差错都可能造成不可估量的损失。如何保证信息的机密性、真实性、不可否认性是密码学研究的重要课题。密码技术是信息安全的保障及核心技术。计算机网络、通信技术的发展和信息时代的到来，给密码学提供了难得的发展机遇，密码理论、密码技术、密码管理等研究与应用进入了一个新的时期。

现代密码技术被应用到了信息技术的所有领域，已从传统的单纯保密功能发展成为一门具有加密与密码分析、数字签名、信息鉴别、身份认证、密钥管理、安全协议等多分支的综合学科。

当前密码技术的研究领域非常广泛、深刻，主要集中在：

1．密码学的信息理论和计算机复杂性理论的研究，如密码中信息泄露的发现和利用、安全密码体制的准则和评测。

2．公开密钥密码理论研究，寻找可构作新的公开密钥算法的数学难题，RSA，椭圆曲线公钥密码算法等密码算法的快速实现。

3．对称密码理论研究，如对称密码的设计准则和评测等。

4．新型安全密码算法的研究，如量子密码、混沌密码理论、DNA 密码、信息隐藏技术等。

5．密码安全协议的研究，如数字签名、身份鉴别、数据完整性、密钥管理、秘密共享等设计理论和方法，虚拟专用网络技术，计算机网络通信安全技术等。

解放军理工大学于 1998 年开设信息安全与对抗方面的课程。本书是在相关讲义和 4 年的教学实践基础上形成的。我们本着务实、求真的目标，力图对密码学的主要理论和技术作比较详细的阐述，使学生不但能够掌握相应的密码学原理，而且能够将其应用于网络安全的实践中。

本书共 11 章，第 1、2 章讲解与现代密码学有关的数学基础知识。第 3 章叙述密码学的基本概念。因课时的限制，我们不准备对传统密码展开讨论，所以仅对传统密码算法作了一点简要介绍，使学生对传统密码不至于一无所知。第 4 章讲解对称密码算法，对于欧洲密码计划的候选算法，教学中可选择其中的一个讲解。第 5～7 章讲解公钥密码算法，数学签名和散列函数，序列密码学。第 8～10 章讲解现代密码学的三个新的重要方向：椭圆曲线密码学、混沌密码学、量子密码学。对已经成熟的椭圆曲线密码学，本书用较多的篇幅进行讲解，这一部分可作为选讲内容和学生毕业设计的阅读材料。第 11 章讲解密码协议。

本书的特点是：几乎对每一个著名的密码体制都给出了一个实用的例子，这是一般的密码学书籍所缺少的，这也是作者的教学体会。学生在编程实践时往往无法对结果进行检验，这些实用的例子使学生可以对自己编制的程序进行检验。

本书可以在 45～60 个理论学时内完成，再配以 15～20 个学时的编程实践。也可结合有关网络编程课程进行实验。

本书的写作得到了解放军理工大学通信工程学院电子信息工程系张雄伟教授、曹耀辉政委、肖军模教授的鼓励、支持和帮助。

在本书的写作过程中，刘爱琴同志作了大量的数据和文字审校工作；于杰山、赵小龙、端木庆峰阅读了本书的初稿，验证了大部分实例和习题；何俊、成必权、解萍同志也校对了部分文字。

作者感谢解放军理工大学通信工程学院教保科许晔峰、岳超，电子信息工程系信息技术教研室的刘军、杨健、任煜、冒俊峰等同志的支持和帮助。

作　者

2003 年 2 月

目　录

第1章　初等数论基础

1.1　素数与因式分解

记号：除特别注明外，英文字母 a，b，c，d，m，n 等都表示正整数。

定义 1-1　如果 a 可以除尽 b，则称 a 整除 b，记为：$a|b$。

如果 $a|b$，$a|c$，则称 a 是 b，c 的一个公因子；如果 a 是 b，c 的公因子中最大者，则称 a 是 b，c 的最大公因子，记为：$a=\gcd(b,c)$，或 $a=(b,c)$。gcd 是 greatest common divisor 的缩写。

可以证明，b，c 的每一个公因子都可以整除 a。

【例 1-1】　$(4,6)=2$，$(15,70)=5$。

定义 1-2　如果 $a|c$，则称 c 是 a 的倍数；如 $a|c$，$b|c$，则称 c 是 a，b 的公倍数。

如果 c 是 a，b 的公倍数中最小者，则称 c 是 a，b 的最小公倍数，记为：$c=\mathrm{lcm}\{a,b\}$，或 $c=[a,b]$。lcm 是 least common multiple 的缩写。

可以证明，c 可以整除 a，b 的任一公倍数。

【例 1-2】　$\mathrm{lcm}\{15,20,30\}=60$。

定义 1-3　除 1 外，只能被 1 和其本身整除的自然数称为素数，不是 1，且非素数的正整数称为合数。

例如 2，3，5，7，11，13 等都是素数；4，6，8，9，10 等都是合数。

引理　若 $a=qb+r$，$0\leqslant r<b$，则 $(a,b)=(b,r)$。

证明　令 $d=(a,b)$，$d'=(b,r)$，则 $d\mid r=a-qb$，$\Rightarrow d\mid(b,r)=d'$，得 $d\leqslant d'$；另一方面，$d'\mid a=qb+r$，$\Rightarrow d'\mid(a,b)=d$，得：$d'\leqslant d$，所以 $d=d'$。

定理 1-1　若 $d=(a,b)$，则存在整数 p，q，使得 $d=pa+qb$。

证明　不妨设 $a>b$。应用一系列简单的除法（称为辗转相除法）可得：

$$
\begin{aligned}
a &= q_0 b + r_0 && 0\leqslant r_0 < b\\
b &= q_1 r_0 + r_1 && 0\leqslant r_1 < r_0\\
r_0 &= q_2 r_1 + r_2 && 0\leqslant r_2 < r_1\\
&\cdots\cdots && \cdots\cdots\\
r_{k-2} &= q_k r_{k-1} + r_k && 0\leqslant r_k < r_{k-1}\\
r_{k-1} &= q_{k+1} r_k
\end{aligned}
$$

依次将 $r_k, r_{k-1}, \cdots, r_1, r_0$ 后一式回代入前一式，可得：$r_k = pa+qb$。

再由引理得：$(a,b)=(b,r_0)=(r_0,r_1)=\cdots=(r_{k-2},r_{k-1})=(r_{k-1},r_k)=r_k$。

所以，$d=(a,b)=r_k$。定理证毕。

这个定理的证明也给出了最大公因子的求法——辗转相除法。

【例 1-3】 求(45,39)。

解：45=39×1+6

39=6×6+3

6=3×2

所以，(45,39)=3。

【例 1-4】 求 p，q 使（124，29）=124p+29q。

解：124=3×29+8

29=3×8+5

8=1×5+3

3=1×2+1

2=1×1

所以(124,39)=1。

回代：

1=3-1×2

=3-1×(5-1×3)=2×3-1×5

=2×(8-1×5)-1×5=2×8-3×5

=2×8-3×(29-3×8)=11×8-3×29

=11×(124-3×29)-3×29=11×124-36×29

所以有：1=11×124+（-36）×29。

定理 1-2 （数的表示定理）每一个正合数，都可表示为素数的乘积。不考虑乘积顺序时，表示法是惟一的。即：对任意 $n\in N$，有：

$$n=p_1^{s_1}p_2^{s_2}\cdots p_t^{s_t},$$

其中 p_1，p_2,…，p_t 是互不相同的素数，s_1，s_2,…，s_t 是正整数。

证明 若 n 是合数，则存在 a，b，使得 $n=ab$；若 a，b 是合数，则又有 $a=ed$，$b=gf$；

继续以上步骤，直到不能分解为止。

这个过程在有限步内完成（否则，n 将变成无穷大），故有：$n=g_1g_2\cdots g_k$，其中 $g_i,i=1,,2,\cdots,l$ 都是素数，将相同素数写成指数形式即得合数的标准分解式。

再证惟一性：

设有两个分解式：$n=g_1g_2\cdots g_k$，$n=h_1h_2\cdots k_l$，则：$h_1h_2\cdots h_l=g_1g_2\cdots g_k$，推得：$h_1 \mid g_1g_2\cdots g_k$。

由于 h_1，g_1，g_2,…，g_k 都是素数，所以，存在 g_i，$h_1=g_i$。

不失一般性，不妨设 $h_1=g_1$。

在等式两边消去 $h_1=g_1$，则等式成为：$h_2h_3\cdots h_l=g_2g_3\cdots g_k$。继续进行同样的步骤，直到 h_l，可知必有 $l=k$，$h_l=g_l$。定理证毕。

定理 1-3 设 $a \geqslant 2$ 是正整数，则：

（1）如果 a 是合数，那么必存在素数 $p \leqslant \sqrt{a}$，$p \mid a$；

（2）如果有素数分解式 $a = p_1 \cdots p_s$，则存在素数 $p \leqslant \sqrt[s]{a}$，$p \mid a$。

证明 （1）如果整除 a 的素数都大于 $\sqrt{a}$，则因 a 是合数，所以至少有两个素数 $p, q > \sqrt{a}$，$p \mid a$，$q \mid a$，从而有 $a \geqslant pq > \sqrt{a}\sqrt{a} = a$，矛盾；

（2）如果结论不成立，则 $p_i > \sqrt[s]{a}, i = 1,2,\cdots,s$，得到 $a = p_1 \cdots p_s > \underbrace{\sqrt[s]{a} \cdots \sqrt[s]{a}}_{s\text{个}} = a$，矛盾，所以结论成立。定理证毕。

根据定理 1-3 可以得到一种寻找素数的有效方法：

Eratoschenes 筛法：要求不超过 N 的所有素数，只要将 1 和不超过 N 的合数去掉即可。

而由定理 1-3（1），这些合数必有素因子 $p \leqslant \sqrt{N}$，因而，如果先求出 $\leqslant \sqrt{N}$ 的素数：$p_1, \cdots, p_k$，然后用这些素数试除 $2, \cdots, N$，则不被 $p_1, \cdots, p_k$ 整除的就是所有素数。

进一步，当得到了 $2, \cdots, N$ 中的所有素数 $p_1, \cdots, p_k$ 后，又可以用其检测 2，…，N，…，N^2 之中的素数了，这一过程继续下去，即可筛出所有素数。

例如要求不超过 N 的所有素数。从素数 2 开始，筛去 $2, \cdots, N$ 中 2 的倍数；那么，剩下数中 $< 2^2 = 4$ 的数 3 就是素数；再用 2，3 去筛后面剩下的数，但 2 已经用过，所以只须用 3 去筛，即筛去 3 的倍数；剩下的数中 $< 3^2 = 9$ 的都是素数。即 2，3，5，7。所以，进一步可以用 5，7 去筛，得到素数 11，13，17，19，23，29，37，41，43，47；依此类推，即可得到所求素数。求 100 之内的所有素数如图 1-1 所示。

	2	3	4	5	6	7	8	(9)	10	11	12	13	14	(15)	16	17	18	19	20
(21)	22	23	24	△25	26	(27)	28	29	30	31	32	(33)	34	△35	36	37	38	(39)	40
41	42	43	44	(45)	46	47	48	[49]	50	(51)	52	53	54	△55	56	(57)	58	59	60
61	62	(63)	64	△65	66	67	68	(69)	70	71	72	73	74	(75)	76	[77]	78	79	80
(81)	82	83	84	△85	86	(87)	88	89	90	[91]	92	(93)	94	△95	96	97	98	(99)	100

图 1-1　100 之内的筛法

可见，所求素数为：2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,83,89,97。

求大素数是数学中的一个难题。密码学应用中，不但需要检测一个整数是否为素数，而且要求计算速度快。进一步，对素数还有更高的要求，即所谓的强素数、安全素数。素性检验和强素数的求取等等都是密码学的重要研究课题，我们将在后面的具体算法中涉及时讲解。

定理 1-4 素数有无穷多个。

证明 用反证法。设有有限个素数 $p_1, \cdots, p_n$，令 $a = p_1 \cdots p_n + 1$，易见 $a > 2$，$p_i \nmid a$，$i = 1,2,\cdots,n$。但是，根据定理 1-3，应有 $p_i \mid a$，矛盾。所以，有无穷多个素数。定理证毕。

1.2 同余式理论

定义 1-4 设 m 是正整数，如果 $m \mid a - b$，即：$a - b = km$，则称 a 和 b 模 m 同余，记

为：$a \equiv b \bmod m$。m 称为这个同余式的摸。

定理 1-5 模 m 的同余关系是等价关系，即满足：

（1）自反性：$a \equiv a \bmod m$；

（2）对称性：若 $a \equiv b \bmod m$，则 $b \equiv a \bmod m$；

（3）传递性：若 $a \equiv b \bmod m$，$b \equiv c \bmod m$，则 $a \equiv c \bmod m$。

证明简单，略去。

定理 1-6 若 $a \equiv b \bmod m$，$c \equiv d \bmod m$，那么：

（1）$a \pm c \equiv b \pm d \bmod m$；

（2）$ac \equiv bd \bmod m$；

（3）若 $c \mid a$，$c \mid b$，$(c,m)=k$，则 $\frac{a}{c} \equiv \frac{b}{c} \bmod \frac{m}{k}$；特别地，如果 $(c,m)=1$，则 $\frac{a}{c} \equiv \frac{b}{c} \bmod m$，即同余式两边可以同除以一个与 m 互素的数 c。

（1），（2）的证明是简单的，我们只证（3）。

证明（3）：设 $a=a'c$，$b=b'c$，$c=c'k$，$m=m'k$，$(c',m')=1$。

则由：$a \equiv b \bmod m$

$\Rightarrow a'c \equiv b'c \bmod m'k$，即：$a'c-b'c=lkm'$，

$\Rightarrow c \mid lkm'$，即：$kc' \mid lkm'$，

$\Rightarrow c' \mid lm'$，但是，$(c',m')=1$，

$\Rightarrow c' \mid l$。

$\Rightarrow a'-b'=\frac{l}{c'}m'$，即 $\frac{a}{c} \equiv \frac{b}{c} \bmod \frac{m}{(c,m)}$。定理证毕。

定义 1-5 $ax \equiv b \bmod m$ 称为线性同余式，满足同余式的整数 x 称为同余式的解。

可以证明，如果 x_1 是该线性同余式的解，则对于任意 $x_2 \equiv x_1 \bmod m$ 也是该同余式的解，但是，反过来却不正确，可见下面的定理 1-7（2）。

定理 1-7 设 $d=(a,m)$，则对于同余式 $ax \equiv b \bmod m$，

（1）有解的充要条件是：$d \mid b$；

（2）如果 x_0 是同余式的一个解，那么同余式的所有解为：$x \equiv x_0 \bmod \frac{m}{d}$。

证明 （1）设 x_0 是同余式的一个解，则存在整数 k，$ax_0-km=b$，于是得：

$d(\frac{a}{d}x_0-\frac{m}{d}k)=b$，即得：$d \mid b$。

反之，若 $d \mid b$，令 $b=b'd$，$a=a'd$，$m=m'd$，则 $(a',m)=1$，由定理 1-1 知，存在整数 p，q，使得：$pa'+qm'=1$，于是：

$$\begin{aligned} b &= bpa'+bqm' \\ &= b'dpa'+b'dqm' \\ &= pb'(a'd)+qb'(m'd) \\ &= pb'a+qb'm \end{aligned}$$

$\Rightarrow a(pb')=b-(qb')m$，即：$a(pb') \equiv b \bmod m$，

所以，pb'是同余式的解。

（2）如果x_0是同余式的解，则易验证x_0+km'也是同余式的解。

反之，若x_0'是同余式的任意一个解，则有：

$ax_0 \equiv b \bmod m$，$ax_0' \equiv b \bmod m$，得到：$ax_0 \equiv ax_0' \bmod m$，

根据定理 1-6（3）得到：$x_0 \equiv x_0' \mod \frac{m}{d}$。定理证毕。

定义 1-6 若$ab \equiv 1 \mod m$，则称b是a模m的逆元。

显然a也是b模m的逆元。

定理 1-8 如果$(a,m)=1$，则a模m的逆元一定存在。

证明 由于$(a,m)=1$，所以，由定理 1-1 知，

存在整数s,t，使得$sa+tm=(a,m)=1$，于是，$as \equiv 1 \mod m$。

记$\tilde{s}=s+km>0$，那么$a\tilde{s}=as+akm \equiv 1 \mod m$，正整数$\tilde{s}$就是$a$模$m$的逆元。定理证毕。

但是，s,t是用回代的方法得到的，因此求解时必须记住每一个中间值，用作回代时使用，这需要巨大的空间开销，显然这是不可取的，不适合密码应用。

稍作观察可以发现，采用从前向后代入的方法，可以避免存储空间问题。例如，例 1-5 可进行如下：

124=3×29+8

8=124−3×29

29=3×8+5

5=29−3×8=29-3×(124-3×29)= −3×124+10×29

8=1×5+3

3=8−1×5=124−3×29−1×(−3×124+10×29)=4×124−13×29

5=1×3+2

2=5−1×3= −3×124+10×29−1×(4×124−13×29)= −7×124+23×29

3=1×2+1

1=3−1×2=4×124−13×29−1×(−7×124+23×29)=11×124+36×29。

可见，这个方法是可行、有效的。下面的定理，给出这一方法的紧凑形式。

定理 1-9 设$r_1 \equiv b_1 u \mod m$，$r_2 \equiv b_2 u \mod m$，$r_1 = qr_2 + r_3$，则

$r_3 \equiv (b_1 - qb_2)u \mod m$。

证明 $r_1 = b_1 u + lm$，$r_2 = b_2 u + km$，

$r_3 = r_1 - qr_2 = b_1 u + lm - q(b_2 u + km) = (b_1 - qb_2)u + (l - qk)m$，所以

$r_3 \equiv (b_1 - qb_2)u \mod m$。定理证毕。

求模逆算法：设$0<u<m$，$(u,m)=1$，求u模m的逆元，即：求x，$0<x<m$，$ux \equiv 1 \bmod m$。

（1）令$r_1 = m$，$r_2 = u$，则：$r_1 = m \equiv 0 \cdot u \mod m$，$r_2 = u \equiv 1 \cdot u \mod m$，即有：

$b_1 = 0$ $b_2 = 1$。

（2）令$r_1 = q_1 r_2 + r_3$，$0 \leqslant r_3 < r_2$，得到$r_3 \equiv (b_1 - q_1 b_2)u \mod m$，记$b_3 = b_1 - q_1 b_2$，则

得到 $r_2 \equiv b_2 u \mod m$，$r_3 \equiv b_3 u \mod m$。

（3）令 $r_2 = q_2 r_3 + r_4, 0 \leqslant r_4 < r_3$，得到 $r_4 \equiv (b_2 - q_2 b_3) u \mod m$，记 $b_4 = b_2 - q_2 b_3$，则得到 $r_4 \equiv b_4 u \mod m$。

（4）继续下去，总之有：

$r_1 \equiv b_1 u \mod m$，$r_2 \equiv b_2 u \mod m$，$r_1 = q_1 r_2 + r_3$，$0 \leqslant r_3 < r_2$，

$r_2 \equiv b_2 u \mod m$，$r_3 \equiv b_3 u \mod m$，$r_2 = q_2 r_3 + r_4$，$0 \leqslant r_4 < r_3$，

……

$r_{k-1} \equiv b_{k-1} u \mod m$，$r_k \equiv b_k u \mod m$，$r_{k-1} = q_{k-1} r_k + r_{k+1}$，$0 \leqslant r_{k+1} < r_k$，

……

由于 $r_2 > r_3 > \cdots > r_k > r_{k+1} \cdots \geqslant 0$，所以，以上操作必终止于有限步，不妨设 $r_{k+1} = 0$，那么必有 $1 = r_k = (r_k, r_{k-1}) = \cdots = (r_3, r_2) = (r_2, r_1) = (u, m)$。

所以由 $r_k \equiv b_k u \mod m$，得 $b_k u \equiv 1 \mod m$，于是所求为：$u^{-1} \equiv b_k \mod m$。

根据以上过程，不难给出模逆算法的流程图 1-2：

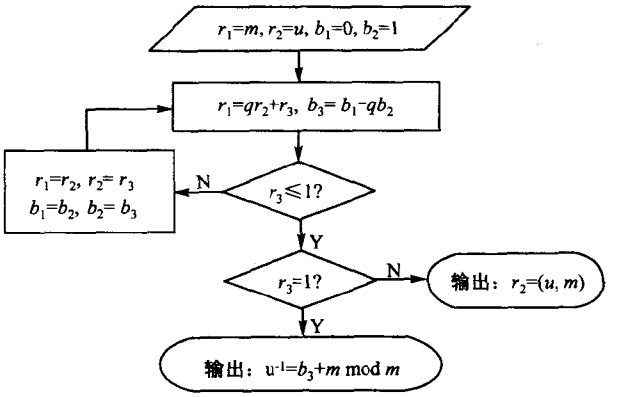


图 1-2　模逆求解流程图

定理 1-10　（中国剩余定理 CRT）设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数，即：$(m_i, m_j) = 1$，$i \neq j$，$i, j = 1,2,\cdots,k$，则同余方程组：

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \\ \cdots\cdots \\ x \equiv b_k \mod m_k \end{cases}$$

模 $[m_1, m_2, \cdots, m_k]$ 有惟一解，即在模 $[m_1, m_2, \cdots, m_k]$ 的意义下，存在惟一的 x，满足：

$$x \equiv b_i \mod [m_1, m_2, \cdots, m_k]，\ i = 1,2,\cdots,m。$$

证明　令 $M = m_1 m_2 \cdots m_k$，$M_i = \dfrac{M}{m_i}$。

由于 $(M_i, m_i) = 1$，所以，由定理 1-8 存在 y_i，使得：$y_i M_i \equiv 1 \bmod m_i$。