信息安全数学基础

韩　琦

计算学部网络空间安全学院

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

Overview

1. 数论

认识数论

数论研究整数集合：

1、2、3、4、5、6、7、8、$\cdots$

各种有意思的数：

- 奇数、偶数
- 平方数（1，4，9，16，25，$\cdots$）、立方数（1，8，27，64，125，$\cdots$）
- 素数、合数
- 三角数（1，3，6，10，15，21，$\cdots$）
- 完全数（6，28，496 $\cdots$）
- 斐波那契数（1，1，2，3，5，8，13，21，$\cdots$）

认识数论

若干典型的数论问题

- **平方和：**勾股数、平方和等于一个数
- **高幂次和：**费马大定理
- **素数无穷：**无穷多个素数？无穷多个除4余1（or 3）的素数？
- **数的形状：**三角数、平方数
- **孪生素数：**相邻的奇数都是素数，3、5、7，11、13，
- **形如N^2+1的素数：**5，17，37，101，197，257，401

数论在信息安全领域有什么应用呢？

- 古典密码术、背包算法
- RSA公钥算法、ElGamal公钥体制、Rabin公钥体制

Detailed overview

1. 数论

整数的除法

问题的引出

整数的四则运算：加(+)、减(−)、乘(×)、除(÷)，只有除的结果可能超出整数环；（*“环”是什么意思？在本课程能找到答案*）

如何保证除法的结果还在整数范围内？

带余除法

设a, b是两个整数，其中$b \neq 0$，则存在两个唯一的整数q, r，使得

$$a = bq + r,\ 0 \leq r < |b| \tag{1.1}$$

成立。

余数、因数、倍数

定义

*称式1.1中的q为a被b除得出的***不完全商***，r为a被b除得出的***余数***，也称为***非负最小余数***，通常记作$< a >_b = r$。*

定义

当式1.1中的$r = 0$时，称b ***整除****a，记作$b|a$，也称b为a 的****因数或约数****，a为b的****倍数****。否则，称b不整除a，记作$b \nmid a$。*

整除的性质

整除这个概念虽然简单，但却是初等数论中的基本概念，由整除的定义和乘法的运算性质，容易得到整除的性质：

定理

设a, b, c是整数，则

(1) 如果$b|a, c|b$，则$c|a$;

(2) 如果$c|a, c|b$，则$c|(a \pm b)$;

(3) 如果$b|a, a|b$，则$a = \pm b$;

(4) 设$m \neq 0$，$b|a$，则$bm|am$。

证明：（提示：根据整除的定义，如果b整除a，则有$a = bq$，据此开始推导和证明...）

辗转相除法

设整数$a, b(\neq 0)$，由带余除法，有下列等式

$$\begin{aligned}
a &= bq_1 + r_1, & 0 &< r_1 < |b| \\
b &= r_1 q_2 + r_2, & 0 &< r_2 < r_1 \\
&\ldots, & &\ldots \\
r_{n-2} &= r_{n-1} q_n + r_n, & 0 &< r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, & r_{n+1} &= 0
\end{aligned} \tag{1.2}$$

因为$|b| > r_1 > r_2 > \ldots$，故经过有限次带余数除法后，总可以得到一个余数是零，即式1.2中$r_{n+1} = 0$。这个过程称为**辗转相除法**。

举例

例 (用辗转相除法分解57（除17）)

解:

$$\begin{aligned}
\mathbf{57 \div 17}: &\quad 57 = 17 \times 3 + 6 \\
\mathbf{17 \div 6}: &\quad 17 = 6 \times 2 + 5 \\
\mathbf{6 \div 5}: &\quad 6 = 5 \times 1 + 1 \\
\mathbf{5 \div 1}: &\quad 5 = 1 \times 5
\end{aligned}$$

代回:

$$\begin{aligned}
6 &= 1 \times 5 \times 1 + 1 \\
17 &= (1 \times 5 \times 1 + 1) \times 2 + 5 \\
57 &= [(1 \times 5 \times 1 + 1) \times 2 + 5] \times 3 + 6 \\
57 &= [(1 \times 5 \times 1 + 1) \times 2 + 5] \times 3 + 1 \times 5 \times 1 + 1
\end{aligned}$$

最大公因数、互素

定义

设$a_1, a_2, \ldots, a_n$是n个不全为零的整数。如果整数d是它们之中每一个的因数，那么d就称为$a_1, a_2, \ldots, a_n$的一个**公因数**。整数$a_1, a_2, \ldots, a_n$的公因数中最大的一个称为**最大公因数**，记作$(a_1, a_2, \ldots, a_n)$。如果$(a_1, a_2, \ldots, a_n) = 1$，就称$a_1, a_2, \ldots, a_n$**互素**或**互质**。

定理

设a, b, c是任意三个不全为零的整数，且$a = bq + c$，其中q是整数，则$(a, b) = (b, c)$。

根据上述定理，对任意整数$a > 0, b > 0$，作辗转相除法，则最后一个非零余数r_n就是(a, b)。

举例

例

求2357与73的最大公因数$(2357, 73)$。

解：*做辗转相除法*：

$$2357 = 73 \times 32 + 21$$
$$73 = 21 \times 3 + 10$$
$$21 = 10 \times 2 + 1$$
$$10 = 1 \times 10$$

所以，$(2357, 73) = 1$。*可见*，2357*与*73*是互素的*。

最大公因数的构造

定理

对任意不全为零的整数a,b，存在整数u,v，使得$au+bv=(a,b)$。

证明： 对两个整数a,b作辗转相除法，并回代

$$
\begin{aligned}
r_n &= r_{n-2} - r_{n-1}q_n \\
&= r_{n-2} - \big(r_{n-3} - r_{n-2}q_{n-1}\big)q_n \\
&= r_{n-2}\big(1 + q_n q_{n-1}\big) - r_{n-3}q_n \\
&= \cdots = au + bv
\end{aligned}
$$

即得$au+bv=(a,b)$。 □

最小公倍数

定义

设$a_1, a_2, \ldots, a_n$是n个整数$(n \geq 2)$。若整数m是这n个数中每一个数的倍数，则m就称为这n个数的**公倍数**。在$a_1, a_2, \ldots, a_n$的一切公倍数中最小的正数称为**最小公倍数**，记作$[a_1, a_2, \ldots, a_n]$。

最小公倍数的计算方法：

利用作辗转相除法，可先求出最大公因数，再由$[a, b] = \frac{|ab|}{(a,b)}$计算最小公倍数。

例

求$[231, 7653]$。

Detailed overview

1. 数论

二元一次不定方程

二元一次不定方程 是指

$$ax + by = c \tag{1.3}$$

其中，a, b, c是给定的整数，$ab \neq 0$。

二元一次不定方程有解的充要条件：

定理

方程式1.3有整数解x, y的充分必要条件是$(a, b)|c$。且式1.3有解时，全部解可以表示为$x = x_0 + \frac{b}{(a,b)}t, y = y_0 - \frac{a}{(a,b)}t$，其中$x_0, y_0$ 为式1.3的任意一组解，t为任意整数。

举例

例

解二元一次不定方程$312x + 753y = 345$。

解： 先确定解的存在性，作辗转相除法

$753 = 312 \times 2 + 129$

$\cdots\cdots$

$9 = 3 \times 3$

所以，$(753, 312) = 3$，而由$3|345$知方程有解。

再回代：

$$\begin{aligned} 3 &= 12 - 9 \times 1 = 12 - (21 - 12 \times 1) = 12 \times 2 - 21 = \cdots\cdots \\ &= 312 \times 12 - (753 - 312 \times 2) \times 29 = 312 \times 70 + 753 \times (-29) \end{aligned}$$

由于$345 \div 3 = 115$，所以

$x_0 = 70 \times 115 = 8050, y_0 = -29 \times 115 = -3335$

因此，二元一次不定方程的全部解为

$x = 8050 + 251t, y = -3335 - 104t$，$t$为任意整数。

多元一次不定方程

多元一次不定方程就是可以下列形式的方程：

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N \tag{1.4}$$

其中，$a_1, a_2, \cdots, a_n, N$都是整数，$n \geq 2$，并且不失一般性，可以假定$a_1, a_2, \cdots, a_n$都不等于零。

定理

不定方程$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N$有整数解的充分必要条件是$(a_1, a_2, \cdots, a_n)|N$。

知道了二元一次不定方程的求解方法，如何求解多元一次不定方程呢？

多元一次不定方程

多元一次不定方程就是可以下列形式的方程：

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N \tag{1.4}$$

其中，$a_1, a_2, \cdots, a_n, N$都是整数，$n \geq 2$，并且不失一般性，可以假定$a_1, a_2, \cdots, a_n$都不等于零。

定理

不定方程$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N$有整数解的充分必要条件是$(a_1, a_2, \cdots, a_n)|N$。

知道了二元一次不定方程的求解方法，如何求解多元一次不定方程呢？

多元一次不定方程的求解

前面的定理提供了一个求解$a_1x_1+a_2x_2+\cdots+a_nx_n=c$的方法，即先顺次求出$(a_1,a_2)=d_2,(d_2,a_3)=d_3,\cdots,(d_{n-1},a_n)=d_n$，若$d_n|c$，则$n$元一次不定方程有解。做方程组

$$\begin{cases} a_1x_1+a_2x_2=d_2t_2 \\ d_2t_2+a_3x_3=d_3t_3 \\ \cdots \\ d_{n-2}t_{n-2}+a_{n-1}x_{n-1}=d_{n-1}t_{n-1} \\ d_{n-1}t_{n-1}+a_nx_n=c \end{cases}$$

首先求出最后一个方程的一切解，然后把t_{n-1}的每一个值带入倒数第二个方程，求出他的一切解，这样做下去即可得出n元一次不定方程的一切解。
在实际解n元一次不定方程时，常把t_i看成常数，求出上面方程组第$i-1$个方程的整数解的一般形式，再从结果中消去$t_2,t_3,\cdots,t_{n-1}$，即可得n元一次不定方程的解。

例题

求解不定方程$50x+45y+36z=10$。

解： 因为$(50,45)=5,(5,36)=1$，又$1|10$，所以此方程有解，原方程可以化为

$$\begin{cases} 50x+45y=5t \\ 5t+36z=10 \end{cases} \text{即} \begin{cases} 10x+9y=t \\ 5t+36z=10 \end{cases}$$

这里t是参数，在第一个方程中，把t看作常量，在第二个方程中，又把t看作变量，分别解之，得

$$\begin{cases} x=t+9k_1 \\ y=-t-10k_1 \end{cases} \text{和} \begin{cases} t=-70+36k_2 \\ z=10-5k_2 \end{cases}$$

这里k_1,k_2是任意整数，消去t得到原方程的通解。

例题

求解不定方程$50x+45y+36z=10$。

分别解之，得

$$\begin{cases} x = t + 9k_1 \\ y = -t - 10k_1 \end{cases} \text{和} \begin{cases} t = -70 + 36k_2 \\ z = 10 - 5k_2 \end{cases}$$

这里k_1, k_2是任意整数，消去t得到原方程的通解。

$$\begin{cases} x = -70 + 9k_1 + 36k_2 \\ y = 70 - 10k_1 - 36k_2 \\ z = 10 - 5k_2 \end{cases}$$

举例：背包公钥密码算法

背包问题

有物品若干及背包一个，由于背包太小，不能将所有物品放入，问如何选择部分物品放入，能使背包的容积得到最充分的利用。

将背包问题稍加演变，给定n个正整数$a_1, a_2, \cdots, a_n$及一个正整数s，已知s是某一些a_i之和，确定这些a_i，这就是**密码学的背包问题**。

从$a_1, a_2, \cdots, a_n$中选出一个子集，很容易算出这个子集之和。但反过来，给定一个子集之和，要确定这个子集，一般来说就很困难了。

举例：背包公钥密码算法

利用背包问题可以得到背包公钥密码：将$a_1, a_2, \cdots, a_n$作为公开密钥，设$\{m_1, m_2, \cdots, m_n\}$为明文，$m_i = 0$或$1$，
令$s = \sum_{i=1}^{n} m_i a_i$，将$s$作为密文，它是$a_1, a_2, \cdots, a_n$的一个部分和。从$s$求解明文$\{m_1, m_2, \cdots, m_n\}$就相当于解背包问题。不过对于一般的$a_1, a_2, \cdots, a_n$，即使合法的接收方也同样难于解密，所以不能用一般的$a_1, a_2, \cdots, a_n$设计密码。在下面一个特殊情况，背包问题将变得很容易解。设

$$a_1 < a_2, a_1 + a_2 < a_3, \cdots, a_1 + a_2 + \cdots + a_{n-1} < a_n$$

即前面一段数之和小于紧跟其后的一个数，这时称$a_1, a_2, \cdots, a_n$为**超递增序列**。

设$a_1, a_2, \cdots, a_n$为超递增的，如以它为公开密钥，
以$s = \sum_{i=1}^{n} m_i a_i$
作为明文$\{m_1, m_2, \cdots, m_n\}$的密文，利用一次不定方程，可以很容易的从$s$解出$\{m_1, m_2, \cdots, m_n\}$。但是由于$a_1, a_2, \cdots, a_n$是公开的，任何人都可以轻松的解密，因此这个密码体制还是不安全的。**(待续)**

同余式定义

定义

给定一个正整数m，如果用m去除两个整数a, b所得的余数相同，则称a, b对模数m**同余**，并称$a \equiv b \pmod{m}$为**同余式**。如果用m 去除两个整数a, b所得的余数不同，则称a, b对模数m不同余，记作$a \not\equiv b \pmod{m}$。

同余式性质

1. $a \equiv b(\mathrm{mod}\ m)$的充分必要条件是$m|a-b$，即有整数$k$使$a = b + km$；
2. 如果$a \equiv b(\mathrm{mod}\ m)$，$\alpha \equiv \beta(\mathrm{mod}\ m)$，则有
   - $ax + \alpha y \equiv bx + \beta y(\mathrm{mod}\ m)$，其中$x, y$为任意的整数
   - $a\alpha \equiv b\beta(\mathrm{mod}\ m)$；
   - $a^n \equiv b^n(\mathrm{mod}\ m)$；
   - $f(a) \equiv f(b)(\mathrm{mod}\ m)$，其中$f(x)$是任意整系数多项式。
3. 如果$ac \equiv bc(\mathrm{mod}\ m)$，且$(m, c) = d$，则$a \equiv b(\mathrm{mod}\ \frac{m}{d})$；
4. 如果$a \equiv b(\mathrm{mod}\ m_i), i = 1, 2, \cdots, n$，则$a \equiv b(\mathrm{mod}\ [m_1, m_2, \cdots, m_n])$；
5. 满足同余方程$x \equiv a(\mathrm{mod}\ m)$的整数集合为$\{x|x = a + km, k \in \mathbb{Z}\}$，其中$\mathbb{Z}$为所有整数的集合。

一次同余方程

定义

一次同余方程是指

$$ax \equiv b(\bmod m) \tag{1.5}$$

其中$a \not\equiv 0(\bmod m), m > 1$。

*如果$x = x_0$满足式1.6，则$x \equiv x_0(\bmod m)$称为**同余方程的解**。有时也把x_0称为同余方程的解。不同的解是指对模数m互不同余的解。*

一次同余方程有解的充要条件

定理

设$(a,m)=d$，则式1.6有解的充分必要条件是$d|b$。且式1.6有解时，恰有d个解，它们是$x\equiv x_0+\frac{m}{d}t(\bmod\ m), t=0,1,\cdots,d-1$。其中$x_0$是式1.6的任意一个解。

注意： 当$(a,m)=1$时，同余方程$ax\equiv 1(\bmod\ m)$恰有一个解x_0，有时称这个解x_0为a模m的**逆**，并记为a^{-1}。

举例

例

解一次同余方程$14x \equiv 26 \pmod{38}$。

解： 作辗转相除法

$$
\begin{aligned}
38 &= 14 \times 3 - 4 \\
14 &= 4 \times 3 + 2 \\
4 &= 2 \times 2
\end{aligned}
$$

所以$(38, 14) = 2|26$，同余方程有两个解。再回代

$$2 = 14 - 4 \times 3 = 14 - (14 \times 3 - 38) \times 3 = 14 \times (-8) + 38 \times 3$$

由$26 \div 2 = 13$，知$x_0 \equiv (-8) \times 13 \equiv -104 \equiv 10 \pmod{38}$是同余方程的解。
再由$38 \div 2 = 19$，知其两个解
为$x \equiv 10, 10 + 19 \equiv 10, 29 \pmod{38}$。

举例

例 (背包公钥密码(续))

取正整数m，使$m > a_1 + a_2 + \cdots + a_n$，再取正整数$u$，使$(u, m) = 1$。$u$和$m$作为私钥，只有接收方知道。

令$b_i \equiv ua_i (\bmod\ m), i = 1, 2, \cdots, n$，将$b_1, b_2, \cdots, b_n$作为公钥，

若$\{m_1, m_2, \cdots, m_n)\}$为明文，令$s = \sum_{i=1}^n m_i b_i$为密文，发方将$s$发给接收方。接收方利用辗转相除法可以找到$w$，使得$uw \equiv 1 (\bmod\ m)$。因$(u, m) = 1$，接收方在收到$s$后，可以算出$(sw)_0$，使$sw \equiv (sw)_0 (\bmod\ m)$，且$0 < (sw)_0 < m$，

则$sw \equiv \sum_{i=1}^n m_i w b_i \equiv \sum_{i=1}^n m_i u w a_i \equiv \sum_{i=1}^n m_i a_i (\bmod\ m)$，显然$\sum_{i=1}^n m_i a_i < \sum_{i=1}^n a_i < m$，可见$\sum_{i=1}^n m_i a_i = (sw)_0$，这是一个超递增背包问题，很容易解出明文$\{m_1, m_2, \cdots, m_n\}$。

作业

1. 求(a,b)、$[a,b]$及使得$au+bv=(a,b)$的整数u,v：
   1.1 $a=72,\ b=60$
   1.2 $a=168,\ b=-180$
2. 解一次不定方程：
   2.1 $3x+92y=17$
   2.2 $42x+70y+105z=56$
3. 解一次同余方程：
   3.1 $24x\equiv 42 \pmod{30}$
   3.2 $90x\equiv 21 \pmod{429}$

Detailed overview

1. 数论

素数与合数

定义

*一个大于1的整数，如果它的正因数只有1和它本身，就称为**素数(或质数或不可约数)**，否则就称为**合数**。*

显然下列性质成立：

1. 若p是一素数，a是任一整数，则有$p|a$或$(p,a)=1$；
2. 若p是一素数，$p|ab$，则$p|a$或$p|b$。

整数分解定理

定理

任一个大于1的整数都能惟一分解成素数的乘积，即对于任一整数$a>1$，有

$$a=p_1p_2\cdots p_n, p_1\le p_2\le\cdots\le p_n$$

其中$p_1,p_2,\cdots,p_n$都是素数。并且若

$$a=q_1q_2\cdots q_m, q_1\le q_2\le\cdots\le q_m$$

其中$q_1,q_2,\cdots,q_n$都是素数，则$m=n, p_i=q_i(i=1,2,\cdots,n)$。

相同的素数因数写成幂的形式：$a=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$，$a_i>0$，称为$a$的**标准分解式**。

Detailed overview

1. 数论

剩余系

定义

设$m > 0$，$C_r = \{a|a = r + qm, q \in \mathbb{Z}\}$，$(r = 0, 1, \cdots, m-1)$，
则$C_0, C_1, \cdots, C_{m-1}$称为模数$m$的**剩余类**。
在$C_0, C_1, \cdots, C_{m-1}$中各取一数$a_j \in C_j, j = 0, 1, \cdots, m-1$，
此m个数$a_0, a_1, \cdots, a_{m-1}$称为模数$m$的一组**完全剩余系**。
特别地，完全剩余系$0, 1, \cdots, m-1$称为模数m的**非负最小完全剩余系**。
如果C_j里面的数与m互素(显然，只需j与m互素，其里面的数就都与m互素)，称C_j为与模数m**互素的剩余类**。
在与m互素的全部剩余类中，各取一数所组成的集合就称为模数m的一组**既约剩余系**。

欧拉函数

定义

欧拉函数$\phi(n)$*是一个定义在正整数集合上的函数，*$\phi(n)$*的值等于序列*$0, 1, \cdots, n-1$*中与*n*互素的数的个数。*

由定义得$\phi(1)=1, \phi(2)=1, \phi(3)=2, \cdots$。当$p$是素数时，$\phi(p)=p-1$。

显然下列性质成立：

1. 模数m的一组既约剩余系含$\phi(m)$个数
2. $\phi(m)$个数作成模数m的一组既约剩余系的充要条件是两两对模数m不同余且都与m互素
3. $(m_1, m_2)=1$时，$\phi(m_1m_2)=\phi(m_1)\phi(m_2)$
4. p为素数，l为正整数时，$\phi(p^l)=p^l-p^{l-1}=p^{l-1}(p-1)$

欧拉函数的计算公式

从而可得欧拉函数的计算公式：

$m = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$，$p_i$为素数，$l_i > 0 (i = 0, 1, \cdots, k)$时，

$$\begin{aligned}
\phi(m) &= (p_1^{l_1} - p_1^{l_1-1})(p_2^{l_2} - p_2^{l_2-1}) \cdots (p_k^{l_k} - p_k^{l_k-1}) \\
&= \prod_{i=1}^{k} (p_i^{l_i} - p_i^{l_i-1}) \\
&= \prod_{i=1}^{k} p_i^{l_i} (1 - \tfrac{1}{p_i}) \\
&= p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k} \prod_{i=1}^{k} (1 - \tfrac{1}{p_i}) \\
&= m \prod_{i=1}^{k} (1 - \tfrac{1}{p_i}) \\
&= m(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_k})
\end{aligned}$$

例 (求$\phi(m)$，$m = 120736$)

设$m = 120736 = 2^5 \times 7^3 \times 11$，则

$$\phi(m) = 2^4 \times 7^2 \times 6 \times 10 = 2^6 \times 3 \times 5 \times 7^2 = 47040$$

欧拉定理

定理（欧拉定理）

若$(a,m)=1$，则$a^{\phi(m)}\equiv 1 \pmod{m}$。

证明： 设$a_1,a_2,\ldots,a_{\phi(m)}$为模数$m$的一组即约剩余系，由于$(a,m)=1$，易证：
$aa_1,aa_2,\ldots,aa_{\phi(m)}$也是$m$的一组即约剩余系（从与$m$互素和两两不同余两个方面证明，用到了同余关系的性质3）。
根据同余关系的性质2，易证两组即约剩余系相乘满足：
$aa_1aa_2\ldots aa_{\phi(m)}\equiv a_1a_2\ldots a_{\phi(m)} \pmod{m}$
即：$a^{\phi(m)}a_1a_2\ldots a_{\phi(m)}\equiv a_1a_2\ldots a_{\phi(m)} \pmod{m}$
再根据性质3，可得：$a^{\phi(m)}\equiv 1 \pmod{m}$
证毕。 □

欧拉定理的证明

由欧拉定理，结合性质2，推得：若$(a, m) = 1$，
则$a^{\phi(m)+1} \equiv a(\bmod\ m)$。

定理（费马小定理）

若p为素数，则$a^p \equiv a(\bmod\ p)$。

证明： 由前推论，有：$a^{\phi(p)+1} \equiv a(\bmod\ p)$
p是素数，则其欧拉函数为：$\phi p = p - 1$，于是$p = \phi p + 1$
于是有：$a^p \equiv a(\bmod\ p)$
证毕。 $\square$

举例：RSA公钥密码算法

应用欧拉定理可以证明RSA公钥密码算法的正确性。Ron Rivest和Adi Shamir以及Leonard Adleman于1978年提出的RSA公钥密码体制至今仍被公认为是一个安全性能良好的密码体制。

RSA公钥密码体制的描述如下：

1. 选取两个大素数p, q。
2. 计算$n = pq, \phi(n) = (p-1)(q-1)$。
3. 随机选取正整数$e, 1 < e < \phi(n)$，满足$(e, \phi(n)) = 1$。
4. 计算d，满足$de \equiv 1 (\mathrm{mod}\ \phi(n))$，$p, q, \phi(n), d$是保密的，$n, e$是公开的。
5. 加密变换：对明文$m, 1 < m < n$，加密后的密文为$c = m^e (\mathrm{mod}\ n)$。
6. 解密变换：对密文$c, 1 < c < n$，解密后的明文为$m = c^d (\mathrm{mod}\ n)$。

RSA算法正确性的证明

证明： 因为$de \equiv 1 (\bmod\ \phi(n))$，故存在$t$，使得$de = 1 + t\phi(n)$
当$(m, n) = 1$时，
$c^d \equiv (m^e)^d \equiv m^{(1+t\phi(n))} \equiv m \cdot m^{\phi(n)t} \equiv m \cdot 1^t \equiv m (\bmod\ n)$
当$(m, n) \neq 1$时，因为$n = pq$且p、q为素数，故(m, n)为p或q，不妨设$(m, n) = p$，则有$p|m$，设$m = bp$，$1 \leq b < q$
由欧拉定理得，$m^{q-1} \equiv 1 (\bmod\ q)$，从而有：
$m^{t\phi(n)} \equiv m^{t(p-1)(q-1)} \equiv (m^{(q-1)})^{t(p-1)} \equiv 1 (\bmod\ q)$，
故存在s，使得$m^{t\phi(n)} = 1 + sq$，进一步，$m^{t\phi(n)+1} = m + sqm = m + sqbp = m + bsn$，由同余式的性质1得：$m^{t\phi(n)+1} \equiv m (\bmod\ n)$，
于是有：$c^d \equiv m^d e \equiv m^{(1+t\phi(n))} \equiv m (\bmod\ n)$
综上，$c^d \equiv m (\bmod\ n)$成立。 □

举例：RSA公钥密码算法

例

设$p=23, q=47, e=3$，明文$m=320$，建立RSA公钥密码体制加密m并解密。

解：$n=pq=23\times 47=1081, \phi(n)=(p-1)(q-1)=22\times 46=1012$；显然$(e,\phi(n))=(3,1012)=1$，利用一次同余方程解法可求得$d=675$，满足$ed\equiv 1(\mathrm{mod}\ \phi(n))$，即$3d\equiv 1(\mathrm{mod}\ 1012)$。
于是可建立RSA公钥密码体制：$p=23, q=47, \phi(n)=1012, d=675$是保密密钥；$n=1081, e=3$是公开密钥。
对于明文$m=320$，加密得密文$c=320^3(\mathrm{mod}\ 1081)=728$，即密文为$c=728$。
解密得明文：$m=728^{675}(\mathrm{mod}\ 1081)=320$。即明文为$m=320$。

RSA算法的安全性

定理

设$n = pq, p, q$是两个不同的素数，则计算$\phi(n)$的值与分解n是等价的，从而在RSA中保密$\phi(n)$是必需的。

证明： 如果已知道n的分解$n = pq$，则易求出$\phi(n)$的值：$\phi(n) = (p-1)(q-1)$。
反之，如果已知道n和$\phi(n)$的值，则易分解出n的因子p和q：
由$n = pq$和$\phi(n) = (p-1)(q-1) = pq-(p+q)+1 = n-(p+q)+1$，即$p+q = n-\phi(n)+1$，从而$p$和$q$是一元二次方程$x^2 - (n-\phi(n)+1)x + n = 0$的两个根。 □

RSA算法实现中的若干问题

形如前面例子中的$m = 728^{675} (\mathrm{mod}\ 1081)$，如何在计算机中计算？

通过模重复平方计算法，将728的指数按照二进制展开，逐次计算，每次只计算一个较小的指数运算，多次迭代。这种方法也常被叫做快速幂算法。

构造密钥时，选择多大的素数？如何判断素数？

目前RSA算法中p和q的长度一般为1024比特以上，生成的N的长度为2048比特以上，E和D的长度和N差不多。
1024比特的RSA算法不应该被用于新的用途，2048比特的RSA算法可以用到2030年，4096比特的算法可以用到2031年。
素数的判定，后面会讲到。

Detailed overview

1. 数论

一次同余方程

定义

***一次同余方程**是指*

$$ax \equiv b \pmod{m} \tag{1.6}$$

其中$a \not\equiv 0 \pmod{m}, m > 1$。

*如果$x = x_0$满足式1.6，则$x \equiv x_0 \pmod{m}$称为**同余方程的解**。有时也把x_0称为同余方程的解。不同的解是指对模数m互不同余的解。*

定理

设$(a, m) = d$，则式1.6有解的充分必要条件是$d|b$。且式1.6有解时，恰有d个解，它们是$x \equiv x_0 + \frac{m}{d}t \pmod{m}, t = 0, 1, \cdots, d-1$。其中$x_0$是式1.6的任意一个解。

举例

例

解一次同余方程$14x \equiv 26 \pmod{38}$。

解： 作辗转相除法

$$\begin{aligned}38 &= 14 \times 3 - 4\\ 14 &= 4 \times 3 + 2\\ 4 &= 2 \times 2\end{aligned}$$

所以$(38, 14) = 2|26$，同余方程有两个解。再回代

$$2 = 14 - 4 \times 3 = 14 - (14 \times 3 - 38) \times 3 = 14 \times (-8) + 38 \times 3$$

由$26 \div 2 = 13$，知$x_0 \equiv (-8) \times 13 \equiv 10 \pmod{38}$是同余方程的解。
再由$38 \div 2 = 19$，
知其两个解为$x \equiv 10 \pmod{38}$, $x \equiv 10 + 19 \equiv 29 \pmod{38}$。

一次同余方程组与孙子定理

一次同余方程组的形式如下：

$$\left.\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\cdots \\ x &\equiv b_k \pmod{m_k} \end{aligned}\right\} \tag{1.7}$$

定理（孙子定理）

设$m_1, m_2, \cdots, m_k$是k个两两互素的正整数，
$m = m_1 m_2 \cdots m_k = m_i M_i (i = 1, \cdots, k)$，则一次同余方程组
式1.7有惟一解

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k \pmod{m}$$

其中$M_i' M_i \equiv 1 \pmod{m_i} (i = 1, \cdots, k)$。

孙子定理(例)

公元5～6世纪(南北朝时期)，《孙子算经》中“物不知数”问题：“今有物，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？”

即求解同余方程组：$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$

这里，$m_1 = 3$, $m_2 = 5$, $m_3 = 7$，$M_1 = 35$, $M_2 = 21$, $M_3 = 15$。

可得，$M_1' = 2$, $M_2' = 1$, $M_3' = 1$，

则：

$x \equiv 35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2 \equiv 233 \equiv 23 \pmod{105}$

快速模幂计算

在RSA算法举例中，解密明文的过程是计算$m = 728^{675} \pmod{1081}$。
已知$1081 = 23 \times 47$，$(23, 47) = 1$。
由孙子定理的证明过程可知，上式满足同余方程组：

$$\begin{cases} m \equiv b_1 \pmod{23} \\ m \equiv b_2 \pmod{47} \end{cases}$$

用模重复平方计算法可得：

$$b_1 \equiv 728^{675} \equiv 15^{675} \equiv 15^{15} \equiv 21 \pmod{23}$$

$$b_2 \equiv 728^{675} \equiv 23^{31} \equiv 38 \pmod{47}$$

用孙子定理求解上面的同余方程组，得$m \equiv 320 \pmod{n}$，
即$m \equiv 320 \pmod{1081}$。

一般同余方程

定义

设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，其中$n>0$，$a_i(i=0,1,\cdots,n)$是整数，又设$m>0$，则：

$$f(x)\equiv 0(\mathrm{mod}\ m)$$

称为模数m的同余方程。若$a_n\not\equiv 0(\mathrm{mod}\ m)$，则称$n$为同余方程式的次数。如果$x=x_0$满足上式，则$x\equiv x_0(bmod\ m)$称为同余方程的解，有时也简称$x_0$为同余方程的解。不同的解是指互不同余的解。

一般同余方程

定理

设$m_1, m_2, \cdots, m_k$是k个两两互素的正整数，$m = m_1 m_2 \cdots m_k$，则同余方程$f(x) \equiv 0(\bmod\ m)$有解的充分必要条件是：

同余方程$f(x) \equiv 0(\bmod\ m_i)$，$(i = 1, 2, \cdots, k)$的每一个有解。

并且，$f(x) \equiv 0(\bmod\ m)$的解与从$f(x) \equiv 0(\bmod\ m_i)$的解得到模$m$的解一致。

如果记同余方程$f(x) \equiv 0(\bmod\ m)$的解的个数为T，记同余方程$f(x) \equiv 0(\bmod\ m_i)$的解的个数为$T_i(i = 1, 2, \cdots, k)$，则$T = T_1 T_2 \cdots T_k$。

上述定理指出了基于模数关系$m = m_1 m_2 \cdots m_k$的同余方程和同余方程组解的关系。

一般同余方程、二次同余方程求解的思路

这里仅就一般形式的同余方程，特别是二次同余方程的求解思路加以介绍，具体展开的内容本课程不做要求。

- 形如$f(x) \equiv 0 (\mathrm{mod}\ m)$的一般同余方程，当$m$不大时，可以将$0, 1, 2, \cdots, m-1$带入方程逐个验算。但$m$很大时，计算量很大；
- 二次同余方程$ax^2 + bx + c \equiv 0 (\mathrm{mod}\ m)$，可通过构造平方式化简为$x^2 \equiv n (\mathrm{mod}\ m)$，$(n, m) = 1$；
- 引入“二次剩余”、“勒让德符号”、“雅克比符号”等概念，构造了二次同余方程解的存在性判断及求解的方法。

零知识证明协议

零知识证明(Zero Knowledge Proof)，是由S.Goldwasser、S.Micali及C.Rackoff 在20世纪80年代初提出的。证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。基于同余方程，可以构建一种零知识证明协议：

设p、q是两个大素数，$n = pq$。假设P想让V相信他知道n的因子，并且P不想让V知道n的因子，则P和V可以执行下面的协议：

1. V随机选取一个大整数x，并计算$y = x^4 \pmod{n}$，V把结果y告诉P；
2. P计算$z = \sqrt{y} \pmod{n}$，P把结果z告诉V；
3. V验证$z = x^2 \pmod{n}$是否成立。

上述协议可以重复执行多次，如果P每次都能正确的计算$\sqrt{y} \pmod{n}$，则V就可以相信P知道n的因子p和q。

Detailed overview

1. 数论

生成一个素数表

观察素数：$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \cdots$

2 is the "oddest prime of all."

定理（无穷多素数定理）

存在无穷多个素数。

证明（欧几里得）：
令数字P为列表中所有素数的乘积，并考虑数字$P+1$，如果$P+1$是素数，我们证明了定理。因此，假设$P+1$不是素数，那么$P+1$可被一些较小的素数p整除。如果p在列表中，则p能被$P+1$和P整除。易证，则p还必须可以整除$(P+1)-P=1$，也就是$p|1$，矛盾，因此p不能在列表中。
例如：{2}开始构造，{2,3,7,43,13,53}

素数计数

素数和合数，哪个更多呢？

偶数计数函数：$E(x)$，素数计数函数：$\pi(x)$。

$$\lim_{x\to\infty}\frac{E(x)}{x}=\frac{1}{2}$$

定理（素数定理）

当x很大时，小于x的素数个数近似等于$x/\ln(x)$，即：

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln(x)}=1$$

1800年左右，高斯与勒让德各自独立提出了该猜想。1896年，Jacques Hadamard与Ch. de la vallée Poussin各自努力去证明该定理；1948年，Paul Erdös与Atle Selberg发现了其“初等”证明。

素数计数(续)

关于素数计数的若干重要猜想：

哥德巴赫猜想

每个大于4的偶数，可以表示成两个素数之和。

I. M. Vinogradov（1937），陈景润（1966）

孪生素数猜想

存在无穷多个素数p使得$p+2$也是素数。

陈景润（1966）

N^2+1猜想

存在无穷多个形如N^2+1的素数。

Hendrik Iwaniec（1978）

梅森素数与完全数

观察形如$a^n-1(n\geq 2)$的素数：

$2^2-1=3$	$2^3-1=7$	$2^4-1=3\cdot 5$	$2^5-1=31$
$3^2-1=2^3$	$3^3-1=2\cdot 13$	$3^4-1=2^4\cdot 5$	$3^5-1=2\cdot 11^2$
$4^2-1=3\cdot 5$	$4^3-1=3^2\cdot 7$	$4^4-1=3\cdot 5\cdot 17$	$4^5-1=3\cdot 11\cdot 31$
$5^2-1=2^3\cdot 3$	$5^3-1=2^2\cdot 31$	$5^4-1=2^4\cdot 3\cdot 13$	$5^5-1=2^2\cdot 11\cdot 71$
$6^2-1=5\cdot 7$	$6^3-1=5\cdot 43$	$6^4-1=5\cdot 6\cdot 37$	$6^5-1=5^2\cdot 311$
$7^2-1=2^4\cdot 3$	$7^3-1=2\cdot 3^2\cdot 19$	$7^4-1=2^5\cdot 3\cdot 5^2$	$7^5-1=2\cdot 3\cdot 2801$
$8^2-1=3^2\cdot 7$	$8^3-1=7\cdot 73$	$8^4-1=3^2\cdot 5\cdot 7\cdot 13$	$8^5-1=7\cdot 31\cdot 151$

由于：$a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots+a^2+a+1)$
a^n-1是合数，除非$a=2$。即使$a=2$，a^n-1也常常是合数。

梅森素数与完全数

命题

对于整数$a \geq 2$与$n \geq 2$，$a^n - 1$是素数，则a必等于2且n一定是素数。

形如$2^p - 1$的素数（其中p是素数），叫做梅森素数。
神父梅森（Marin Mersenne，1588-1648）在1644年断言：

$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$时，$2^p - 1$是素数，且是使得$2^p - 1$为素数的仅有的小于258的素数。

1876年E. Lucas证明了$2^{127} - 1$是素数，这一纪录直到20世纪50年代才被打破。

梅森素数与完全数

什么是完全数？

完全数所有的真因子（即除了自身以外的约数）的和，恰好等于它本身。

完全数有多少？

第一个完全数是6，第二个完全数是28，第三个完全数是496，后面的完全数还有8128、33550336等。截至2018年，共找到51个。

- 所有的完全数都是三角形数。
- 所有的完全数的倒数都是调和数。
- 除6以外的完全数，都可以表示成连续奇立方数之和，并规律式增加。
- 除6以外的完全数，各位数字辗转式相加个位数是1。

梅森素数与完全数

定理（欧几里得完全数公式）

如果2^p-1是素数，则$2^{p-1}(2^p-1)$是完全数。

定理（欧拉完全数定理）

如果n是偶完全数，则n是$n=2^{p-1}(2^p-1)$形式，其中2^p-1是梅森素数。

问题

是否存在无穷多个梅森素数？

问题

是否存在奇完全数？

Detailed overview

1. 数论

模数的阶

定义

设$m > 0$,$(a, m) = 1$,称使$a^l \equiv 1 (\mathrm{mod}\ m)$成立的最小正整数$l$为$a$ 对**模数m的阶**，记为$ord_m(a)$,有时在模数m不变时，也简记为$ord(a)$。

阶的性质

1. 如果$a \equiv a' (\mathrm{mod}\ m)$，则$ord_m(a) = ord_m(a')$。
2. $a^n \equiv 1 (\mathrm{mod}\ m)$的充分必要条件是$ord_m(a)|n$，从而$ord_m(a)|\phi(m)$。
3. 记$ord_m(a) = l$，则$1, a, a^2, \cdots, a^{l-1}$对模数$m$两两不同余。
4. 记$ord_m(a) = l, \lambda > 0, ord_m(a^\lambda) = l_\lambda$，则$l_\lambda = \frac{l}{(\lambda, l)}$，从而$ord_m(a^\lambda) = l$对$\phi(l)$个数$a^\lambda, (\lambda, l) = 1, 0 < \lambda \leq l$都成立。

原根及其存在性

定义（原根）

设整数$m > 0, (g, m) = 1$,如果$ord_m(g) = \phi(m)$,则称g为模数m的**一个原根**。

定理（1）

设$m > 0, (g, m) = 1$,则g为(模数)m的一个原根的充分必要条件是$g, g^2, \cdots, g^{\phi(m)}$为模数$m$的一组既约剩余系。

定理（2）

整数m有原根的充分必要条件是$m = 2, 4, p^a, 2p^a$($a \geq 1, p$为奇素数)。

定理（3）

设p是奇素数,则模p必有原根。

阶的计算方法

设整数a满足$(a,m)=1, m>0$，因为$ord_m(a)|\phi(m)$，故$ord_m(a)$可通过依次计算$a^{d_1}, a^{d_2}, \cdots, a^{d_s}$模$m$的余数是否等于1求出，这里$1=d_1<d_2<\cdots<d_s=\phi(m)$是$\phi(m)$的所有正因数。

定理（4）

设$m=\prod_{i=1}^{s} p_i^{l_i}$为标准分解式，记$ord_{p_i^{l_i}}(a)=f_i(i=1,2,\cdots,s)$，$ord_m(a)=f$，则$f$等于$f_1, f_2, \cdots, f_s$的最小公倍数：$f=[f_1, f_2, \cdots, f_s]$.

定理（5）

设p是一个素数,$a \neq \pm 1, (a,p)=1, ord_{p^j}(a)=f_j$，则$f_{j+1}=f_j$或者$f_{j+1}=pf_j$。进一步，

1. 当$p\neq 2$时，又设$p^i || a^{f_2}-1$（即$p^i | a^{f_2}-1$但$p^{i+1} \nmid a^{f_2}-1$），则有$f_j=\begin{cases} f_2, & 2\le j\le i \\ p^{j-i}f_2, & j>i \end{cases}$
2. 当$p=2$时，又设$a=2^r a_1+1, 2\nmid a_1, r\ge 2$，则有$f_j=\begin{cases} 1, & 1\le j\le r \\ 2, & j=r+1 \\ 2^{j-r}, & j>r+1 \end{cases}$。
   设$a=2^r a_1-1, 2\nmid a_1, r\ge 2$，则有$f_j=\begin{cases} 1, & j=1 \\ 2, & 2\le j\le r+1 \\ 2^{j-r}, & j>r+1 \end{cases}$

例

设$m=648, a=343$，计算$ord_m(a)$。

解 $m=648=2^3\times 3^4, a=343=7^3$，

由$7=2^3-1$根据定理5的(2)，得$ord_{2^3}(7)=2$；

由$7\not\equiv 1(\mathrm{mod}\ 3^2), 7^2\equiv 4\not\equiv 1(\mathrm{mod}\ 3^2), 7^3\equiv 1(\mathrm{mod}\ 3^2)$，根据阶的定义，得$ord_{3^2}(7)=3$；

再由$7^3-1=342=3^2\times 2\times 19$，根据定理5的(1) 及$i=2$，

得$ord_{3^4}(7)=3^{4-2}\times 3=3^3$；

根据定理4，得$ord_{2^3\times 3^4}(7)=[2,3^3]$；

最后根据阶的性质(4)，得$ord_m(a)=\frac{2\times 3^3}{(3,2\times 3^3)}=2\times 3^2=18$。

原根的计算方法

定理

设奇素数p满足如下标准素因子分解$p-1=\prod_{i=0}^{s}p_i^{a_i}, 2=p_0<p_1<\cdots<p_s$。又设整数$a$满足如下条件$(a,p)=1, a^{\frac{p-1}{p_i}}\not\equiv 1 \pmod p, i=0,1,\cdots,s$，则$a$为$p$的原根。

例 (求素数$p=47$的一个原根)

解 *对$p=47$，有标准素因子分解$47-1=46=2\times 23$。*

1. 取整数$a=2, (2,47)=1, 2^{23}\equiv 1 \pmod{47}$，失败。
2. 取整数$a=3, (3,47)=1, 3^{23}\equiv 1 \pmod{47}$，失败。
3. 取整数$a=5, (5,47)=1, 5^{23}\equiv -1\not\equiv 1 \pmod{47}$,
   $5^2=25\not\equiv 1 \pmod{47}$，根据定理5-7知$a=5$是$p=47$的一个原根。

离散对数问题

离散对数问题

1. 若a是素数p的一个原根，则相对于任意整数b，$(b \pmod p \neq 0)$，必然存在唯一的整数i，$(1 \leq i \leq p-1)$，使得$b \equiv a^i \pmod p$，i称为b的以a为基数且模p的幂指数，即离散对数。
2. 对于函数$y \equiv g^x \pmod p$，其中，g为素数p的原根，y与x均为正整数，已知g、x、p，计算y是容易的；而已知y、g、p，计算x是困难的，即求解y的离散对数x是困难的。
3. 离散对数的求解为数学界公认的困难问题。

例：Diffie-Hellman密钥交换

Alice和Bob通过公开信道协商密钥：

1. Alice或Bob选取一个安全的大素数p和它的原根a，p和a都可以公开；
2. Alice选取一个随机数x满足$1 \le x \le p-2$，Bob选取一个随机数y满足$1 \le y \le p-2$，各自保密；
3. Alice把$a^x \pmod p$发给Bob，Bob把$a^y \pmod p$发给Alice;
4. Alice计算$K = (a^y)^x \pmod p$，Bob计算$K' = (a^x)^y \pmod p$，易证$K = K'$，于是Alice和Bob协商得到共同的秘钥。

例：ElGamal公钥密码体制

1. 选取大素数p和p的一个原根a，$(a,p)=1, 1<a<p$。
2. 随机选取整数$d, 2\le d\le p-2$，计算$\beta=a^d \pmod p$。
   p,a,β是公开的加密密钥，d是保密的解密密钥。
3. 明文空间为Z_p^*，密文空间为$Z_p^*\times Z_p^*$。
4. 加密变换：对任意明文$m\in Z_p^*$，秘密随机选取一个整数k，$2\le k\le p-2$，密文为$c=(c_1,c_2)$，其中$c_1=a^k \pmod p), c_2=m\beta^k \pmod p$。
5. 解密变换：对任意密文$c=(c_1,c_2)\in Z_p^*\times Z_p^*$，明文为$m=c_2(c_1^d)^{-1} \pmod p$。

例

ElGamal加密算法实例

- 由上例知素数$p = 47$有一个原根为$a = 5, (5, 47) = 1, 1 < 5 < 47$
- 取$d = 7, 2 \leq 7 \leq 47 - 2$，计算$\beta = 5^7 \pmod{47} = 11$
- 对明文$m = 13 \in Z_{47}^*$，取$k = 8, 2 \leq 8 \leq 47 - 2$
- 加密得密文$c = (8, 15)$，其中$8 = 5^8 \pmod{47}, 15 = 13 \times 11^8 \pmod{47}$
- 解密得明文$m = 15 \times (8^7)^{-1} \pmod{47} = 13$，其中$(8^7)^{-1} \pmod{47} = 4$为$8^7 x \equiv 1 \pmod{47}$的解。

素数的简单判别法–整除判别法

定理

设正整数$p > 1$，*如果对于所有的正整数*$q, 1 < q \leq \sqrt{p}$，*都有*$q \nmid p$，*则*p*为素数。*

例 (用整除判别法证明$p = 97$是一个素数)

证明： *由*$\sqrt{p} = \sqrt{97} < \sqrt{100} = 10$*及小于10的素数2,3,5,7都不能整除*$p = 97$: $p = 97 = 2 \times 48 + 1 = 3 \times 32 + 1 = 5 \times 19 + 2 = 7 \times 13 + 6$，*由整除判别法就得到*$p = 97$*是一个素数。*

素数的简单判别法–威尔逊判别法

定理

设p是大于1的正整数，则p是一个素数的充分必要条件是$(p-1)! \equiv -1 (\bmod\ p)$。

例 (用威尔逊判别法证明$p=23$是一个素数)

证明： $(p-1)! = (23-1)! = 22! \equiv -1 (\bmod\ 23)$，*故23是一个素数。*

素数的确定判别法1

定理（莱梅，D.H.Lehmer)

设正奇数$p>1, p-1=\prod_{i=1}^{s} p_i^{a_i}, 2=p_1<p_2<\cdots<p_s$，$p_i(i=1,\cdots,s)$为素数。如果对每个$p_i$，都有$a_i$，满足$a_i^{\frac{p-1}{p_i}}\not\equiv 1 \pmod p$和$a_i^{p-1}\equiv 1 \pmod p, i=1,\cdots,s$，则$p$为素数。

例 (用莱梅判别法证明$p=37$是一个素数)

证明： $p-1=37-1=36=2^2\times 3^2$，

取$p_1=2, a_1^{37-1}\equiv 1 \pmod{37}, a_1^{\frac{37-1}{2}}\equiv -1\not\equiv 1 \pmod{37}$，

取$p_2=3, a_2^{37-1}\equiv 1 \pmod{37}, a_2^{\frac{37-1}{3}}\equiv -1\not\equiv 1 \pmod{37}$，由莱梅判别法就得到$p=37$是一个素数。

素数的确定判别法2

定理（普罗兹，Proth)

设正奇数$p > 1, p-1 = mq$，其中q是一个奇素数且满足$2q+1 > \sqrt{p}$(即$m < 4(q+1)$)。如果有a满足条件$a^{p-1} \equiv 1 \pmod p$和$a^m \not\equiv 1 \pmod p$，则p为素数。

例 (用普罗兹判别法证明$p = 31$是一个素数)

证明： $p = 31 = 6 \times 5 + 1, q = 5$是一个奇素数，且$2q + 1 = 2 \times 5 + 1 = 11 > \sqrt{31}$，又有$a = 3$满足$a^{31-1} = a^6 \equiv 16 \not\equiv 1 \pmod{31}$，由普罗兹判别法就得到$p = 31$是一个素数。

作业

1. 判断下列整数是否为素数：
   1.1 67
   1.2 $73 = 2^3 \times 3^2 + 1$
   1.3 $2543 = 62 \times 41 + 1$

谢谢！

hanqi_xf@hit.edu.cn