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. 课程介绍

2. 数论

3. 近世代数

4. 数理逻辑基础

课程介绍

Detailed overview

1. 课程介绍

1.1 信息安全中的数学

1.2 课程主要内容

1.3 课程基本信息

三个数学难题

一、 大整数因数分解问题：

给定两个素数p和q，计算其乘积$n = p \times q$是容易的，但从n求p和q呢？

例：

$p = 2000000000000002559$，$q = 8000000000000001239$，$p \times q = 16000000000000022950000000000003170601$

从n分解出p和q是非常困难的！

RSA公开密钥算法的理论基础

三个数学难题

二、 离散对数问题：

已知有限循环群$G =< g >= \{g^k | k = 0, 1, 2, \cdots\}$及其生成元$g$和阶$n = |G|$。

(i) 给定整数a计算元素$g^a = h$很容易；

(ii) 给定元素h，计算整数$x, 0 \leq x \leq n$使得$g^x = h$非常困难。

三、 椭圆曲线离散对数问题：

已知有限域$\boldsymbol{F}_p$上的椭圆曲线群

$E(\boldsymbol{F}_p) = \{(x, y) | \in \boldsymbol{F}_p \times \boldsymbol{F}_p,\ \ y^2 = x^3 + ax + b,\ \ a, b \in \boldsymbol{F}_p\} \cup \{O\}$

及点$P = (x, y)$的阶为一个大素数。

(i) 给定整数a，计算点$aP = (x_a, y_a) = Q$很容易；

(ii) 给定点Q，计算整数x，使得$xP = Q$非常困难。

Detailed overview

1. 课程介绍

1.1 信息安全中的数学

1.2 课程主要内容

1.3 课程基本信息

课程主要内容

1. 数论部分

   整除性、同余性、二次剩余、素数、因子分解、同余式、欧拉定理、扩展的欧几里德算法和中国剩余定理。

2. 近世代数部分

   群、子群、交换群、循环群、群上的离散对数；环、子环、交换环、整数环、多项式环；域、子域、有限域、有限域上的多项式。

3. 数理逻辑部分

   命题逻辑、谓词逻辑、模态逻辑、逻辑与信息安全。

4. 信息安全新进展的数学支撑

   无条件安全与一次一密、量子密码中的数学、混沌中的数学、后量子密码中的数学。

Detailed overview

1. 课程介绍

1.1 信息安全中的数学

1.2 课程主要内容

1.3 课程基本信息

课程基本信息

- **课程名称：**信息安全数学基础—Mathematical Foundations of Information Security
- **开课时间：**2022年9月5日–2022年11月30日
- **课程负荷：**3-5小时/周
- **成绩构成：**出勤，作业，课堂报告（翻转课堂），期末考试
- **课程特点：**看似高大上&枯燥，实则"其乐无穷"！
  不要当成一门纯粹的数学课去学，带着“工欲善其事，必先利其器”的态度去准备未来学习和工作的“屠龙宝刀”！顺便，体验一下数学之美！

Overview

1. 课程介绍
2. 数论
3. 近世代数
4. 数理逻辑基础

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

2. 数论

2.2 整数的可除性及辗转相除法

2.3 不定方程

2.4 整数的唯一分解

2.5 整数的同余

2.6 同余方程

2.7 素数

2.8 原根与素性检测

整数的除法

问题的引出

整数的四则运算：加$(+)$、减$(-)$、乘$(\times)$、除$(\div)$，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

$$a = bq + r,\ 0 \leq r < |b| \tag{2.1}$$

成立。

余数、因数、倍数

定义

称式2.1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2.1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

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < |b| \\
b &= r_1 q_2 + r_2, & 0 < r_2 < r_1 \\
&\ldots, & \ldots \\
r_{n-2} &= r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, & r_{n+1} = 0
\end{aligned} \tag{2.2}$$

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2.2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:

$\mathbf{57 \div 17}:\quad 57 = 17 \times 3 + 6$

$\mathbf{17 \div 6}:\quad 17 = 6 \times 2 + 5$

$\mathbf{6 \div 5}:\quad 6 = 5 \times 1 + 1$

$\mathbf{5 \div 1}:\quad 5 = 1 \times 5$

代回:

$$6 = 1 \times 5 \times 1 + 1$$

$$17 = (1 \times 5 \times 1 + 1) \times 2 + 5$$

$$57 = [(1 \times 5 \times 1 + 1) \times 2 + 5] \times 3 + 6$$

$$57 = [(1 \times 5 \times 1 + 1) \times 2 + 5] \times 3 + 1 \times 5 \times 1 + 1$$

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：*

$$
\begin{aligned}
2357 &= 73 \times 32 + 21 \\
73 &= 21 \times 3 + 10 \\
21 &= 10 \times 2 + 1 \\
10 &= 1 \times 10
\end{aligned}
$$

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

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

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

2. 数论

2.2 整数的可除性及辗转相除法

2.3 不定方程

2.4 整数的唯一分解

2.5 整数的同余

2.6 同余方程

2.7 素数

2.8 原根与素性检测

二元一次不定方程

二元一次不定方程 是指

$$ax + by = c \tag{2.3}$$

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2.3有整数解x, y的充分必要条件是$(a, b)|c$。且式2.3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2.3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：

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N \tag{2.4}$$

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：

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N \tag{2.4}$$

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$a \equiv b (\mod m)$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$a \not\equiv b (\mod m)$。

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

$$ax \equiv b(\mathrm{mod}\ m) \tag{2.5}$$

其中$a \not\equiv 0(\mathrm{mod}\ m), m > 1$*。*

如果$x = x_0$*满足式2.6，则*$x \equiv x_0(\mathrm{mod}\ m)$*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2.6有解的充分必要条件是$d|b$。且式2.6有解时，恰有d个解，它们是$x\equiv x_0+\frac{m}{d}t(\mathrm{mod}\ m), t=0,1,\cdots,d-1$。其中$x_0$是式2.6的任意一个解。

注意：当$(a,m)=1$时，同余方程$ax\equiv 1(\mathrm{mod}\ m)$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$14x \equiv 26 (\mathrm{mod}\ 38)$。

解：作辗转相除法

$$38 = 14 \times 3 - 4$$
$$14 = 4 \times 3 + 2$$
$$4 = 2 \times 2$$

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

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$b_i \equiv ua_i (\mathrm{mod}\ m), i = 1, 2, \cdots, n$，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$uw \equiv 1 (\mathrm{mod}\ m)$。因$(u, m) = 1$，接收方在收到$s$后，可以算出$(sw)_0$，使$sw \equiv (sw)_0 (\mathrm{mod}\ m)$，且$0 < (sw)_0 < m$，则$sw \equiv \sum_{i=1}^{n} m_i w b_i \equiv \sum_{i=1}^{n} m_i uw a_i \equiv \sum_{i=1}^{n} m_i a_i (\mathrm{mod}\ m)$，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（二选一）

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 $24x\equiv 42(\mathrm{mod}\ 30)$
   - 3.2 $90x\equiv 21(\mathrm{mod}\ 429)$

编程作业： 编写一个解同余方程$ax\equiv b(\mathrm{mod}\ m)$的程序，输入$a,b,m$，判断方程是否有解，若有解则给出通解。

Detailed overview

2. 数论

2.2 整数的可除性及辗转相除法

2.3 不定方程

2.4 整数的唯一分解

2.5 整数的同余

2.6 同余方程

2.7 素数

2.8 原根与素性检测

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*

$$a = p_1 p_2 \cdots p_n, p_1 \leq p_2 \leq \cdots \leq p_n$$

其中$p_1, p_2, \cdots, p_n$*都是素数。并且若*

$$a = q_1 q_2 \cdots q_m, q_1 \leq q_2 \leq \cdots \leq q_m$$

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

2. 数论

2.2 整数的可除性及辗转相除法

2.3 不定方程

2.4 整数的唯一分解

2.5 整数的同余

2.6 同余方程

2.7 素数

2.8 原根与素性检测

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，$\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$
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，

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

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$a^{\phi(m)} \equiv 1 (\mathrm{mod}\ m)$。

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：
$aa_1 aa_2 \ldots aa_{\phi(m)} \equiv a_1 a_2 \ldots a_{\phi(m)} (\mathrm{mod}\ m)$
即：$a^{\phi(m)} a_1 a_2 \ldots a_{\phi(m)} \equiv a_1 a_2 \ldots a_{\phi(m)} (\mathrm{mod}\ m)$
再根据性质3，可得：$a^{\phi(m)} \equiv 1 (\mathrm{mod}\ m)$
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$a^{\phi(m)+1} \equiv a (\mathrm{mod}\ m)$。

定理（费马小定理）

若p为素数，则$a^p \equiv a (\mathrm{mod}\ p)$。

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

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$m = c^d (\mathrm{mod}\ n)$。

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算法正确性的证明

证明： 因为$de \equiv 1(\mathrm{mod}\ \phi(n))$，故存在$t$，使得$de = 1 + t\phi(n)$
当$(m,n) = 1$时，
$c^d \equiv (m^e)^d \equiv m^{(1+t\phi(n))} \equiv m \cdot m^{\phi(n)t} \equiv m \cdot 1^t \equiv m(\mathrm{mod}\ n)$
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，$m^{q-1} \equiv 1(\mathrm{mod}\ q)$，从而有：
$m^{t\phi(n)} \equiv m^{t(p-1)(q-1)} \equiv (m^{(q-1)})^{t(p-1)} \equiv 1(\mathrm{mod}\ q)$，
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：$m^{t\phi(n)+1} \equiv m(\mathrm{mod}\ n)$，
于是有：$c^d \equiv m^d e \equiv m^{(1+t\phi(n))} \equiv m(\mathrm{mod}\ n)$
综上，$c^d \equiv m(\mathrm{mod}\ n)$成立。 □

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

2. 数论

2.2 整数的可除性及辗转相除法

2.3 不定方程

2.4 整数的唯一分解

2.5 整数的同余

2.6 同余方程

2.7 素数

2.8 原根与素性检测

一次同余方程

定义

一次同余方程是指

$$ax \equiv b(\mathrm{mod}\ m) \tag{2.6}$$

其中$a \not\equiv 0(\mathrm{mod}\ m), m > 1$*。*

如果$x = x_0$*满足式2.6，则*$x \equiv x_0(\mathrm{mod}\ m)$*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2.6有解的充分必要条件是*$d|b$*。且式2.6有解时，恰有*d*个解，它们是*$x \equiv x_0 + \frac{m}{d}t(\mathrm{mod}\ m), t = 0, 1, \cdots, d-1$*。其中*$x_0$*是式2.6的任意一个解。*

举例

例

解一次同余方程$14x \equiv 26 (\mathrm{mod}\ 38)$。

解：作辗转相除法

$$38 = 14 \times 3 - 4$$
$$14 = 4 \times 3 + 2$$
$$4 = 2 \times 2$$

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

一次同余方程组与孙子定理

一次同余方程组的形式如下：

$$\left.\begin{aligned} x &\equiv b_1 (\mathrm{mod}\ m_1) \\ x &\equiv b_2 (\mathrm{mod}\ m_2) \\ &\cdots \\ x &\equiv b_k (\mathrm{mod}\ m_k) \end{aligned}\right\} \tag{2.7}$$

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2.7有惟一解

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k (\mathrm{mod}\ m)$$

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

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：$\begin{cases} x \equiv 2(\mathrm{mod}\ 3) \\ x \equiv 3(\mathrm{mod}\ 5) \\ x \equiv 2(\mathrm{mod}\ 7) \end{cases}$

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：

$x \equiv 35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2 \equiv 233 \equiv 23(\mathrm{mod}\ 105)$

快速模幂计算

在RSA算法举例中，解密明文的过程是计算$m = 728^{675} (\mathrm{mod}\ 1081)$。
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：

$$\begin{cases} m \equiv b_1 (\mathrm{mod}\ 23) \\ m \equiv b_2 (\mathrm{mod}\ 47) \end{cases}$$

用模重复平方计算法可得：

$$b_1 \equiv 728^{675} \equiv 15^{675} \equiv 15^{15} \equiv 21 (\mathrm{mod}\ 23)$$

$$b_2 \equiv 728^{675} \equiv 23^{31} \equiv 38 (\mathrm{mod}\ 47)$$

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

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$a_n\neq 0(\mathrm{mod}\ m)$，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$f(x) \equiv 0 (\mod m)$有解的充分必要条件是：

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

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

如果记同余方程$f(x) \equiv 0 (\mod m)$的解的个数为T，记同余方程$f(x) \equiv 0 (\mod m_i)$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$y = x^4 (\mathrm{mod}\ n)$，V把结果$y$告诉P；
2. P计算$z = \sqrt{y} (\mathrm{mod}\ n)$，P把结果$z$告诉V；
3. V验证$z = x^2 (\mathrm{mod}\ n)$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$\sqrt{y} (\mathrm{mod}\ n)$，则V就可以相信P知道$n$的因子$p$和$q$。

Detailed overview

2. 数论

2.2 整数的可除性及辗转相除法

2.3 不定方程

2.4 整数的唯一分解

2.5 整数的同余

2.6 同余方程

2.7 素数

2.8 原根与素性检测

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$P+1P=1$，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

2. 数论

2.2 整数的可除性及辗转相除法

2.3 不定方程

2.4 整数的唯一分解

2.5 整数的同余

2.6 同余方程

2.7 素数

2.8 原根与素性检测

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

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

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

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

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

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$f_j = \begin{cases} f_2, & 2 \leq j \leq i \\ p^{j-i} f_2, & j > i \end{cases}$
2. 当$p=2$时，又设$a=2^r a_1+1, 2 \nmid a_1, r \geq 2$，则有$f_j = \begin{cases} 1, & 1 \leq j \leq r \\ 2, & j = r+1 \\ 2^{j-r}, & j > r+1 \end{cases}$。设$a=2^r a_1-1, 2 \nmid a_1, r \geq 2$，则有$f_j = \begin{cases} 1, & j = 1 \\ 2, & 2 \leq j \leq r+1 \\ 2^{j-r}, & j > r+1 \end{cases}$

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5-5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5-5的(1)及$i=2$得$ord_{3^4}(7)=3^{4-2}\times 3=3^3$；根据定理5-4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$(a,p)=1, a^{\frac{p-1}{p_i}} \not\equiv 1(\mathrm{mod}\ p), i=0,1,\cdots,s$，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$a=2,(2,47)=1, 2^{23}\equiv 1(\mathrm{mod}\ 47)$，失败。*
2. *取整数$a=3,(3,47)=1, 3^{23}\equiv 1(\mathrm{mod}\ 47)$，失败。*
3. *取整数$a=5,(5,47)=1, 5^{23}\equiv -1\not\equiv 1(\mathrm{mod}\ 47)$，$5^2=25\not\equiv 1(\mathrm{mod}\ 47)$，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，$(b(\mathrm{mod}\ p) \neq 0)$，必然存在唯一的整数$i$，$(1 \leq i \leq p-1)$，使得$b \equiv a^i(\mathrm{mod}\ p)$，$i$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$y \equiv g^x(\mathrm{mod}\ p)$，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$1 \leq x \leq p-2$，Bob选取一个随机数y满足$1 \leq y \leq p-2$，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$d, 2 \leq d \leq p-2$，计算$\beta = a^d (\mathrm{mod}\ p)$。
   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，$2 \leq k \leq p-2$，密文为$c=(c_1, c_2)$，其中$c_1 = a^k (\mathrm{mod}\ p), c_2 = m\beta^k (\mathrm{mod}\ p)$。
5. 解密变换：对任意密文$c=(c_1, c_2) \in Z_p^* \times Z_p^*$，明文为$m = c_2 (c_1^d)^{-1} (\mathrm{mod}\ p)$。

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*$\beta = 5^7 (\mathrm{mod}\ 47) = 11$
- *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$8 = 5^8 (\mathrm{mod}\ 47), 15 = 13 \times 11^8 (\mathrm{mod}\ 47)$
- *解密得明文*$m = 15 \times (8^7)^{-1} (\mathrm{mod}\ 47) = 13$，*其*
  中$(8^7)^{-1} (\mathrm{mod}\ 47) = 4$*为*$8^7 x \equiv 1 (\mathrm{mod}\ 47)$*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$(p-1)! \equiv -1 (\mathrm{mod}\ p)$。

例 (用威尔逊判别法证明$p = 23$是一个素数)

证明：$(p-1)! = (23-1)! = 22! \equiv -1 (\mathrm{mod}\ 23)$，*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$a_i^{\frac{p-1}{p_i}} \not\equiv 1(\mathrm{mod}\ p)$和$a_i^{p-1} \equiv 1(\mathrm{mod}\ p), i=1,\cdots,s$，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$p_1=2, a_1^{37-1} \equiv 1(\mathrm{mod}\ 37), a_1^{\frac{37-1}{2}} \equiv -1 \not\equiv 1(\mathrm{mod}\ 37)$，
取$p_2=3, a_2^{37-1} \equiv 1(\mathrm{mod}\ 37), a_2^{\frac{37-1}{3}} \equiv -1 \not\equiv 1(\mathrm{mod}\ 37)$，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$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$和$a^m \not\equiv 1 (\mathrm{mod}\ p)$，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$a^{31-1} = a^6 \equiv 16 \not\equiv 1 (\mathrm{mod}\ 31)$，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 $2543 = 62 \times 41 + 1$

编程作业

实现一种素性判断的方法，并比赛从1开始寻找素数(限时一分钟，同样平台上运行)。

Overview

1. 课程介绍

2. 数论

3. 近世代数

4. 数理逻辑基础

第二章 近世代数

何为近世代数？

- 近世代数也叫抽象代数。
- 代数是数学的其中一门分支，当中可大致分为初等代数学和近视代数（抽象代数）学两部分。
- 初等代数学是指19世纪上半叶以前发展的代数方程理论，主要研究某一代数方程（组）是否可解，如何求出代数方程所有的根〔包括近似根〕，以及代数方程的根有何性质等问题。
- 法国数学家伽罗瓦〔1811-1832〕在1832年运用「群」的思想彻底解决了用根式求解多项式方程的可能性问题。他是第一个提出「群」的思想的数学家，一般称他为近世代数创始人。他使代数学由作为解代数方程的科学转变为研究代数运算结构的科学，把代数学由初等代数时期推向近世代数时期。

伽罗华（Évariste Galois）

他是一个天才少年, 15岁学习数学, 短短5年就创造出对后世影响深远的“群论”, 带来数学的革命。他也是一个悲情少年, 两次升学未成, 三次论文发表被拒, 两次被捕入狱, 20岁时就因与情敌对决而黯然离世……

本章概述

近世代数与编码

近世代数简而言之就是群、环、域的故事，不同的约束条件造就不同的精彩世界。

近世代数是纠错码和密码学的重要数学基础。

本章主要介绍以下几个问题：

- 群
- 环
- 域
- 信息安全中的代数

Detailed overview

3. 近世代数

3.2 群

3.3 环

3.4 域

3.5 代数与信息安全

准备：集合上的运算

近世代数中群、环、域的定义都是基于集合的，通过对集合上运算的约束，将集合构造成具有不同特性的新对象。

集合

具有共同属性的事物的总体。

定义（集上的二元运算）

设S为集合，映射

$$\eta : \begin{cases} S \times S & \to & S \\ (x, y) & \mapsto & z \end{cases}$$

称为集合S上的二元运算。

群的定义

定义（群）

设三元组$(G,\cdot,1)$中G为集合，$\cdot$为集G上的二元运算，1为G中一个元。若$(G,\cdot,1)$满足：

- *$G1$(乘法结合律)：$a\cdot(b\cdot c)=(a\cdot b)\cdot c$，$a,b,c\in G$；*
- *$G2$(单位元)：$1\cdot a=a\cdot 1=a$，$a\in G$；*
- *$G3$(逆元)：对$a\in G$，有$a'\in G$使得$a\cdot a'=a'\cdot a=1$。*

*则称$(G,\cdot,1)$为**群**，简称群G，1称为群G的**单位元**，a'称为a的**逆元**。*

若$(G,\cdot,1)$还满足$G4$(**交换律**)：$a\cdot b=b\cdot a$，$a,b\in G$，则称G为**交换群**。
若$(G,\cdot,1)$仅满足$G1,G2$，则称G为**有单位元的半群**。
若$(G,\cdot,1)$满足$G1,G2,G4$，则称G为**有单位元的交换半群**。

举例

例

设$(Z,+,0)$中Z为整数集，$+$为整数的加法，0为整数零，

- $(Z,+,0)$中有$(a+b)+c=a+(b+c)$，故$G1$成立；
- 又有$a+0=0+a=a$，故$G2$成立；
- 最后有$a+(-a)=(-a)+a=0$，这里$(-a)$表示与a对应的负整数，因而$G3$成立；
- 再$a+b=b+a$，故$G4$成立。

从而$(Z,+,0)$为交换群。

举例

例

设$(Q^*,\cdot,1)$中Q^*为零以外的所有有理数的集合，$\cdot$为有理数乘法，1为整数1，则$(Q^*,\cdot,1)$满足$G1,G2,G3$和$G4$。故$(Q^*,\cdot,1)$为交换群。

例

设$GL_n(R)$为n阶实数可逆方阵的集合，$\cdot$为两矩阵的乘法，I为单位阵，则$(GL_n(R),\cdot,I)$为群。$GL_n(R)$称为实数域R上n阶一般线性群。

举例

例 (希尔密码)

在希尔密码(Hill Cipher)中加密变换为

$$(y_1 y_2 \cdots y_m) = (x_1 x_2 \cdots x_m) M \, mod \, 26$$

这里密钥$M \in GL_m(Z_{26}), x_i, y_i \in Z_{26}, Z_{26} = \{0, 1, \cdots, 25\}$，*$x_i$为明文，$y_i$为密文。（式??右边的行向量*$(x_1, x_2, \cdots, x_m)$*与矩阵*$M$*乘是先进行通常的实数行向量与实数矩阵乘再对所得行向量的每一分量取模26）*

加密过程

字母$AB \cdots Z$分别对应$0, 1, \cdots, 25$，加密前先将明文字母串变换为Z_{26}上的数字串，然后再按上述表达式每次m个数字的将明文数字串变换为密文数字串，最后将密文数字串变换为密文字母串。

补充：

定理

设$\mathbf{A}=(a_{ij})$为一个定义在$\mathbf{Z}_{26}$上的$n\times n$矩阵，若$\mathbf{A}$在$mod\,26$上可逆，则有：

$$\mathbf{A}^{-1}=(det\mathbf{A})^{-1}\mathbf{A}^{*}(mod\,26)$$

这里，$\mathbf{A}^{*}$是$\mathbf{A}$的伴随矩阵。

子群

定义（子群）

设$(G,\cdot,1)$为群，A为G的子集合。若$1\in A$且$(A,\cdot,1)$构成群，则称A为G的**子群**，并记为$A\leq G$。

例

证明$nZ=\{0,\pm n,\pm 2n\cdots\}$为整数群$(Z,+,0)$的子群。

证：

- $nZ\subseteq Z$
- $0\in A$
- $(nZ,+,0)$为群

循环群

定义（循环群）

*若群G的每一个元都能表成一个元素a的方幂，则G称为由a生成的**循环群**，记作$G =< a >$，a称为循环群G的**生成元**。*

根据元素的阶的性质，循环群$G =< a >$共有两种类型：

1. 当生成元a是无限阶元素时，则G称为无限阶循环群。
2. 如果a的阶为n，即$a^n = 1$，那么这时$G =< a >=< 1, a, a^2, \cdots, a^{n-1} >$，则$G$称为由$a$所生成的$n$阶循环群，注意此时$1, a, a^2, \cdots, a^{n-1}$两两不同。

置换与对称群

定义（置换）

$S=\{1,2,\cdots,n\}$，映射$\sigma: S \to S$是可逆的，则称σ为S上的**置换**；

定义（对称群）

全体S上的置换所成的集合记为S_n，命1表示恒等置换，在S_n中以$\sigma(i)$表示i在置换σ下的像，定义S_n中两元素σ与η的乘积为

$$[\sigma \cdot \eta](i)=\sigma(\eta(i))$$

则$(S_n,\cdot,1)$成群，群S_n称为n次**对称群**。

举例

例 (置换密码)

在置换密码(Permutation Cipher)中加密变换为

$$(y_1 \ y_2 \ \cdots \ y_m) = (\sigma(x_1) \ \sigma(x_2) \ \cdots \ \sigma(x_m))$$

这里$x_i, y_i \in S = \{1, 2, \cdots, m\}$，$x_i$为明文，$y_i$为密文，$\sigma \in S_m$，$S_m$为$\{1, 2, \cdots, m\}$上$m$次对称群。加密时按上述表达式每次$m$个字符的将明文串变换为密文串。

设置换密码中$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4$，则对应明文$MAGAZINE$的密文为$AMAGEZIN$。

举例

例 (代换密码)

在代换密码(Substitution Cipher)中加密变换为

$$y = \sigma(x)$$

这里$x, y \in \Sigma = \{A, B, \cdots, Z\}$，*$x$为明文，$yi$为密文，*$\sigma \in S_{ym\Sigma}$，*$S_{ym\Sigma}$为$\Sigma$上的对称群。加密时按上述表达式逐字符的将明文串变换为密文串。*

设代换密码

中$\sigma = \begin{pmatrix} ABCDEFGHIJKLMNOPQRSTUVWXYZ \\ DCABIJHGFEZYXWVUTSRQPONMLK \end{pmatrix}$，则对应明文$ESJCACDVVZ$的密文为$IREADABOOK$。

作业

- 证明$(S_n, \cdot, 1)$为群。
- 设$(Z_2^m, \oplus, 0)$中$Z_2^m = \{(a_1 a_2 \cdots a_m) | a_i \in \{0,1\}\}$，$Z_2^m$中运算$\oplus$为两向量逐位在$Z_2$中作运算$\oplus_2$(也称作逐位异或)，0为$m$维全零向量。证明$(Z_2^m, \oplus, 0)$为群。
- 设$\sigma = \begin{pmatrix} 12345678 \\ 73154682 \end{pmatrix}$，求$\sigma$在$S_8$中的逆$\sigma^{-1}$。

群上的离散对数

不同代数系统中都有各自的对数(离散对数)问题，有的可以找到快速算法，有的则尚未找到快速算法。
尚未找到快速算法的离散对数问题，可以看作一个数学上的“难题”，能够用来构造密码学算法或协议。

例 $((Z_n^*, \otimes_n, 1))$

设$\otimes_n$为模n乘，三元组$(Z_n, \otimes_n, 1)$满足G1、G2和G4，为有单位元的交换半群，但其一般不为群，因为当n为合数时，Z_n中某些元不存在逆元。

当n为素数时，对$a \in Z_n^* = \{1, 2, \cdots, n-1\}$有$a' \in Z_n^*$使

得$a \otimes_n a' = 1$，即Z_n^*中每个元都有逆元，故$(Z_n^*, \otimes_n, 1)$为群。

群上的离散对数

例 ($(Z_n^*, \otimes_n, 1)$上的离散对数)

设n为素数，在$(Z_n^*, \otimes_n, 1)$中可定义

$a^m = a \otimes_n a \otimes_n \cdots \otimes_n a$（$m$个$a$，$m$为整数）

对已知的$a, b \in Z_n^*$，求整数x，使得 $a^x = b$的问题称为Z_n^*上的离散对数问题。该问题迄今无快速算法，被应用于Diffie-Hellman密钥交换协议中。

例 (群上的离散对数)

对$a, b \in G$（G为交换群），求整数x使得$b = a^x$。

群上离散对数问题中G为交换群，G的运算写成+，则群上的离散对数问题表示为：求整数x使得$b = xa$。

此种形式的离散对数问题应用于椭圆曲线密码体制（ECC）中。

Detailed overview

3. 近世代数

3.2 群

3.3 环

3.4 域

3.5 代数与信息安全

环的定义

定义（环）

设五元组$(R,+,\cdot,0,1)$中，R为集合，$+$与$\cdot$为集R上二元运算，0与1为R中元。若$(R,+,\cdot,0,1)$满足：

- $R1$(加法交换群)：$(R,+,0)$是交换群
- $R2$(乘法半群)：$(R,\cdot,1)$是有单位元的半群
- $R3$(乘法对加法的分配律)：

  $a\cdot(b+c)=a\cdot b+a\cdot c$，$(b+c)\cdot a=b\cdot a+c\cdot a, a,b,c\in R$

则称$(R,+,\cdot,0,1)$为**环**，简称环R。

环的定义(续)

- $+$与$\cdot$称为环R的**加法与乘法**；
- 1称为环的**单位元**；
- 0称为环的**零元**；
- 若$a'' \in R$使$a'' \cdot a = 1$，则称a''为a的**逆元**，写为a^{-1}；
- 若$a' \in R$使$a' + a = 0$，则称a'为a的**负元**，写为$-a$；
- $(R, +, 0)$称为环R的**加法群**；
- $(R, \cdot, 1)$称为环R的**乘法半群**。

交换环、体、域

定义（交换环）

若环$(R,+,\cdot,0,1)$*满足*

- $R4$*(乘法半群交换)：*$(R,\cdot,1)$*为交换半群。*

则称R*为***交换环***。*

定义（体，域）

若环$(R,+,\cdot,0,1)$*满足*

- $R5$*：*$(R^*,\cdot,1)$*为群，这里*$R^*=R-\{0\}$*，则称*R*为***体***

- $R6$*：*$(R^*,\cdot,1)$*为交换群，则称*R*为***域***

举例

例

整数集Z在整数$+$与整数$\cdot$下为交换环，称为整数环$(Z,+,\cdot,0,1)$，简记为环Z。

证明

- $(Z,+,0)$是交换群
- $(Z,\cdot,1)$是有单位元的交换半群
- 乘法对加法的分配律：

  $a\cdot(b+c)=a\cdot b+a\cdot c$，$(b+c)\cdot a=b\cdot a+c\cdot a$

举例

例

有理数集Q在有理数加法$+$与有理数乘法$\cdot$下为域，称为有理数域$(Q,+,\cdot,0,1)$，简记为域Q。

证明

- $(Q,+,0)$是交换群
- $(Q,\cdot,1)$是有单位元的半群
- 乘法对加法的分配律：

  $a\cdot(b+c)=a\cdot b+a\cdot c$，$(b+c)\cdot a=b\cdot a+c\cdot a$
- $(Q^*,\cdot,1)$是交换群

整环

定义（零因子）

设$a, b \in R$，且$a \neq 0, b \neq 0$，若$a \cdot b = 0$，则称a与b为环R中的**零因子**。

定义（整环）

环R若无零因子，则称R为无零因子环。交换的无零因子环称为**整环**。

例

在环Z_{26}中13和2是零因子。

理想、主理想

定义（理想）

若I为环R的加法群的子群，且对任$a \in I$和任$r \in R$有$ar \in I$和$ra \in I$，则称I为环R的**理想**。

定义（主理想）

若I为交换环R的理想。若$I = \{ra | r \in R\}$，则称I为环R的**主理想**，并记为$I = (a)$。

例

在整数环$(Z, +, \cdot, 0, 1)$中，令$nZ = \{0, \pm n, \pm 2n, \cdots\}$，则$nZ$为环$Z$的理想，且$nZ$为环$Z$的主理想，此时$nZ = (n)$。

翻转课堂/大作业（小论文）

翻转课堂–10月12日（下周三）

- **报名**：发送邮件到dxjsj_hit@126.com，写清楚：姓名、学号、要讲的内容；
- **范围**：初等数论部分，围绕一个主题准备相应的材料（报告+PPT）；
- **要求**：每人20分钟，建议：讲15分钟，提问、交流5分钟；
- **成绩**：同学互评。

or 大作业/小论文（结课前提交）

- **主题**：“素数与信息安全”
- **要求**：查阅资料，阐述自己的心得和观点；严格按照学术论文格式要求，撰写500-1000字的阅读报告，鼓励使用LaTeX书写。

多项式环

定义（环上的多项式）

设x为文字，R为交换环，$x \notin R$。定义R上多项式集

$$R[x] = \{f(x) = \sum_{i=0}^{n} a_i x^i | n \in Z, a_i \in R\}$$

- $f(x) = \sum_{i=0}^{n} a_i x^i$称为交换环$R$上关于文字$x$的多项式；
- $a_i x^i$称为$f(x)$的第i次项，a_i为$f(x)$的第i次项系数；$a_0 x^0$ 写为a_0。
- 当$a_n \neq 0$时，$a_n x^n$称为$f(x)$的首项，n称为$f(x)$的次数，记为$\partial f(x) = n$；特别当$a_n = 1$时，称$f(x)$为首1多项式；
- 称$0 \in R$为$R[x]$中的零多项式，并约定$\partial(0) = -\infty$(负无穷大)，任意非负整数n，$n + (-\infty) = -\infty$。

加法与乘法

下面定义$R[x]$中的$+$与$\cdot$：
设$f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{j=0}^{m}b_jx^j$，定义

$$f(x)+g(x)=\sum_{i=0}^{max\{m,n\}}(a_i+b_i)x^i$$

$$f(x)\cdot g(x)=\sum_{k=0}^{m+n}(\sum_{i+j=k}a_ib_j)x^k$$

定义

设R为交换环，五元组$(R[x],+,\cdot,0,1)$称为R上的多项式环，其中$+$与$\cdot$如上述定义。

举例

例

设Q与R分别为有理数域与实数域，$Q[x]$与$R[x]$为有理多项式环与实多项式环。

例

令$f(x)=2x^2+1, g(x)=13x^3+24x^2+1 \in Z_{26}[x]$，

求$f(x)+g(x)$和$f(x)g(x)$

定理

设R为整环，$f(x), g(x) \in R[x]$，则：

1. $\partial(f(x)g(x)) = \partial f(x) + \partial g(x)$
2. $\partial(f(x)+g(x)) = \max(\partial f(x), \partial g(x))$

举例

例：多项式环的主理想

设$f(x)=\sum_{i=0}^{n}a_ix^i\in Z[x]$，

则$(f(x)=f(x)z(x)|z(x)\in Z[x])$为$Z[x]$的主理想。

例：纠错码之—循环码

设F为域，环$(F[x]_{x^n-1},+,\cdot,0,1)$中$F[x]_{x^n-1}$为域$F$上次数小于$n$的多项式集合，$+$与$\cdot$分别为两多项式的模$x^n-1$加与乘，该环称为剩余类多项式环。该环的由$x^n-1$的因式，$n-k$次多项式$g(x)$生成的理想$I=\{f(x)=v_0+v_1x+\cdots+v_{n-1}x^{n-1}|$有次数小于$k$的多项式$h(x)$使$f(x)=h(x)g(x)\}$具有如下性质：

若$v_0+v_1x+\cdots+v_{n-1}x^{n-1}\in I$，

则$v_{n-1}+v_1x+\cdots+v_{n-2}x^{n-1}\in I$。$I$为循环纠错码。

作业

- 设$Z_n = \{0, 1, \cdots, n-1\}$，$\oplus_n, \otimes_n$分别是模$n$加和模$n$乘，五元组$(Z_n, \oplus_n, \otimes_n, 0, 1)$为环，称为剩余类环，简记为环$(Z_n, +, \cdot, 0, 1)$或$Z_n$。试证明该结论。
- 证明Z_p为域，这里p为素数。
- 证明有零因子的环不为域。

Detailed overview

3. 近世代数

3.2 群

3.3 环

3.4 域

3.5 代数与信息安全

域的定义

定义（域）

设五元组$(F,+,\cdot,0,1)$中，F为集合，$+$和$\cdot$为集合F上的二元运算，0和1为F中元。若$(F,+,\cdot,0,1)$满足：

- $F1$(加法交换群)：$(F,+,0)$是交换群
- $F2$(乘法交换群)：$(F^*,\cdot,1)$是交换群，这里$F^*=F-0$
- $F3$(乘法对加法的分配律)：$a\cdot(b+c)=a\cdot b+a\cdot c$，$a,b,c\in F$

则称$(F,+,\cdot,0,1)$为**域**，简称域F。

域的定义

- $+$和$\cdot$称为域F的加法和乘法。
- 1称为F的单位元。
- 0称为域的零元。
- 若$a' \in F$使$a' + a = 0$，则称a'为a的负元，写为$-a$。
- 若$a" \in F$使$a" \cdot a = 1$，则称$a"$为a的逆元，写为a^{-1}。
- $(F, +, 0)$称为域F的加法群，$(F^*, \cdot, 1)$称为域F的乘法群。
- 在约定$a - b = a + (-b), a/b = ab^{-1}$后，域中便有了“减法”与“除法”运算。

举例

例 (有理数域)

五元组$(Q,+,\cdot,0,1)$中，Q为有理数集合，0和1为有理数0和1，$+$和$\cdot$称为有理数+和$\cdot$。$(Q,+,\cdot,0,1)$满足域的定义，称为有理数域Q。

例 (实数域)

五元组$(R,+,\cdot,0,1)$中，R为实数集合，0和1为实数0和1，$+$和$\cdot$称为实数+和$\cdot$。$(R,+,\cdot,0,1)$满足域的定义，称为实数域R。

例 (复数域)

五元组$(C,+,\cdot,0,1)$中，C为复数集合，0和1为复数0和1，$+$和$\cdot$称为复数+和$\cdot$。$(C,+,\cdot,0,1)$满足域的定义，称为复数域C。

Galois域

定义

设F是一个域，如果F含有无限多个元素，则称F为**无限域**。相反，如果F含有有限个元素，则称为**有限域**或**Galois域**，并把F中元素的个数称为F的**阶**。若F含有q个元素，可简记为$GF(q)$。

例

在域$GF(2)$中仅有两个元0和1，故称二元域。元0和1可由电信号的低和高实现，$\oplus_2$可由数字信号的异或实现，$\otimes_2$可由数字信号的与实现，所以二元域$GF(2)$就成为信息科学技术领域及信息安全领域应用最多的域之一。

域的基本性质

定理

设F是个域，那么在F中下列运算规则成立：

- *加法消去律：设$a, b, c \in F$，如果$a + c = b + c$，则一定有$a = b$。*
- *乘法消去律：设$a, b, c \in F$，且$c \neq 0$，如果$a \cdot c = b \cdot c$，则一定有$a = b$。*
- *对于任意的$a \in F$，都有$-(-a) = a$。*
- *对于任意的$a \in F$，且$a \neq 0$，都有$(a^{-1})^{-1} = a$。*
- *对于任意的$a \in F$，都有$a \cdot 0 = 0$。*

域的基本性质

定理

- 对于任意的$a, b \in F$，若$a \cdot b = 0$，则一定有$a = 0$或$b = 0$。
- 对于任意的$a, b \in F$，都有$-(a + b) = (-a) + (-b)$。
- 对于任意的$a, b \in F$，都有$a \cdot (-b) = (-a) \cdot b = -a \cdot b$。
- 对于任意的$a, b \in F$，都有$(-a) \cdot (-b) = a \cdot b$。
- 对于任意的$a, b \in F$，且$a \neq 0, b \neq 0$，都有$(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$。
- 对于任意的$a \in F$，且$a \neq 0$，都有$(-a)^{-1} = -a^{-1}$。

带余除法

定理（带余除法）

设$f(x)$和$g(x)$为$F[x]$中的多项式，且$g(x) \neq 0$，则存在惟一的两个多项式$q(x)$和$r(x)$，使得

$$f(x) = q(x)g(x) + r(x), \quad \partial r(x) < \partial g(x) \tag{3.1}$$

称$f(x)$为被除式，$g(x)$为除式，$q(x)$为商式，$r(x)$为余式。

上式中，若$r(x) = 0$，则称$g(x)$是$f(x)$的**因式**，或称$f(x)$是$g(x)$的**倍式**，还称$f(x)$能被$g(x)$整除，记作$g(x)|f(x)$。

公因式

公因式

- 设$f(x), g(x), q(x)$是$F[x]$中的多项式，且$q(x) \neq 0$。如果$q(x)$既是$f(x)$的因式，又是$g(x)$的因式，则称$q(x)$为$f(x)$和$g(x)$的**公因式**。
- 如果$f(x)$和$g(x)$不全为0，则$f(x)$和$g(x)$的公因式中次数最高的首1多项式称为$f(x)$和$g(x)$的**最高公因式**，记作$(f(x), g(x))$。
- 如果$(f(x), g(x)) = 1$，则称$f(x)$与$g(x)$**互素**。

公倍式

公倍式

- 设$f(x), g(x), q(x)$是$F[x]$中的多项式，且$q(x) \neq 0$。如果$q(x)$既是$f(x)$的倍式，又是$g(x)$的倍式，则称$q(x)$为$f(x)$和$g(x)$的**公倍式**。
- 如果$f(x)$和$g(x)$不全为0，则$f(x)$和$g(x)$的公倍式中次数最低的首1多项式称为$f(x)$和$g(x)$的**最低公倍式**，记作$[f(x), g(x)]$。

域上的多项式

引理

设$f(x)$、$g(x)$、$q(x)$、$r(x)$是$F[x]$中的多项式，
若$f(x) = q(x)g(x) + r(x)$，则

$$(f(x), g(x)) = (g(x), r(x))$$

定理

设$f(x)$和$g(x)$为$F[x]$中不等于0的多项式，则必存在$F[x]$中的两个多项式$a(x)$和$b(x)$，使得

$$(f(x), g(x)) = a(x)f(x) + b(x)g(x) \tag{3.2}$$

定理证明中给出的辗转相除法是一种求两个多项式的最高公因式的重要算法，称为Euclid算法。

举例

例

设$f(x)=x^6+x^4+x+1$，$g(x)=x^4+x+1$为$GF(2)$上的多项式，用Eulid算法求出$(f(x),g(x))$。

解

$$x^6+x^4+x+1=(x^2+1)(x^4+x+1)+(x^3+x^2)$$

$$x^4+x+1=(x+1)(x^3+x^2)+(x^2+x+1)$$

$$x^3+x^2=x(x^2+x+1)+x$$

$$x^2+x+1=(x+1)x+1$$

$$x=1x+0$$

所以$(f(x),g(x))=1$。

举例(续)

进一步把上述各式改写如下(在$GF(2)$上+等于−):

$$
\begin{aligned}
x^3+x^2 &= x^6+x^4+x+1+(x^2+1)(x^4+x+1)\\
x^2+x+1 &= x^4+x+1+(x+1)(x^3+x^2)\\
x &= x^3+x^2+x(x^2+x+1)\\
1 &= x^2+x+1+(x+1)x\\
x &= 1x+0
\end{aligned}
$$

把x, x^2+x+1, x^3+x^2依次代入表达式$1=x^2+x+1+(x+1)x$中:

$$
\begin{aligned}
1 &= (x^2+x+1)+(x+1)[(x^3+x^2)+x(x^2+x+1)]\\
&= (x+1)(x^3+x^2)+(x^2+x+1)(x^2+x+1)\\
&= (x+1)(x^3+x^2)+(x^2+x+1)[(x^4+x+1)+(x+1)(x^3+x^2)]\\
&= (x^3+x)(x^3+x^2)+(x^2+x+1)(x^4+x+1)\\
&= (x^3+x)[(x^6+x^4+x+1)+(x^2+1)(x^4+x+1)]+(x^2+x+1\\
&= (x^3+x)(x^6+x^4+x+1)+(x^5+x^2+1)(x^4+x+1)
\end{aligned}
$$

最后得到 $(f(x),g(x))=(x^3+x)f(x)+(x^5+x^2+1)g(x)$

既约多项式、可约多项式

设$f(x)$是$F[x]$中的一个多项式，且$\partial f(x) \geq 1$。如果$f(x)$的因式只有常数$c(c \neq 0)$或$cf(x)$，则称$f(x)$为域F上的**不可约多项式**或**既约多项式**。否则，称$f(x)$为域F上的**可约多项式**。

注意：多项式的可约性与所在的域F密切相关。

例

多项式x^2-2在有理数域Q中是既约的，但在实数域R中却是可约的，即$x^2-2=(x+\sqrt{2})(x-\sqrt{2})$。

例

多项式x^2+1在有理数域Q和实数域R中都是既约的，但在复数域C中却是可约的，即$x^2+1=(x+i)(x-i)$。

既约多项式分解、根

定理

域F上的次数≥ 1的多项式都可以分解成一些域F上的既约多项式的乘积。如果不计这些既约多项式在乘积中的先后顺序，那么这些分解还是惟一的。

设$f(x)$是$F[x]$中的多项式，如果当$x = a$时$f(a) = 0$，则称a为$f(x)$的一个根。

因为一次多项式一定是既约多项式，根据上面定理可知，域F上的n次多项式最多只能分解为n个一次多项式的乘积。因此，域F上的n次多项式在域F中最多有n个根。

多项式的同余

定义

如果域F上的多项式$f(x)$和$g(x)$被$m(x)$相除有相同的余式，即：

$$f(x)=q_1(x)m(x)+r(x),\ g(x)=q_2(x)m(x)+r(x),\ \partial r(x)<\partial m(x)$$

或者$r(x)=0$，则称$f(x)$和$g(x)$关于模$m(x)$同余，简记为：

$$f(x)=g(x)\mod m(x)$$

引理

$f(x)=g(x)\mod m(x)$，当且仅当$m(x)|(f(x)-g(x))$。

同余运算的基本性质

定理

设$f(x)$、$g(x)$、$q(x)$、$r(x)$、$m(x)$是域F上的多项式，则

1. $f(x) = f(x) \mod m(x)$(自反性)
2. $f(x) = g(x) \mod m(x)$，当且仅当$g(x) = f(x) \mod m(x)$(对称性)
3. 若$f(x) = g(x) \mod m(x)$且$g(x) = q(x) \mod m(x)$，则$f(x) = q(x) \mod m(x)$(传递性)

同余运算的基本性质(续)

定理

1. 若$f(x) = g(x) \mod m(x)$且$q(x) = r(x) \mod m(x)$，
   则$f(x) + q(x) = g(x) + r(x) \mod m(x)$
2. 若$f(x) = g(x) \mod m(x)$且$q(x) = r(x) \mod m(x)$，
   则$f(x) - q(x) = g(x) - r(x) \mod m(x)$
3. 若$f(x) = g(x) \mod m(x)$且$q(x) = r(x) \mod m(x)$，
   则$f(x)q(x) = g(x)r(x) \mod m(x)$
4. 若$q(x)f(x) = q(x)g(x) \mod m(x)$且$(q(x), m(x)) = 1$，
   则$f(x) = g(x) \mod m(x)$

剩余类

用域F上的一个n次多项式去除$F[x]$中所有多项式，所得的余式的次数一定小于n。设余式的一般形式如下：

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0, \quad a_i \in F$$

设域F含有q个元素，则共有q^n个不同的余式。把具有相同余式的多项式归为一类，并称为一个剩余类。这样$F[x]$中的所有多项式便划分为q^n个剩余类。

例

设$f(x) = x^3 + 1$为$GF(2)$上的多项式，用它去除$GF(2)$上的所有多项式，可以把所有$GF(2)$上的多项式划分为以下8个剩余类：

$\{0\}, \{1\}, \{x\}, \{x+1\}, \{x^2\}, \{x^2+1\}, \{x^2+x\}, \{x^2+x+1\}$

子域、扩域

定理

设$p(x)$是域F上的一个n次既约多项式，记$F[x]_{p(x)}$为模$p(x)$的全体余式集合，
即$F[x]_{p(x)} = \{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots a_1 x + a_0, a_i \in F\}$，并对于任意的$f(x)$和$g(x) \in F[x]_{p(x)}$，定义以下的模加和模乘运算：

$$f(x) + g(x) = (f(x) + g(x))_{p(x)} \quad f(x) \cdot g(x) = (f(x) \cdot g(x))_{p(x)}$$

*则$F[x]_{p(x)}$关于所定义的加法和乘法运算构成域。如果F包含q个元素，则$F[x]_{p(x)}$是一个包含q^n个元素的有限域$GF(q^n)$，而且F是这个$GF(q^n)$的**子域**。*

根据上述定理，F是$F[x]_{p(x)}$的子域，$F[x]_{p(x)}$是F的**扩域**。从F到$F[x]_{p(x)}$是经过$p(x)$实现的，所以又称$F[x]_{p(x)}$是由$p(x)$扩成的域。

举例

例

由$GF(2)$上的4次既约多项式$p(x) = x^4 + x + 1$扩成的$GF(2^4)$如下表所示：

4位向量形式	多项式形式	4位向量形式	多项式形式
0000	0	1011	$x^3 + x + 1$
0001	1	0101	$x^2 + 1$
0010	x	1010	$x^3 + x$
0100	x^2	0111	$x^2 + x + 1$
1000	x^3	1110	$x^3 + x^2 + x$
0011	$x + 1$	1111	$x^3 + x^2 + x + 1$
0110	$x^2 + x$	1101	$x^3 + x^2 + 1$
1100	$x^3 + x^2$	1001	$x^3 + 1$

数据组与多项式

定义

设$f(x)$为$GF(2)$上的$n-1$次多项式，A为$GF(2)$上的n位数据组，

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0, \quad a_i \in GF(2)$$
$$A = (a_{n-1}, a_{n-2}, \cdots, a_1, a_0), \quad a_i \in GF(2)$$

定义映射如下：

$$f(x) \leftrightarrow A$$

显然，这种映射关系是一对一的映射，该映射将一个多项式转换成一个数据组，反过来，也可将一个数据组转换成一个多项式。

应用实例

有限域上的多项式在高级数据加密标准(AES)中的应用

AES进行加解密数据处理的数据单位主要为字节和字(4个字节)。为了能够进行字节和字的加法、乘法等运算，AES采用有限域的多项式表示法来表示字节和字。具体地，AES采用$GF(2)$上的既约多项式

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

作为运算模，用其余式构成$GF(2^8)$。这样，一个字节就可视为一个多项式，并视为$GF(2^8)$中的一个元素。字节的相加定义为$GF(2)$上多项式的相加。字节的相乘定义为$GF(2)$上多项式的相乘，并取模$m(x)$。

应用实例(续)

例如，字节$9BH + 6FH$就可表示为如下的多项式加

$$(x^7+x^4+x^3+x+1)+(x^6+x^5+x^3+x^2+x+1) = x^7+x^6+x^5+x^4+x^2$$

上述多项式系数相加

$$(10011011) \oplus (01101111) = (11110100) = F4H$$

又如

$$(x^6+x^4+x^2+x+1)\cdot(x^7+x+1) = x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$$

而

$$x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1 \quad mod \quad x^8+x^4+x^3+x+1 = x^7+x^6+$$

这恰好完成了字节$57H \times 83H = C1H$的运算。

应用实例(续)

AES定义了$GF(2^8)$上的一个倍乘函数xtime(x)，用以实现字节的按模移位：

$$\text{xtime}(x) = x \cdot f(x) \mod x^8 + x^4 + x^3 + x + 1$$

例如，设字节为$57H$，则

$$\begin{aligned} \text{xtime}(57) &= x(x^6 + x^4 + x^2 + x + 1) \mod x^8 + x^4 + x^3 + x + 1 \\ &= (x^7 + x^5 + x^3 + x^2 + x) \mod x^8 + x^4 + x^3 + x + 1 \\ &= AEH \end{aligned}$$

这样就实现了把字节$57H$循环左移一位，用向量表示为xtime$(01010111) = (10101110)$。

若有字节$93H$，则有：

$$\begin{aligned} \text{xtime}(93) &= x(x^7 + x^4 + x + 1) \mod x^8 + x^4 + x^3 + x + 1 \\ &= (x^5 + x^4 + x^3 + x^2 + 1) = 3DH \end{aligned}$$

也即xtime$(10010011) = (00111101)$，注意，在这里并不是普通的循环左移，而是在模$m(x)$条件下的循环左移。

有限域的加法特性

在有理数域Q、实数域R和复数域C中，任意多个1相加都不等于0。而在有限域中，因为元素的个数有限，所以下面的元素序列中不可能没有相同的元素：

$$1, 1+1=2\cdot 1, 1+1+1=3\cdot 1, 1+1+1+1=4\cdot 1, \cdots$$

设在此序列中有$i\cdot 1=j\cdot 1, 1\le i<j$，则有$(j-i)\cdot 1=0$。
令$p=j-i$，则有$p\cdot 1=0$

定义（域的特征）

设F是一个域，而1是其乘法单位元。如果对应任意的正整数m，都有$m\cdot 1\neq 0$，则称域F的特征是0。如果有一个正整数m，使得$m\cdot 1=0$，而且适合此条件的最小正整数为p，则称域F的特征是p。

有限域的加法特性

定理

设F是一个域，F的特征要么是0，要么是一个素数p。

证明：假设F的特征是0，则定理成立。假设F的特征不是0，则必存在一个正整数m，使得$m \cdot 1 = 0$。设满足此条件的最小正整数p，证明p一定是素数。假设p不是素数，则p可分解成$p = p_1 p_2, 1 < p_1, p_2 < p$。于是

$$p \cdot 1 = p_1 p_2 \cdot 1 = (p_1 \cdot 1)(p_2 \cdot 1) = 0$$

因此有$p_1 \cdot 1 = 0$ 或$p_2 \cdot 1 = 0$
这与p的最小性相矛盾，所以p一定是素数。

有限域的加法特性

例

只有0和1两个元素的二元域$GF(2)$和由$GF(2)$上的n次既约多项式扩成的有限域$GF(2^n)$的特征都是2。

根据前定理，特征为0的域一定是无限域，而有限域的特征一定是一个素数。

注意：此论断的逆命题不成立。例如，系数取自$GF(p)$的全体有理数函数的集合

$$S = \{\frac{f(x)}{g(x)} | f(x), g(x) \text{ 是} GF(p) \text{上的多项式}\}$$

便构成一个特征为p的无限域。之所以是无限域，是因为对$f(x)$和$g(x)$的次数没有限制。

有限域的加法特性

定理

设F是特征为p的一个有限域，对于任意$a, b \in F$都有

$$(a+b)^p = a^p + b^p$$

证明：根据牛顿二项式定理，$(a+b)^p = \sum_{k=0}^{p} C_p^k a^k b^{p-k}$ 注意到其中$C_p^0 = C_p^p = 1$，而对于$1 \le k \le p-1, C_p^k = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k}$。因为$C_p^k$是正整数，$p$是素数，所以$\frac{(p-1)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k}$一定是整数，也就是说$p|C_p^k$，因此$C_p^k = 0 \ mod \ p$。

例

设$f(x) = x^4 + x + 1$是$GF(2)$上的多项式，则

$(f(x))^2 = (x^4 + x + 1)^2 = x^8 + x^2 + 1$

有限域的乘法特性

引理

设G是一个有限交换群，a是G的一个n阶元素，k是任意正整数，则a^k是$\frac{n}{(n,k)}$阶元素。特别a^k是n阶元素，当且仅当$(n,k)=1$。

定理

任一有限域的乘法群都是循环群。

定理 (Fermat定理)

$GF(p^n)$中的任一元素a都满足等式 $a^{p^n}=a$

或者说都是方程 $x^{p^n}-x=0$

的根。还可以说 $x^{p^n}-x=\prod_{a\in F}(x-a)$

注：该定理说明方程$x^{p^n}-x=0$没有重根，而且$GF(p^n)$的全部元素就是它的全部根。

有限域的乘法特性

定义（本原元）

有限域$GF(q)$乘法群的生成元(即阶为$q-1$的元素)为$GF(q)$的本原元。

一个有限域往往不只有一个本原元。根据前面引理可以算出有限域本原元的个数。考虑有q个元素的有限域$GF(q)$，根据定理，$GF(q)$的乘法群是循环群，这就是说，$GF(q)$至少有一个本原元a使得

$$a^0 = 1, a, a^2, \cdots, a^{q-2}$$

就是$GF(q)$的乘法群的全体元素。根据引理，元素$a^i (i = 1, 2, \cdots, q-2)$的阶为$q-1$，当且仅当$(i, q-1) = 1$。因此，$GF(q)$的本原元个数为$\phi(q-1)$。($\phi(x)$为欧拉函数，表示在小于$x$且与$x$互素的正整数的个数。例如$\phi(5) = 4, \phi(6) = 2$)。

有限域的乘法特性

例

考查由$GF(2)$上的既约多项式x^4+x+1扩成的有限域$GF(2^4)$，其全体非零元素构成循环群。设a是一个本原元，则$GF(2^4)$的循环群共有$\phi(2^4-1)=\phi(15)=8$个本原元：

$$a, a^2, a^4, a^7, a^8, a^{11}, a^{13}, a^{14}$$

4个5阶元素

$$a^3, a^6, a^9, a^{12}$$

两个3阶元素

$$a^5, a^{10}$$

最小多项式与本原多项式

Fermat定理说明，$GF(p^n)$上的每一个元素都满足$x^{p^n} - x = 0$，其中$x^{p^n} - x$是$GF(p)$上的首1多项式。但是$GF(p^n)$的元素除了满足这一多项式外，还可能满足其他次数更低的多项式。由此导出最小多项式和本原多项式的概念。

定义

$GF(p^n)$的任一元素a的最小多项式是以a为根的次数最低的$GF(p)$上的首1多项式，记作$M(x)$。本原元的最小多项式称为本原多项式。

最小多项式与本原多项式

例

考查由$GF(2)$上的既约多项式x^4+x+1扩成的有限域$GF(2^4)$。

设a是一个本原元，$GF(2^4)$的部分元素的最小多项式如下：

$$
\begin{array}{rcccl}
0 & \leftrightarrow & 0 & \leftrightarrow & M(x)=x \\
1 & \leftrightarrow & 1 & \leftrightarrow & M(x)=x+1 \\
x & \leftrightarrow & a & \leftrightarrow & M(x)=x^4+x+1 \\
x^3 & \leftrightarrow & a^3 & \leftrightarrow & M(x)=x^4+x^3+x^2+x+1 \\
x^2+x & \leftrightarrow & a^5 & \leftrightarrow & M(x)=x^2+x+1
\end{array}
$$

作业

1. 求下列各组$GF(2)$上的多项式组的最高公因式
   - $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1, g(x) = x^4 + x^2 + x + 1$
   - $f(x) = x^5 + x^4 + x^2 + 1, g(x) = x^3 + x + 1$
2. 写出$GF(2)$上多项式$x^4 + 1$为模的所有剩余类
3. $p(x) = x^2 + x + 1$是$GF(2)$上的既约多项式，由$p(x)$扩成域$GF(2^2)$，写出其加法和乘法表

Detailed overview

3. 近世代数

3.2 群

3.3 环

3.4 域

3.5 代数与信息安全

概述

近世代数在计算机特别是信息安全领域有广泛的应用，是很多重要技术的理论基础和理论工具，比如：

- 纠错码
- 伪随机序列
- 古典密码算法
- AES密码算法
- 椭圆曲线密码

椭圆曲线

概述

椭圆曲线是指由韦尔斯特拉斯(Weierstrass)方程

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

所确定的平面曲线，其中系数$a_i(i = 1, 2, \cdots, 6)$定义在某个域上。

椭圆曲线密码是基于有限域上椭圆曲线有理点群的一种密码系统，其数学基础是利用椭圆曲线上的点构成的Abelian加法群构造的离散对数的计算困难性。

主要内容

1. 椭圆曲线的基本概念
2. 加法原理
3. 有限域上的椭圆曲线

基本概念

设K是一个域，域K上的Weierstrass方程是：

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.3}$$

其中$a_1, a_2, a_3, a_4, a_6 \in K$。
式3.3的判别式为：

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

其中

$$\begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = a_1a_3 + 2a_4 \\ b_6 = a_3^2 + 4a_6 \\ b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \end{cases}$$

基本概念

定义

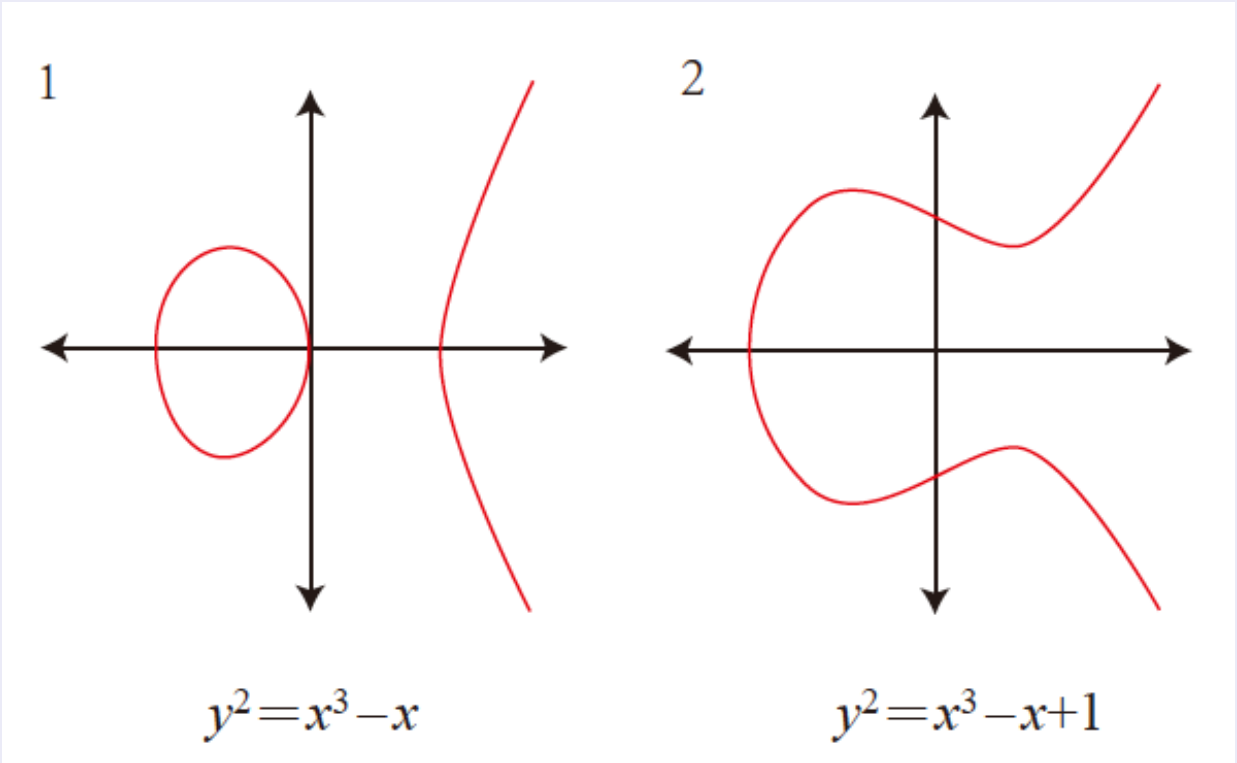
当$\Delta \neq 0$，域K上的点集

$$E:\{(x,y)|y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\}\cup\{O\} \quad (3.4)$$

其中$a_1,a_2,a_3,a_4,a_6 \in K$，$\{O\}$为无穷远点，称为域$K$上的椭圆曲线。这时，$j=(b_2^2-24b_4)^3/\Delta$称为椭圆曲线$E$的$j-$不变量，记作$j(E)$。

认识椭圆曲线

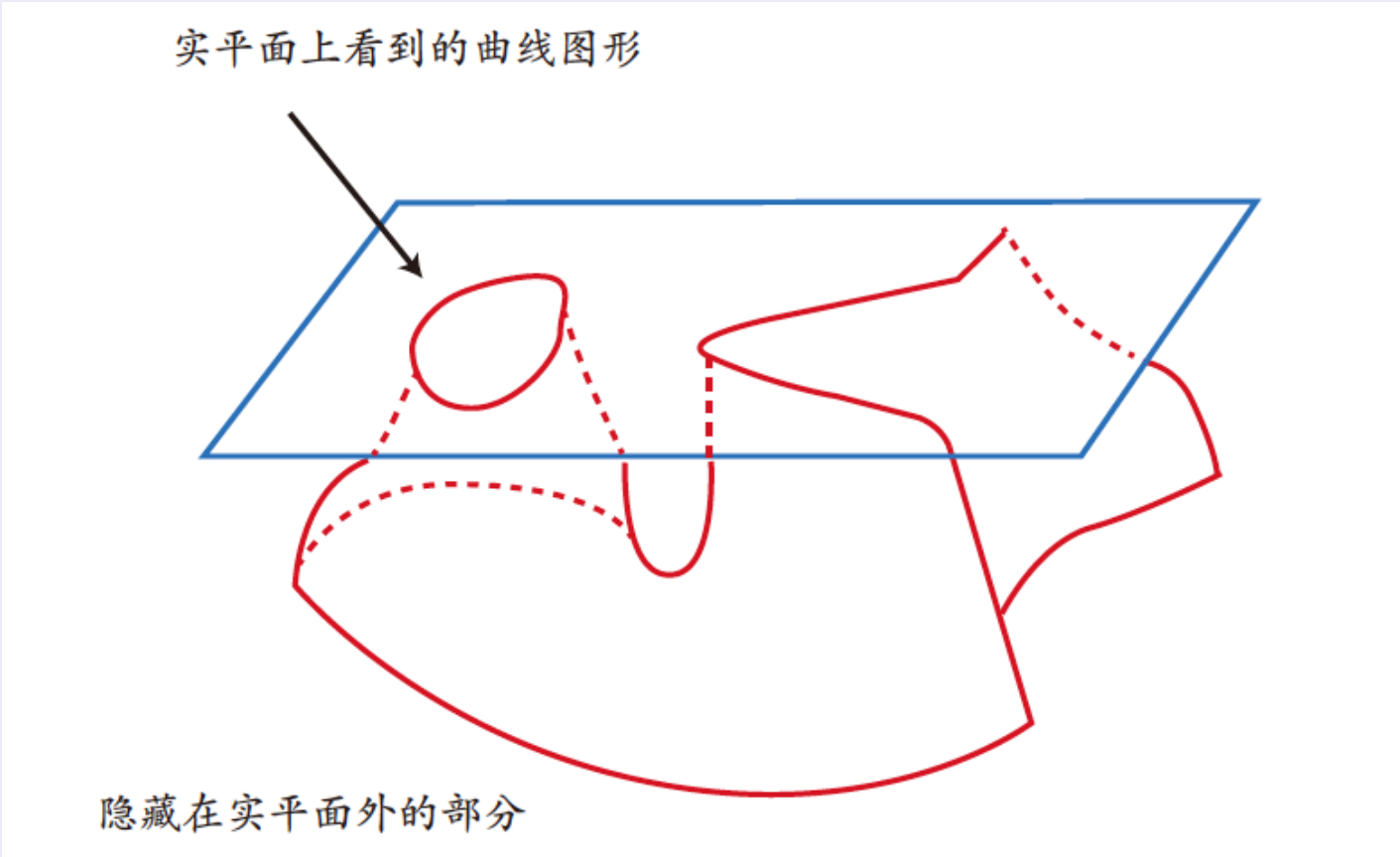
曲线形状



实验...

认识椭圆曲线

更深层次的认识



加法原理

首先定义$\oplus$运算：

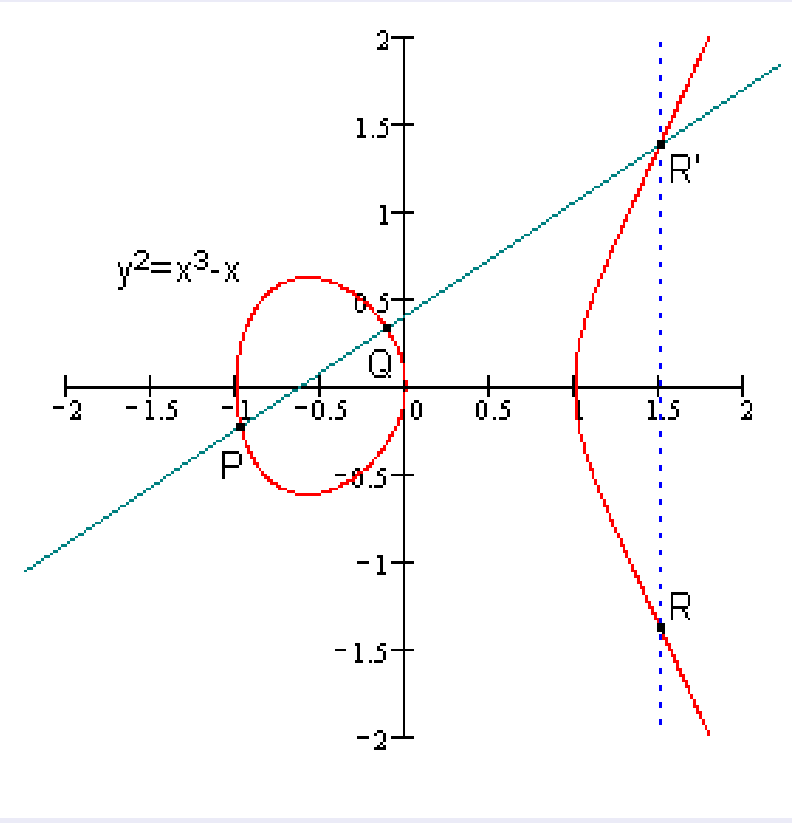
设E是由式3.4定义的域K上的椭圆曲线，定义E上的运算法则，记作$\oplus$。

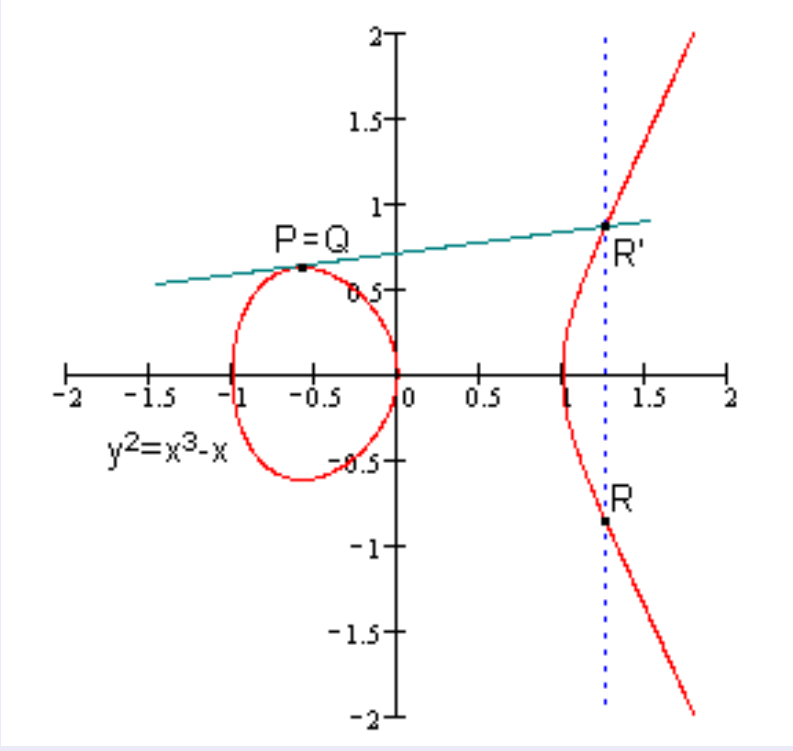
运算法则

设P, Q是E上的两个点，L是过P和Q的直线(过P点的切线，如果$P = Q$)，R'是L与曲线E相交的第三点。设L'是过R'和O的直线，则$P \oplus Q$就是L'与E相交的第三点R。

加法原理

运算法则





加法原理

定理

E上运算法则$\oplus$具有如下性质：

1. *如果直线L交E于点P, Q, R(不必是不同的)，则$(P \oplus Q) \oplus R = O$；*
2. *对任意$P \in E$，$P \oplus O = P$；*
3. *对任意$P, Q \in E$，$P \oplus Q = Q \oplus P$；*
4. *设$P \in E$，存在一个点，记作$-P$，使得$P \oplus (-P) = O$；*
5. *对任意$P, Q, R \in E$，有$(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$*

这就是说，E对于运算规则$\oplus$构成一个交换群。

下面给出定理中群运算的精确公式：

加法原理

定理

设椭圆曲线E的一般Weierstrass方程为

$$E:\{(x,y)|y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\}\cup\{O\}$$

设$P_1=(x_1,y_1),P_2=(x_2,y_2)$是曲线$E$上的两个点，则

$$-P_1=(x_1,-y_1-a_1x_1-a_3)$$

取

$$\lambda=\begin{cases}\frac{y_2-y_1}{x_2-x_1}, & x_1\neq x_2\\ \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, & x_1=x_2\end{cases}$$

加法原理

定理（续）

如果$P_3 = (x_3, y_3) = P_1 + P_2 \neq O$，则$x_3, y_3$可以由公式给出

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - a_1 x_3 - y_1 - a_3 \end{cases}$$

不同域上的椭圆曲线有不尽相同的运算法则：

- 实数域R上的椭圆曲线；
- 素域$F_p(p > 3)$上的椭圆曲线；

有限域上的椭圆曲线

密码学中椭圆曲线密码采用的是有限域上的椭圆曲线，有限域上的椭圆曲线是指曲线方程定义式3.3所有的系数都是某一有限域F_p中的元素(其中p为一大素数)。其中最为常见的是由方程

$$y^2 \equiv x^3 + ax + b (\mathrm{mod}\, p) \quad (a, b \in F_p,\ 4a^3 + 27b^2 (\mathrm{mod}\, p) \neq 0) \quad (3.5)$$

有限域上的椭圆曲线：举例

例

$p = 23,\ a = b = 1,\ 4a^3 + 27b^2 (\mathrm{mod} 23) \equiv 8 \neq 0$，*即椭圆曲线式3.5为*$y^2 \equiv x^3 + x + 1 (\mathrm{mod} 23)$，*其图形是连续曲线。我们感兴趣的是曲线在第一象限的整数点，设*$E_p(a, b)$*表示式3.5所定义的椭圆曲线上的点集*$\{(x, y) | 0 \leq x < p,\ 0 \leq y < p,$*且*$x, y$*均为整数*$\}$*。下表给出了*$E_{23}(1, 1)$*：*

$(0,1)$	$(0,22)$	$(1,7)$	$(1,16)$	$(3,10)$	$(3,13)$	$(4,0)$	$(5,4)$	$(5,19)$
$(6,4)$	$(6,19)$	$(7,11)$	$(7,12)$	$(9,7)$	$(9,16)$	$(11,3)$	$(11,20)$	$(12,4)$
$(12,19)$	$(13,7)$	$(13,16)$	$(17,3)$	$(17,20)$	$(18,3)$	$(18,20)$	$(19,5)$	$(19,18$

$E_p(a,b)$的产生

一般来说，$E_p(a,b)$由以下方式产生：

1. 对每一$x(0 \leq x < p$且x为整数)，计算$x^3 + ax + b (\mathrm{mod} p)$；
2. 决定步骤1中求得的值在模p下是否有平方根，如果没有，则曲线上没有与这一x相对应的点；如果有，则求出两个平方根($y = 0$时只有一个平方根)。

$E_p(a,b)$的产生–举例

例

求满足方程$E: y^2 \equiv x^3 + x + 1 (\mathrm{mod} 23)$的所有点。

解：对$x = 0, 1, \cdots, 22$分别求出y

- $x = 0, y^2 \equiv 1 (\mathrm{mod} 23), y \equiv 1, 22 (\mathrm{mod} 23)$
- $x = 1, y^2 \equiv 3 (\mathrm{mod} 23), y \equiv 7, 16 (\mathrm{mod} 23)$
- $x = 2, y^2 \equiv 11 (\mathrm{mod} 23)$，无
- $x = 3, y^2 \equiv 8 (\mathrm{mod} 23), y \equiv 10, 13 (\mathrm{mod} 23)$
- $x = 4, y^2 \equiv 0 (\mathrm{mod} 23)$，无
- $\ldots$

$E_p(a,b)$上的加法

设$P,Q \in E_p(a,b)$，则：

1. $P+O=P$；
2. 如果$P=(x,y)$，$-P=(x,-y)$是P的加法逆元；
3. 点P的倍数定义为：在P点做椭圆曲线的切线，设切线与曲线交于点S，定义$2P=P+P=-S$，类似的可定义$3P=P+P+P$。

$E_p(a,b)$上的加法(续)

4. 设$P=(x_1,y_1)$, $Q=(x_2,y_2)$, $P\neq Q$，则$P+Q=(x_3,y_3)$由以下规则确定：

$$x_3 \equiv \lambda^2 - x_1 - x_2 (\mathrm{mod} p)$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod} p)$$

其中，

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1}, & P \neq Q \\ \frac{3x_1^2+a}{2y_1}, & P = Q \end{cases} (\mathrm{mod} p)$$

椭圆曲线密码算法

椭圆曲线密码算法(ECC)的安全性依赖于有限域上点群元素求阶，同样也属于离散对数难题。令F_p为有限域，E为F_p上的椭圆曲线，P为E上的点，且阶为素数n，并记$D = \{1, 2, \cdots, n-1\}$。算法描述如下：

- 信息传递各方通过参数组(p, E, P, n)选取私钥$d \in D$，并计算公钥$Q = dP$。
- 信息发送方表示明文M为E上的点。
- 随机选择$k \in D$，并利用接收者的公钥Q计算和发送$C = (C_1, C_2) = (kP, M + kQ)$。
- 信息接收者用自己保存的私钥d进行解密：$M = C_2 - dC_1$

Overview

1. 课程介绍

2. 数论

3. 近世代数

4. 数理逻辑基础

概述

逻辑学(logic)是由古希腊学者亚里士多德创建的，是探索、阐述和确立有效推理原则的学科。传统的逻辑学用自然语言表示各种命题形式和推理形式，但是自然语言常常具有多义性，因此并不适合精确的表示命题和推理。而数理逻辑则是用数学的方法来研究关于推理、证明等问题的学科，以其特有的人工符号来书写逻辑法则，突出体现了方便、精确的优势。

经典命题逻辑和一阶谓词逻辑在计算机科学中应用最为广泛，也是数理逻辑中最成熟的部分，而命题逻辑是数理逻辑的最基础部分，谓词逻辑是在它的基础上发展起来的。而模态逻辑与以陈述句为基础的经典逻辑不同，允许出现虚拟语句（“可能”、“必然”），是关于必然性和可能性的逻辑，是程序的语义描述和知识的形式表示的有力工具。

Detailed overview

4. 数理逻辑基础

4.2 经典命题逻辑

4.3 经典一阶逻辑

4.4 非经典逻辑

命题逻辑

命题逻辑(propositional logic)是数理逻辑的基础，以命题为研究对象，研究基于命题的符号逻辑体系及推理规律。我们的课程主要介绍以下几个问题：

1. 简单命题与复合命题：什么是命题，命题联结词及其含义；
2. 命题公式与赋值：命题逻辑公式的归纳定义，命题公式的真值表；
3. 等值演算：命题公式的等值赋值，重要的等值式；
4. 命题公式的范式：析取范式与合取范式；
5. 命题演算系统：使用命题逻辑公式进行推理的形式系统。

简单命题与复合命题

在经典命题逻辑中，**命题**(proposition)是可以判断真假的陈述句。
命题必须为陈述句，不能为疑问句、祈使句、感叹句等，例如：

- 2大于1；
- $\sqrt{3}$是无理数；
- 有两条腿、直立行走的是人。

而下面的句子不是命题：

- 大海啊，全是水！
- 当时你的车速只有70公里/小时？
- 上天赐我们一支真正的国家队吧！

注意！不是所有的陈述句都是命题，无法判断其真假的陈述句也不是命题：

- 我正在说谎；
- $x + y > 10$。

那些我们现在无法判断其真假的陈述句，但是只要它具有唯一的真假值，就也是命题，比如：

- 2012年有大灾难；
- 我40岁的时候能买得起劳斯莱斯；
- 玛雅文明毁于殷商的远洋舰队。

如果命题的真值为真，则称为**真命题**，否则称为**假命题**。

命题变量、命题常量

命题常量：

命题符号p代表命题常量，则意味着它是某个具体命题的符号化；

命题变量：

命题符号p代表命题变量，则意味着它可指代任何具体命题。

一般地，如果没有特殊说明，命题符号p、q等是命题变量。

简单命题与复合命题：

不能分成更简单的陈述句的命题为**简单命题**(或叫**原子命题**)，否则称为**复合命题**。

命题联结词

复合命题使用命题联结词联结简单命题而来，命题联结词如表所示：

Table: 联结词

联结词	符　号	称　谓	读　法
非	$\neg$	否定	$\neg p$读作“非p”
与	$\wedge$	合取	$p \wedge q$读作“p且q”
或	$\vee$	析取	$p \vee q$读作“p或q”
如果$\cdots$，那么$\cdots$	$\rightarrow$	蕴含	$p \rightarrow q$读作“p蕴含q”或者“如果p则q”
当且仅当	$\leftrightarrow$	等价	$p \leftrightarrow q$读作“p与q等价”或者“p当且仅当q”

真值关系

复合命题与简单命题之间的真值关系可以用表2给出，其中0代表假，1 代表真。

Table: 复合命题真值表

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

联结词优先级

逻辑联结词（逻辑运算符）

优先级的顺序为：$\neg$、$\wedge$、$\vee$、$\rightarrow$、$\leftrightarrow$，若有括号时，先进行括号内运算。

例如：

$$p \rightarrow (q \vee \neg p) \wedge (q \vee r) \leftrightarrow \neg q$$

的运算顺序为：

1. $\neg p$和$\neg q$；
2. $q \vee \neg p$和$q \vee r$；
3. $(q \vee \neg p) \wedge (q \vee r)$；
4. $\rightarrow$；
5. $\leftrightarrow$。

举例

设p：小明聪明，q：小明用功。

1. 小明既聪明又用功；
2. 小明虽然聪明，但不用功；
3. 小明不但聪明，而且用功；
4. 小明不是不聪明，而是不用功。

若用p表示“小明聪明”，q表示“小明用功”，则上述命题表达式分别如下：

1. $p \wedge q$；
2. $p \wedge \neg q$；
3. $p \wedge q$；
4. $\neg(\neg p) \wedge \neg q$。

命题逻辑公式

定义

命题逻辑公式(propositional logic formula)由以下子句归纳定义：

1. *命题常量或命题变量是命题逻辑公式，称为命题逻辑公式的原子项；*
2. *如果A、B是命题逻辑公式，则$(\neg A)$、$(A \wedge B)$、$(A \vee B)$、$(A \to B)$和$A \leftrightarrow B$也是命题逻辑公式；*
3. *所有的命题逻辑公式都通过1.和2.得到。*

命题逻辑公式

定理（关于命题逻辑公式的性质）

设R是某个性质，如果有：

1. 对于所有的原子项p，都满足性质R；
2. 如果对任意的公式A和B都满足性质R，就有$(\neg A)$、$(A \wedge B)$、$(A \vee B)$、$(A \to B)$和$A \leftrightarrow B$也满足性质R。

那么，所有的公式A就都满足性质R。

命题逻辑公式

任意命题逻辑公式A具有下列6种形式之一，且只具有其中一种形式：

1. A为原子项
2. $(\neg A)$
3. $(A \wedge B)$
4. $(A \vee B)$
5. $(A \to B)$
6. $(A \leftrightarrow B)$

定义（真值赋值）

对命题公式的一次真值赋值t是从所有命题变量所组成的集合到集合$\{0,1\}$的函数。

命题逻辑公式

定义（真值赋值）

命题公式A在真值赋值$t : U \to \{0, 1\}$下的真值$t(A)$递归定义如下：

1. 如果命题公式A是命题常量p，则如果p为真，$t(A) = 1$，否则$t(A) = 0$；
2. 如果命题公式A是一个命题变量p，则$t(A) = t(p)$；
3. 若$t(A) = 0$则$t(\neg A) = 1$，否则$t(\neg A) = 0$；
4. 若$t(A) = t(B) = 1$，则$t(A \wedge B) = 1$，否则$t(A \wedge B) = 0$；
5. 若$t(A) = t(B) = 0$，则$t(A \vee B) = 0$，否则$t(A \vee B) = 1$；
6. 若$t(A) = 0$或者$t(B) = 1$，则$t(A \to B) = 1$，否则$t(A \to B) = 0$；
7. 若$t(A) = t(B)$，则$t(A \leftrightarrow B) = 1$，否则$t(A \leftrightarrow B) = 0$。

定义（永真式、矛盾式、可满足式）

*如果命题公式A在任意的真值赋值函数$t : U \to \{0,1\}$下的真值$t(A)$都为1，则称命题公式A为**永真式**(tautology)(或称重言式)；如果命题公式A在任意的真值赋值函数下的真值都为0，则称A为**矛盾式**(contradiction)；如果A不是矛盾式，则称为**可满足式**。*

定义（集合与永真式）

*使用符号Σ来表示一组命题公式所构成的集合，定义Σ在真值赋值函数$t : U \to \{0,1\}$下的真值$t(\Sigma)$为：$t(\Sigma) = 1$当且仅当Σ中任意公式A有$t(A) = 1$，否则定义$t(\Sigma) = 0$。说Σ是可满足的，如果存在某个真值赋值函数t使得$t(\Sigma) = 1$，这时称t满足Σ。设Σ是一组命题公式的集合，说命题公式A是以Σ**为前提的永真式**，如果满足对任意满足Σ的真值赋值函数t都有$t(A) = 1$，这时记为$\Sigma \models A$.*

如果Σ为空集，则$\Phi \models A$表示A为永真式。

命题公式的等值

定义（等值）

当$\Sigma = \{A_1, A_2, \cdots, A_n\}$时，也记$\Sigma \models A$为$A_1, A_2, \cdots, A_n \models A$。如果有$A \models B$且$B \models A$，则称命题公式$A$ 与B等值，记为$A \Leftrightarrow B$。

于是，显然有下面的定理：

定理

$A \Leftrightarrow B$当且仅当$A \leftrightarrow B$是永真的。

逻辑等价式

设A、B、C是任意的命题公式，易证明下面逻辑等价式：

- **双重否定律：** $A \Leftrightarrow (\neg(\neg A))$
- **等幂律：** $A \Leftrightarrow (A \wedge A)$，$A \Leftrightarrow (A \vee A)$
- **交换律：** $(A \vee B) \Leftrightarrow (B \vee A)$，$(A \wedge B) \Leftrightarrow (B \wedge A)$
- **结合律：**
  $((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C))$，$((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C))$
- **分配律：** $(A \vee (B \wedge C)) \Leftrightarrow$
  $(A \vee B) \wedge (A \vee C))$，$(A \wedge (B \vee C)) \Leftrightarrow (A \wedge B) \vee (A \wedge C))$
- **德摩根律：**
  $(\neg(A \vee B)) \Leftrightarrow ((\neg A) \wedge (\neg B))$，$(\neg(A \wedge B)) \Leftrightarrow ((\neg A) \vee (\neg B))$
- **吸收律：** $(A \vee (A \wedge B)) \Leftrightarrow A$，$(A \wedge (A \vee B)) \Leftrightarrow A$

逻辑等价式(续)

- 零律：$(A \vee 1) \Leftrightarrow 1$，$(A \wedge 0) \Leftrightarrow 0$
- 同一律：$(A \vee 0) \Leftrightarrow A$，$(A \wedge 1) \Leftrightarrow A$
- 排中律：$(A \vee (\neg A)) \Leftrightarrow 1$
- 矛盾律：$(A \wedge (\neg A)) \Leftrightarrow 0$
- 蕴涵等值律：$(A \to B) \Leftrightarrow ((\neg A) \vee B)$
- 等价等值律：$(A \leftrightarrow B) \Leftrightarrow ((A \to B) \wedge (B \to A))$
- 假言易位律：$(A \to B) \Leftrightarrow ((\neg B) \to (\neg A))$
- 等价否定等值律：$(A \leftrightarrow B) \Leftrightarrow ((\neg A) \leftrightarrow (\neg B))$
- 归谬论：$((A \to B) \wedge (A \to (\neg B))) \Leftrightarrow (\neg A)$

等值演算

定理

设有$A \Leftrightarrow A'$和$B \Leftrightarrow B'$，则有：

1. $(\neg A) \Leftrightarrow (\neg A')$
2. $(A \wedge B) \Leftrightarrow (A' \wedge B')$
3. $(A \vee B) \Leftrightarrow (A' \vee B')$
4. $(A \to B) \Leftrightarrow (A' \to B')$
5. $(A \leftrightarrow B) \Leftrightarrow (A' \leftrightarrow B')$

等值演算

定义

如果命题公式A中只出现命题变量、命题常量、命题联接符号$\neg$、$\wedge$和$\vee$ 则称为限制性(命题)公式。定义：

1. 对于限制性公式A，将其中的命题联接符号$\wedge$换成$\vee$，命题联接符号$\vee$换成$\wedge$得到的公式称为A的对偶公式(dual formula)，记为A^{op}；
2. 对于限制性公式A，将其中出现的所有原子项(命题变量或命题常量)p换成$\neg p$得到的公式称为A的内否式，记为$A^{\neg}$。

等值演算

定理

设公式A、B都是限制性公式，有：

1. $(A^{op})^{op} \equiv A$，$(A^{\neg})^{\neg} \equiv A$
2. $(A \vee B)^{op} \equiv A^{op} \wedge B^{op}$，$(A \vee B)^{\neg} \equiv A^{\neg} \vee B^{\neg}$
3. $(A \wedge B)^{op} \equiv A^{op} \vee B^{op}$，$(A \wedge B)^{\neg} \equiv A^{\neg} \wedge B^{\neg}$
4. $(A^{op})^{\neg} \equiv (A^{\neg})^{op}$

等值演算

定理

设公式A是任意的限制性公式，有

1. $(\neg A)^{op} \Leftrightarrow \neg(A^{op})$，$(\neg A)^{\neg} \Leftrightarrow \neg(A^{\neg})$
2. $(A^{op})^{\neg} \Leftrightarrow \neg A$

推论

设公式A和B都是限制性公式，有$A \Leftrightarrow B$则$(A^{op})^{\neg} \Leftrightarrow (B^{op})^{\neg}$。

范式

定义

由有限个简单合取式构成的析取式称为析取范式(disjunctive normal form)，由有限个简单析取式构成的合取式称为合取范式(conjunctive normal form)。析取范式和合取范式统称为范式(normal form)。一个析取范式是矛盾式当且仅当它的每个简单合取式都是矛盾式。一个合取范式是永真式当且仅当它的每个简单析取式都是永真式。

定理

任意命题公式都存在与之等值的析取范式与合取范式。

命题演算系统定义

定义（命题演算系统）

命题演算系统(system of propositional calculus)P定义如下：

- *P的符号表包括：*
  1. *命题变元：小写英文字母并可加下标。*
  2. *联结词：$\neg$、$\rightarrow$。*
  3. *辅助符号：(,)(圆括号)。*
- *P的公式归纳定义如下：*
  1. *命题变元是公式。*
  2. *若A是公式，则$(\neg A)$也是公式。*
  3. *若A和B是公式，则$(A \rightarrow B)$也是公式。*
  4. *所有公式都是通过有限次使用1、2和3得到。*

命题演算系统定义(续)

定义 (命题演算系统(续))

- P的公理模式有如下3个：
  1. **肯定前件律：** $(A \to (B \to A))$
  2. **分配律：** $((A \to (B \to C))) \to ((A \to B) \to (A \to C))$
  3. **逆否定律：** $(((\neg A) \to (\neg B)) \to (B \to A))$
- P的规律只有一条：
  1. **分离规则：** 由A和$(A \to B)$可得到B

命题演算系统

定义

命题演算系统P中的证明是由P中公式组成的一个序列：$A_1, A_2, \cdots, A_n$使得对每个$i(1 \leq i \leq n)$，下列两个条件之一成立：

1. A_i是公理，或者
2. A_i是由上述序列中A_i之前的某两个公式$A_j, A_k(1 \leq j, k \leq i)$应用分离规则得到。

此时$A_1, A_2, \cdots, A_n$称为A_n的一个证明，而A_n称为P的一个内定理，记为$\vdash A_n$。

定理（传递规则T_r）

设A、B、C是P中的3个公式，若$\vdash A \to B$，且$\vdash B \to C$，则$\vdash A \to C$。

命题演算系统

定义

设Σ是P中的一个公式集，称P中的公式序列：$A_1, A_2, \cdots, A_n$为前提Σ下推出A_n的一个证明，如果对每个$i(1 \leq i \leq n)$，下列3个条件之一成立：

1. A_i是公理，或者
2. $A_i \in \Sigma$，或者
3. A_i是由上述序列中A_i之前的某两个公式$A_j, A_k(1 \leq j, k \leq i$应用分离规则得到。

此时记为$\Sigma \vdash A_n$。

演绎定理

定理（演绎定理）

设Σ是P中的公式集，A和B是P中的两个公式，若$\Sigma \cup \{A\} \vdash B$，则$\Sigma \vdash A \to B$。

定理（演绎定理的逆定理）

设Σ是P中的公式集，A和B是P中的两个公式，若$\Sigma \vdash A \to B$，则$\Sigma \cup \{A\} \vdash B$。

由以上两个定理得到：

推论

$\{A_1, A_2, \cdots, A_n\} \vdash A$当且仅当$\vdash (A_1 \to (A_2 \to \cdots \to (A_n \to A) \cdots))$。

命题演算系统

定理

设Σ是P中的公式集，$A_1, A_2, \cdots, A_n$为P中的公式，若有$\Sigma \vdash A_1, \Sigma \vdash A_2, \cdots, \Sigma \vdash A_n$，且$A_1, A_2, \cdots, A_n \vdash A$，则$\Sigma \vdash A$。

定理

合取的引入和消除规则：

1. **合取的引入：** $A, B \vdash A \wedge B$
2. **合取的消除：** $A \wedge B \vdash A, B$(这代表$A \wedge B \vdash A$及$A \wedge B \vdash B$)

命题演算系统

定理

析取的引入和消除规则：

1. **析取的引入：** $A \vdash A \vee B, A \vdash B \vee A$
2. **析取的消除：** $A \to B, C \to B, A \vee C \vdash B$

定理

对于P的任意一个公式A，若有$\vdash A$，则A是一个永真式。

定理

不存在P的一个公式A，使得$\vdash A$和$\vdash (\neg A)$都成立。

定理

若A是P的永真式，则有$\vdash A$。

作业

作业1：将下列命题符号化：

- 选小王或小李中的一人当连长
- 小王是计算机系的学生，她生于1992年或者1993年，她是三好学生

作业2：判断下面A、B两个公式是否等值

- $A = \neg(p \vee q)$，$B = \neg p \vee \neg q$
- $A = p \to (q \to r)$，$B = (p \wedge q) \to r$
- $A = p \leftrightarrow q$，$B = (p \to q) \vee (q \to p)$

Detailed overview

4. 数理逻辑基础

4.2 经典命题逻辑

4.3 经典一阶逻辑

4.4 非经典逻辑

概述及基本概念

命题逻辑中，原子命题是不能再分割的。

一阶逻辑(first-order logic)对原子命题进行进一步分解，并在此基础上建立起了一个完整体系。

一阶逻辑又称为谓词逻辑(predicate logic)。一阶逻辑中，命题被分解为个体和谓词两部分。

- **个体**：是指可独立存在的客体，可以是一个具体的事物，也可以是一个抽象的概念。
- **谓词**：是用来刻画个体的性质及事物关系的词。
- **函词**：是对个体所进行的某种变换。

  （函词与谓词的区别在于，函词作用在个体上，而产生另一个个体，而谓词作用在个体上产生的是一个命题。）
- **个体常项**：是表示具体或特定的个体的个体词。
- **个体变项**：是表示抽象或泛指的个体词。

基本概念

- **函数**：在个体域上可以定义函数，函数只能作用在个体上，而不允许作用在谓词上。
- **“一阶”的含义**：个体处于0阶，对个体的判断处于一阶。函数作用于0阶的个体得到个体，而谓词作用于个体得到处于一阶的命题。
- **谓词的元数**：谓词可包含个体变项的数量。
- **量词**：参与判断个体的数量。
  - 全称量词($\forall$)：作用个体域中所有的个体
  - 存在量词($\exists$)：作用个体域中某些个体

一阶逻辑语言的符号

一阶逻辑语言的符号包括：

1. **个体常项**：通常用排在前面的小写字母表示，$a, b, c, \cdots, a_i, b_i, c_i, \cdots$
2. **个体变项**：通常用排在后面的小写字母表示，$x, y, z, \cdots, x_i, y_i, z_i, \cdots$
3. **函数符号**：通常用排在中间的小写字母表示，$f, g, h, \cdots, f_i, g_i, h_i, \cdots$
4. **谓词符号**：通常用排在中间的大写字母表示，$F, G, H, \cdots, F_i, G_i, H_i, \cdots$
5. **量词符号**：全称量词$\forall$、存在量词$\exists$
6. **联接符号**：$\neg$、$\wedge$、$\vee$、$\leftrightarrow$、$\rightarrow$
7. **辅助符号**：(、)、,(逗号)

举例

例

将下列命题符号化：

- *凡是有理数都可以写成分数*
- *教室里有同学没吃早饭*
- *在我们班中，不是所有同学都近视*
- *任给*$\varepsilon > 0$，*存在*$\delta > 0$，*如果*$|x - a| < \delta$，*则*$|f(x) - b| < \varepsilon$

举例

例

$P(x)$表示“x是素数”，$E(x)$表示“x是偶数”，$Q(x)$表示“x是奇数”，$N(x,y)$表示“x可以整除y”：

- $P(5)$
- $(\exists x)(E(x) \vee N(x,6))$
- $(\forall x)(E(x) \to (\forall y)(N(x,y) \to E(y)))$

一阶逻辑语言的项

定义

一阶逻辑语言的项(term)递归定义如下：

1. 个体常项和个体变项是项。
2. 若$f(x_1, x_2, \cdots, x_n)$是n元函数，$t_1, t_2, \cdots, t_n$是n个项，则$f(t_1, t_2, \cdots, t_n)$是项。
3. 一阶逻辑语言的所有项都通过有限次使用上述步骤生成。

合式公式

定义

一阶逻辑语言的合式公式(well-formed formula)递归定义如下：

1. *若*$F(x_1, x_2, \cdots, x_n)$*是*n*元谓词，*$t_1, t_2, \cdots, t_n$*是*n*个项，*
   则$F(t_1, t_2, \cdots, t_n)$*是合式公式，此类合式公式称为原子公式。*
2. *若*A*、*B*是合式公式，*
   则$(\neg A), (A \wedge B), (A \vee B), (A \to B), (A \leftrightarrow B)$*也是合式公式。*
3. *若*A*是合式公式，则*$(\forall x)A, (\exists x)A$*也是合式公式。*
4. *一阶逻辑语言的所有公式都通过有限次使用上述步骤生成。*

一些说明

- 称公式$(\forall x)A$中的A为量词$(\forall x)$的**辖域**(scope)
- 称公式$(\exists x)A$中A为量词$(\exists x)$的**辖域**
- 称变元x在公式A中的某处出现是**约束出现**，如果该出现处于量词$(\forall x)$或$(\exists x)$的辖域内，或者就是量词中x
- 若x在公式A中的某处出现不是约束出现，则此出现称为**自由出现**。
- 设变元x在公式A中出现，如果x在A中的所有出现都是约束出现，则称x为A的**约束变元**(bounded variable)，否则称x为A的**自由变元**(free variable)。

换名规则、替换原则

换名规则

R-FL1(换名规则)：对于公式$(\forall x)A$或$(\exists x)A$，设变元y不在A中出现，则将其中$(\forall x)$或$(\exists x)$改为$(\forall y)$或$(\exists y)$，且将A中出现的所有x都改成y，得到公式$(\forall y)A$或$(\exists y)A$与原公式等价。

替换原则

R-FL2(替换原则)对于公式$A(x)$，设y不在A中出现，将其中所有自由出现的x改为y，得到公式$A(y)$与原公式等价。

等值式

设A和B是一阶逻辑中任意的两个公式，若$A \leftrightarrow B$是永真式，则称A 与B等值，记为$A \Leftrightarrow B$，称$A \Leftrightarrow B$为**等值式**。
下面定理给出与量词无关、一阶逻辑特有的一些等值式：

E-FL1(消除量词)在有限个体域$D = \{a_1, z_2, \cdots, a_n\}$中：

1. $(\forall x)A(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \cdots \wedge A(a_n)$
2. $(\exists x)A(x) \Leftrightarrow A(a_1) \vee A(a_2) \vee \cdots \vee A(a_n)$

E-FL2(量词否定等值式)

1. $\neg(\forall x A(x)) \Leftrightarrow \exists x(\neg A(x))$
2. $\neg(\exists x A(x)) \Leftrightarrow \forall x(\neg A(x))$

等值式(续)

E-FL3(收缩与扩张等值式)下述等值式中，变元x不在B中出现：

1. $\forall x(A(x) \vee B) \Leftrightarrow (\forall x A(x)) \vee B$
2. $\forall x(A(x) \wedge B) \Leftrightarrow (\forall x A(x)) \wedge B$
3. $\forall x(A(x) \to B) \Leftrightarrow (\exists x A(x)) \to B$
4. $\forall x(B \to A(x)) \Leftrightarrow B \to (\forall x A(x))$
5. $\exists x(A(x) \vee B) \Leftrightarrow (\exists x A(x)) \vee B$
6. $\exists x(A(x) \wedge B) \Leftrightarrow (\exists x A(x)) \wedge B$
7. $\exists x(A(x) \to B) \Leftrightarrow (\forall x A(x)) \to B$
8. $\exists x(B \to A(x)) \Leftrightarrow B \to (\exists x A(x))$

等值式(续)

E-FL4(量词分配等值式)

1. $(\forall x(A(x) \wedge B(x)) \Leftrightarrow (\forall x A(x)) \wedge (\forall x B(x))$
2. $(\exists x(A(x) \vee B(x)) \Leftrightarrow (\exists x A(x)) \vee (\exists x B(x))$

E-FL5(量词顺序变换等值式)

1. $\forall x \forall y(A(x,y)) \Leftrightarrow \forall y \forall x(A(x,y))$
2. $\exists x \exists y(A(x,y)) \Leftrightarrow \exists y \exists x(A(x,y))$

前束范式

设A为一阶逻辑公式，若A具有如下形式：$Q_1x_1Q_2x_2\cdots Q_nx_nB$，则称$A$为前束范式(prenex normal form)。其中$Q_i(1\leq i\leq n)$是$\forall$或$\exists$，B为不含量词的公式。

定理

对于任意的一阶逻辑公式A，都存在与之等值的前束范式。

一阶逻辑的推理

一阶逻辑的推理形式与命题逻辑类同：

定义

*称蕴涵式$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \to B$为推理的**形式结构**，*
*$A_1, A_2, \cdots, A_k$为推理的**前提**，B为推理的**结论**。*
若$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \to B$为永真式，则称从前提$A_1, A_2, \cdots, A_k$推出结论$B$的推理正确(或说有效)，$B$是$A_1, A_2, \cdots, A_k$的逻辑结论或称有效结论，否则称推理不正确。
若从前提$A_1, A_2, \cdots, A_k$推出结论B的推理正确，则记为$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow B$。

一阶逻辑推理及规则

定义

一个描述推理过程的一阶公式序列$A_1, A_2, \cdots, A_n$，其中的每个一阶公式或者是已知的前提，或者是由某些前提应用推理规则得到的结论，满足这样条件的公式序列$A_1, A_2, \cdots, A_n$称为结论A_n的证明。

一阶逻辑的推理可使用命题逻辑的推理规则有3条：

- R-FL3(前提引入规则) 在证明的任何步骤都可以引入已知的前提
- R-FL4(结论引入规则)在证明的任何步骤都可以引入这次已经得到的结论作为后续证明的前提
- R-FL5(置换规则)在证明的任何步骤上，一阶公式中的任何子公式都可用与之等值的公式置换，得到证明的公式序列的另一公式

推理定律

一些重要的推理定律如下：

- T-FL1(附加律)：$A \Rightarrow (A \vee B)$
- T-FL2(化简律)：$(A \wedge B) \Rightarrow A, (A \wedge B) \Rightarrow B$
- T-FL3(假言推理)：$A \rightarrow B \wedge A \Rightarrow B$
- T-FL4(拒取式)：$(A \rightarrow B) \wedge \neg B \Rightarrow \neg A$
- T-FL5(析取三段论)：$(A \vee B) \wedge \neg B \Rightarrow A$
- T-FL6(假言三段论)：$(A \rightarrow B) \wedge (B \rightarrow C) \Rightarrow (A \rightarrow C)$
- T-FL7(等价三段论)：$(A \leftrightarrow B) \wedge (B \leftrightarrow C) \Rightarrow (A \leftrightarrow C)$
- T-FL8(构造性二难)：$(A \rightarrow B) \wedge (C \rightarrow D) \wedge (A \vee C) \Rightarrow (B \vee D)$

推理定律

定理

$(A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge A) \Rightarrow B$当且仅

当$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow A \to B$

定理

$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow B$当且仅当$\neg(A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge \neg B)$是永真式。

或者说$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow B$当且仅

当$(A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge \neg B)$是矛盾式。

推理定律

一阶逻辑中还有如下特有的推理定律：

- T-FL9：$(\forall x A(x)) \vee (\forall x B(x)) \Rightarrow \forall x(A(x) \vee B(x))$
- T-FL10：$\exists x(A(x) \vee B(x)) \Rightarrow (\exists x A(x)) \vee (\exists x B(x))$
- T-FL11：$(\forall x(A(x) \to B(x)) \Rightarrow (\forall x A(x)) \to (\forall x B(x))$
- T-FL12：$\forall x(A(x) \to B(x)) \Rightarrow (\exists x A(x)) \to (\exists x B(x))$

全称量词消除规则

R-UI(全称量词消除规则)：

- (i) $\forall x A(x) \Rightarrow A(y)$
- (ii) $\forall x A(x) \Rightarrow A(c)$
  成立的条件如下：
- (1) x是$A(x)$的自由变元；
- (2) 在(i)中，y为不在$A(x)$中约束出现的变元，y可以在$A(x)$中自由出现，也可在证明序列中前面的公式中出现；
- (3)在(ii)中，c为任意的个体常项，可以是证明序列中前面公式所指定的个体常项。

全称量词引入规则

R-UG(全称量词引入规则)：

$$A(y) \Rightarrow \forall x A(x)$$

成立的条件如下：

- (1) y是$A(y)$中自由出现；
- (2) 替换y的x要选择在$A(y)$中不出现的变元符号。

存在量词引入规则

R-EG(存在量词引入规则)：

$$A(c) \Rightarrow \exists x A(x)$$

成立的条件如下：

- (1) c是$A(c)$中是特定的个体常项；
- (2) 替换c的x要选择在$A(c)$中不出现的变元符号。

存在量词消除规则

R-EI(存在量词消除规则)：

$$\exists x A(x) \Rightarrow A(c)$$

成立的条件如下：

- (1) c是特定的个体常项，c不能在前面的公式序列中出现
- (2) c不在$A(x)$中出现
- (3) $A(x)$中自由出现的个体变元只有x

举例

例

将命题“没有不守信用的人是可以信赖的；有些可以信赖的人是受过教育的。因此，有些受过教育的人是守信用的”符号化，并研究其推理是否正确。

解：要引入的谓词包括：
$P(x)$表示“x是守信用的人”；
$Q(x)$表示“x是可信赖的人”；
$S(x)$表示“x是受过教育的人”。
前提可符号化为：$\neg(\exists x(\neg P(x) \wedge Q(x))), \exists x(Q(x) \wedge S(x))$。
结论可符号化为：$\exists x(S(x) \wedge P(x))$。

Detailed overview

4. 数理逻辑基础

4.2 经典命题逻辑

4.3 经典一阶逻辑

4.4 非经典逻辑

从经典逻辑到非经典逻辑

经典数理逻辑（Classically mathematical logic）

- **命题逻辑**：命题、连接词、命题逻辑公式、命题逻辑演算系统；
- **谓词逻辑**：个体、谓词、量词、一阶逻辑公式、等值演算、推理。

自然地，人们会考虑扩充经典数理逻辑系统的概念，以建立更加广义的逻辑系统。

- “必然”vs.“可能”
- 时间语义
- “知道”vs.“认可”、“永远”vs.“将会”……

模态逻辑

“所有”vs.“存在”

“车上的所有人都是大学生”的否定：

“并非车上的所有人都是大学生”$\rightarrow$“存在车上的人不是大学生”

“必然”vs.“可能”

“小明必然能拿到博士学位”的否定：

“不是小明必然能拿到博士学位”$\rightarrow$“小明可能拿不到博士学位”

模态逻辑是在经典逻辑的基础上引入描述自然语言中“必然”和“可能”的逻辑符号而得到的逻辑系统。

针对经典命题逻辑的扩充称为**模态命题逻辑**；

针对经典谓词逻辑的扩充称为**模态谓词逻辑**。

模态命题逻辑

模态词

- 必然操作：$\Box$，$\Box A$表示无论什么场合均有事实A；
- 可能操作：$\Diamond$，$\Diamond A$表示对某些场合有事实A。

定义（基本符号）

1. *变量*：x，y，p，q
2. *连接词*：$\neg$，$\wedge$，$\vee$，$\rightarrow$，$\leftrightarrow$
3. *模态词*：$\Box$，$\Diamond$
4. *括号*：(，)

模态命题逻辑

定义（公式）

- 原子公式：变量是原子公式
- 合式公式（简称公式）：
  - 原子公式是公式；
  - 如P、Q是公式，则$\neg P$、$P \wedge Q$、$\Box P$是公式；
  - 公式由且仅由上述两式经有限步而成。

注：还有另外一种考虑5种连接词的定义方法。

模态命题逻辑

转化为合式公式的一些规则

- $P \vee Q$相当于$\neg(\neg P \wedge \neg Q)$
- $P \to Q$相当于$\neg P \vee Q$
- $P \leftrightarrow Q$相当于$(P \to Q) \vee (Q \to P)$
- $\Diamond P$相当于$\neg\Box\neg P$

另外，

- $P \Rightarrow Q$相当于$\Box(P \to Q)$
- $P \Leftrightarrow Q$相当于$\Box(P \leftrightarrow Q)$

然后，公理系统、规则、逻辑运算...

模态谓词逻辑

模态谓词逻辑的语言只是由模态算子加上低阶谓词演算的语言就可得到，其系统可称为一阶模态谓词演算系统。

定义（公理体系）

一阶模态谓词演算系统的公理体系由如下组成：

1. *一阶谓词演算系统的公理及推理规则；*
2. *模态逻辑正规系统的公理及推理规则；*
3. *关于模态词与不同量词关系的公理及推理规则。*

作业

1. 将下列命题符号化：
   - 1.1 小王是游泳冠军或百米赛跑冠军。
   - 1.2 如果我上街，我就去花店看看，除非我很累。
2. 验证下列等值式：
   - 2.1 $((p \to q) \to r) \Leftrightarrow ((\neg q \wedge p) \vee r)$
   - 2.2 $((p \vee q) \to r) \Leftrightarrow ((p \to r) \wedge (q \to r))$
   - 2.3 $(p \to (q \wedge r)) \Leftrightarrow ((p \to q) \wedge (p \to r))$
3. 将下列命题符号化：
   - 3.1 会叫的狗未必会咬人。
   - 3.2 每个人的外祖母都是他母亲的母亲。
   - 3.3 小莉是非常聪明和美丽的。

作业

4. 将下列公式翻译成自然语言，并确定其真值，这里假定个体域是正整数：

   4.1 $(\exists x)(\forall y)F(x,y)$，其中$F(x,y)$表示$x+y=y$。

   4.2 $(\forall x)(\exists y)N(x,y)$，其中$N(x,y)$表示$y=2\times x$。

5. 将下述命题符号化，并研究其推理是否正确：

   所有的有理数都是实数；所有的无理数也是实数；虚数不是实数。因此，虚数既不是有理数，也不是无理数。

谢谢！

hanqi_xf@hit.edu.cn