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. 近世代数

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

1. 近世代数

1.2 群

1.3 环

1.4 域

1.5 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

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

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

$$(y_1y_2\cdots y_m)=(x_1x_2\cdots x_m)M mod\, 26$$

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$\mathsf{mod}\,26$上可逆，则有：

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

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$A\le G$。

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

1. 近世代数

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$nZ = (n)$。

大作业（小论文）

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$f(x)=\sum_{i=0}^{n} a_i x^i$，$g(x)=\sum_{j=0}^{m} b_j x^j$，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$f(x)=\sum_{i=0}^{n} a_i x^i \in Z[x]$，

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

1. 近世代数

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

$$f(x) = q(x)g(x) + r(x), \quad \partial r(x) < \partial g(x) \tag{1.1}$$

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

$$(f(x),g(x))=a(x)f(x)+b(x)g(x) \tag{1.2}$$

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

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

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，

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

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：

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$i\cdot 1 = j\cdot 1, 1 \leq i < j$，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$1 \leq k \leq p-1, C_p^k = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k}$。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$C_p^k = 0 \bmod p$。

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-回顾循环群

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。

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$(n,k)=1$。

引理

设G是一个有限交换群，a是G的一个m阶元素，b是G的一个n阶元素，并假设$(n,m)=1$，则ab是一个mn阶元素。

引理

设G是一个有限交换群。假定G中元素的阶最大为n，则G中任何元素的阶都是n的因子。

有限域的乘法特性

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：*

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

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

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：

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.3}$$

其中$a_1, a_2, a_3, a_4, a_6 \in K$。
式1.3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

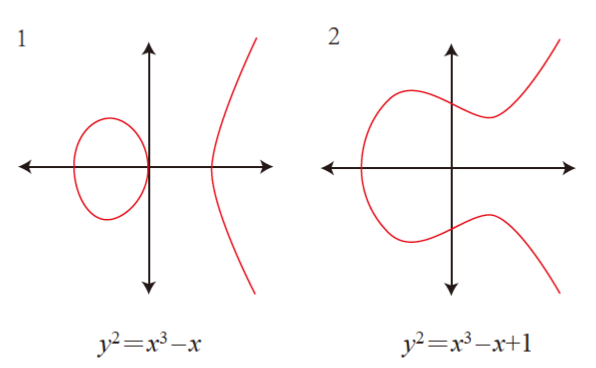
当$\Delta \neq 0$，域K上的点集

$$E : \{(x,y) | y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\} \quad (1.4)$$

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

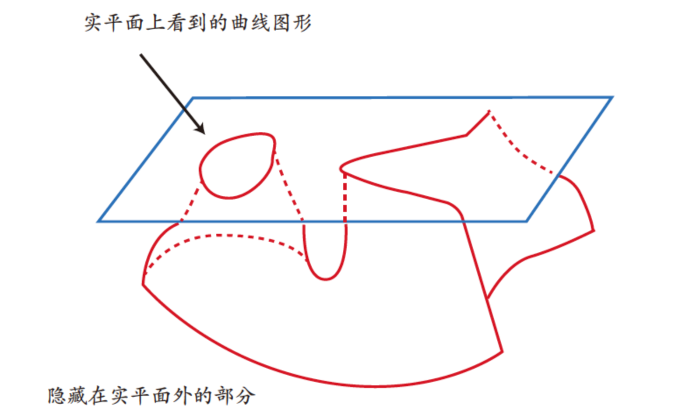
曲线形状



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：

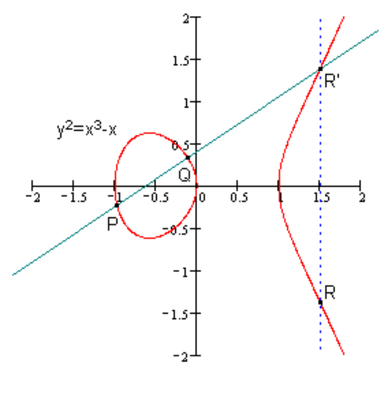
设E是由式1.4定义的域K上的椭圆曲线，定义E上的运算法则，记作$\oplus$。

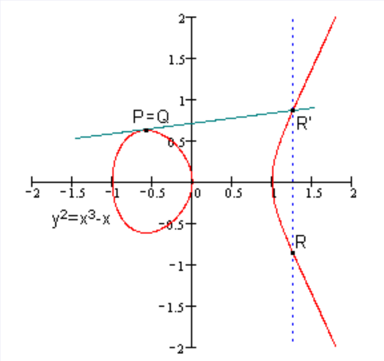
运算法则

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

$$\begin{cases} x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2 \\ y_3=\lambda(x_1-x_3)-a_1x_3-y_1-a_3 \end{cases}$$

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1.3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

$$y^2 \equiv x^3 + ax + b \pmod p \quad (a, b \in F_p,\ 4a^3 + 27b^2 \pmod p \neq 0) \tag{1.5}$$

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1.5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1.5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：$M = C_2 - dC_1$

谢谢！

hanqi_xf@hit.edu.cn