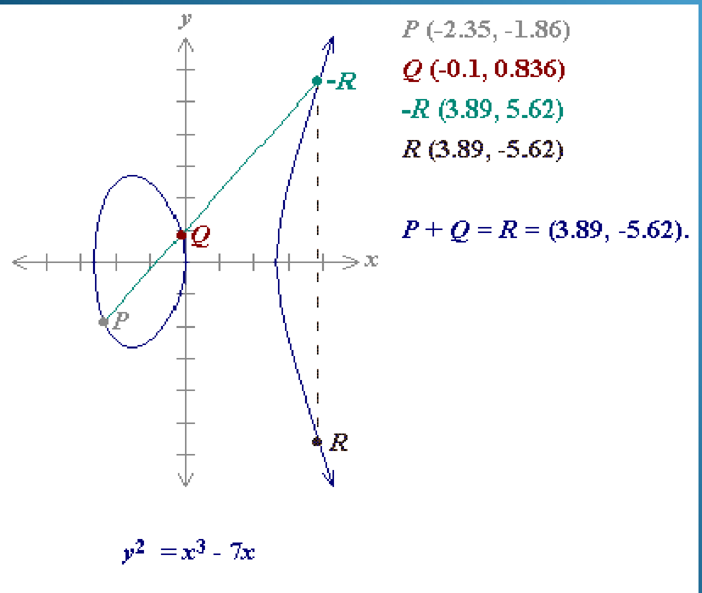

# 密码理论与技术

# –计算机密码学理论与应用

第一部分：数学基础（3）




$$ed = 1 \bmod \varphi(N)$$

$$Y = M^e \bmod N$$

$$M = Y^d \bmod N$$

# Fermat公式、Euler公式及Lagrange公式

- 上节课主题的回顾：
- (1) 特例：Fermat公式，p素且$a^{p-1}$=1 mod $p$
- (2) Euler函数$\phi$(N)及其重要的性质
- (3) Euler公式 $a^{\phi(N)}$ =1 mod $N$

- 本节课的主题：有限群、交换群、子群、Lagrange定理。
- （参阅Stallings教程4.4节）

# Euler公式的推广(1)

- (1) 群(Group)
- 
- (i) 回顾在离散数学课程中学习过的群的概念，这是一个抽象的数学对象，它统一刻画了许多数学对象的代数性质。
- (ii) 正是在这一抽象、统一的基础上，我们才能最清晰地理解前面的Euler定理和Fermat定理这类看似非常意外的结论为什么确实是普遍正确的。
- (iii) 群对构造先进安全方案有着实质性的应用。

# Euler公式的推广(2)

- (2) 群的定义
- 群是具有二元算术运算的一个集合G，将该运算记为*，x,y,z表示G的任意元素，运算*须具有以下性质：
- (i) 任何两个元素*运算的结果仍然是G的一个元素：封闭性
- (ii) x*y=y*x: 交换性
- (iii) (x*y)*z=x*(y*z)：结合性
- (iv) 存在一个元素*e*, 使x**e*=*e**x=x对任何x都成立，元素*e*称单位元；
- (v) 对任何x都存在一个元素，记做$x^{-1}$，满足$x*x^{-1}=x^{-1}*x=e$: 可逆性。

- 计算机领域所涉及的群均为有限群；
- G的元素个数称做群的阶，用记号|G|表示。

# Euler公式的推广(3)

- (3) 群的实例
-
- 例(i) N是正整数，$Z^*_N$≡{$1 \le a \le N-1$：$a$与N互素}，+和×分别表示$Z^*_N$上的模N加法和模N乘法，于是：
- $(Z^*_N, \times)$是群(习题：逐一验证群的性质、其单位元素是1、该群的阶是$\varphi(N)$)。
- 特别地，若$p$是素数则$(Z^*_p, \times)$是$p-1$阶群。
-
- 注意：$(Z^*_N, +)$并不是群(提示：+运算在该集合上封闭吗？)。
-
- 例(ii) N是正整数，$QR_N$≡{$1 \le a \le N-1$：存在整数$x$满足$x^2 = a \bmod N$有解}，*表示$QR_N$上模N乘法，$(QR_N, *)$是群，群的单位元素是1。

# Euler公式的推广(4)

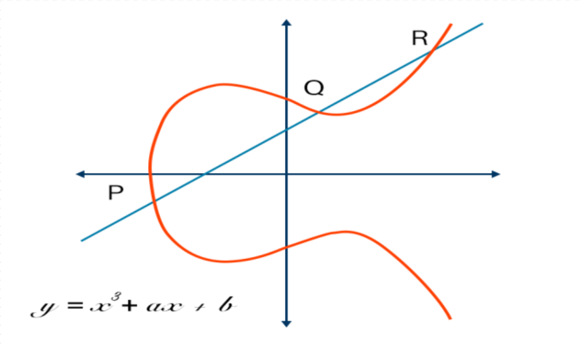
- (3) 群的实例
- 

例(iii) p是素数，$F_p$≡{0,1,…,p-1}、$F^*_p$≡$F_p$\{0}，在$F_p$上定义模p的加法运算+，在$F^*_p$上定义模p的乘法运算×，于是($F^*_p$, ×)和($F^p$,+)都是群，阶分别为p-1和p(习题；逐一验证之)。

- 
- 这个例子的特殊之处，在于同一个集合$F_p$上有两种群运算，两种运算之间还满足通常我们所熟悉的加法和乘法之间的分配律(习题：验证之)，这使$F_p$具有比单纯的群更为丰富的性质。
- 
- 带+和×这两种运算的集合$F_p$称做特征为 *p* 的素域。素域是有限域(即仅有有限个元素的域)的一类特殊情形。

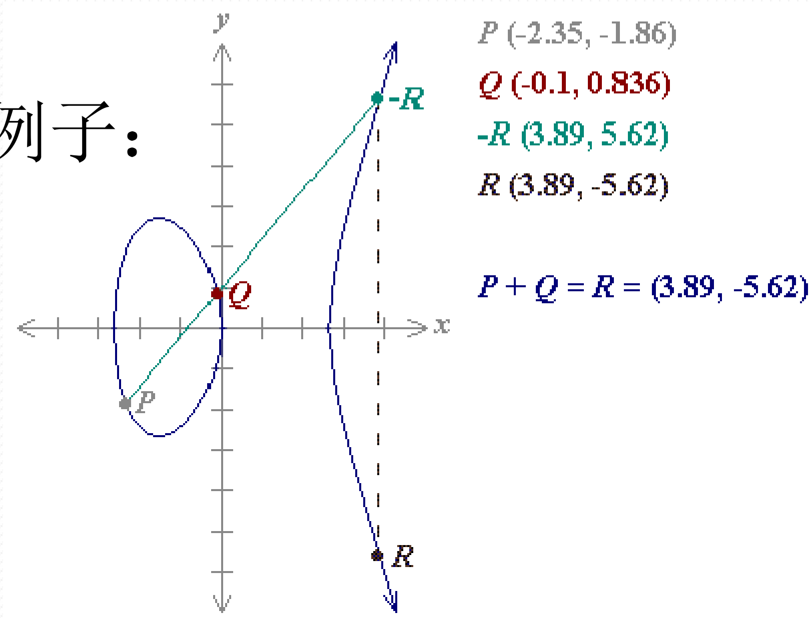
# Euler公式的推广(5)

- (3) 群的实例

- 例(iv) 设$F_q$是有限域、阶为素数q，A、B∈$F_q$是给定的常数，$F_q$上的
- 椭圆曲线$E/F_q$是集合
- $\{(x,y): y^2=x^3+Ax+B\}$
- 在$E/F_q$上可以定义点的一种运算“+”使 $(x_1,y_1)+(x_2,y_2)=(x_3,y_3)$，例如对$p\neq 2$、3的情形，$x_3$和$y_3$按照以下公式计算：
- $$x_3=-x_1-x_2+\left(\frac{y_1-y_2}{x_1-x_2}\right)^2,\qquad y_3=-y_1-\left(\frac{y_1-y_2}{x_1-x_2}\right)(x_3-x_1)$$
-
- 

# Euler公式的推广(6)

- (3) 群的实例
- 
- 在算法领域的其他(无限)群的例子：
- 向量的加法群；
- 矩阵加法群；
- 可逆矩阵的乘法群；
- 多项式的加法群；
- 【问题】多项式是否按乘法构成群？




$y^2 = x^3 - 7x$

# Euler公式的推广(7)

- (4) 子群的概念和性质
-
- 设G是群，H是G的子集。
- 如果G上的群运算应用于H的元素恰使H也是一个群，则H定义做G的子群。
- 例(i)：所有偶数构成整数加法群的子群。
- 例(ii)：在群G中某个元素$a$生成的子集$\{e,a,a^2,a^3,\ldots,a^{d-1}\}$必定是一个子群（为什么），这里$d$是满足$a^n=e$的最小的正数，称为$a$的阶(order)或周期。这个子群称为$a$生成的循环子群(cyclic subgroup)，常记为$\langle a\rangle$.

- 【习题】若$d$是群元素$a$的阶，N是使得$a^N=e$的任何整数，则必有$d|N$。
- 提示：应用Euclid第一定理，设N=qd+r，$0\le r<d$，根据群运算的性质证明$a^r=e$，于是
- r必定为0（为什么？注意$0\le r<d$），从而 $d|N$。

# Euler公式的推广(8)

- (4) 子群的概念和性质
-
- *Lagrange*定理：G是g阶有限群，H是G的h阶子群，则
- h | g
- 证明概要：在G上建立一个关系~：G的元素$a$和b满足关系$a$~$b$当且仅当存在H的某个元素h使$a$=bh。验证以下性质（习题）：
- (i) 对任何元素$a$恒有$a$~$a$ (ii)$a$~$b$则$b$~$a$ (iii)$a$~$b$、$b$~$c$和$a$~$c$，因此~是一个等价关系。
- 进一步验证性质 (iv)：~在群G上划分的每个等价类都恰与子群H有相同的大小。
- 因此，G的阶g = 全部~等价类的大小之和 = kh。证毕。

# Euler公式的推广(9)

- (4) 子群的概念和性质

- (i) Lagrange定理的推论之一：设G是$g$阶群，$a$是G的某个元素，d是$a$的阶，则$d|g$。
- 证明概要：对G中$a$的循环子群$\langle a\rangle$应用Lagrange定理，并注意子群$\langle a\rangle$的阶恰为d。
- (ii)推论之二：设G是$g$阶群，$a$是G的某个元素，则$a^g = e$。
- 证明：设$d$是$a$的阶，由以上推论有$g=kd$，故$a^g = a^{kd} = (a^d)^k = e^k = e$.

- (iii)回到Euler公式：考虑群$G=Z_N^*$的例子，其阶$g=\phi(N)$，单位元素为1，由上述推论，对任何$a$属于G有$a^{\phi(N)} = 1 \bmod N$。

# Euler公式的推广(10)

- 下节课内容：

- 一、二次剩余理论概要（补充材料，参阅Stinson教程）
- 二次方程$x^2=a \bmod p$可解性、二次互反律、
- *Legendre*和*Jaccobi*符号的算法、密码学中的应用。

- 二、素域$F^*_p$和扩域$F_{p^d}$的基本性质（Stallings教程4.5~4.7）