离散对数
Discrete Logarithm

非对称加密算法基于困难假设

- 大整数因式分解
  - RSA, Rabin
- 离散对数
  - El Gamal
- 椭圆曲线上的离散对数
  - 椭圆曲线上的El Gamal

El Gamal密码体制

El Gamal密码体制基于离散对数问题。我们首先在有限乘法群 $(G, .)$ 中描述这个问题。

对于一个 n 阶元素 $\alpha \in G$，定义 $\langle \alpha \rangle = \{\alpha^i : 0 \le i \le n-1\}$

容易看到，$\langle \alpha \rangle$ 是 G 的一个子群，$\langle \alpha \rangle$ 是一个 n 阶循环群。

经常使用的一个例子是，取 G 为 Z_p（p 为素数）上的乘法群，α 为模 p 的生成元。这时有 $n = |\langle \alpha \rangle| = p - 1$

El Gamal密码体制

离散对数：

实例：乘法群 $(G, .)$ ，两个元素 $\alpha, \beta \in G$

问题：找到一个唯一的整数 a，$0 \leq a \leq n-1$，

满足 $\alpha^a = \beta$

El Gamal密码体制

我们将这个整数 a 记为 $\log_{\alpha} \beta$ ，称为 β 的离散对数。

在密码中主要应用离散对数问题的如下性质：

求解离散对数(可能)是困难的，而其逆运算指数运算可以应用平方-乘方法有效地计算。换句话说，在适当的群 G 中，指数函数是单向函数。

El Gamal密码体制

Z_p^* 上的El Gamal密码体制

设 p 是一个素数，使得 $(Z_p^*, \cdot)$ 上的离散对数问题是难处理的，

令 $\alpha \in Z_p^*$ 是一个生成元。令 $P = Z_p^*$，$C = Z_p^* \times Z_p^*$ 定义

$K = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod{p}\}$，$p, \alpha, \beta$ 是公钥，p, a 是私钥。

对 $K = (p, \alpha, a, \beta)$，以及一个(秘密)随机数 $k \in Z_{p-1}$，定义

$e_K(x, k) = (y_1, y_2)$，其中 $y_1 = \alpha^k \bmod p$ 且 $y_2 = x\beta^k \bmod p$

对 $y_1, y_2 \in Z_p^*$，定义 $d_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p$

El Gamal密码体制

在El Gamal密码体制中，加密运算是随机的，因为密文既依赖于明文又依赖于加密方选择的随机数 k，因此对于同一个明文会有许多($p-1$个)可能的密文。

例：设 $p = 2579$，$\alpha = 2$。α 是模p 的生成元。令 $a = 765$

所以 $\beta = 2^{765} \bmod 2579 = 949$，假设Alice现在想要传送消息 $x = 1299$ 给Bob, 如果她选择 $k = 853$ 作为随机数，那么她计算 $y_1 = 2^{853} \bmod 2579 = 435, y_2 = 1299 * 949^{853} \bmod 2579 = 2396$

El Gamal密码体制

Bob收到密文$(435,2396)$后，他计算

$$x = 2396 * \left(435^{765}\right)^{-1} \bmod 2579 = 1299$$

这正是Alice加密的明文。

显然，如果其他人可以计算 $a = \log_{\alpha} \beta$，那么El Gamal密码体制就是不安全的。

El Gamal密码体制安全的一个必要条件就是Z_p^*上的离散对数问题是难处理的。为此p应该至少取300个十进制位，$p-1$应该具有一个较“大”的素数因子。

El Gamal体制的安全性

El Gamal是否正确?
El Gamal是否高效?
El Gamal是否安全?

Diffie-Hellman问题

离散对数问题（Discrete Logarithm）：

已知一个乘法群$(G,\cdot)$，一个n阶元素$\alpha \in G$和元素$\beta \in G$,

计算$a = \log_{\alpha}{}^{\beta}$。

计算Diffie-Hellman问题（CDH, Computational Diffie-Hellman）：

已知一个乘法群$(G,\cdot)$，一个n阶元素$\alpha \in G$,两个元素$\beta,\gamma \in G$,

计算$\delta \in G$满足$\log_{\alpha}{}^{\delta} = \log_{\alpha}{}^{\beta} \times \log_{\alpha}{}^{\gamma}$。

判定Diffie-Hellman问题（DDH, Decision Diffie-Hellman）：

已知一个乘法群$(G,\cdot)$，一个n阶元素$\alpha \in G$,两个元素$\beta,\gamma,\delta \in G$,

判定$\log_{\alpha}{}^{\delta} = \log_{\alpha}{}^{\beta} \times \log_{\alpha}{}^{\gamma}$是否成立。

El Gamal 安全性

- 如果El Gamal加密算法无法抵抗选择明文攻击，那么DDH问题不是计算困难的。

- 如何证明？

$$\left\langle g^x, g^y, g^{xy} \right\rangle, \left\langle g^x, g^y, g^z \right\rangle$$

El Gamal安全性

- 解决DDH问题的概率？

$$\langle g^x, g^y, g^{xy} \rangle, \langle g^x, g^y, g^r \rangle$$

$$\langle g^x, g^y, g^z \rangle$$

PubKey：g^x

$$Enc: m_i \rightarrow r_i, \langle g^{r_i}, m_i g^{xr_i} \rangle$$

$$m_0^*, m_1^* \rightarrow \langle g^y, m_b g^z \rangle$$

$$Enc: m_i \rightarrow r_i, \langle g^{r_i}, m_i g^{xr_i} \rangle$$

$$b^*$$

1/2 or other ans

El Gamal安全性

作业：证明该定理

定理 如果 DDH 问题是困难的, ElGamal加密方案在IND-CPA安全模型下是可证明安全的，L=2。

DUE：June 10 ， 2020
Email：bitcrypto2020@163.com
Format: any you like

Diffie-Hellman问题

ElGamal体制的解密等价于求解CDH问题。

（1）解决了CDH问题 $\Rightarrow$ 求出明文。

已知β, y_1计算δ，则$x = y_2\delta^{-1}$

（2）区分出明文 $\Rightarrow$ 解决了DDH问题

给定(β, γ, δ)

定义$y_1 = \gamma$,随机选择$y_2 \in <\alpha>$,调用解密算法得到x,

则$\delta = y_2 x^{-1}$

El Gamal密码体制

El Gamal密码体制可以在任何离散对数问题难处理的群中实现。

除了乘法群 Z_p^* ，还有两类群也是合适的候选者。

有限域 F_{p^n} 的乘法群；

定义在有限域上的椭圆曲线的群。

为此，下面介绍群、环、域的定义以及区别联系。

群、环、域

半群

称代数系统<S，*>为半群，如果*运算满足结合律。

典型的半群如：<Z+,+>，<N，•>，其中Z+代表正整数。

群、环、域

群

称代数结构<G，*>为群（groups），如果

（1）<G，*>为一半群。

（2）<G，*>中有单位元e。

（3）<G，*>中每一元素都有逆元。

其中，若 * 运算满足交换律，则称该群为交换群或阿贝尔群。

典型的群如：<Z,+>，<Q+，•>，其中Q+代表正有理数

群、环、域

环

称代数结构<R,+,•>为环（ring），如果

（1）<R ,+>是阿贝尔群。

（2）<R ,•>是半群。

（3）乘运算对加运算可分配，即对任意元素a,b,c ∈R，有

a（b＋c）＝ ab+ac ， （b＋c）a = ba+ca

典型的环如： <Z,+,•>(Z为整数集，+,•为数加与数乘运算)

群、环、域

域

称< F,+, • >为域（fields），如果< F,+, • >为环,且

< F-{0}, • >为阿贝尔群。

典型的域如：<Q，＋， • >，其中Q为有理数。

但是<Z，＋， • >不是域。为什么？

有限域

当 p 是素数时，Z_p 是一个域。

如果 $q = p^n$，p 是素数，$n \geq 1$ 是整数，就存在一个具有 q 个元素的域。这类域的构造方法如下：

假定 p 是素数。定义 $Z_p[x]$ 是变元 x 的所有多项式的集合。按照通常多项式的乘法和加法定义（并且模 p 约化系数），我们构造一个环。对于 $f(x), g(x) \in Z_p[x]$，如果存在 $q(x) \in Z_p[x]$ 满足 $g(x) = q(x)f(x)$，则说 $f(x)$ 整除 $g(x)$，记作 $f(x) \mid g(x)$

有限域

对 $f(x) \in Z_p[x]$，f 的次数 $\deg(f)$ 定义为 f 的项中最高次数。

假定 $f(x), g(x), h(x) \in Z_p[x]$，且 $\deg(f) = n \geq 1$。如果

$f(x) \mid (g(x) - h(x))$ 则定义 $g(x) \equiv h(x) (\bmod f(x))$

我们注意到，多项式同余与整数的同余有着非常相似之处。

我们要定义一个“模 $f(x)$”的多项式环，记作 $Z_p[x]/(f(x))$

为此，基于模 $f(x)$ 同余的观点，从 $Z_p[x]$ 构造 $Z_p[x]/(f(x))$，

类似于由 Z 构造 Z_m

有限域

假定 $\deg(f) = n$，用 $f(x)$ 去除 $g(x)$，得到(唯一)商 $q(x)$ 和 $r(x)$

其中，$g(x) = q(x)f(x) + r(x)$ ，并且 $\deg(r) < n$

这可以由多项式的长除法实现。因此 $Z_p[x]$ 中任何多项式模 $f(x)$

同余于唯一的次数至多 $n-1$ 的多项式。

定义 $Z_p[x]/(f(x))$ 的元素是 $Z_p[x]$ 中所有 p^n 个次数不超过 $n-1$

的多项式。加法和乘法与 $Z_p[x]$ 中相同，并且模 $f(x)$ 约化。

有了这两个运算，$Z_p[x]/(f(x))$ 是一个环。

有限域

Z_m是一个域当且仅当 m是素数，乘法逆元可以通过欧几里得算法求得。对于$Z_p[x]/(f(x))$ 有类似的情形。多项式中类似于素性的概念是不可约性，定义如下所述。

定义6.2　一个多项式 $f(x) \in Z_p[x]$称为不可约，如果不存在多项式$f_1(x), f_2(x) \in Z_p[x]$，满足$f(x) \in f_1(x)f_2(x)$，其中$\deg(f_1) > 0$且$\deg(f_2) > 0$

有限域

一个重要的事实是，$Z_p[x]/(f(x))$是域当且仅当 $f(x)$是不可约的。

$Z_p[x]/(f(x))$ 中元素的乘法逆元可以直接通过改进的(扩展)欧几里得算法计算。

例：我们构造一个具有八个元素的域。这可以通过在 Z_2 中找一个次数为3的不可约多项式做到。因为任何和常数项为0的多项式都可以被 x 整除，因而是可约的，我们只需要考虑具有常数项为 1 的多项式。有 4 个这样的多项式。

有限域

$$f_1(x) = x^3 + 1$$
$$f_2(x) = x^3 + x + 1$$
$$f_3(x) = x^3 + x^2 + 1$$
$$f_4(x) = x^3 + x^2 + x + 1$$

有限域

由于 $f_2(x)$ 和 $f_3(x)$ 都是不可约的，所以我们可以其构造域。

这里使用 $f_2(x)$ 构造域 $Z_2[x]/(x^3 + x + 1)$

8 个域元素如下：0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1

由于任意两个域元素的乘积模 $x^3 + x + 1$ 约化后，余式的次数至多是 2，因此是域中的元素。

例如，计算 $Z_2[x]/(x^3 + x + 1)$ 中的 $(x^2 + 1)(x^2 + x + 1)$

有限域

例如，计算 $Z_2[x]/(x^3+x+1)$ 中的 $(x^2+1)(x^2+x+1)$

首先在 $Z_2[x]$ 中计算乘积，得到 x^4+x^3+x+1。

随后用 x^3+x+1 去除，得到表达式：

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

因此，在域 $Z_2[x]/(x^3+x+1)$ 中有：

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

有限域

下面给出一个域中非零元素的乘法表，将多项式 $a_2x^2 + a_1x + a_0$

简写为有序三元组 $a_2a_1a_0$

	001	010	011	100	101	110	111
001	001	010	011	100	101	110	111
010	010	100	110	011	001	111	101
011	011	110	101	111	100	001	010
100	100	011	111	110	010	101	001
101	101	001	100	010	111	011	110
110	110	111	001	101	011	010	100
111	111	101	010	001	110	100	011

有限域

通过直接应用扩展的欧几里得算法，可以计算域元素的逆元。

最后域中非零多项式是一个7阶乘法群，由于7是素数，所以域中除0和1外，任何元素都是本原元。

例如，计算x 的幂可以囊括域中的所有非零元素：

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

有限域

域的存在性和唯一性

可以证明，在$Z_p[x]$中，对任意给定的次数$n \geq 1$，至少存在一个不可约多项式。因此，对所有的整数$n \geq 1$以及所有的素数p存在具有p^n个元素的有限域。

通常，$Z_p[x]$中有许多次数为n的不可约多项式，但是可以证明有任何两个不可约多项式构造的域是同构的。因此，存在唯一的p^n个元素的有限域，记为F_{p^n}

有限域

当 $n = 1$ 时，F_p 与 Z_p 相同。

最后可以证明，如果存在 r 个元素的有限域，那么一定存在某个素数 p，以及某个整数 $n \geq 1$，使得 $r = p^n$

注意到乘法群 Z_p^* 是一个阶为 $p-1$ 的循环群。事实上，任何有限域的乘法群都是循环群：$F_{p^n} \setminus \{0\}$ 是一个阶为 $p^n - 1$ 的循环群。

椭圆曲线

实数上的椭圆曲线

椭圆曲线被描述为一个二元方程解的集合

模 p 定义的椭圆曲线在公钥密码学中非常重要

定义6.3

设 $a,b\in \mathrm{R}$ 是满足 $4a^3+27b^2\neq 0$ 的常实数

方程 $y^2=x^3+ax+b$ 的所有解 $(x,y)\in \mathrm{R}\times \mathrm{R}$ 连同一个无穷远点 O

组成的集合 E ，称为一个非奇异椭圆曲线

椭圆曲线

实数上的椭圆曲线

如果 $4a^3+27b^2\neq 0$ 是保证方程 $y^2=x^3+ax+b$ 有三个不同解（实数或复数）的充要条件。如果 $4a^3+27b^2=0$，则对应椭圆曲线为奇异椭圆曲线。

假定 E 是一个非奇异椭圆曲线，在 E 上定义一个二元运算，使其成为一个阿贝尔群，这个二元运算常用加法表示。无穷远点 O 将是单位元。

椭圆曲线

实数上的椭圆曲线

因此，对于所有 $P \in E$ 有 $P+O=O+P=P$

假设 $P, Q \in E$，其中 $P(x_1, y_1), Q(x_2, y_2)$

我们分三种情况考虑：

1. $x_1 \neq x_2$

2. $x_1 = x_2, y_1 = -y_2$

3. $x_1 = x_2, y_1 = y_2$

椭圆曲线

1. $x_1 \neq x_2$

定义 L 是通过 P 和 Q 的直线。L 交 E 于 P 和 Q，容易看出，L 还交 E 于第三点，记为 R’。对于 x 轴反射 R’，得到一点 R。

定义 $P + Q = R$

这里首先给出计算 R 的代数公式。首先，直线 L 的方程为

$y = \lambda x + \upsilon$，其斜率是 $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

并且 $\upsilon = y_1 - \lambda x_1 = y_2 - \lambda x_2$

椭圆曲线

为了算出$E \cap L$ 中的点，将$y = \lambda x + \upsilon$代入到E的方程中得到$\left(\lambda x + \upsilon\right)^2 = x^3 + ax + b$等价于

$$x^3 - \lambda^2 x^2 + \left(a - 2\lambda\upsilon\right)x + b - \upsilon^2 = 0$$

上式的三个根中，P和Q是其中的两个点，所以x_1和x_2是方程的两个根。由于该方程是实数域上的三次方程，所以第三个根应该也是实数根，记为x_3。三根之和是二次项系数λ^2的相反数，所以$x_3 = \lambda^2 - x_1 - x_2$

椭圆曲线

设$R(x_3, y_3)$，则$R'(x_3, -y_3)$

又由于R'在直线上，所以$\lambda = \dfrac{-y_3 - y_1}{x_2 - x_1}$ **斜率**

即 $y_3 = \lambda(x_1 - x_3) - y_1$

所以对于 $x_1 \neq x_2$，可以导出$P + Q$ 的一个计算公式

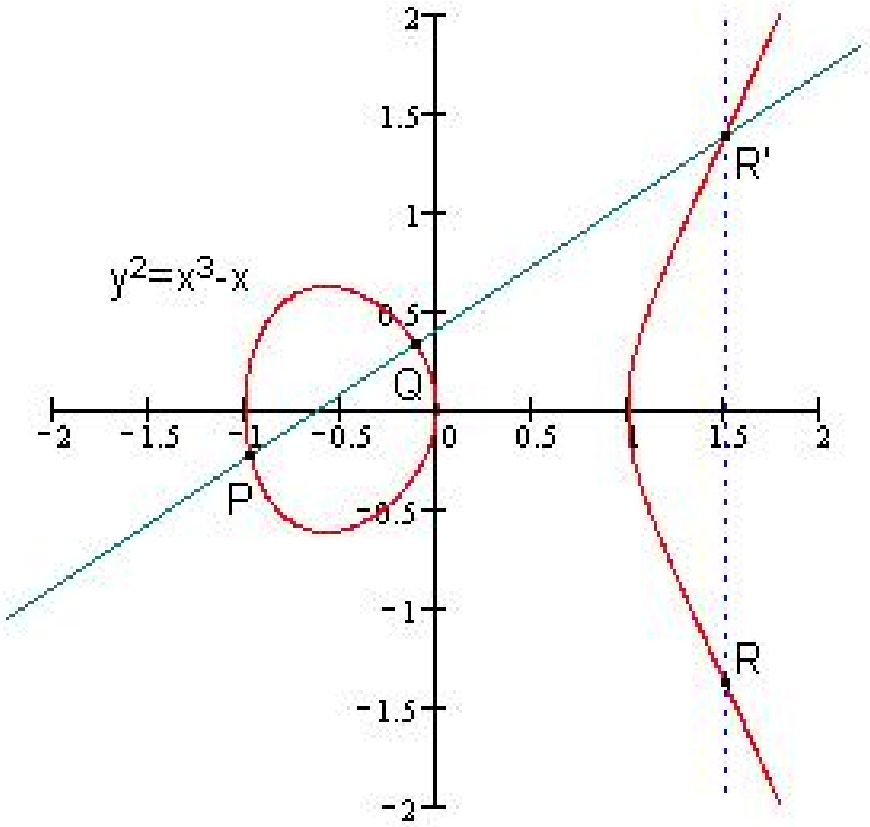
$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

其中 $x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

椭圆曲线



$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

椭圆曲线

2. $x_1 = x_2, y_1 = -y_2$

当$x_1 = x_2, y_1 = -y_2$时，定义

$$(x, y) + (x, -y) = O, (x, y) \in E$$

因此(x, y)与$(x, -y)$是关于椭圆曲线加法运算互逆的。

椭圆曲线

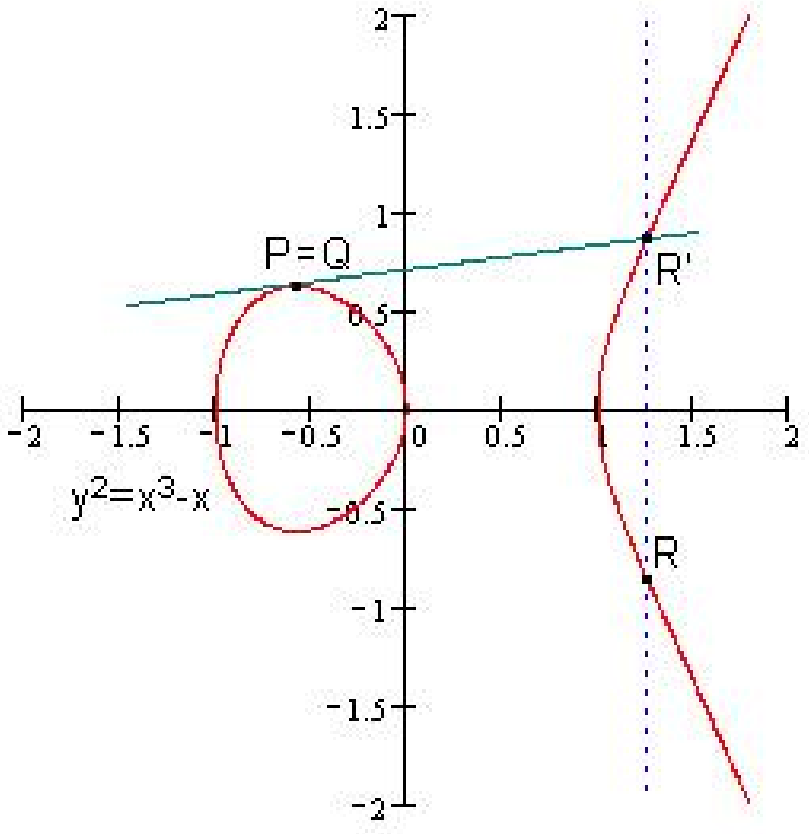
3. $x_1 = x_2, y_1 = y_2$

这就相当于$P(x_1, y_1)$与自己相加。可以假定$y_1 \neq 0$，否则就是情形2。这里定义L是E在P点的切线。此时利用微积分知识计算L的斜率：

$$2y\frac{dy}{dx} = 3x^2 + a \Rightarrow \lambda = \frac{dy}{dx} = \frac{3x^2 + a}{2y}$$

替换$x = x_1, y = y_1$，得到切线斜率为$\lambda = \frac{3x_1^2 + a}{2y_1}$

椭圆曲线



$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

$$x_3 = \lambda^2 - x_1 - x_1$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

椭圆曲线

到此为止，按照前述定义，加法运算具有下列性质：

1. 加法在集合 E 上是封闭的。

2. 加法是可交换的。

3. O 是加法的单位元。

4. E 上每个点有关于加法的逆元。

要证明 $(E,+)$ 是阿贝尔群，尚需证明加法是可结合的，但是方法比较繁杂，这里不做过多讨论。

椭圆曲线

模素数的椭圆曲线

设 $p > 3$ 是素数。Z_p 上的同余方程 $y^2 \equiv \left(x^3 + ax + b\right) \bmod p$ 的所有解 $\left(x, y\right) \in Z_p \times Z_p$，连同无穷远点 O，共同构成 Z_p 上的椭圆曲线 $y^2 \equiv x^3 + ax + b$。其中 $a, b \in Z_p$ 并且满足 $4a^3 + 27b^2$ 恒不等于 0 的常量。

椭圆曲线

E 上的加法运算定义如下(设所有的运算都在 Z_p 中)：

假设 $P(x_1, y_1), Q(x_2, y_2)$ 是 E 上的点。

如果 $x_1 = x_2$ 且 $y_2 = -y_1$ 则 $P + Q = O$

否则 $P + Q = (x_3, y_3)$

其中
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

且
$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1} & P = Q \end{cases}$$

椭圆曲线

最后，对于所有的$P \in E$，定义$P+O=O+P=P$

Z_p上的椭圆曲线虽然不像实数域上的椭圆曲线那样具有直观的几何解释，然而同样的公式可以用来定义加法运算，$(E,+)$仍然是一个阿贝尔群。

例：设E是Z_{11}上的椭圆曲线$y^2 = x^3 + x + 6$。首先确定E的点。这可以通过对每个$x \in Z_{11}$，计算$(x^3+x+6) \bmod 11$。对于给定的x，测试$z = x^3 + x + 6$是否二次剩余。

椭圆曲线

X	$x^3 + x + 6 \bmod 11$	是二次剩余吗	y
0	6	**N**	
1	8	**N**	
2	5	**Y**	4,7
3	3	**Y**	5,6
4	8	**N**	
5	4	**Y**	2,9
6	8	**N**	
7	4	**Y**	2,9
8	9	**Y**	3,8
9	7	**N**	
10	4	**Y**	2,9

椭圆曲线

E 有13个点。因为任意素数阶的群是循环群，因此 E 同构于 Z_{13}

任何非无穷远点都是 E 的生成元。假设取生成元 $\alpha = (2,7)$

可以计算 α 的“幂”（因为群的运算是加法，可以写成 α 的倍数）

要计算 $2\alpha = (2,7) + (2,7)$ 首先计算

$$\lambda = (3 \times 2^2 + 1)(2 \times 7)^{-1} \bmod 11$$

$$= 2 \times 3^{-1} \bmod 11$$

$$= 2 \times 4 \bmod 11 = 8$$

椭圆曲线

所以有

$$x_3 = 8^2 - 2 - 2 \bmod 11 = 5$$

$$y_3 = 8(2 - 5) - 7 \bmod 11 = 2$$

因此，$2\alpha = (5,2)$

下一个乘积是 $3\alpha = 2\alpha + \alpha = (5,2) + (2,7)$

$$\lambda = (7 - 2)(2 - 5)^{-1} \bmod 11$$

$$= 5 \times 8^{-1} \bmod 11$$

$$= 5 \times 7 \bmod 11 = 2$$

椭圆曲线

所以有

$$x_3 = 2^2 - 5 - 2 \bmod 11 = 8$$

$$y_3 = 2(5 - 8) - 2 \bmod 11 = 3$$

因此，$3\alpha = (8,3)$

如此继续，可以看到 $\alpha = (2,7)$ 确实是生成元

$\alpha = (2,7)$	$2\alpha = (5,2)$	$3\alpha = (8,3)$
$4\alpha = (10,2)$	$5\alpha = (3,6)$	$6\alpha = (7,9)$
$7\alpha = (7,2)$	$8\alpha = (3,5)$	$9\alpha = (10,9)$
$10\alpha = (8,8)$	$11\alpha = (5,9)$	$12\alpha = (2,4)$

椭圆曲线

例：设 $\alpha = (2,7)$，Bob的私钥是 7 ，有 $\beta = 7\alpha = (7,2)$

这样，加密运算是 $e_K(x, k) = (k(2,7), x + k(7,2))$ ，其中

$x \in E$ 及 $0 \le k \le 12$ ，解密运算是 $d_K(y_1, y_2) = y_2 - 7y_1$

假设 Alice 要加密明文 $x = (10,9)$ 。如果随机选择了 $k = 3$

那么她要计算 $y_1 = 3(2,7) = (8,3)$ $y_2 = (10,9) + 3(7,2) = (10,2)$

所以 $y = ((8,3), (10,2))$。

Bob解密密文 $y = ((8,3), (10,2))$ 过程如下：

椭圆曲线

Bob解密密文 $y = ((8,3),(10,2))$ 过程如下：

$$
\begin{aligned}
x &= (10,2) - 7(8,3) \\
&= (10,2) - (3,5) \\
&= (10,2) + (3,6) \\
&= (10,9)
\end{aligned}
$$