第10章 椭圆曲线密码学

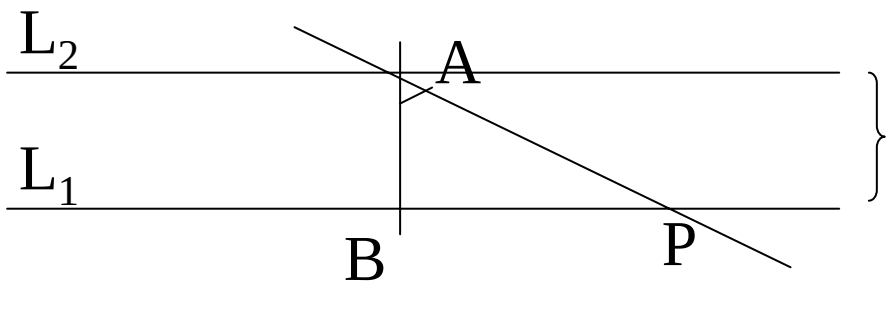
椭圆曲线密码学是由美国学者**Neil Koblitz**与**Victor Miller**在**1985**年各自独立创建起来的。**RSA**与**ElGamal** 加密体制中,如果使用长度为**1024**比特的模数才可以达到基本的安全等级，那么对于椭圆曲线**(ECC)**加密体制来说，按目前公开的密码攻击方法，只要使用长度为**160**比特的模数，就可以达到这个安全等级。

参见：www.certicom.com

1 有关的基本概念

(1) 无穷远元素（无穷远点，无穷远直线）

平面上任意两相异直线的位置关系有相交和平行两种。引入无穷远点，是两种不同关系统一。



AB⊥L_1，L_2∥L_1，直线AP由AB起绕A点依逆时针方向转动，P为AP与L_1的交点。

$\angle BAP \to \pi/2 \Longrightarrow AP \to L_2$

可以设想L_1上有一点P_∞，它为L_2和L_1的交点，被称之为无穷远点。

●注意:直线L_1上的无穷远点只能有一个

（因为过A点只能有一条平行于L_1的直线L_2，而两直线的交点只能有一个。）

结论：

1*. 平面上一组相互平行的直线，有公共的无穷远点。

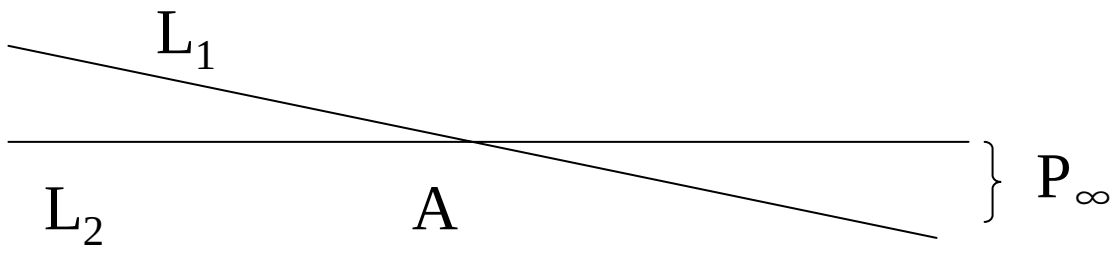
（为与无穷远点相区别，把原来平面上的点叫做平常点）

2* .平面上相交于点A的两直线L_1,L_2有不同的无穷远点。

原因：若否，则L_1和L_2有公共的无穷远点P_∞，则过两相异点A和P_∞有相异两直线，与几何公理相矛盾。

3*. 全体无穷远点构成一条无穷远直线。

注：欧式平面添加上无穷远点和无穷远直线，自然构成射影平面。



(2) 齐次坐标

解析几何中引入坐标系，用代数的方法研究欧氏空间。这样的坐标法也可推广至射影平面上，建立平面射影坐标系 ,(齐次坐标系).

平面上两相异直线L_1,L_2，其方程分别为：

L_1: $a_1x+b_1y+c_1=0$

L_2: $a_2x+b_2y+c_2=0$

其中a_1,b_1不同时为0；a_2,b_2也不同时为0。

设

$$D=\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \qquad D_x=\begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix} \qquad D_y=\begin{vmatrix} c_1 & a_1 \\ c_2 & a_2 \end{vmatrix}$$

若$D\neq 0$，则两直线L_1,L_2相交于一平常点$P(x,y)$，其坐标为$\mathbf{x=D_x/D}$，$\mathbf{y=D_y/D}$.

也可以将这组解表示为：$\mathbf{x/D_x=y/D_y=1/D}$

(约定：分母$\mathbf{D_x}$，$\mathbf{D_y}$有为**0**时，对应的分子也要为**0**）

上述表示可抽象为（$\mathbf{D_x}$，$\mathbf{D_y}$，**D**).

若 **D=0**，则$\mathbf{L_1 /\!/ L_2}$，此时$\mathbf{L_1}$和$\mathbf{L_2}$交于一个无穷远点$\mathbf{P_\infty}$.

这个点$\mathbf{P_\infty}$可用过原点**O**且平行于$\mathbf{L_2}$的一条直线**L**来指出他的方向，而这条直线**L**的方程就是：$\mathbf{a_2x+b_2y=0.}$

为把平常点和无穷远点的坐标统一起来，把点的坐标用（X，Y，Z)表示，X，Y，Z不能同时为0，且对平常点（x，y)来说，有Z≠0，x=X/Z，y=Y/Z，于是有：

$$\frac{X/Z}{D_x} = \frac{Y/Z}{D_y} = \frac{1}{D}$$

相当于说 X / Dx = Y / Dy = Z / D，　.

有更好的坐标抽象(X,Y,Z) ;Z=0时它表示无穷远点。

注解1：实数c≠0，则(cX,cY,cZ)为一等价类,代表元为（X,Y,Z)。实质上用（X:Y:Z)表示的3个分量中，只有两个是独立的，具有这种特征的坐标就叫齐次坐标。

例1：求点（1,2）在新的坐标体系下的坐标。

解：∵X/Z=1，Y/Z=2（Z≠0）∴X=Z，Y=2Z ∴坐标为（Z:2Z:Z），Z≠0。即（1:2:1）（2:4:2）等形如（t:2t:t），其中t≠0的坐标，都是（1,2）在新的坐标体系下的坐标,用代表元（1:2:1) 表示即可 .

例2：求平行线L1：X+2Y+3Z=0 与L2：X+2Y+Z=0相交的无穷远点。

解：因为L1∥L2 ,所以有Z=0， X+2Y=0；所以坐标为（-2Y:Y:0），Y≠0。即（-2:1:0）为这个无穷远点的坐标 .

注解2.欧氏直线L在平面直角坐标系Oxy上的方程为：

$$ax+by+c=0$$

则L上任一平常点(x,y)的齐次坐标为(X,Y,Z)，$Z\neq 0$，代入得：$aX+bY+cZ=0$

L上的无穷远点的坐标(X,Y,Z)应满足$aX+bY=0$，$Z=0$;

平面上无穷远直线的方程自然为：$Z=0$!!

(3)任意域上的椭圆曲线

K为域，K上的射影平面$P^2(K)$是一些等价类的集合{(X:Y:Z)}。考虑下面的**Weierstrass**方程(次数为3的齐次方程)：

$$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$

(其中系数$a_i\in K$)

Weierstrass方程被称为光滑或非奇异的是指对所有适合以下方程的射影点$P=(X:Y:Z) \in P^2(K)$来说，

$$F(X,Y,Z)=Y^2Z+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2-a_6Z^3=0$$

在P点的三个偏导数 $\partial F/\partial X, \partial F/\partial Y, \partial F/\partial Z$ 之中至少有一个不为 0。**若否，则称这个方程为奇异的。**

●**椭圆曲线E的定义：**

椭圆曲线E是一个光滑的**Weierstrass**方程在$P^2(K)$中的全部解集合。

$$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$

注：

a) **在椭圆曲线E上恰有一个无穷远点,即(0:1:0) ,用 θ 表示.**

b) 可用非齐次坐标的形式来表示椭圆曲线的Weierstrass方程:

设 **x=X/Z，y=Y/Z**，于是原方程转化为：

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \quad (※)$$

椭圆曲线E就是方程（※)在射影平面$P^2(K)$上的全部平常点解，外加一个y轴上的无穷远点θ组成的集合。

c) 若方程(1) 的系数$a_1,a_3,a_2,a_4,a_6 \in K$，此时椭圆曲线E被称为定义在K上，用E/K表示。如果E能被限定在K上，那么E的K－有理点集合表示为E(K)，它为E中的全体有理坐标点的集合外加无穷远点θ。

(4)实域R上的椭圆曲线

设K=R，此时的椭圆曲线可表为平面上的通常曲线上的点，外加无穷远点θ。

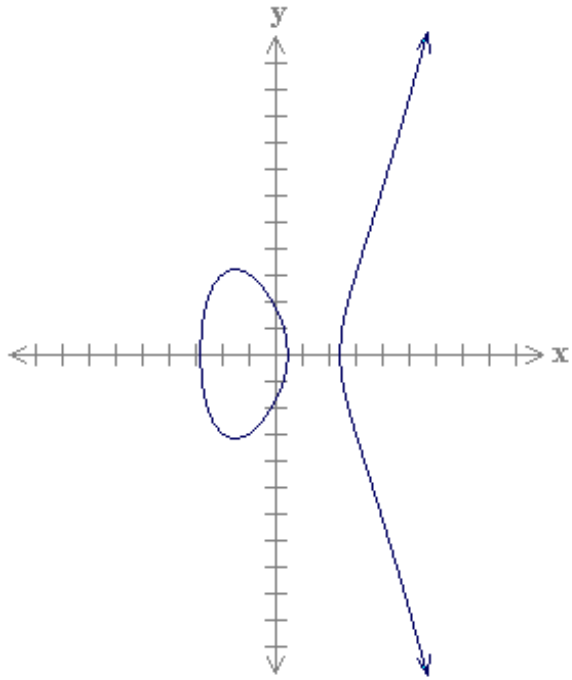
实域**R**上的椭圆曲线方程

$$E: y^2 = x^3 + ax + b$$

其系数满足关系式

$$4a^3 + 27b^2 \neq 0$$

满足该方程的所有点 (x,y) ，外加无穷远点 θ 一起构成的集合,被视为由该方程决定的椭圆曲线 。



可以按几何关系定义椭圆曲线上点的加法运算。

实域R上椭圆曲线点的加法运算法则

点$P=(x,y)$对X轴的反射点$-P=(x,-y)$被称为点$P=(x,y)$的负点(逆元) ,(x ,y) + (x,-y) = θ .

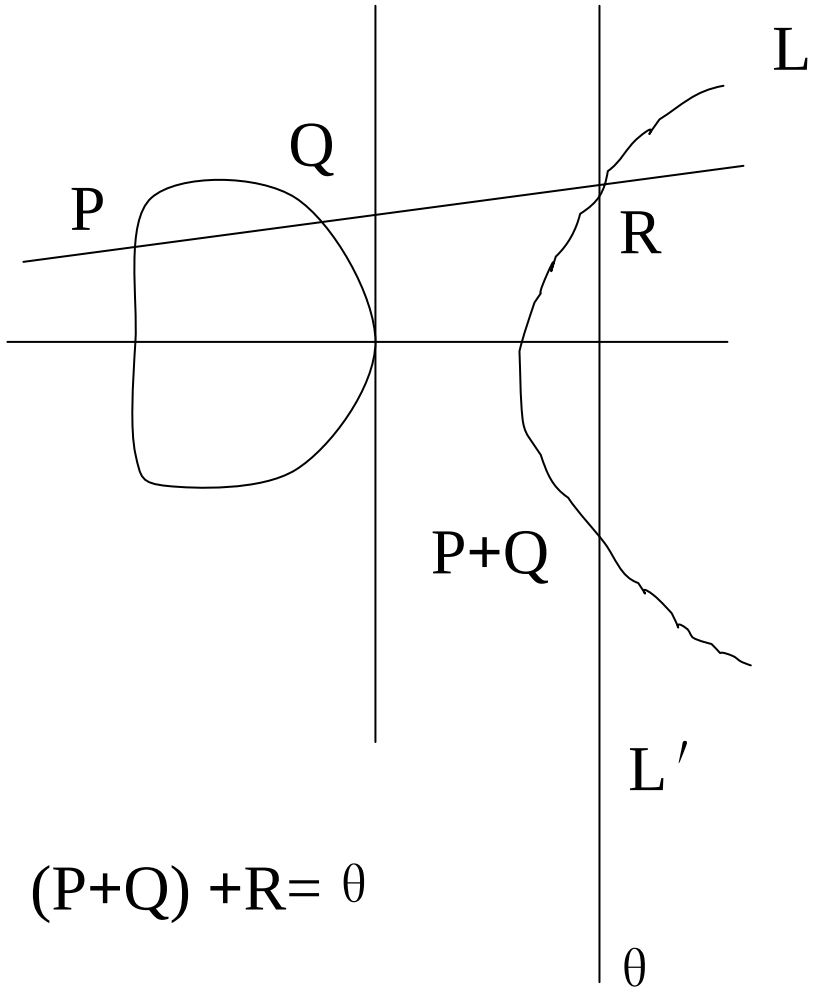
两相异点加运算：*P*、*Q*为椭圆曲线上相异两点，有$P+Q=R$，点*R*是经过*P*、*Q*两点的直线与曲线相交之点的唯一负点。

倍点运算：点*P* 的倍点2*P*是经过点*P*的切线与椭圆曲线相交之点的负点（逆元）。若点P重复加最小的次数n，就得nP= θ ，则称点P的阶（周期）为n。

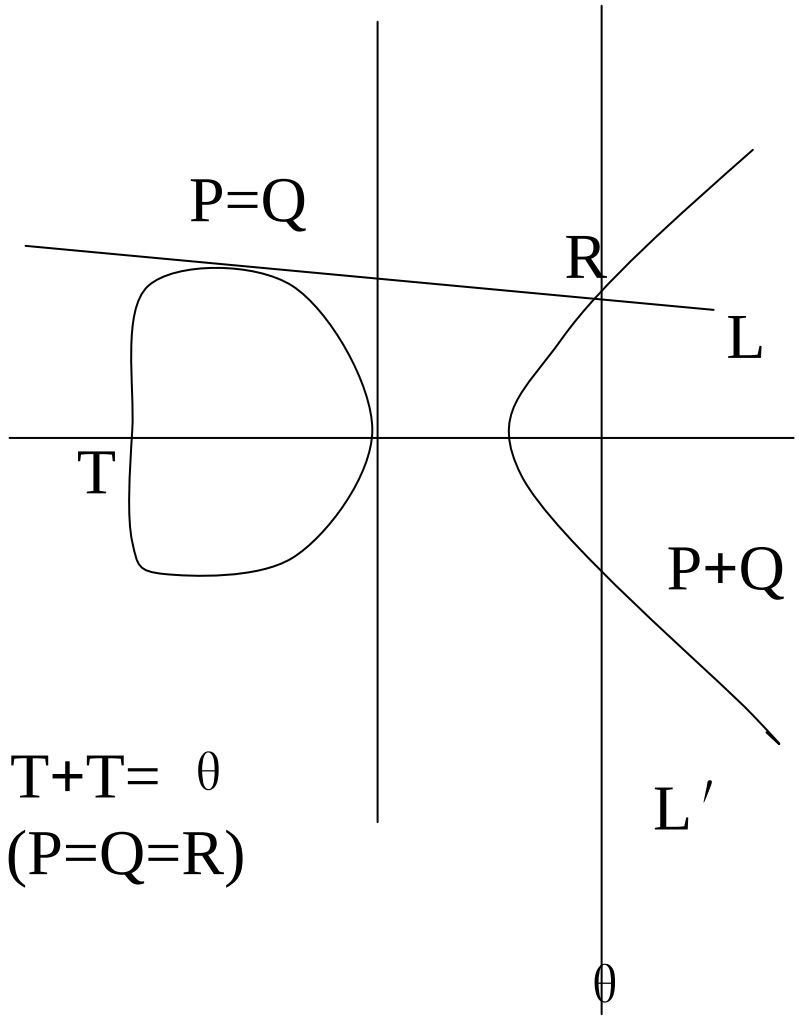
具体描素为：

设L ∈ $P^2(R)$为一条直线。因为E的方程是三次的，所以L可与E在$P^2(R)$恰有三个交点，记为P,Q,R（注意：如果L与E相切，那么P,Q,R可以不是相异的）。按下述方式定义E上运算⊕：

设P,Q ∈ E，L为联接P,Q的直线（若P=Q，则L取过P点的切线）；设R为L与E的另一个交点；再取连接R与无穷远点 θ (= (0:1:0))的直线L′。则L′与E的另一个交点定义为P + Q。



(P+Q) +R= θ



T+T= θ

(P=Q=R)

上面的图像为椭圆曲线$y^2=x^3-x$的具体图象。然而，用此图象来说明计算点的加法运算规则，并不失一般性。下面针对一般的方程(※)给出的椭圆曲线上的点 $P=(x_1,y_1)$、$Q=(x_2,y_2)$，来计算 $P\oplus Q=(x_3,y_3)$=?

由$P\oplus Q$的定义，设$y=\alpha x+\beta$为通过P,Q两点直线L的方程，可算出：

当$P\neq Q$时：$\alpha=(y_2-y_1)/(x_2-x_1)$，$\beta=y_1-\alpha x_1$

易见，直线L上的一个点（$x, \alpha x+\beta$)是在椭圆曲线E上，

当且仅当$(\alpha x+\beta)^2=x^3+ax+b$ ；

$$P+Q=(x_1,y_1)+(x_2,y_2)=(x_3,y_3)=(x_3,-(\alpha x_3+\beta))$$

其中，$x_3=\alpha^2-x_1-x_2=((y_2-y_1)/(x_2-x_1))^2-x_1-x_2$;

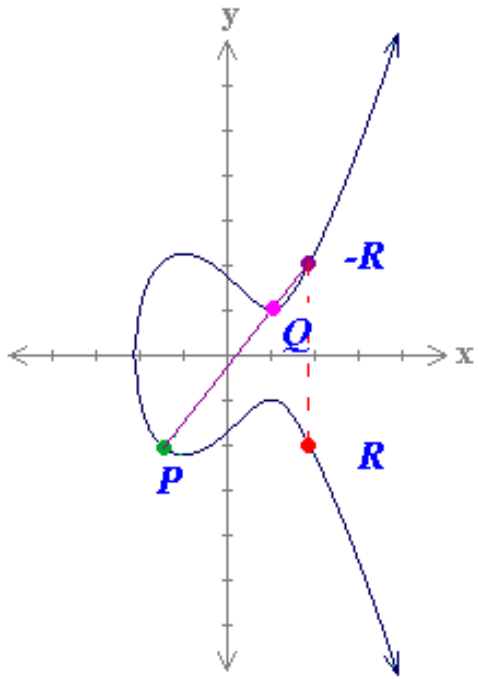
$y_3=-y_1+((y_2-y_1)/(x_2-x_1))(x_1-x_3)$

当$P=Q$时： $P+Q=(x_3, y_3)$算得：

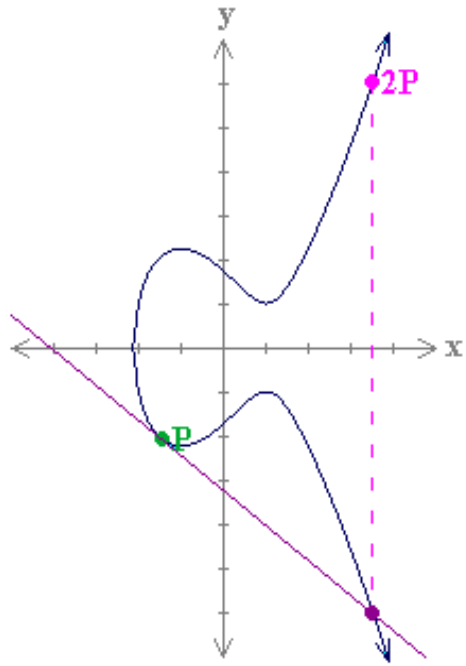
$x_3=((3x_1^2+a)/2y_1)^2-2x_1$;

$y_3=-y_1+((3x_1^2+a)/2y_1)(x_1-x_3)$ 。

图左表示两相异点相加;右图表两个相同点相加



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



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

注：

a) 如果直线**L**与**E**相交与三点**P,Q,R**(不一定相异），那么 **(P+Q)+R=** θ **(**从图中可见）。

b) 任给**P**∈**E, P +** θ **=P (**此时设**Q=** θ **，**易见**L=L′)**；

c) 任给**P,Q**∈**E**有： **P + Q =Q +P**；

d) 设**P**∈**E**，那么可以找到 **- P**∈**E**使**P +**（ **-P**）**=** θ ；

e) 任给**P,Q,R**∈**E**，有**(P + Q) +R= P +(Q +R)**

综上所述，知**E**对**+**运算形成一个**Abel**群。

f) 上述规则可开拓到任意域上，特别是有限域上。假定椭圆曲线是定义在有限域F_q上（$q=p^m$)，那么

$$E(F_q)=\{(x,y)\in F_q\times F_q \mid y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\}\cup\{\theta\}$$

不难验证它对“**+**”运算也形成一个**Abel**群。

2 有限域上椭圆曲线的+运算

令F_q表示q个元素的有限域，用$E(F_q)$表示定义在F_q上的一个椭圆曲线E。

定理1.(Hass定理) $E(F_q)$的点数用$\#E(F_q)$表示，则

$$|\#E(F_q)-q-1|\leqslant 2q^{1/2}$$

(1) F_p（素域，p为素数）上椭圆曲线

令p>3，$a,b\in F_p$，满足$4a^3+27b^2\neq 0$，由参数a和b定义的F_p上的一个椭圆曲线方程为：

$$y^2=x^3+ax+b$$

它的所有解(x,y)，($x\in F_p$，$y\in F_p$)，连同“无穷远点” θ 组成的集合记为$E(F_p)$，由Hass定理知：

$$p+1-2p^{1/2}\leqslant \#E(F_p) \leqslant p+1+2p^{1/2}$$

集合$E(F_p)$有如下加法规则：任给$(x,y) \in E(F_p)$,

(i) $\theta + \theta = \theta$ （单位元素）

(ii) $(x,y) + \theta = (x,y)$,

(iii) (iii) $(x,y) + (x,-y) = \theta$,

(iv) 令$(x_1,y_1),(x_2,y_2)$为$E(F_p)$中非互逆元并且互不相等，

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

$x_3 = \alpha^2 - x_1 - x_2$ ， $y_3 = \alpha(x_1 - x_3) - y_1$,斜率 $\alpha = (y_2 - y_1)/(x_2 - x_1)$

(v)（倍点运算规则）

设$(x_1,y_1) \in E(F_p), y_1 \neq 0$，则$2(x_1,y_1) = (x_3,y_3)$，

其中$x_3 = \alpha^2 - 2x_1$, $y_3 = \alpha(x_1 - x_3) - y_1$; $\alpha = (3x_1^2 + a)/(2y_1)$

注：若#$E(F_p)=p+1$，曲线$E(F_p)$称为超奇异的，否则称为非超奇异的。

例子1：F_{23}上的一个椭圆曲线

令$y^2=x^3+x+1$是F_{23}上的一个方程(a=b=1)，则该椭圆曲

线方程在F_{23}上的解为($y^2=x^3+x+1$的点)：

(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)；θ。

群$E(F_{23})$有28个点（包括无穷远点θ）。

例子2：F_{23} ,点P=(0,1)是椭圆曲线 $E: y^2 = x^3 + 12x + 1$ 点的生成元.

P = (0, 1), $2P$ = (13,13),

$3P$ = (5, 5), $4P$ = (3, 15) ,

$5P$ = (6, 17), $6P$ = (19, 2),

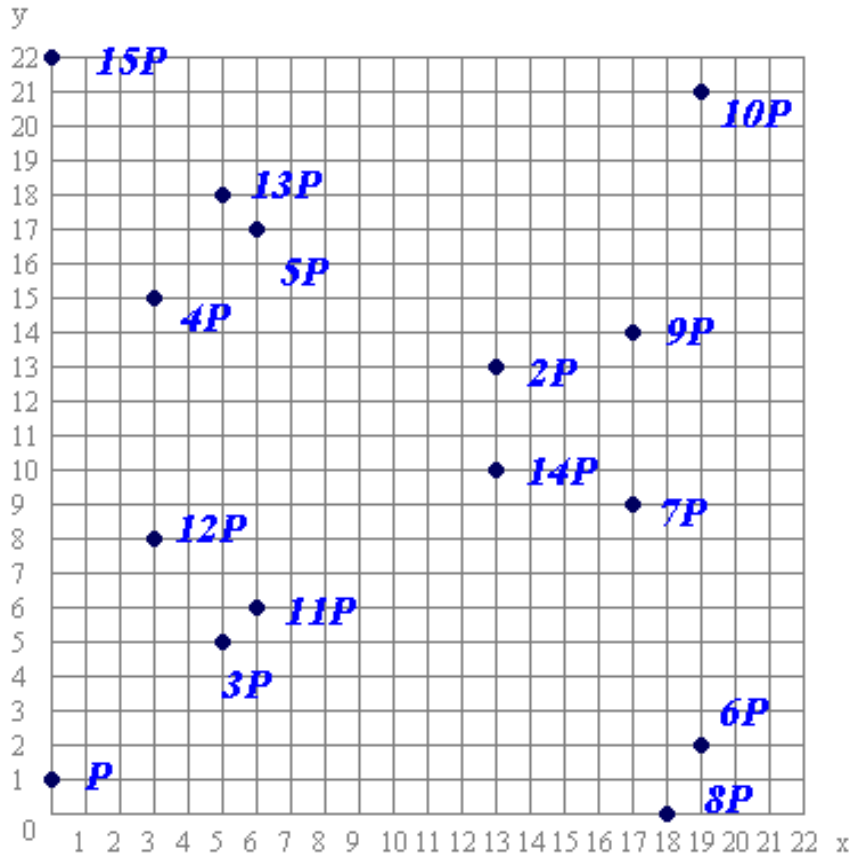
$7P$ = (17, 9), $8P$ = (18, 0),

$9P$ = (17, 14), $10P$ = (19, 21),

$11P$ = (6, 6) , $12P$ = (3, 8),

$13P$ = (5,18),$14P$ = (13,10),

$15P$ = (0, 22) ,16P= θ



例子3：F_{23}上的椭圆曲线 $E: y^2 = x^3 + 16x + 10$ 上的两点

P=(18 ,14) 、Q=(5,10) .求解P+Q =?

解：

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

$$= \frac{4}{13} \bmod 23$$

$$= 18$$

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

$$= 18^2 - 18 - 5 \bmod 23$$

$$= 2$$

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

$$= 18(18 - 2) - 14 \bmod 23$$

$$= 21$$

$$\therefore P + Q = R = (2,21)$$

(2) F_2m上的椭圆曲线

F_{2^m}上由参数$a,b \in F_{2^m}$，$b \neq 0$定义的一个非超奇异椭圆曲线$E(F_{2^m})$是方程

$$y^2+xy=x^3+ax^2+b$$

的解集合(x,y)，其中$x,y \in F_2m$，连同 θ 。

$E(F_{2^m})$的加法规则如下：

(i) $\theta + \theta = \theta$

(ii) 任给$(x,y) \in E(F_{2^m})$，则$(x,y) \oplus \theta = (x,y)$

(iii) 任给$(x,y) \in E(F_{2^m})$，则$(x,y)+(x,x+y)= \theta$，

即点(x,y)的逆为$(x,x+y)$.

(iv) 两个相异且不互逆的点的加法规则：

令$(x_1,y_1),(x_2,y_2) \in E(F_{2^m})$且有$x_1 \neq x_2$则

$(x_1,y_1)\oplus(x_2,y_2)=(x_3,y_3)$，其中

$x_3=\alpha^2+\alpha+x_1+x_2+a$;

$y_3=\alpha(x_1+x_3)+x_3+y_1$.

其中 $\alpha=(y_2+y_1)/(x_2+x_1)$

(v) 倍点规则

令$(x_1,y_1)\in E(F_{2^m})$，其中$x_1\neq 0$。则

$2(x_1,y_1)=(x_3,y_3)$，其中

$x_3=\alpha^2+\alpha+a$, $y_3=x_1^2+(\alpha+1)x_3$, 这里$\alpha=(x_1+y_1/x_1)$

易见，群$E(F_{2^m})$为Abel群。

例：F_{2^4}上的一个椭圆曲线

$f(x)=x^4+x+1$为F_2上的一个不可约多项式，易见

$F_{2^4}=F_2[x] / (f(x)) = \{(k_0,k_1,k_2,k_3) \mid (k_0,k_1,k_2,k_3)=k_0+k_1\alpha+k_2\alpha^2+k_3\alpha^3$，　α 为**f(x)**的零点，$k_i \in F_2\}$

假定F_{2^4}上的非超奇异椭圆曲线有下述方程定义：

$y^2+xy=x^3+\alpha^4x^2+1$，注意$f(\alpha)=0$。

方程应表为：

$$(1000)y^2 + (1000)xy = (1000)x^3 + (1100)x^2 +(1000)$$

3 椭圆曲线密码体制

1985年，N. Koblitz和V. Miller分别独立提出了椭圆曲线密码体制(ECC)，其依据就是定义在椭圆曲线点的加群上的离散对数问题的难解性。

（1）知**E(F_q)**对点的“＋”运算形成一个**Abel**群.

设p∈E(F_q)，可以定义点**p**的周期: 使

p＋p ＋…… ＋ p= θ　　(共有 t个p相加）

成立的最小正整数 t,此时 t 被称为点 p的周期,记Π(p)=t。

若Q **=m·p=p** ＋ …… ＋ **p**　　(共有m个**p**相加)

定义

$m=\log_p Q$ (m为以p为底Q的对数）。

(注意,椭圆曲线上的点p生成群$E(F_q)$的t阶循环子群)，若t很大，就会使得求解$m=\log_p Q$问题在计算上难处理。

（2） 建立椭圆曲线密码体制

选取基域F_q，F_q的椭圆曲线具体给定为确定的形式。在$E(F_q)$中选一个周期很大的点，如选了一个点

$P=(x_p,y_p)$，

它的周期为一个大的正整数n，记$\Pi(P)=n$。

注意：在这个密码体制中，具体的曲线及点P和它的n都是公开信息。密码体制的形式采用ElGamal体制，是完全类比过来。

a)密钥的生成

Bob(使用者）执行了下列计算：

i) 在区间**[1,n-1]**中随机选取一个整数d。

ii) 计算点**Q:=dP** (d个P相⊕）

iii) Bob公开自己的公开密钥—— **$(E(F_q),p,n,Q)$**

iv) Bob的私钥为整数**d**！

Alice要发送消息m给Bob，Alice执行：

i) 查找Bob的公钥**$(E(F_q),p,n,Q)$**,

ii) 将m表示成一个域元素**$m \in F_q$**,

iii) 在区间**[1，n-1]**内选取一个随机数k,

iv) 依据Bob的公钥计算点 **$(x_1,y_1):=kP$**(k个P相⊕ ）

v) 计算点**$(x_2,y_2):=kQ$**,如果**$x_2=0$**,则回到第iii)步

vi) 计算$C:=m\cdot x_2$

vii) 传送加密数据(x_1,y_1,C)给Bob

b) Bob的解密过程

Bob收到Alice的密文(x_1,y_1,C)后，执行

i) 使用私钥d，计算点$(x_2，y_2):=d(x_1,y_1)$，再计算F_q中$x_2^{-1}=?$

Ii)通过计算$m:=C\cdot x_2^{-1}$，恢复出明文数据m。

4　椭圆曲线密码学中的进一步知识

（1）.椭圆曲线的同构

两个椭圆曲线是同构的，是指它们作为仿射（代数）簇是同构的。即定义在域K上的两个椭圆曲线E_1/K和E_2/K

E_1：$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$

E_2：$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$

它们在K上是同构的（$E_1/K \cong E_2/K$）是指存在$u,r,s,t \in K$，$u \neq 0$使得做变量替换（x,y）→(u^2x+r, u^3y+u^2sx+t)后，使方程E_1变换成方程E_2。

注：1°椭圆曲线的同构关系是一个等价关系。

2° 若在K上有$E_1 \cong E_2$，由上述变量替换，可将方程E_1转化为方程E_2，自然有方程系数间的关系式:

$$
\begin{cases}
u\bar{a}_1 = a_1 + 2s \\
u^2\bar{a}_2 = a_2 - sa_1 + 3r - s^2 \\
u^3\bar{a}_3 = a_3 + ra_1 + 2t \\
u^4\bar{a}_4 = a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st \\
u^6\bar{a}_6 = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1
\end{cases}
$$

有结论：

3° 在K上的两个椭圆曲线E_1/K和E_2/K是同构的$\Leftrightarrow \exists\, u,r,s,t \in K,\ u \neq 0$,使得上述关系式成立。

（2）椭圆曲线的判别式和j—不变量。

设E是用非齐次坐标形式来表示的Weierstrass方程：

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

下面定义一些量：

$$d_2= a_1^2+4a_2$$

$$d_4= 2a_4+a_1a_3$$

$$d_6= a_3^2+4a_6$$

$$d_8= a_1^2a_6+4a_2a_6 -a_1a_3 a_4 +a_2 a_3^2 -a_4^2$$

$$c_4= d_2^2-24d_4$$

$$\triangle = -d_2^2d_8-8d_4^3 -27d_6^2 + 9\, d_2d_4d_6$$

$$j(E)= c_4^3 / \triangle$$

量Δ被称为Weierstrass方程的判别式。

如果Δ ≠ 0，j(E)被称为椭圆曲线E的j不变量。

定理1，Weierstrass方程E为椭圆曲线⇔Δ ≠ 0.

定理2，如果两个椭圆曲线E_1/K和E_2/K是同构的，那么$j(E_1)=j(E_2)$。反之，若K是代数闭域，则由$j(E_1)=j(E_2)$可推出 $E_1/K \cong E_2/K$ 。

（3）当charK≠2,3时的椭圆曲线E/K，

设E/K为椭圆曲线

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

1° 若charK ≠ 2,可设

$$(x,y) \longrightarrow (x\ ,\ y-(a_1/2)\,x-a_3/2)$$

将 E/K 变换为 E′/K： $y^2=x^3+b_2x^2+b_4x+b_6$

注意，在K上有E≅E′ 。

2° 若charK ≠ 2 ,3，可设

$(x , y) \longrightarrow ((x-3b_2)/36 , y/216)$

将 E′/K 变换为 E′′/K： $y^2 = x^3+ax+b$

易见， E/K ≌ E′′/K 。

下面总是假设charK ≠ 2 ,3，于是椭圆曲线 E / K 有形式：

$y^2=x^3+ax+b$ $a,b \in K$ 。

按（2）中的公式计算：

$\triangle = -16（4a^3 +27b^{2)}$

$j(E) = -1728(4a)^3/\triangle$

由E为椭圆曲线，自然有 $\triangle \neq 0$。我们有

定理3， E_1/K: $y^2 = x^3+ax+b$ 和

E_2/K: $y^2 = x^3+ \bar{a}\, x+b$

在域K上同构$\Leftrightarrow \exists\, u \in K^*$使得

$u^4\, \bar{a} = a$, $\bar{a^6}b=b$ 。

注：在K上，若有$E_1 \cong E_2$，那么同构映射可刻画为

$\varphi: E_1 \longrightarrow E_2$　　使

$\varphi: (x, y) \longrightarrow (u^{-2}x, u^{-3}y)$　。

椭圆曲线E: $y^2 = x^3 + ax + b$ 的点的加法公式：

若 $p = (x_1, y_1) \in E$，那么 $-p = (x_1, -y_1)$

若 $Q = (x_2, y_2) \in E$, $Q \neq -p$ 那么

$p + Q = (x_3, y_2)$, 其中

$\mathbf{x_3} = \lambda^2 - x_1 - x_2$

$\mathbf{y_3} = \lambda(x_1 - x_3) - \mathbf{y_1}$

这里 $\lambda =$ $\begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{。若 } p \neq Q \\ (3x_1^2 + a)/2y_1 & \text{。若 } p = Q \end{cases}$

例子：E: $y^2=x^3+x+6$ 为定义在F_{11}上的椭圆曲线。

（因为 $\triangle = -16(4a^3+27b^2) =$

$-16(4\times 1^3+27\times 6^2)= -5(4+5\times 3)= -5\times 8=-7=4\neq 0$)

那么F_{11}上的W有理点为

E（ F_{11}）={O，（2，4），（2，7），（3，5），（3，6），

（5，2），（5，9），（7，2），（7，9），（8，3），

（8，8），（10，2），（10，9）}；利用加法公式和算法规则得

（2，4）+（2，7）= O，

（2，4）+（3，5）=（7，2） 并且

（2，4）+（2，4）=（5，9）

#

（4）charK= 2时的椭圆曲线E/K

E/K： $y^2+ \bar{a}_1xy+ \bar{a}_3y=x^3+ \bar{a}_2x^2+ \bar{a}_4x+ \bar{a}_6$

利用前述公式可算得　　$j(E)= (\bar{a}_1)^{12}/\ \triangle$

若$j(E) \neq 0$ （即 $\bar{a}_1 \neq 0$），可做替换

（x, y） ⟶ $(\bar{a}_1^2x+ \bar{a}_3/\ \bar{a}_1,\ \bar{a}_1^3y+(\bar{a}_1^2\ \bar{a}_4+ \bar{a}_3^2)/\ \bar{a}_1^3)$

将曲线E变化为曲线

E_1/K： $y^2 +xy = x^3+a_2x^2+a_6$

对此时的曲线说来，可算出 $\triangle = a_6$， $j(E_1)= 1/a_6$

若$j(E)= 0$，（即 $\bar{a}_1 = 0$），可做替换

（x, y） ⟶ $(x+ \bar{a}_2,\ y)$

将曲线E变换为曲线 E_2/K： $y^2 + a_3y = x^3+a_4x+a_6$

对此时的曲线说来，$\triangle = a_3^4$， $j(E_2)= 0$.

j(E) ≠ O 时的E的加法公式:

设$P=(x_1, y_1) \in E_1$，此时有$-P=(x_1, y_1+x_1)$

若$Q=(x_2, y_2)$ 且 $Q \neq -P$， 则$P+Q=(x_3, y_3)$ 其中

$$x_3 = \begin{cases} (y_1+y_2)^2/(x_1+x_2)^2+(y_1+y_2)/(x_1+x_2)+x_1+x_2+a_2 & P \neq Q \\ x_1^2 + a_6/x_1^2 & P = Q \end{cases}$$

$$y_3 = \begin{cases} [(y_1+y_2)/(x_1+x_2)](x_1+x_3)+x_3+y_1 & P \neq Q \\ x_1^2+(x_1+y_1/x_1)x_3+x_3 & P = Q \end{cases}$$

j(E)= O时的E的加法公式:

设P= (x_1, y_1) ∈ E_2 , 则- P= (x_1， $y_1 + a_3$ ）

再设Q=(x_2, y_2) ∈ E_2 , 并且Q ≠ - P　那么

P+Q = (x_3， y_3 ）　这里

$$X_3 = \begin{cases} (y_1 + y_2)^2/(x_1 + x_2)^2 + x_1 + x_2 & P \neq Q \\ (x_1^4 + a_4^2)/a_3^2 & P = Q \end{cases}$$

$$y_3 = \begin{cases} [(y_1 + y_2)/(x_1 + x_2)](x_1 + x_3) + y_1 + a_3 & P \neq Q \\ [(x_1^2 + a_4)/a_3](x_1 + x_3) + y_1 + a_3 & P = Q \end{cases}$$

(5)椭圆曲线的群结构

设E为定义在F_q上的椭圆曲线（$q = P^m$, P为素数）。用符号$\#E(F_q)$表示$E(F_q)$中的点数。

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

易见，$\forall x \in F_q$,E上至多对应两个解(x, y_1)，(x, y_2)

所以 $\#E(F_q) \leqslant 2q+1$ (有一个无穷远点O ） 。

我们期望，对每一次选择$x \in F_q$ ，使上述椭圆方程在F_q 中有唯一解的概率为1/2，若是这样就有 $\#E(F_q) \approx q$ 。事实上，这个结论是正确的。有

定理（Hasse). 设 $\#E(F_q) = q + 1 - t$，那么

$|t| \leqslant 2\sqrt{q}$ 。

注：Hasse 定理引出的一个重要结果是，可用概率多项式时间，从椭圆曲线$E(F_q)$上一致随机地检测出它的所有点。若随机选择$x_1 \in F_q$ ，x_1为$E(F_q)$上某点的x—坐标的概率至少为 $\frac{1}{2} - 1/\sqrt{q}$ 。

若x_1为$E(F_q)$上的点的x—坐标，那么求解y_1使得$(x_1, y_1) \in E(F_q)$是可在多项式时间内完成的。见文献：

M.BEN — OR, "Probabilistic algorithms in finite fields"

22nd Annual Symposium on Foundations of Computer Science, 394 ~ 398,1981.

定义（超奇异椭圆曲线）椭圆曲线上E被称为是超奇异的（Supersingular)是指$\#E(F_q) = q+1-t$，其中$p \mid t$ $(q = P^m)$。否则E被称为是非超奇异的（non--Supersingular)。

有重要结论：

E为F_q上的椭圆曲线，E为超奇异的充要条件为：对于$\#E(F_q) = q+1-t$中，有$t^2 = 0, q, 2q, 3q$, 或$4q$。

定理：E为超奇异的椭圆曲线，此时$\#E(F_q) = q+1-t$，有如下结果:

1°若$t^2 = q, 2q, 3q$, 那么$E(F_q)$是循环群。

2° 若$t^2=4q$, 那么$t = 2\sqrt{q}$ 时 有

$E(F_q) \cong Z_{\sqrt{q}-1} \oplus Z_{\sqrt{q}-1}$。

$t = -2\sqrt{q}$时，有 $E(F_q) \cong Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$

3° 若$t = 0$ 并且$q \neq 3(\mathrm{mod}4)$，那么$E(F_q)$ 是循环群。

若$t = 0$ 并且$q = 3(\mathrm{mod}4)$，那么或者$E(F_q)$ 是循环群，或者$E(F_q) \cong Z_{(q+1)/2} \oplus Z_2$。

椭圆曲线E也可视为域 F_q 的扩域$F_q^k = L$上的曲线。此时 $E(F_q)$ 为$E(L)$上的子群。我们有

<u>定理</u>. 设E为定义在F_q上的 一个椭圆曲线，且设 $t= q+1 - \#E(F_q)$,那么$\#E(F_q^k) = q^k +1- \alpha^k - \beta^k$ ，其中α 、β为 $x^2 - tx+q$的根。

- Koblitz, N. (1985). Elliptic curve cryptosystems. Mathematics of Computation, 48, 203-209.
- Menezes, A. and Vanstone, S. (1993). Elliptic curve cryptosystems and their implementation. Journal of Cryptology, 6, 209-224.
- Miller, S. Victor. (1985). Use of elliptic curves in cryptography. Advances in Cryptology- CRYPTO'85, 218, 417-426.