第8章椭圆曲线&第7章有限域参考答案

计算证明

1. (15分)已知 $E_{11}(1,6)$上一点 $G(2,7)$，求 $2G$ 到 $13G$ 的所有值.

解 $E_{11}(1,6):y^2=x^3+x+6 \pmod{11}$，对点 $G=(2,7)$ 有：

(1) $2G=G+G:\ k=\dfrac{3\times 2^2+1}{2\times 7}=8 \pmod{11}$

$$\begin{cases} x_3=k^2-2x_1=5 \pmod{11} \\ y_3=k(x_1-x_3)-y_1=2 \pmod{11} \end{cases}$$

$2G=(5,2)$

(2) $3G=2G+G:\ k=\dfrac{7-2}{2-5}=2 \pmod{11}$

$$\begin{cases} x_3=k^2-x_1-x_2=8 \pmod{11} \\ y_3=k(x_1-x_3)-y_1=3 \pmod{11} \end{cases}$$

$3G=(8,3)$

同理可得，$4G=(10,2)$，$5G=(3,6)$，$6G=(7,9)$，$7G=(7,2)$，$8G=(3,5)$，$9G=(10,9)$，$10G=(8,8)$，$11G=(5,9)$，$12G=(2,4)$，$13G=O$.

2. (15分)已知$E_{17}(3,1)$上一点 $Q=(15,y_Q)$，求 Q 坐标及 Q 的阶.

解 $E_{17}(3,1):y^2=x^3+3x+1 \pmod{17}$. 将 Q 代入得到: $y_Q^2=4$，解得 $y_Q=2,15 \pmod{17}$.

则 $Q=(15,2)$ 或 $Q=(15,15)$.

(1) $Q=(15,2)$:

$2Q=Q+Q:\ k=\dfrac{3\times 15^2+3}{2\times 2}=8 \pmod{17}$

$$\begin{cases} x_3=k^2-2x_1=0 \pmod{17} \\ y_3=k(x_1-x_3)-y_1=16 \pmod{17} \end{cases}$$

$2Q=(0,16)$

$3Q=2Q+Q:\ k=\dfrac{16-2}{-15}=7 \pmod{17}$

$$\begin{cases} x_3=k^2-x_1-x_2=0 \pmod{17} \\ y_3=k(x_1-x_3)-y_1=1 \pmod{17} \end{cases}$$

$3Q=(0,1)$

则 $5Q = 2Q + 3Q = O$. 易知，$4Q \neq O$. 则 $\operatorname{ord} Q = 5$.

（2）$Q = (15, 15) = -(15, 2)$，则 $\operatorname{ord} Q = 5$.

综上，$Q = (15, 2)$ 或 $Q = (15, 15)$. $\operatorname{ord} Q = 5$.

3. 由多项式 $p(x) = x^4 + x + 1$ 定义的域 $\mathbb{F}_{2^4}$，选取生成元 $g = (0010)$ (表示多项式 x)：

（1）(15分) 求 $\mathbb{F}_{2^4}$ 上椭圆曲线：$y^2 + xy = x^3 + g^4x^2 + 1$ 上的所有点；

（2）(10分) 验证 $P_1 = (g^6, g^8)$，$P_2 = (g^3, g^{13})$是椭圆曲线上的点，并求$P_1 + P_2$ 和 $2P_1$.

解 （1）由生成元 g 易得：$\mathbb{F}_{2^4} = \{0, 1, g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}, g^{13}, g^{14}\}$

$+$	0	1	g	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}	g^{11}	g^{12}	g^{13}	g^{14}
0	0	1	g	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}	g^{11}	g^{12}	g^{13}	g^{14}
1	-	0	g^4	g^8	g^{14}	g	g^{10}	g^{13}	g^9	g^2	g^7	g^5	g^{12}	g^{11}	g^6	g^3
g	-	-	0	g^5	g^9	1	g^2	g^{11}	g^{14}	g^{10}	g^3	g^8	g^6	g^{13}	g^{12}	g^7
g^2	-	-	-	0	g^6	g^{10}	g	g^3	g^{12}	1	g^{11}	g^4	g^9	g^7	g^{14}	g^{13}
g^3	-	-	-	-	0	g^7	g^{11}	g^2	g^4	g^{13}	g	g^{12}	g^5	g^{10}	g^8	1
g^4	-	-	-	-	-	0	g^8	g^{12}	g^3	g^5	g^{14}	g^2	g^{13}	g^6	g^{11}	g^9
g^5	-	-	-	-	-	-	0	g^9	g^{13}	g^4	g^6	1	g^3	g^{14}	g^7	g^{12}
g^6	-	-	-	-	-	-	-	0	g^{10}	g^{14}	g^5	g^7	g	g^4	1	g^8
g^7	-	-	-	-	-	-	-	-	0	g^{11}	1	g^6	g^8	g^2	g^5	g
g^8	-	-	-	-	-	-	-	-	-	0	g^{12}	g	g^7	g^9	g^3	g^6
g^9	-	-	-	-	-	-	-	-	-	-	0	g^{13}	g^2	g^8	g^{10}	g^4
g^{10}	-	-	-	-	-	-	-	-	-	-	-	0	g^{14}	g^3	g^9	g^{11}
g^{11}	-	-	-	-	-	-	-	-	-	-	-	-	0	1	g^4	g^{10}
g^{12}	-	-	-	-	-	-	-	-	-	-	-	-	-	0	g	g^5
g^{13}	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	g^2
g^{14}	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0

表 1: $\mathbb{F}_{2^4}$ 上的加法群表

$y^2 + xy = x^3 + g^4x^2 + 1$ 在$\mathbb{F}_{2^4}$上的所有点：

x	y	**点** (x, y)
—	—	O
0	1	$(0, 1)$
1	g^6, g^{13}	$(1, g^6), (1, g^{13})$
g	无解	—
g^2	无解	—
g^3	g^8, g^{13}	$(g^3, g^8), (g^3, g^{13})$

x	y	点 (x,y)
$g^4=g+1$	无解	—
$g^5=g^2+g$	g^3,g^{11}	$(g^5,g^3),(g^5,g^{11})$
$g^6=g^3+g^2$	g^8,g^{14}	$(g^6,g^8),(g^6,g^{14})$
$g^7=g^3+g+1$	无解	—
$g^8=g^2+1$	无解	—
$g^9=g^3+g$	g^{10},g^{13}	$(g^9,g^{10}),(g^9,g^{13})$
$g^{10}=g^2+g+1$	g,g^8	$(g^{10},g),(g^{10},g^8)$
$g^{11}=g^3+g^2+g$	无解	—
$g^{12}=g^3+g^2+g+1$	$0,g^{12}$	$(g^{12},0),(g^{12},g^{12})$
$g^{13}=g^3+g^2+1$	无解	—
$g^{14}=g^3+1$	无解	—

综上，共有16个点，分别是：O, $(0,1)$, $(1,g^6),(1,g^{13})$, $(g^3,g^8),(g^3,g^{13})$, $(g^5,g^3),(g^5,g^{11}),(g^6,g^8),(g^6,g^{14})$, $(g^9,g^{10}),(g^9,g^{13}),(g^{10},g),(g^{10},g^8),(g^{12},0),(g^{12},g^{12})$.

（2）由（1）易知，P_1, P_2均在该椭圆曲线上.

易知，$\mathbb{F}_{2^4}$上椭圆曲线方程 $y^2+xy=x^3+g^4x^2+1$ 是一般形式的Weierstrass方程 $a_1=a_6=1$, $a_3=a_4=0$, $a_2=g^4$ 的情况.

则 $\begin{cases}x_3=k^2+k+g^4+x_1+x_2\\y_3=k(x_1+x_3)+x_3+y_1\end{cases}$，$k=\begin{cases}\dfrac{y_2+y_1}{x_2+x_1}, & x_1\neq x_2\\[2ex]\dfrac{x_1^2+y_1}{x_1}, & x_1=x_2\end{cases}$

i. P_1+P_2:

$$k=\frac{g^{13}+g^8}{g^3+g^6}=\frac{g^3}{g^2}=g$$

$$\begin{cases}x_3=g^2+g+g^4+g^6+g^3=1\\y_3=g(g^6+1)+1+g^8=g^{13}\end{cases}$$

则 $P_1+P_2=(1,g^{13})$.

ii. $2P_1$:

$$k=\frac{(g^6)^2+g^8}{g^6}=\frac{g^9}{g^6}=g^3$$

$$\begin{cases}x_3=g^6+g^3+g^4+0=g^{10}\\y_3=g^3(g^6+g^{10})+g^{10}+g^8=g^8\end{cases}$$

则 $2P_1=(g^{10},g^8)$.

4.（1）(5分)求 $\mathbb{F}_2$ 上的三次本原多项式，并据此给出域 $\mathbb{F}_8$的矩阵表示;

（2）(5分)验证对其加法和乘法运算满足域结构的定义；

（3）(5分)计算 $\mathbb{F}_8$ 上所有元素的阶.

解 （1）$\mathbb{F}_2[x]$ 中三次不可约多项式有两个：$f(x)=x^3+x+1$, $g(x)=x^3+x^2+1$. 在 $\mathbb{F}_{2^3}$ 上验证可知，$\operatorname{ord} f(x)=\operatorname{ord} g(x)=7$，则 $f(x)$, $g(x)$ 均为 $\mathbb{F}_2$ 上的三次本原多项式. 可以由 $f(x)$ 得到其伴随矩阵为：

$A=\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}$，可以得到 $\mathbb{F}_8=\{0,I=A^7,A,A^2,A^3,A^4,A^5,A^6\}$. 即：

$$\mathbb{F}_8=\left\{\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix},\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix},\begin{pmatrix}0&1&0\\0&1&1\\1&0&1\end{pmatrix},\begin{pmatrix}1&0&1\\1&1&1\\0&1&1\end{pmatrix},\begin{pmatrix}0&1&1\\1&1&0\\1&1&1\end{pmatrix},\begin{pmatrix}1&1&1\\1&0&0\\1&1&0\end{pmatrix},\begin{pmatrix}1&1&0\\0&0&1\\1&0&0\end{pmatrix}\right\}$$

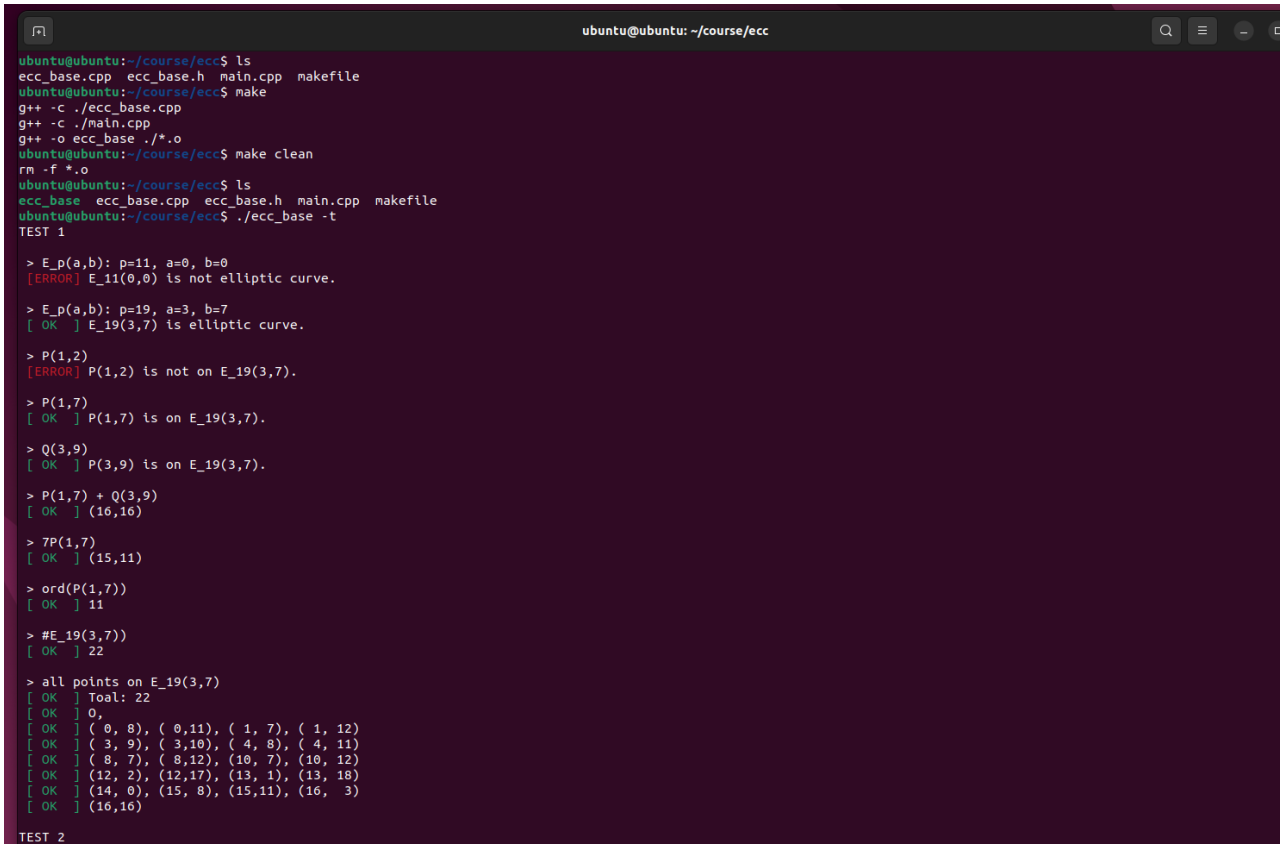
（2）略（首先验证 $\mathbb{F}_8$ 是幺环. 无零因子是应为除零元外，行列式都为1. 逆元易知. 交换需要逐次验证.）

（3）（注意这里的阶是对乘法而言）零元0的阶没有意义，对乘法运算 $\mathbb{F}_8^*$ 是循环群，则 $\operatorname{ord} I=1$，$\operatorname{ord} A=\operatorname{ord} A^2=\operatorname{ord} A^3=\operatorname{ord} A^4=\operatorname{ord} A^5=\operatorname{ord} A^6=7$.

编程练习(基于C/C++)

(30分)实现基本的 Z_p 上的椭圆曲线 $E_p(a,b)$ 的计算，平台可以是Windows/Linux/macOS，具体如下：

1. 功能要求：
   - 给定参数 p,a,b，判断 $E_p(a,b)$ 是否为椭圆曲线；
   - 判断给定的点 P,Q 是否在椭圆曲线 $E_p(a,b)$ 上；
   - 对在椭圆曲线 $E_p(a,b)$ 上的两点 P,Q，计算 $P+Q$；
   - 对在椭圆曲线 $E_p(a,b)$ 上的点 P，使用倍加-和算法计算 mP；
   - 对在椭圆曲线 $E_p(a,b)$ 上的点 P，计算阶$\operatorname{ord}(P)$；
   - 对在椭圆曲线 $E_p(a,b)$，计算阶$\#E$；
   - 对在椭圆曲线 $E_p(a,b)$，计算所有点；
   - 其他功能的进一步扩展……
2. 编程要求：
   - 不允许使用第三方的库；
   - 按照面向对象的编程思想，封装类，调用公有接口实现；
   - 符合一定的编程规范；
   - 利用之前的知识模块解耦实现：如扩展Euclid算法求逆、二次互反律求Legendre符号、群的一些基础知识等；
   - 在实现功能的基础上，尽可能提高计算的效率等.
3. 示例演示：



4. 提交要求：
   - 源码文件：*.cpp、*.h
   - PE文件：.exe等
   - 演示说明视频：<3min，包含对写好的测试样例的演示和对核心部分的讲解说明
   - 实验报告：2123456张三椭圆曲线编程练习报告.doc 或 2123456张三椭圆曲线编程练习报告.pdf