第七章

11. 给出商环 $Z_2[x]/(x^2+x+1)$ 上的加法表和乘法表，问次商环是否为域。

解题思路：$Z_2[x]/(x^2+x+1)=\{0,1,x,x+1\}$

加法表

+	**0**	**1**	**x**	**x+1**
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

乘法表

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	1	x+1
x+1	0	x+1	x+1	1

由两表可知，乘法满足交换律，有单位元，有逆元，是一个域

20. 设 $f(x)=x^3+x+1\in GF(2)[x]$，试证明模 $f(x)$ 的剩余类环 $GF(2)[x]/(f(x))$ 是域，并给出域中所有非零元的逆元。

证明：因为 f(x)是三次的，那么 f(x)可约必有一次因式。

又因为 f(0)=1, f(1)=1，故 f(x)没有一次因式，因此，f(x)不可约。

因此，$GF(2)[x]/(f(x))$ 是域。

非零元：1，x，x+1，x^2，x^2+1，x^2+x，x^2+x+1

分别用扩展欧几里得算法求出逆元：

元素	1	**x**	**x+1**	$\mathbf{x^2}$	$\mathbf{x^2+1}$	$\mathbf{x^2+x}$	$\mathbf{x^2+x+1}$
逆元	1	$\mathbf{x^2+1}$	$\mathbf{x^2+x}$	$\mathbf{x^2+x+1}$	**x**	**x+1**	$\mathbf{x^2}$

例如，x^2+x+1 的逆元求解过程如下：

由

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

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

知

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

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

$$=(x^2+x+1)+(x+1)[(x^3+x+1)+(x+1)(x^2+x+1)]$$

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

故$(x^2+x+1)^{-1}=x^2$

第八章

3. 椭圆曲线 E_{11}（1,6）表示 $y^2\equiv x^3+x+6 \bmod 11$，求其上所有点。

二次剩余：

y	0	1	2	3	4	5	6	7	8	9	10
y^2	0	1	4	9	5	3	3	5	9	3	1

x	0	1	2	3	4	5	6	7	8	9	10
x^3+x+6	6	8	5	3	8	4	8	2	9	7	4
y			3 7	5 6		2			3 8		2

故椭圆曲线所有的点为：{（2，3），（2，7），（3，5），（3，6），（5，2），（8，3），（8，8），（10，2）}

4. 已知点 G=（2,7）在椭圆曲线 E_{11}（1,6）上，求 2G 和 3G

解题思路：椭圆曲线 E_{11}（1,6）表示 $y^2\equiv x^3+x+6 \bmod 11$

G=（2,7）　　所以 2G=（2,7）+（2,7）

$\lambda_3=\dfrac{3\times 2^2+1}{2\times 7}\bmod 11=8\bmod 11$　所以α=$7-8\times 2\bmod 11=2\bmod 11$

故 $x_3=8^2-2-2\bmod 11=5$　$y_3=-8\times 5-2\bmod 11=2$

所以 2G=（5,2）

3G=2G+G=（5,2）+（2,7）

所以 $\lambda_4=\dfrac{7-2}{2-5}\bmod 11=2\bmod 11$　$\alpha=7-2\times 2\bmod 11=3\bmod 11$

故 $x_4=2^2-5-2\bmod 11=8$　$y_4=-2\times 8-3\bmod 11=3$

所以 3G=（8,3）

5. 写出 GF（7）上椭圆曲线 E：$y^2=x^3-2$所有的点，计算曲线 E 上（3,2）+（5,5）的和，计算曲线 E 上（3,2）+（3,2）的和。

解题思路：椭圆曲线 E 所有的点是：{（3,2），（3,5），（6,2），（6,5），（5,2），（5,5）}

① 计算（3,2）+（5,5）

$$\lambda_3=\frac{y_2-y_2}{x_2-x_1}=\frac{5\text{-}2}{5\text{-}3}\bmod 7=5\bmod 7 \qquad \alpha_3=y_1-\lambda_1\times x_1 \bmod 7=2-5\times 3\bmod 7=1\bmod 7$$

$$x_3=\lambda_3^2-x_1-x_2 \bmod 7=3 \quad y_3=-\lambda_3 x_3-\alpha_3=5$$

故（3, 2）+（5, 5）=（3, 5）

② 计算（3, 2）+（3, 2）

$$\lambda_4=\frac{3x_1^2}{2y_1}=\frac{3\times 3^2}{2\times 2}\bmod 7=5\bmod 7 \quad \alpha_4=y_1-\lambda_4 x_1=1\bmod 7$$

$$x_4=\lambda_4^2-x_1-x_2=5^2-3-3\bmod 7=5 \quad y_4=-\lambda_4 x_4-\alpha_4=2$$

故（3, 2）+（3, 2）=（5, 2）