密码学作业005 学号 20131910023 姓名 金洋

椭圆曲线与密码学问题  
1. 任取平面上的一条三次曲线, 是否构成椭圆曲线?

答：否。椭圆曲线对三次曲线的系数、判别式都有要求；

2. 写出椭圆曲线的标准形式。

答：，其中；

3. 任取有限域GF(23)上的一条椭圆曲线，计算其上的全部有理点。

答：

列表如下

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| x3+x+1 | 3 | 11 | 8 | 0 | 16 | 16 | 6 | 15 | 3 | 22 | 9 | 16 | 3 | 22 | 10 | 19 | 9 | 9 | 2 | 17 | 14 | 22 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| y^2 | 1 | 4 | 9 | 16 | 2 | 13 | 3 | 18 | 12 | 8 | 6 | 6 | 8 | 12 | 18 | 3 | 13 | 2 | 16 | 9 | 4 | 1 |

得有理点：

(1,7) (1,16) (3,10) (3,13) (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)

4. 一条光滑曲线应该满足什么条件？

答：从参数角度，若和在[,]上连续，且+在不等于零，则由参数方程确定的曲线为光滑曲线。

5. 椭圆曲线上有无穷远点.

答：按照定义的加法，若相加的两点纵坐标相反（记为P和P'），此时在曲线上直接寻找无法找到相加的和所对应的那一点，所以我们人为地创造一点“无穷远点”，所以有PP’=O;

6. x^3+Ax+B=0 的根的互异性的充分必要条件是什么?予以证明.

答：x^3+Ax+B=0的三根互异

不妨设x^3+Ax+B=0的三根为

又f(x)=x^3+Ax+B=0的三根互异f(x)没有重因式f(x)与f’(x)没有公因式



（1）当A，B均不为0时：

利用辗转相除法：

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

f(x)与f’(x)没有公因式0

（2）当A=0，三根相同，这种情况不满足，所以应保证A不为0；

当A不为0，B为0，至少两根相同，所以A，B都不能为0；

1. 任取椭圆曲线上的两个有理点作一条直线, 证明这条直线与椭圆曲线的第三个交点也是有理点.

答：设和是EC上的有理点（即），以下证明第三点仍然是有理点。

直线可以表示为

当直线为割线时

当直线为切线时，根据，得

所以 

联立得

所以得

所以

特别的，当P、Q关于x轴对称，相加的第三点记为无穷远点（也是有理点）；

综上直线与椭圆曲线的第三个交点也是有理点；

8. 简述二元运算的定义.

答：设A是非空集合，则A×A到A的任一映射f，成为A上的二元运算；

9. 简述椭圆曲线的有理点集上能够定义二元运算的理由.

答：椭圆曲线上任意两个有理点得到第三点，第三点是唯一且确定的，因此这是一种映射；

此外，有理点集是非空的，由7的证明可知，这里的加法对于有理点集是封闭的；

综上椭圆曲线的有理点集上能够定义二元运算。

10. 给出上述二元运算的仿射坐标表示.

令

①P+O=P;

②对于P=(x,y)≠O，-P=(x,x+y);

③



其中，并满足

当时，令，则

当时，；