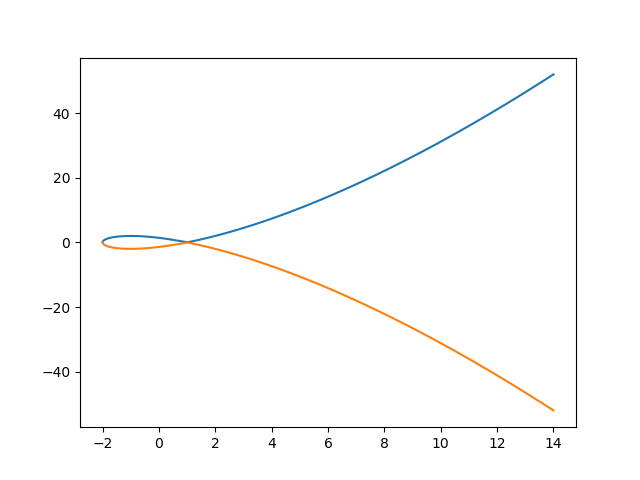
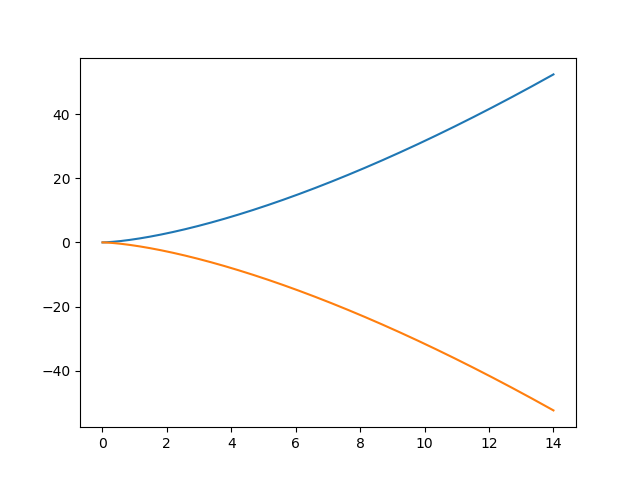
椭圆曲线定义：

a

当4a^3+27b^2=0时:



a = -3,b=2时在(1,0)点出无法计算切线



a = 0, b = 0时,在0,0点无法计算切线

## 群

* **闭包**。如果a和b都是G的元素，那a+b都是G元素
* **组合性**。(a+b)+c=a+(b+c)
* **单位元**。存在确切的一个值，称之为单位元，0可以保证该等式成立 a+0=0+a=a
* **逆元**。每个成员都有一个相反数：对于任意值a必定存在b使得a+b=0

如果加上第五条这要求：

* **交换性**a+b=b+a

这样的群我们称之为 [阿贝尔群](https://link.jianshu.com?t=https://zh.wikipedia.org/wiki/%E9%98%BF%E8%B2%9D%E7%88%BE%E7%BE%A4" \t "_blank)。

# 椭圆曲线上的群:

a

逆元的定义:

(x,y)的逆元为(x,-y)，因为椭圆曲线为x轴对称的图形，所以(x,-y)一定存在

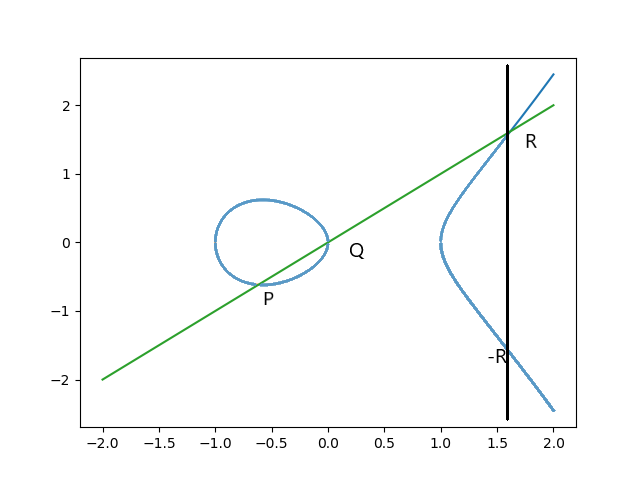
加法的定义:

P+Q为:点P点Q形成直线与椭圆曲线的交点的逆元

注:如果P=Q，则为过P点切线的交点的逆元

P+Q+R=0

P+Q=-R



单位元:

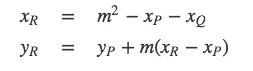
无穷远点为单位元

公式:

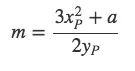
785822-e9777c7fcafca805_看图王785822-fed9da41ba13d3e4_看图王

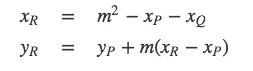
P不等于Q的情况:

785822-64d2f81fa9a952f8_看图王



P等于Q的场景：

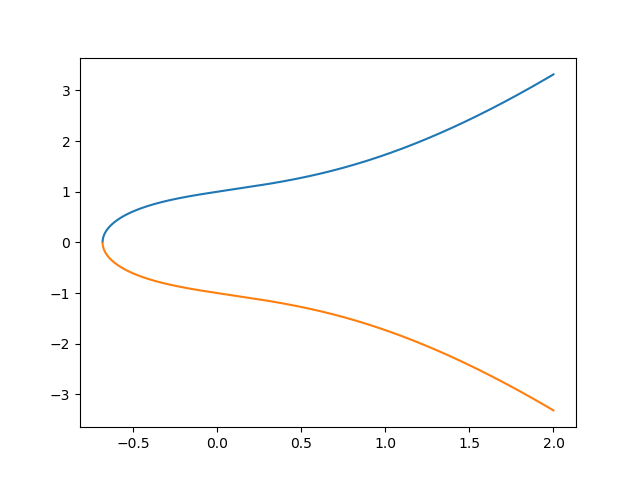




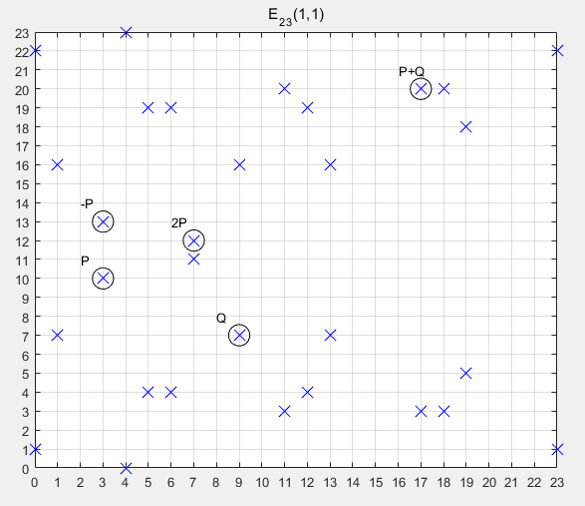
# 有限域的情形:

加法：a+b=a+b%p

乘法：a\*b=a\*b%p



a = 1 ,b = 1



y^2 = x^3+x^2+1

例:

(0,1),(0,22):

x:0 y^2 = 1

当y=1时:

1^2 % 23=1

当y=22时:

22^2 % 23 = 484 %23 = 1

x与x^2

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

