**椭圆曲线密码学简介**

目录

[**椭圆曲线密码学简介** 1](#_Toc100910712)

[实数域的椭圆曲线及其群运算规则 1](#_Toc100910713)

[椭圆曲线（Elliptic Curves） 2](#_Toc100910714)

[群论（Groups） 4](#_Toc100910715)

[椭圆曲线的群法则（The group law for elliptic cirves） 4](#_Toc100910716)

[几何加法（Geometric addition） 6](#_Toc100910717)

[代数加法（Algebraic addition） 8](#_Toc100910718)

[标量乘法（Scalar multiplication） 10](#_Toc100910719)

[对数（Logarithm） 11](#_Toc100910720)

[有限域的椭圆曲线及离散对数问题 11](#_Toc100910721)

[模p的整数域（The field of integers modulo p） 12](#_Toc100910722)

[模p除法（Division modulo p） 12](#_Toc100910723)

[点加法（Point addition） 15](#_Toc100910724)

[代数加法（Algebraic sum） 16](#_Toc100910725)

[椭圆曲线群的阶（The order of an elliptic curve group） 16](#_Toc100910726)

[ECDH加密算法和ECDSA数字签名 16](#_Toc100910727)

[领域参数（Domain parameters） 17](#_Toc100910728)

[随机曲线（Random curves） 18](#_Toc100910729)

[椭圆曲线密码学（Elliptic Curve Cryptography） 19](#_Toc100910730)

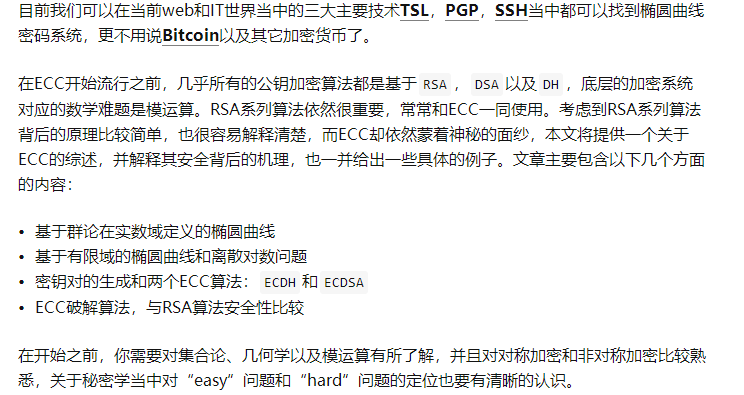
[ECDH加密算法（Encryption with ECDH） 20](#_Toc100910731)

[ECDHE 21](#_Toc100910732)

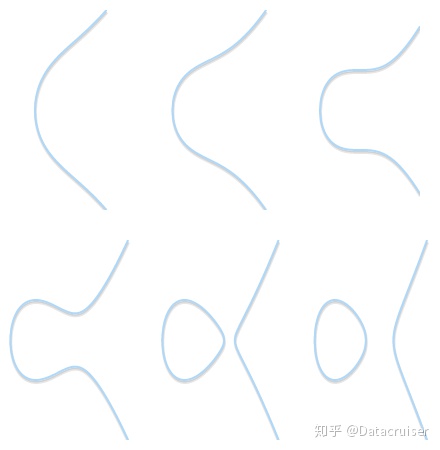
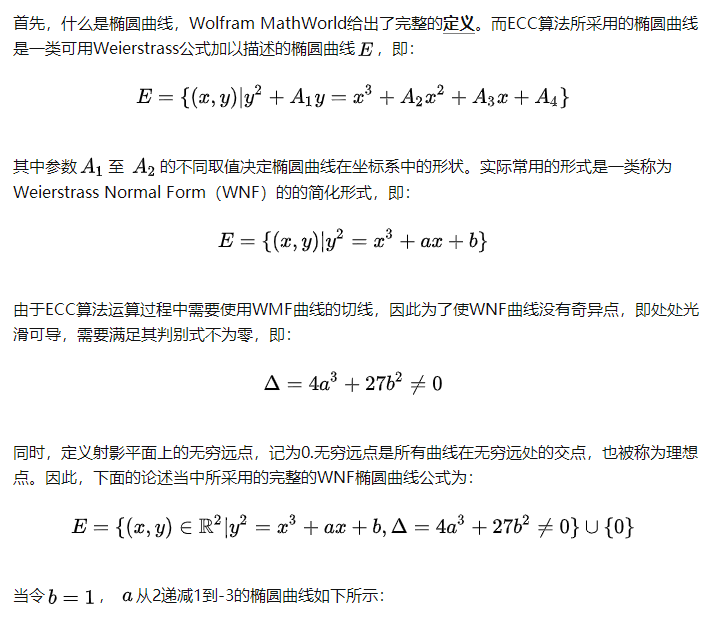
[ECDSA数字签名算法（Signing with ECDSA） 22](#_Toc100910733)

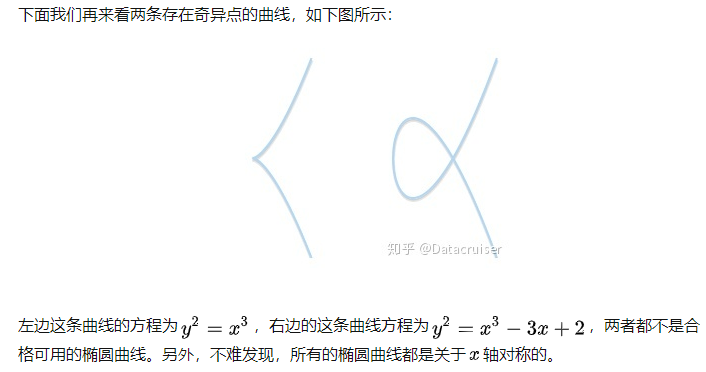
# 实数域的椭圆曲线及其群运算规则

<https://zhuanlan.zhihu.com/p/102807398>

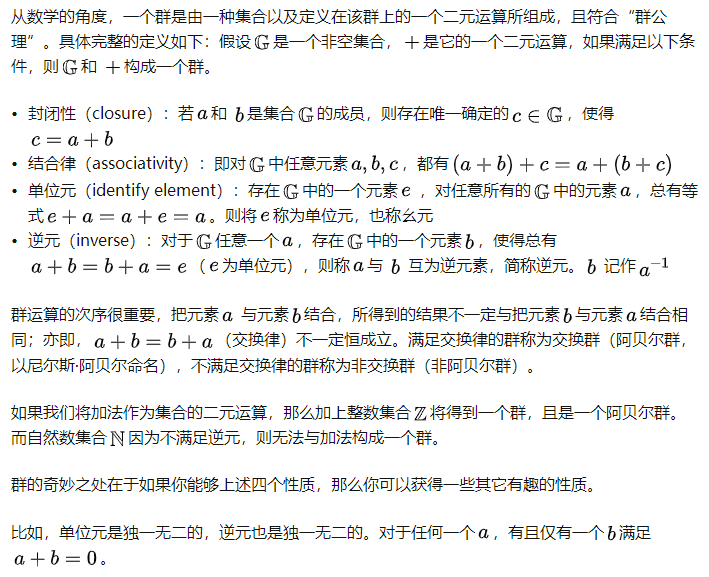


## 椭圆曲线（Elliptic Curves）

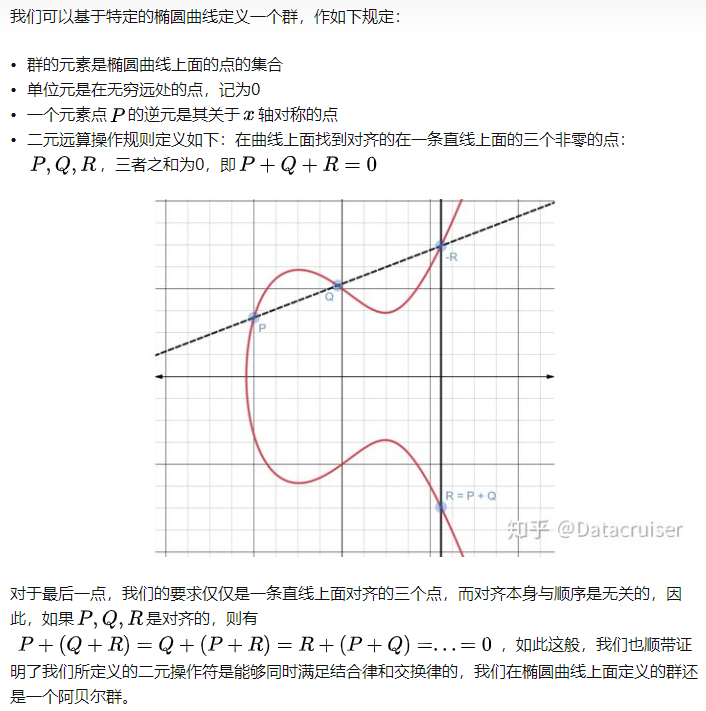




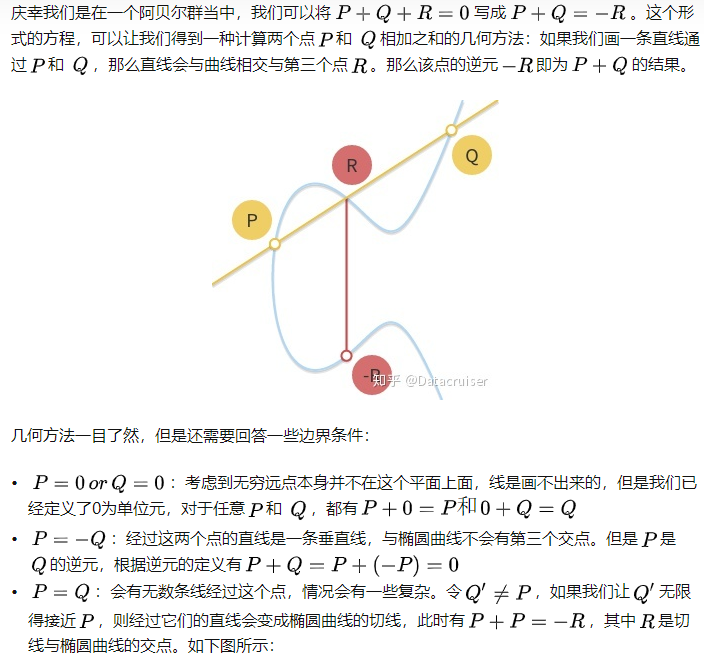
## 群论（Groups）

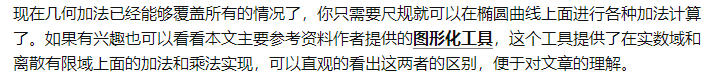
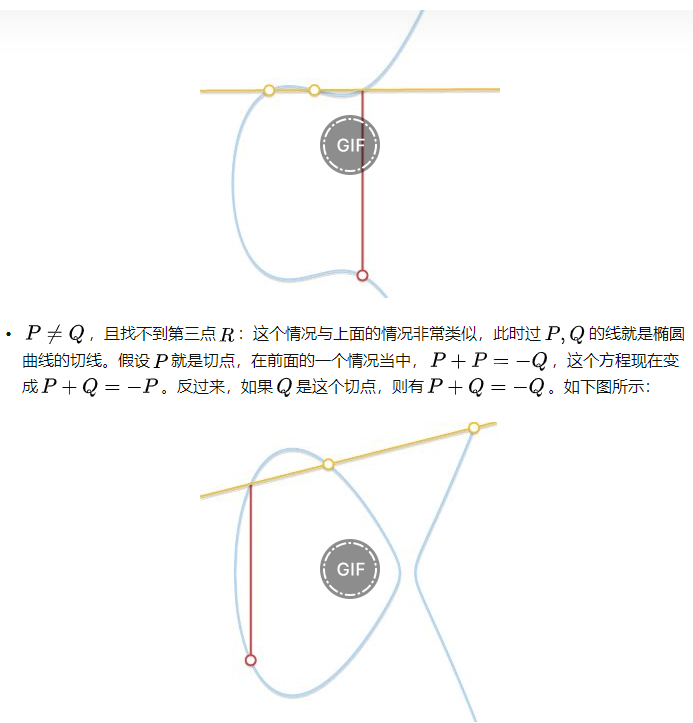


## 椭圆曲线的群法则（The group law for elliptic cirves）

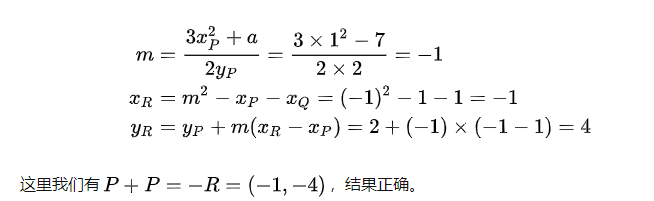
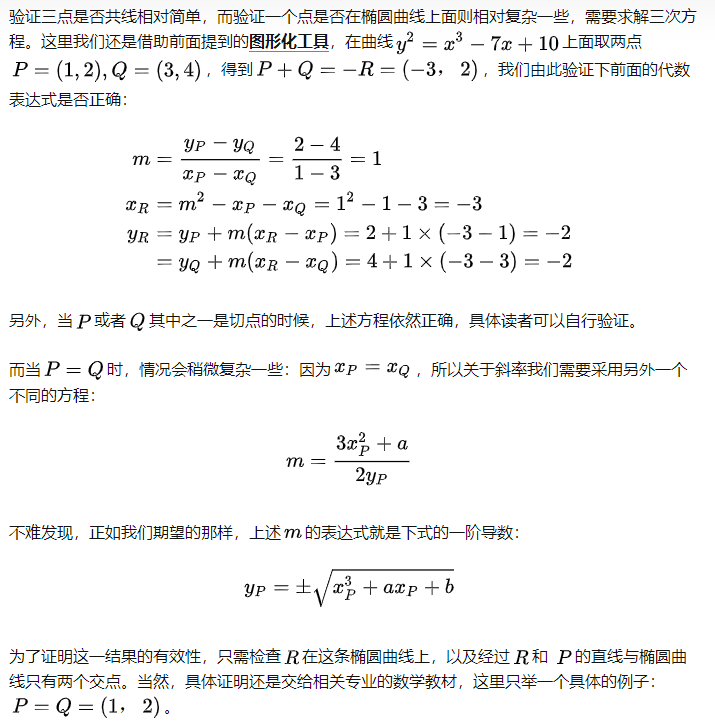
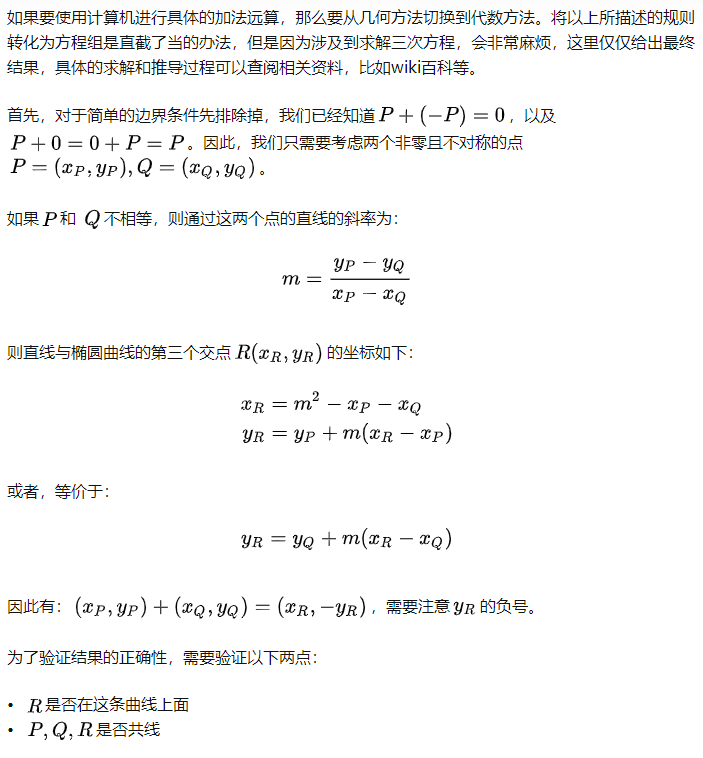


## 几何加法（Geometric addition）

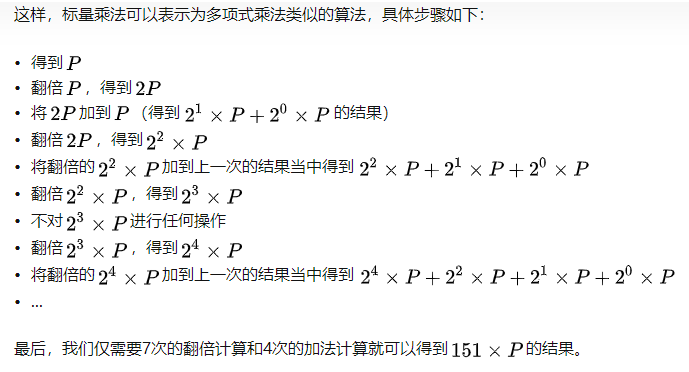
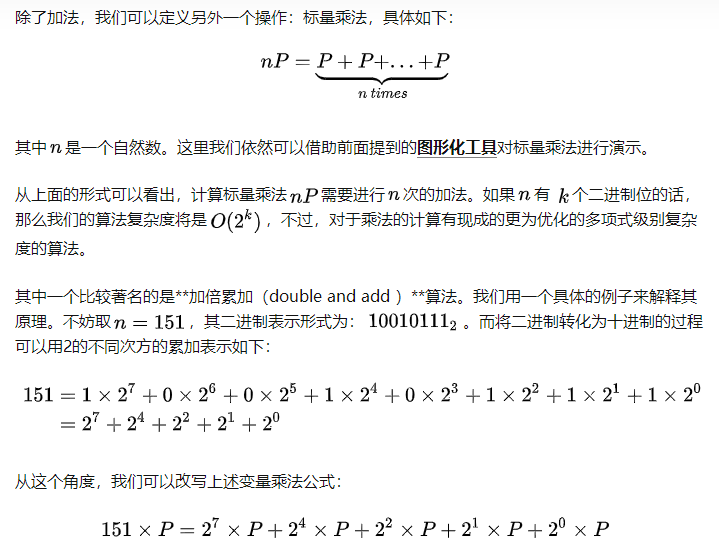




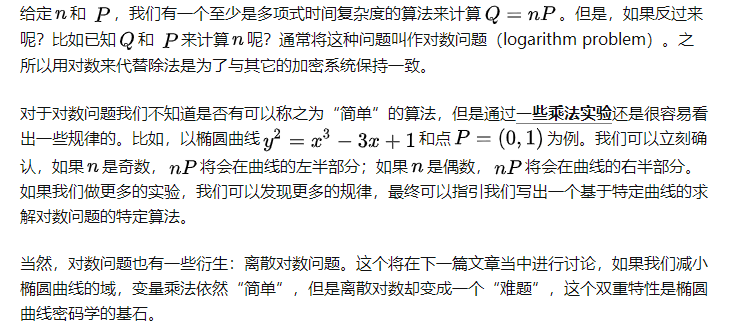
## 代数加法（Algebraic addition）



## 标量乘法（Scalar multiplication）

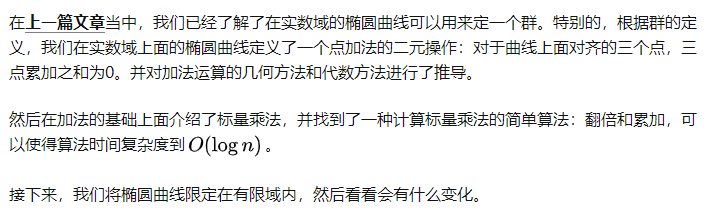


## 对数（Logarithm）

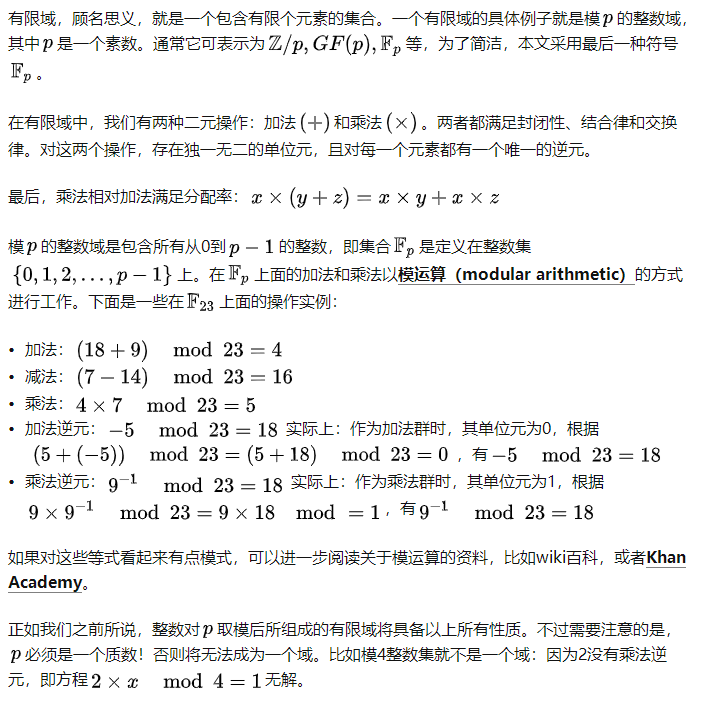


# 有限域的椭圆曲线及离散对数问题

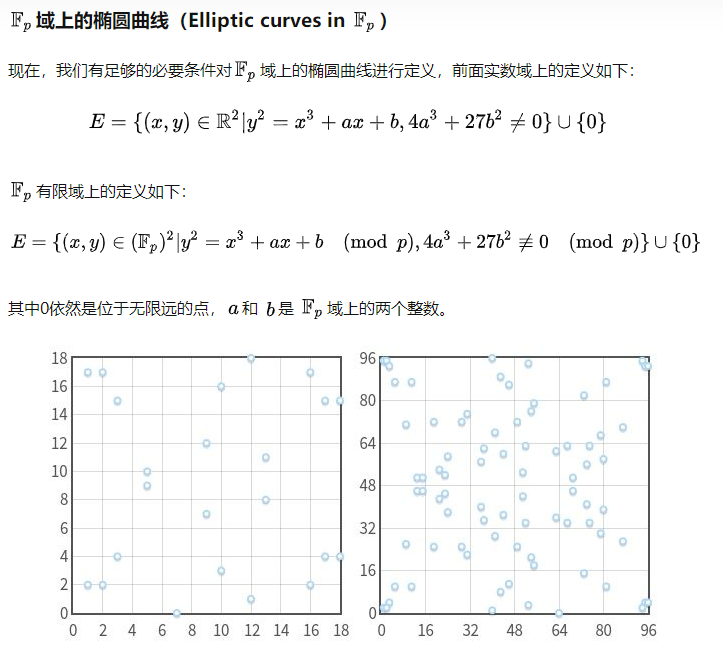
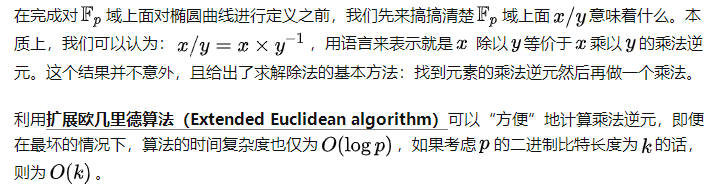
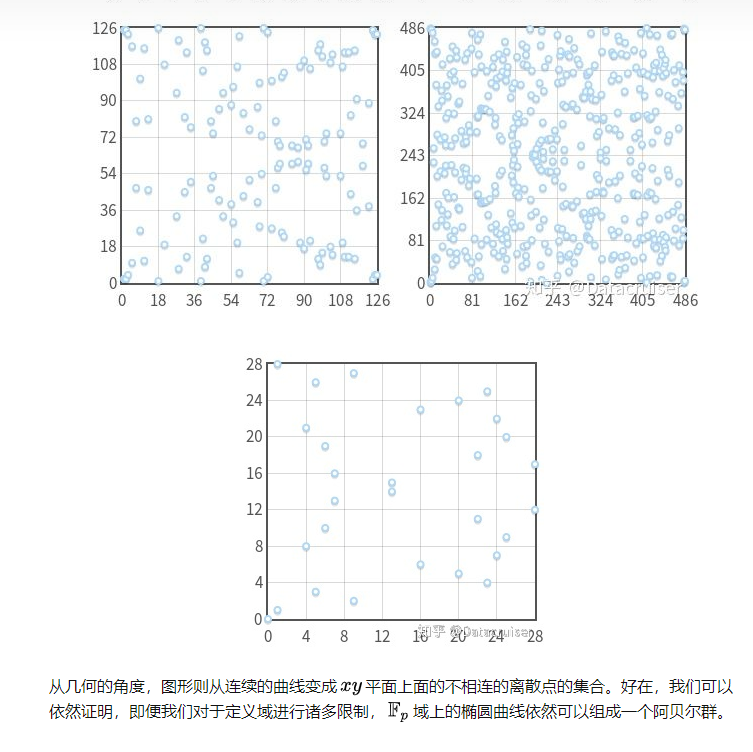
<https://zhuanlan.zhihu.com/p/104531745>



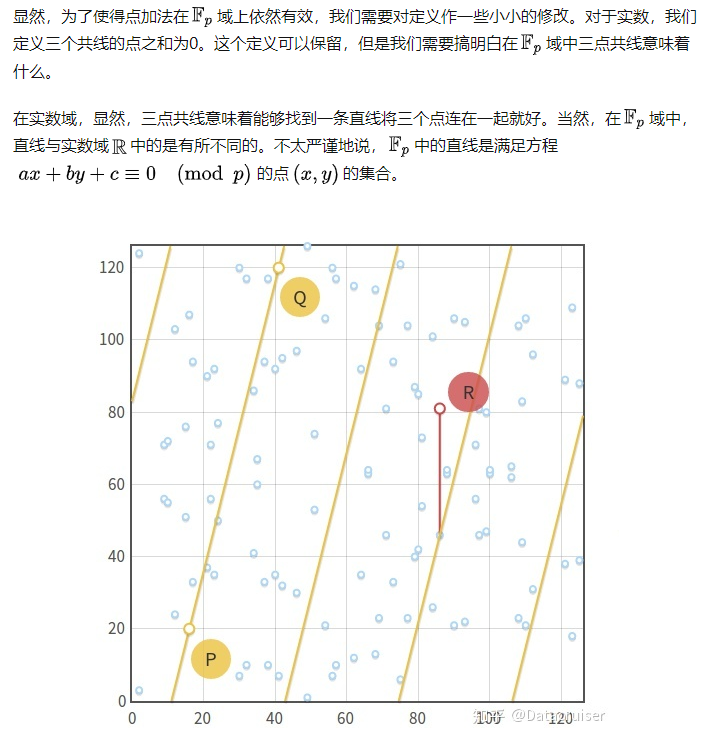
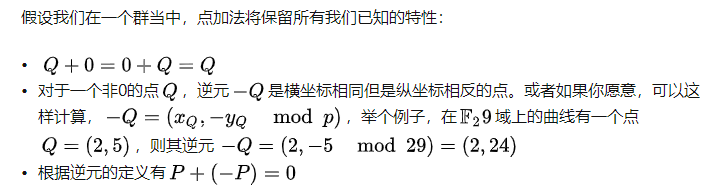
## 模p的整数域（The field of integers modulo p）



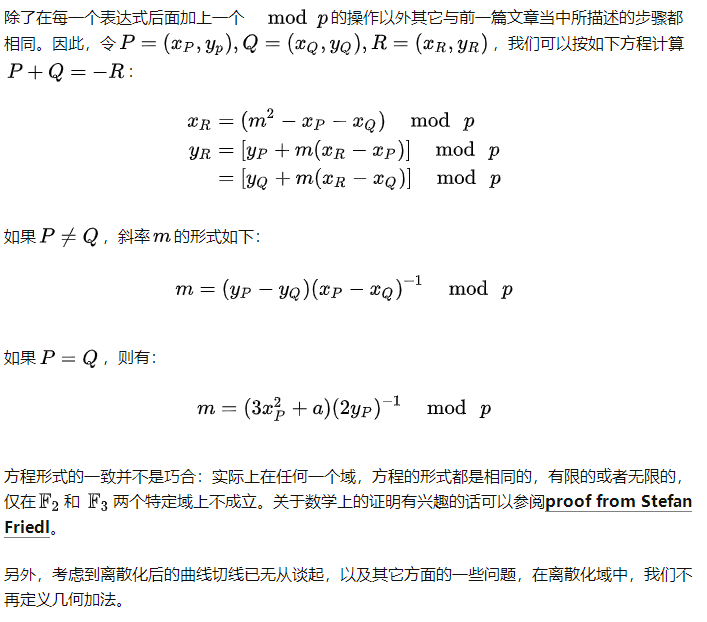
## 模p除法（Division modulo p）

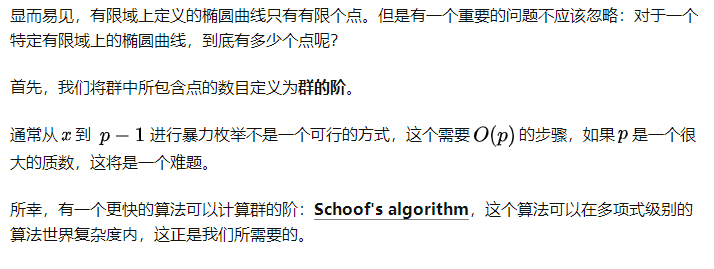
## 点加法（Point addition）

## 代数加法（Algebraic sum）



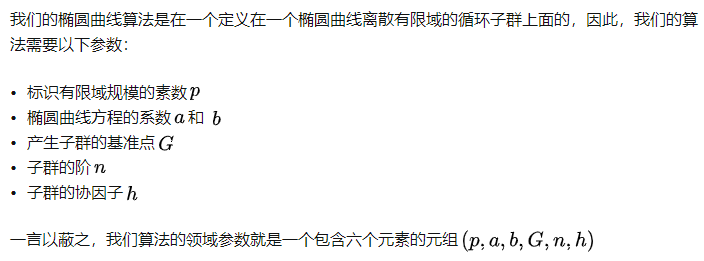
## 椭圆曲线群的阶（The order of an elliptic curve group）

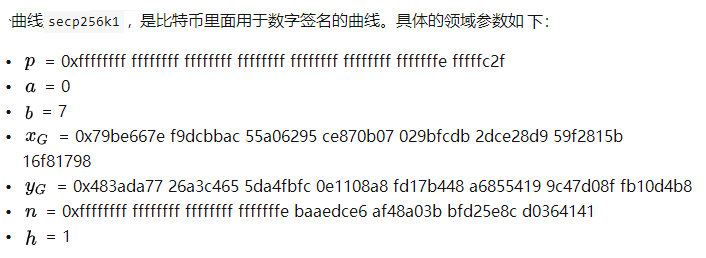


# ECDH加密算法和ECDSA数字签名

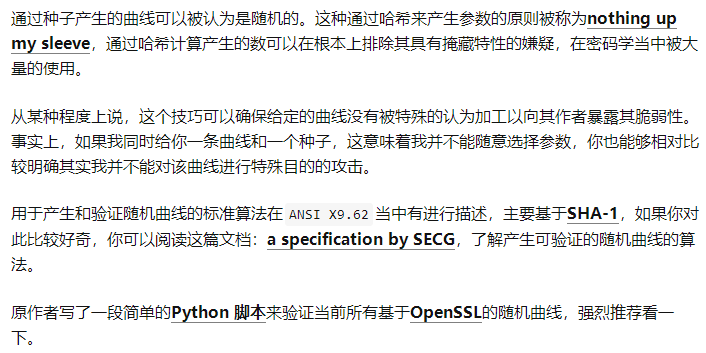
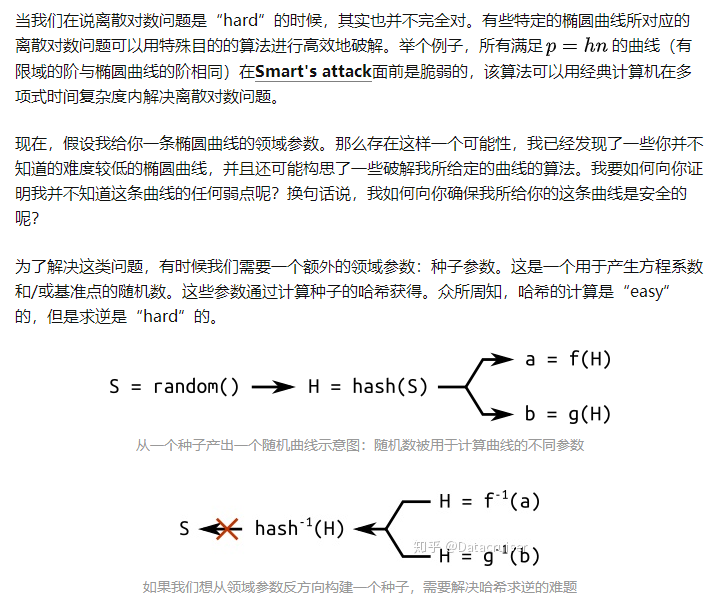
<https://zhuanlan.zhihu.com/p/107599962>

## 领域参数（Domain parameters）

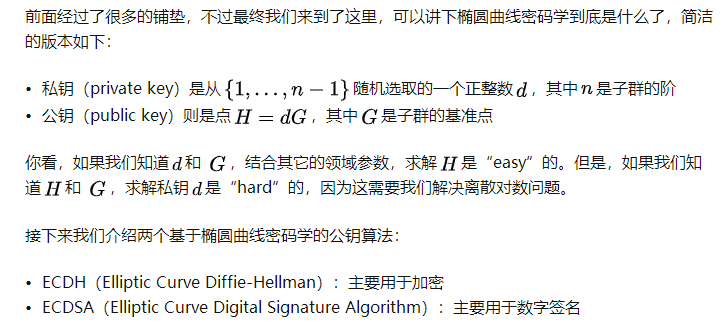




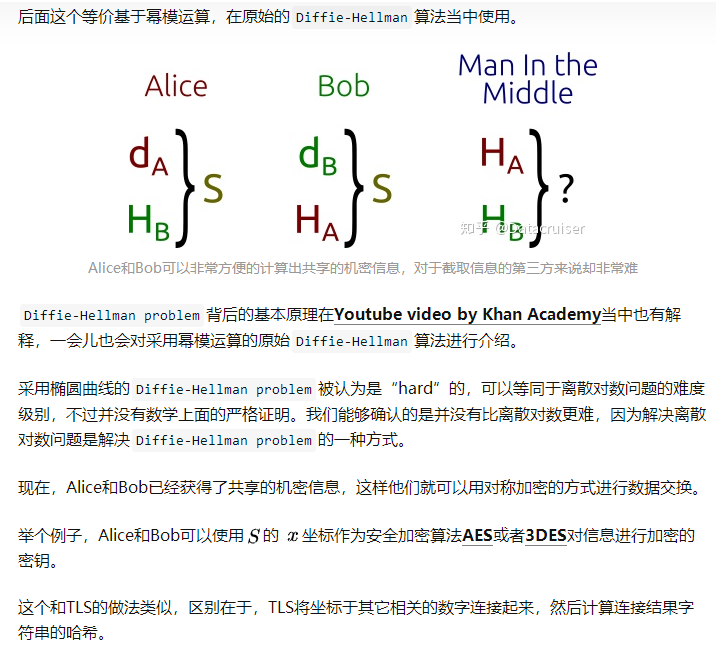
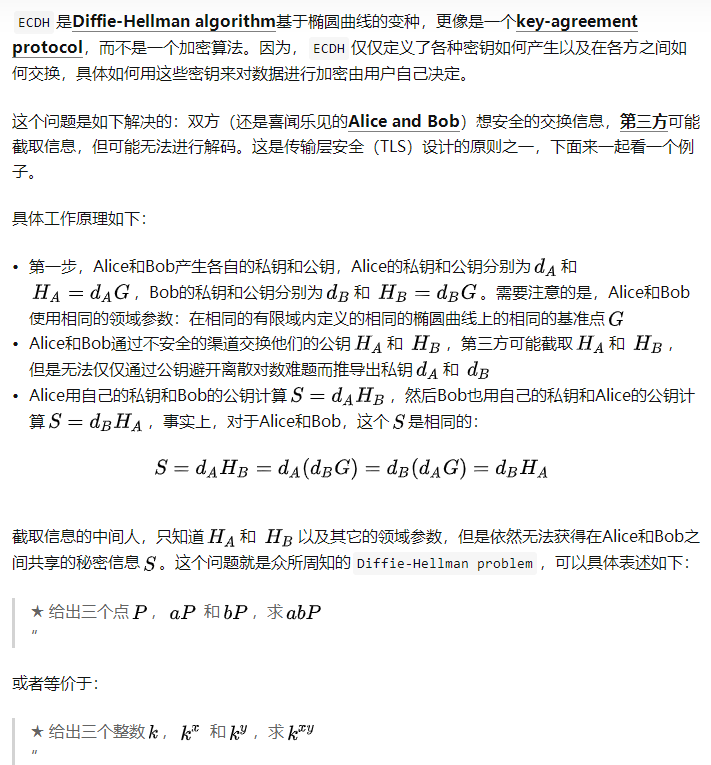
## 随机曲线（Random curves）



## 椭圆曲线密码学（Elliptic Curve Cryptography）

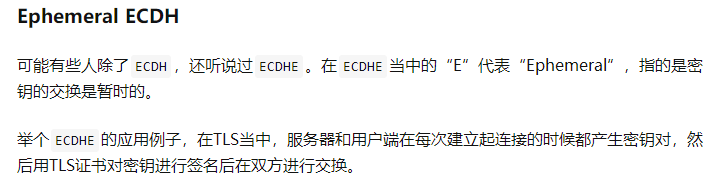


## ECDH加密算法（Encryption with ECDH）



## ECDHE

每次交互都使用临时密钥对



## ECDSA数字签名算法（Signing with ECDSA）

