

CRYPTO入门之“乘法逆元”在CTF中的应用（1）

原创

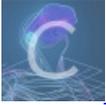
laugholy 于 2021-01-06 20:28:12 发布 123 收藏

分类专栏: [笔记](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_45986910/article/details/112295603

版权



[笔记 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

乘法逆元的概念和解法（好好学离散数学）

乘法逆元: 是指数学领域群G中任意一个元素a, 都在G中有唯一的逆元a', 具有性质 $a \times a' = a' \times a = e$, 其中e为该群的单位元。

简单说就是x满足于 $ax \equiv 1 \pmod f$ 的最小整数, 称x是模f的乘法逆元。

回顾下离散数学(忘得差不多了) $a \equiv b \pmod c$ 指的是 $|a-b|$ 可以被c整除, eg:

$90 \equiv 0 \pmod{10}$ 因为 $90-0=90$ 可以被10整除。

同余式, 也就是包含 \equiv 的等价式, 有以下性质:

- 1.反身性: $a \equiv a \pmod m, a \equiv a \pmod m$;
- 2.对称性: $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m, a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$;
- 3.传递性: $a \equiv b \pmod m, b \equiv c \pmod m \Rightarrow a \equiv c \pmod m, a \equiv b \pmod m, b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$;
- 4.相加: $a \equiv b \pmod m, c \equiv d \pmod m \Rightarrow a \pm c \equiv b \pm d \pmod m, a \equiv b \pmod m, c \equiv d \pmod m \Rightarrow a \pm c \equiv b \pm d \pmod m$;
- 5.相乘: $a \equiv b \pmod m, c \equiv d \pmod m \Rightarrow a \times c \equiv b \times d \pmod m, a \equiv b \pmod m, c \equiv d \pmod m \Rightarrow a \times c \equiv b \times d \pmod m$;
- 6.除法: $ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod{m \div \gcd(m,c)}, ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod{m \div \gcd(m,c)}$;
- 7.幂运算: $a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m, a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$ 。

如何解乘法逆元呢

费马小定理:

对于质数p, 当a是一个与p互质的整数时有: $a^{p-1} \equiv 1 \pmod p$

即可化为 $a \cdot a^{p-2} \equiv 1 \pmod p$

貌似可以看出来了! a、p如果是互质的质数, 那么a的乘法逆元就是 $a^{p-2} \pmod p$, $\pmod p$ 的原因就是要求最小的整数。

扩展欧几里得:

基本算法: 对于不完全为0的非负整数a, b, $\gcd(a, b)$ 表示a, b的最大公约数, 必然存在整数对x, y, 使得 $\gcd(a, b) = ax + by$ 。

对比一下 $ax \equiv 1 \pmod p$ 可以化成 $ax - kp = 1$ (k为整数), 令 $k = -k$, 且a, p互质, 那么就可用上扩展欧几里得了。

算法链接: <https://www.cnblogs.com/wkfvawl/p/9350867.html>