

python中国余数定理_CTF现代密码

原创

[weixin_39994296](#) 于 2020-12-20 10:52:25 发布 172 收藏

文章标签: [python中国余数定理](#)

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_39994296/article/details/111725679

版权

原标题: CTF现代密码

前言:

在CTF的密码题目中, RSA以其加密算法之多且应用之广泛, 所以在比赛中是最常见的题目。学习密码学并不难, 但首先得打好数学基础, 并在攻破密码的学习之路上持之以恒。今天我们就来打开RSA加密世界的第一扇门。

数论基础:

- 1.素数
- 2.公约数与公倍数
- 3.欧拉函数
- 4.欧几里得算法
- 5.扩展欧几里得算法
- 6.同余
- 7.模运算
- 8.逆
- 9.中国剩余定理
- 10.逆元与同余式定理

1.素数:

定义:

一个大于1的自然数, 除了1和它本身外, 不能被其他自然数整除(除0以外)的数称之为素数(质数); 否则称为合数。

如:

$3 \times 4 = 12$, 不是素数。

11除了等于 11×1 以外, 不能表示为其它任何两个整数的乘积, 所以11是一个素数。

关于素数有以下事实:

(1)如果 p 是素数, 且 $p \mid ab$ (表示 ab 能被 p 整除), 则 $p \mid a$ 或 $p \mid b$, 即 p 至少整除 a 与 b 中的一个。

(2)(算术基本定理)每个整数 $n \geq 2$,均可分解成素数幂之积:

$n =$

若不计因数的顺序,这个分解式是唯一的。其中 $k \geq 1$, $(1 \leq k)$ 是两两互不相同的素数, $(1 \leq k)$ 是正整数。

(3)素数有无穷多个。

2.最大公约数与最小公倍数

定义1:

设,是两个整数。如果 $d |$ 且 $d |$, 那么d就称为是和的公约数(或公因数)我们把和的公约数中最大的称为和的最大公约数,记作 $\gcd(,)$ 。

当 $\gcd(,) = 1$ 时,我们称和是互素的。

定义2:

设,是两个整数。如果 $|$ 且 $|$, 那么就称为是和的公倍数。我们把和的正的公倍数中的最小的称为和的最小公倍数,记作。

3.欧拉函数

定义:

对正整数 n ,欧拉函数是小于或等于 n 的数中与 n 互质的数的个数,

记作: $\varphi(n)$ 。

例如: $\varphi(8) = 4$,因为1, 3, 5, 7均与8互质。

性质:

(1)若 n 为一素数 P ,则: $\varphi(P) = P-1$

(2)如果 P 是素数, $k \geq 1$ 则: $\varphi(P^k) = (P-1) \times P^{k-1}$

例如: 求 $\varphi(16)$,由于 $16 = 2 \times 2 \times 2 \times 2$,故 $\varphi(16) = (2-1) \times 16 = 8$

(3)若 n 为任意两个互质的数 a, b 的积,则: $\varphi(a \times b) = \varphi(a) \times \varphi(b)$

例: 求 $\varphi(40)$,由于 $40 = 5 \times 8$,所以 $\varphi(40) = \varphi(5) \times \varphi(8) = 4 \times 4 = 16$

(4)对于整数 $n \geq 2$,根据算术基本定理, n 可以分解成唯一的形如 $n = p_1^{k_1} \times p_2^{k_2} \times \dots \times p_r^{k_r}$ 的分解式,则: $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})$

4.欧几里得(Euclid)算法

欧几里得算法又称为辗转相除法,用于求两个数的最大公约数。

原理: $\text{GCD}(x, y) = \text{GCD}(y, x \bmod y)$, $x > y$

1.python

代码实现

2.python第三方库:

```
gmpy2.gcd(a,b) #
```

求a,b的最大公约数

5. 扩展欧几里得算法

定义:

在已知 x, y 时, 求解一组解 a, b , 使得 $ax+by = \text{GCD}(x, y)$

算法输入: 两个正整数 x 和 y

算法输出: x 和 y 的最大公因数 $\text{gcd}(x, y)$ 及满足等式 $ax+by=\text{gcd}(x, y)$ 的整数 a 和 b

python代码实现:

gmpy2

库函数 $\text{gcdext}()$

6. 同余

定义:

设 a, b 是整数, $n \neq 0$, 如果 $n|(a-b)$, 则称 a 和 b 模 n 同余, 记为 $a \equiv b \pmod{n}$, 整数 n 称为模数。

由于 $n|(a-b)$ 等价于 $-n|(a-b)$, 所以 $a \equiv b \pmod{n}$ 与 $a \equiv b \pmod{-n}$ 等价。因此, 一般我们总假定模数 $n \geq 1$ 。

同余的性质

性质1:

自反性: $a \equiv a \pmod{m}$

对称性: $a \equiv b \pmod{m}, \leftrightarrow b \equiv c \pmod{m} \leftrightarrow a \equiv c \pmod{m}$

性质2:

(1)若 $a \equiv b \pmod{m}, c \equiv d \pmod{m}$

则: $a \pm c \equiv b \pm d \pmod{m}, ac \equiv bd \pmod{m}$

特别的, 对于一个整数 e , 都有 $a \pm e \equiv b \pm e \pmod{m}, ae \equiv be \pmod{m}$

(2)若 $a \equiv b \pmod{m}, k > 0$, 则 $ak \equiv bk \pmod{mk}$

(3)若 $a \equiv b \pmod{m}$, d 是 a, b 的公因数, 则 \equiv

(4)若 $a \equiv b \pmod{m}, d|m, d > 0$, 则: $a \equiv b \pmod{d}$

(5)若 $a \equiv b \pmod{m}$, 则:

(6) $(a \times b) \pmod{m} = (a \pmod{m} \times b \pmod{m}) \pmod{m}$

(7) $\pmod{m} = \pmod{m}$

7. 模运算

定义:

a 模 n 的运算给出了 a 对模 n 的余数, 这种运算称为模运算。注意: 模运算的结果是从0到 $n-1$ 的一个整数。

模运算就像普通的运算一样，它是可交换、可结合、可分配的。而且，对每一个中间结果进行模 m 运算后再进行模 m 运算，其作用与先进行全部运算，然后再进行模 m 运算所得到的结果是一样的。例如：

$$(a+b)\bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$(a-b)\bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$$

$$(a \times b)\bmod m = ((a \bmod m) \times (b \bmod m)) \bmod m$$

$$(a \times (b+c))\bmod m = ((a \times b) \bmod m + (a \times c) \bmod m) \bmod m$$

这些性质对于密码学中的数学计算非常的重要，模运算可以将所有中间结果和最后结果限制在一个范围内。对于一个 k 位的模数 n ，任何、加、减、乘的中间结果将不会超过 $2k$ 位长，这样避免了巨大的中间结果，使得计算机能够有效的处理数据。

如：计算 $(a^7) \bmod n$ ，不要直接进行7次乘法和一个大数的模运算：

$$(a \times a \times a \times a \times a \times a \times a) \bmod n$$

相反，应该进行三次比较小的乘法和三次比较小的模化简：

这样就可以避免巨大的中间结果出现。

8.逆

定义：

若 $m \geq 1$ ， $\gcd(a,m)=1$ ，则存在 c 使得：

$$ca \equiv 1 \pmod{m}$$

我们把 c 称为 a 对模 n 的逆，记作，在模数已经指明的情况下，有时也记作。

在 $\gcd(a,m)=1$ 时，我们可以使用扩展欧几里得算法来求 a 的逆元：，这是因为：扩展欧几里得算法可以找到整数 x,y 使得 $ax+my=1$ ，这样

9.中国剩余定理

中国剩余定理(Chinese remainder theorem, CRT)，又称孙子定理，最早可见于中国南北朝时期(公元5世纪)的数学著作《孙子算经》中，为一次同余方程组的起源。

定理(CRT):

设 m_1, \dots, m_k 是两两互素的正整数， $M = \dots$

$$M_i = (i=1,2,$$

$\dots,k)$ ，则同余方程组：

有唯一解： $x \equiv a_i \pmod{M_i}$

其中 $a_i \equiv 1 \pmod{m_i}$ ， $i=1,2,\dots,k$

代码实现：

10.逆元与同余式定理

1模运算重要公式：

$$(a+b) \% m = (a \% m + b \% m) \% m$$

$$(a-b) \% m = (a \% m - b \% m) \% m$$

$$(a*b) \% m = (a \% m * b \% m) \% m$$

$$\% m = \% m$$

2威尔逊定理: (wilson's theorem)

若 p 为素数, 则: $(p-1)! \equiv -1 \pmod{p}$ □ 推导: $(p-2)! \equiv 1 \pmod{p}$;

其逆定理同样成立。即: 若 $(p-1)! \equiv -1 \pmod{p}$, 则 p 为素数

3二次探测定理:

定义:

若 p 是素数且 0

证明: 由于 $\equiv 1 \pmod{p}$, 所以: $-1 \equiv 0 \pmod{p}$, 即 $(x+1)(x-1) \equiv 0 \pmod{p}$

4费马小定理(Fermat):

若 a 为正整数, P 是一质数, 则: $\text{GCD}(a,p)=1$

那么, 推论:

, 推论: $a \equiv a \pmod{p}$

5欧拉定理(Euler):

若 a 与 m 互质, 则:

后记:

数论基础的知识点比较杂乱繁多, 这篇文章写的时候尽可能的去精简了, 其中的定理及公式是必须要牢记于心的。返回搜狐, 查看更多

责任编辑: