Cryptohack刷题记录(二) Mathematics部分 Modular Math WriteUp

原创

Mr_AgNO3 于 2022-01-24 00:53:48 发布 666 收藏
文章标签： 算法 python 密码学

本文链接：https://blog.csdn.net/u010883831/article/details/122660063

文章目录

MATHEMETICS

> 刚考完信安就忘完了…

MODULAR MATH

1. Quadratic Residues

模平方根

> 取$p=29$ 有

> We say that an integer `x` is a *Quadratic Residue* if there exists an `a` such that $ a^2=x\mod p$. If there is no such solution, then the integer is a *Quadratic Non-Residue*.

题目：

给了

$p=29$ $ints=[14,6,11]$ ，找到三个书中的QR的那一个(QR和QNR叫模平方剩余和模非平方剩余)，解出这个数

数值比较小，暴力解吧

```
>>> for t in [14,6,11]:
 for i in range(1,29):
  if pow(i,2,29) == t:
   print(f"{i} ^2 = {t} mod 29")

8 ^2 = 6 mod 29
21 ^2 = 6 mod 29
```

flag就是 8

---

2. Legendre Symbol

勒让德符号

是这么个规律

$$QR * QR = QR \quad QR * QNR = QNR \quad \cdots$$

题目：

给了 p 和包含10个元素的数组 ints

从 ints 中找出模 p 的一个二次剩余，计算这个数的模平方根，较大的那个数即flag

```
>>> for i in ints:
 l = pow(i,p//2,p)
 if l == p-1:
  pass
 else:print(ints.index(i))

5
```

```
>>> a = ints[5]
>>> pow(a,p//2,p)
1
```

接下来解方程

$$x \equiv a \mod p$$

```
>>> p%4
3
```

刚刚计算过勒让德符号 $\left(\frac{\cdot}{\cdot}\right) = 1$

则有

$$a$$

直接计算即可

```
>>> t = pow(a,p//4+1,p)
>>> pow(t,2,p) == a
True
>>> t
93291799125366706806545638475797430512104976066103610269938025709952247020061090804870186195285998727680200979853848718589126765742550855954805290253592144209552123062161458584575060939481368210688629862036958857604707468372384278049741369153506182660264876115428251983455344219194133033177700490981696141526
```

t即flag

---

3. Modular Square Root

Tonelli-Shanks算法是一种计算模平方根的算法

任何非2的素数都是 $p\equiv 1$ 求者

上一道题已经使用过了，对于4k+3型的素数，计算模平方根的方式很简单，但对于4k+1型的素数并不能这种方法计算

对于$r \equiv a \mod p$，Tonelli-Shanks算法能够计算r

该算法要计算椭圆曲线的交点，不深入讨论，但Sage已经有内置的方法实现

遂用Sage解方程

不知道他说的那个算法在Sage内是否有具体的函数实现，反正我是硬解出来了

```
sage: R.<x> = Zmod(p)[]
sage: f = x^2-a
sage: rr = f.roots()
```

```
sage: rr
[(28169512554311284614348161812907461395482195258388583125795498809297226147214152907614055638917789190356917578259717792167302913007927989841763977292434488782635964253677743342038748567333074043589267896292373028724763808006697707070301035339291758998923066001985927788808579330075671953036025191791621915640175242425390397212674797332132801882880223506177201168864920484993546017284338829512010922075018689505381642887042980971582058343875078178369658959872713920819264583922833549718236114238208656512834907615480533847317213916370643490217558998772245221613115612095307127021531635016235312901503409039130368210 41, 1),
(23623393076830486383277732985804892989321375055205003883382710520537347478623517796473141768179533590718715600411252899192471460749071516127626408681996211865595220683380326009913118822240160212226722431393621804612326467324658488404254582579308878565833796009677617385967828778513184893556798228131551230457052851120994481464267551101600025155924188504321036418158110715484562842635078055894450736575653818505213679696756997607553107846235770764400377476817603024349249321136400617387776011946222441927580241808539162444272540654419625572825728491627727407989896479486452073497374574454404050571568975083685319391 20, 1)]
sage: min(rr[0][0],rr[1][0])
23623393076830486383277732985804892989321375055205003883382710520537347478623517796473141768179533590718715600411252899192471460749071516127626408681996211865595220683380326009913118822240160212226722431393621804612326467324658488404254582579308878565833796009677617385967828778513184893556798228131551230457052851120994481464267551101600025155924188504321036418158110715484562842635078055894450736575653818505213679696756997607553107846235770764400377476817603024349249321136400617387776011946222441927580241808539162444272540654419625572825728491627727407989896479486452073497374574454404050571568975083685319391 20
```

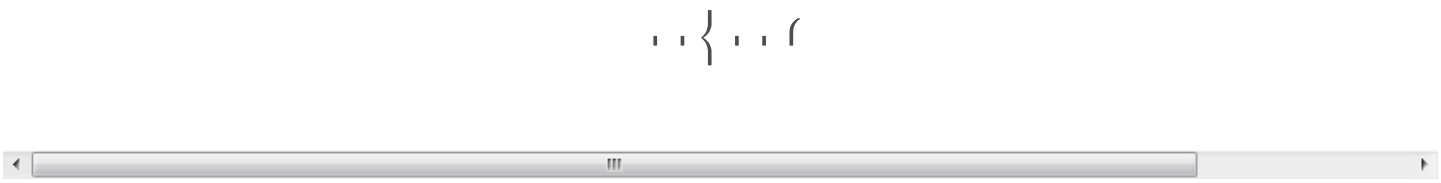
解出两个根，较小的一个为flag

---

4. Chisese Remainder Theorem

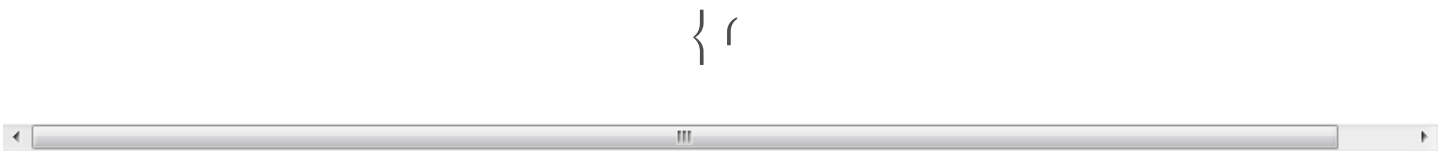
中国剩余定理 CRTyyds!!

对于方程组



题目：

已知



进入sage

首先对 935 进行分解

```
sage: factor(935)
5 * 11 * 17
```

则

```
>>> a = (2*11*17*invert(11*17,5) + 3*5*17*invert(5*17,11) + 5*5*11*invert(5*11,17))%n
>>> a
mpz(872)
```

flag是 `872`