Proof

pq分开处理

显然可以将pq分开处理 之后跑CRT

p

由于p-1不是5的倍数 直接用欧拉定理降幂可以搞到c^2 之后cipolla求出所有可能的m

q->q^3

一个容易的想法是 先处理出m在对q取模的情况的解 之后在扩展到q^3

可以先考虑扩展到q^2

假设已经求出m满足$m^{10} \equiv c \ (mod \ q)$

不妨设$m' \equiv (kq+m) \ (mod \ q^2)$

则有$(kq+m)^{10} \equiv c \ (mod \ q^2)$

展开后 消去所有含有q^2及以上的项 并移项 得

$$10kqm^9 \equiv c - m^{10} \ (mod \ q^2)$$

容易看出 由于m已经被求出 所以右边是已知的常数 左侧可以表示为Xqk 且X显然与q互质

不妨设右侧值为Y 也容易证明 右侧显然是q的倍数

移项 即

$$Xqk - Y = 0 \ (mod \ q^2)$$

显然可以化为

$$k = Y(Xq)^{-1} \ (mod \ q)$$

显然右侧可以为0 可以直接解出k并且k有$q-1$种取值

解出k后 就得到$(m')^{10} \equiv c \ (mod \ q^2)$

同理 可以得到对q^3取模的结果

q

考虑如何解出最初关于模q的m 原式$m^{10} \equiv c \ (mod \ q)$ 不能直接解出m 是因为$\varphi(q) \equiv 0 \ (mod \ 10)$

所以考虑能不能让m的指数与$\varphi(q)$互质 一个想法是考虑构造一个X 使其满足

$$m^{X+10} \equiv cm^X \ (mod\ q)$$

如果能消去右侧m^X的影响 那么m就是可解的

可以想到 令左右两边同时做幂运算 特殊构造的X就可以消去右侧m^X

构造X,Y 满足$XY=\varphi(q)$且X不为10的倍数

那么

$$(m^{X+10})^Y \equiv c^Y m^{XY} \ (mod\ q)$$

即

$$(m^{X+10})^Y \equiv c^Y \ (mod\ q)$$

不妨设g为关于q的原根 那么可以得到所有1关于q的Y次剩余

$$x_i = g^{\frac{i\varphi(q)}{Y}}$$

那么上式就可化为(解集扩大)

$$m^{X+10} \equiv cg^{\frac{i\varphi(q)}{Y}} \ (mod\ q)$$

显然 枚举i后 右侧为常数 左侧$X+10$与$\varphi(q)$互质 可以直接求出m

由于解集被扩大了 因此需要二次验证一下m是否正确

至此就可以得到模q意义下所有合法的m

也就可以直接解出flag了

q^3

不过wp里面采用的是直接求出模q^3的做法 其实是结合了上面两个步骤后的方法

考虑上面的证明 发现 直接替换成q^3也是成立的 唯一需要证明的是 所有1关于q^3的Y次剩余的值是$g^{\frac{i\varphi(q)}{Y}}$

不如考虑证明这个性质 如果存在关于q的原根g 那么

$$g^x \equiv N \ (mod\ q^k)$$

中N共有$\varphi(q^k)$种取值 且能覆盖到$[0,q^k)$内所有不为q的倍数的值

且这样我们可以认为g是关于q^k的'原根' 那么上面开十次方的性质也就显然成立

这块可以考虑结合第一部分的证明 为了简单 后面钦定$k=2$

考虑对于任何满足条件的N都能找到唯一的x 那么性质显然成立

那么可以将x表示为$a(q-1)+b$ 则有

$$g^{a(q-1)+b} \equiv N \ (mod\ q^2)$$

那么得到这个式子

$$(g^{q-1})^a g^b \equiv N \ (mod\ q)$$

即

$$g^b \equiv N \ (mod\ q)$$

显然这个b对于固定的N是可求的 唯一的 范围为$[0, q-1)$

因此在求解a的时候可以将b视为常数

那么可得

$$(g^{q-1})^a \equiv Ng^{-b} \ (mod\ q^2)$$

容易证明 g^{q-1}关于q取模的情况下也是一个关于q的原根 设其为G

并设g^{q-1}关于q^2取模下为$Xq+G$ 显然X, G均为常数

则有

$$(Xq+G)^a \equiv Ng^{-b} \ (mod\ q^2)$$

展开移项 消去含q^2的项 得

$$G^a + aXqG^{a-1} \equiv Ng^{-b} \ (mod\ q^2)$$

这个式子里面有不少常数 移项一下 得

$$aq \equiv (Ng^{-b} - G^a)(XG^{a-1})^{-1} \ (mod\ q^2)$$

左右必为q的倍数 可以左右两边同除q后解得a 并且对于固定的N a也是唯一的

且显然a可以为$[0, q)$的任意数

因此可以得到 对于任何满足条件的N 都有唯一对应的x 满足$g^x \equiv N \ (mod\ q^2)$

推广一下可以得到q^3的情况

就证明了性质 所有1关于q^3的Y次剩余

$$x_i = g^{\frac{i\varphi(q^3)}{Y}}$$

在求解的时候 令$Y = 10$ $X = \varphi(q^3)/Y$ 即可求出所有m关于q^3取模的值

推广

这个算法普适性可能并不是太强 显然这个算法的计算次数是与Y成正比的

如果要求某个数关于$p = 998244353$的二次剩余 那么这个最小的Y为2^{23} 显然超出了可接受范围

希望出题人不要发现这个方法的某些优化后闷声造大题

(虽说可能还会被MMA爆++过去 听说MMA可过后我整个人就自闭了)