CUSTPRIM解题报告

绍兴一中 洪华敦

CUSTPRIM

【简要题意】

定义三元组(a, b, c)的乘法运算，其中$c = 11\ or\ c = 24$

def multiply((a1,b1,c1), (a2,b2,c2)):

s = (a1a2 + b1b2 + c1c2) + (a1b2 + b1a2) + (c1 + c2)

t = floor[s/2] + 16(c1 + c2) - c1c2

A = (t - 2(a1b2 + b1a2) - (a1c2 + c1a2) + 33(a1 + a2)+(b1b2 - a1a2))

B = (t - 5(a1b2 + b1a2) - (c1b2 + b1c2) + 33(b1 + b2)+(2b1b2 + 4a1a2))

if s is even:

return (A-540,B-540,24)

else:

return (A-533,B-533,11)

定义单位元A是对于任何B满足$A * B = B$的三元组

定义$zero\ A$是对于任何B满足$A * B = A$的三元组

定义一个三元组是素数当且仅当这个三元组不能表示成两个非零非单位元的三元组的乘积

给定一个三元组，求他是否是素数

【解题思路】

首先，作者题解中有一句话：

要发现这个结论非常难，说实话，我也不知道该如何从题面推到结论

令ω是满足方程$\omega^2 = \omega - 3$的解，$\omega = \frac{1+\sqrt{-11}}{2}$

有个结论，对于每个三元组(a,b,c)，有到域$Z[\omega]$映射$\phi(a,b,c)=(33-2*a-c)+(b-a)*\omega$

通过带入计算可以发现$\phi((a1,b1,c1)*(a2,b2,c2))=\phi(a1,b1,c1)*\phi(a2,b2,c2)$

根据定义，显然有以下性质:

$\phi(a+b)=\phi(a)+\phi(b)$

$\phi(ab)=\phi(a)\phi(b)$

并且我们可以发现ϕ的逆运算：

当a是偶数时，令$a=2k$，$\phi^{-1}(a+b\omega)=(11-k,11-k+b,11)$

当a是奇数时，令$a=2k+1$，$\phi^{-1}(a+b\omega)=(4-k,4-k+b,24)$

我们可以发现，(a,b,c)是素数当且仅当$\phi(a,b,c)$在域$Z[\omega]$下是素数

于是问题就转化成了判定域$Z[\omega]$下的数$a+b\omega$是否是素数

我们可以发现域$Z[\omega]$是一个欧几里得域，即对于值$a\ b$，必定存在$q\ r$，满足：

$a=qb+r$，$f(r)<f(b)\ or\ r=0$

其中$f(r)$是距离函数，这里定义为复平面上一个点到原点的距离的平方，即$f(a+b\omega)=a^2+ab+3b^2$

证明如下：

首先证明一条定理：

对于域$Q[\omega]$中的每个元素x，必定存在一个域$Z[\omega]$中的值n使得$f(x-n)<1$

证明如下：

我们称满足以上定理的x是$good$的，我们尝试证明$Q[\omega]$中的所有元素都是$good$的，我们可以发现以下几点性质：

(1)对于$m\in Z[\omega]$，如果$x\in Q[\omega]$是$good$的，那么$x-m$也是$good$的

(2)如果$x\in Q[\omega]$是$good$的，那么$-x$也是$good$的

这两条性质都很显然，就不证明了

令$a+b\omega$是$Q[\omega]$中的一个元素，我们可以发现$\lfloor a\rfloor+\lfloor b\rfloor\omega$是$Z[\omega]$中的一个元素

根据性质(1)，我们只需要证明$(a-\lfloor a\rfloor)+(b-\lfloor b\rfloor)\omega$是$good$的即可

问题转化成了证明一个元素$a+b\omega$是$good$的，其中$0\leq a,b<1$

若$a+b>1$，我们可以套用性质(1)和性质(2)转化成证明$(1-a)+(1-b)\omega$是$good$的，于是这里只讨论$a+b\leq 1$的

显然当对于$a+b\leq 1$且$0\leq a,b<1$的元素$a+b\omega$，有$f(a+b\omega)<1$

现在可以证明$Z[\omega]$是个欧几里得域了

对于元素a,b，根据上面的定理，存在q使得$f(a/b-q)<1$，令$r=a-qb$，于是有$f(r/b)<1$，于是$f(r)<f(b)$

由于是个欧几里得域，于是扩展欧几里得定理就适用了

定义共轭$(a+b\omega)'=(a+b-b\omega)$

有以下几个性质

(1)x''=x

(2)$(x+y)'$=$x'+y'$

(3)$(xy)'$=$x'y'$

(4)如果x是质数，那么x'也是质数

(5)如果$x|y$，那么$x'|y'$

(6)如果g是a和b的gcd，那么g'是a'和b'的gcd

(7)x是个整数，当且仅当$x=x'$

我们定义$Nx=xx'$

然后Nx有以下性质：

(1)$N(a+b\omega)=a^2+ab+3b^2$，也就是f函数

(2)$Nx \geq 0$

(3)$Nx = 0$当且仅当$x = 0$

(4)$Nx = N(x')$

(5)$x|Nx$

(6)如果$x|y$，那么$Nx|Ny$

(7)$N(xy) = Nx * Ny$

(8)$Nx = 1$当且仅当x是单位元

于是有以下定理：

若Nx是质数，那么x也是域$Z[\omega]$下的素数

根据上面的性质可以很容易证明这个定理，这里略过

如果x是域$Z[\omega]$的素数，那么Nx是素数或素数的平方

证明：

令$Nx = \Pi_{i=1}^{k} p_i$，由于$x|Nx$且x是素数，所以x是某些p_i的约数，所以$Nx|Np_i = p_i^2$，所以Nx可以是$1, p_i, p_i^2$

定理：

如果p是一个奇质数，且$abs(p) \neq 11$，则$p = xx'$，其中x与x'是域$Z[\omega]$的质数

证明：

令a等于模p域下的$\sqrt{-11}$，于是有$p|a^2 + 11$

令x是p与$a + 1 - 2\omega$的gcd，根据扩展欧几里得定理，这里存在元素A，B满足$x = Ap + B(a + 1 - 2\omega)$

根据共轭的性质，所以有x'是$(a+1-2\omega)'$和p'的gcd，显然$p' = p$，$(a+1-2\omega)' = (a - 1 + 2\omega)$。

所以有x'=$Ap + B(a - 1 + 2\omega)$

所以有：

$$xx' = (Ap + B(a + 1 - 2\omega))(Ap + B(a - 1 + 2\omega))$$

$$xx' = A^2p^2 + ABp(2a) + B^2(a^2 + 11)$$

$$xx' = p * (A^2p + AB(2a) + B^2\frac{a^2 + 11}{P})$$

所以$p|xx'$，且x与x'都不是单位元

令g是x与$a-1+w\omega$的gcd，根据扩展欧几里得定理，存在C，D使得$Cx+D(a-1+2\omega) = g$

由于$g|(a+1-2\omega)$，所以$g|(a+1-2\omega+a-1+2\omega)$，所以$g|2a$，又因为$g|p$，所以$g|1$

所以对于某个h有$gh = 1$

$$Cx + D(a - 1 + 2\omega) = g$$

$$Chx + Dh(a - 1 + 2\omega) = gh = 1$$

$$Ch(xp) + Dhp(a - 1 + 2\omega) = p$$

所以$x'|p$，所以$xx'|xp$，又因为$x|p$且$x'|a-1+2\omega$，所以$xx'|p(a-1+2\omega)$，所以$xx'|Ch(xp)+Dhp(a-1+2\omega) = p$

因为$xx'|p$且$p|xx'$，所以$p = xx'$

定理：若p是奇质数且$abs(p) \neq 11$，且-11在$mod\,p$域下没有二次剩余，则p在$Z[\omega]$中是质数

证明：

若p在域$Z[\omega]$下不是质数，令$p = xy$，其中x与y都不是单位元，$Nx * Ny = Np = p^2$，由于x与y不是单位元，所以$Nx = Ny = p$

令$x = a + b\omega$

$$p = Nx$$
$$p = a^2 + ab + 3b^2$$
$$4p = 4a^2 + 4ab + 12b^2$$
$$4p = (2a + b)^2 + 11b^2$$
$$0 \equiv (2a + b)^2 + 11b^2 \ (mod\, p)$$
$$(2a + b)^2 \equiv -11b^2 \ (mod\, p)$$
$$[(2a + b)b^{-1}]^2 \equiv -11 \ (mod\, p)$$

所以$(2a + b)b^{-1}$是-11的二次剩余，注意这里b的逆元是显然存在的

定理：如果x是一个质数，且$Nx = p^2$，那么$x = p$或$x = -p$

证明：首先，如果p不能被表达成乘积的形式，那么$xx' = p^2$，则$x = p$或$x = -p$

否则设$p = yy'$，则$p^2 = y^2(y')^2$，那么x只能是$\pm y^2$或$\pm yy'$或$\pm(y')^2$，然而他们都不是质数，所以不成立

于是就得出结论：

(1)若x不是整数，那么x是质数当且仅当Nx是质数

(2)若x是整数，那么x是质数，当且仅当x是质数，且要么$abs(x) = 2$，要么$abs(x) \neq 11$且-11在模x域下没有二次剩余

于是直接上$miller\ rabin$即可