№Программа извлечения квадратных корней по составному модулю:

```
p=Integer("5")

q=Integer("7")

print("Take two prime numbers p=", p,"and q=",q  )

n=Integer()

print("Compute composite module n=:", n.Mul(p,q))

x=Integer("4")

print("Take a quadratic residue modulo n",x)

gcd=Integer()

a=Integer()

b=Integer()

print("Solve Diofant's equation ap+bq=gcd, gcd=", gcd.ExEuclid(p,q,a,b),"a=",a, "b=", b)

ap=Integer()

bq=Integer()

print("Compute ap modulo n ap=",ap.ModMul(a,p,n))

print("Compute bq modulo n bq=",bq.ModMul(b,q,n))

x1=Integer()

x2=Integer()

y1=Integer()

y2=Integer()

print("Compute square root of x modulo p x1=",x1.ModSqrt(x,p))

print("Compute square root of x modulo q y1=",y1.ModSqrt(x,q))

print("Compute the second square root of x modulo p x2=",x2.SubInFp(p,x1,p))

print("Compute the second square root of x modulo q y2=",y2.SubInFp(q,y1,q))

x1bq=Integer()

x2bq=Integer()

y1ap=Integer()

y2ap=Integer()

print("Compute x1*bq mod n x1bq=" , x1bq.ModMul(x1,bq,n) )
```

```
print("Compute x2*bq mod n x2bq=" , x2bq.ModMul(x2,bq,n) )

print("Compute y1*ap mod n y1ap=" , y1ap.ModMul(y1,ap,n) )

print("Compute y2*ap mod n y2ap=" , y2ap.ModMul(y2,ap,n) )

u1=Integer()

u2=Integer()

u3=Integer()

u4=Integer()

print("Compute the first square root of x modulo n", u1.ModAdd(x1bq,y1ap,n))

print("Compute the second square root of x modulo n", u2.ModAdd(x1bq,y2ap,n))

print("Compute the third square root of x modulo n", u3.ModAdd(x2bq,y1ap,n))

print("Compute the forth square root of x modulo n", u4.ModAdd(x2bq,y2ap,n))

>>>
```