

#Программа генерации квадратичных вычетов и псевдоквадратов

q=Integer()

p=Integer()

r=Integer()

p=Integer()

q=Integer()

print("generate the first prime number of length n bits p=",p.GeneratePrime(5))

print("generate the second prime number of length m bits q=",q.GeneratePrime(7))

print("compute the composite module n=",n.Mul(p,q))

d=Integer()

print("generate one more prime number of length r bits ",d.GeneratePrime(6))

print("compute the Legendre symbol for d to p legdp=", Integer.LegendreSymbol(d,p))

print("compute the Legendre symbol for d d to q legdp=", Integer.LegendreSymbol(d,q))

print("compute the Yacobi symbol for d to n Yavobidn=", Integer.JacobySymbol(d,n))

legdp=Integer()

legdp=Integer.LegendreSymbol(d,p)

legdq=Integer

legdq=Integer.LegendreSymbol(d,q)

yac=Integer()

print("Compute the product of Legendre Symbols yac=",yac.Mul(Integer(legdp),Integer(legdq)))