```
#Программа вычисления порядков элементов простого поля, символов Лежандра и тестирования
#образующего элемента.

p=Integer("127")

print("Take a prime p=", p )

a=Integer(3)

go=Integer()

print("compute the group GF(p)* order:",go.Sub(p,Integer("1")))

v=FactorizationAlgorithms(go).MsieveDecomposition()

print("group GF(p)* factorization:", v.toList())

print("Take a residue a=", a)

b=Integer()

print("compute b =a^2 mod p :", b.PowInFp(a,Integer(2),p))

print("a is group GF(p)* generator:",a.isGenerator(p,v))

print("b is group GF(p)* generator:",b.isGenerator(p,v))

ao=Integer()

print("element a order=", ao.elementOrder(p,a,v,go))

bo=Integer()

print(" element b order:", bo.elementOrder(p,b,v,go))

print("Legendre symbol of a to p=",Integer.LegendreSymbol(a,p))

print("Legendre symbol of b to p=",Integer.LegendreSymbol(b,p))

eulerpower=Integer()

print(" eulerpower=(p-1)/2=",eulerpower.Div(go,Integer(2)))

aeulerpower=Integer()

print("Euler criterion: a^{eulerpower}=a^{(p-1)/2}=",aeulerpower.PowInFp(a,eulerpower,p) )

baeulerpower=Integer()

print("Euler criterion:b^{eulerpower}=b^{(p-1)/2}=",baeulerpower.PowInFp(b,eulerpower,p) )
```