In [35]:
```
p = random_prime(2^64, 2^60)
Zp = IntegerModRing(p)
Zp
```

Out[35]:
```
Ring of integers modulo 3203672931176972929
```

In [36]:
```
a, b = Zp.random_element(), Zp.random_element()
E = EllipticCurve(Zp, [a, b])
E, a, b
```

Out[36]:
```
(Elliptic Curve defined by y^2 = x^3 + 2499296702048346838*x + 978187736268
658107 over Ring of integers modulo 3203672931176972929,
 2499296702048346838,
 978187736268658107)
```

In [37]:
```
P = E.random_element()
```

In [38]:
```
E.order(), P.order()
```

Out[38]:
```
(3203672931050669160, 533945488508444860)
```

In [39]:
```
mens = Zp(1234)
```

In [40]:
```
k = 30
```

In [41]:
```
j = 0
x = k*mens + j
while legendre_symbol(x^3+a*x+b, p) == -1:
    j += 1
    x = k*mens + j
print(j, x)
```

```
3 37023
```

In [42]:
```
y = sqrt(Zp(x^3+a*x+b))
y
```

Out[42]:
```
867481172839543729
```

In [43]:
```
y^2 == x^3+a*x+b
```

Out[43]:
```
True
```

In [45]:
```
E(x,y)
```

Out[45]:
```
(37023 : 867481172839543729 : 1)
```

In [48]:
```
floor(ZZ(E(x,y)[0])/k)
```

Out[48]:
```
1234
```

In [ ]: