

```
R = Integers(5959)
def is_field(): return True
R.is_field = is_field
e = EllipticCurve(Integers(5959), [1201,1])
P = e.point([0,1,1])
```

```
m = lcm(range(1,21))
```

```
m*P
```

```
(666 : 3229 : 1)
```

```
e = EllipticCurve(Integers(5959), [389,1])
P = e.point([0,1,1])
```

```
m*P
```

```
Exception (click to the left for traceback):
```

```
ZeroDivisionError: Inverse of 1414 does not exist
```

```
gcd(1414, 5959)
```

```
101
```

```
def ECM(N, a, m):
    R = Integers(N)
    # Trick SAGE into thinking that R is a field!
    def is_field(): return True
    R.is_field = is_field
    e = EllipticCurve(R, [a,1])
    P = e.point([0,1,1])
    print m*P
```

```
ECM(5959, 389, lcm(range(1,21)))
```

```
Exception (click to the left for traceback):
```

```
ZeroDivisionError: Inverse of 1414 does not exist
```

```
n = 997 * 10007; n
```

```
9976979
```

```
ECM(n, randrange(n), lcm(range(1,50)))
```

```
Exception (click to the left for traceback):
```

```
ZeroDivisionError: Inverse of 9819453 does not exist
```

```
gcd(9819453, n)
```

```
997
```

