

University of Waikato
Department of Mathematics Number Theory Assignment 7

5. Let $n = 199843247$ Using the elliptic curve

$$E: y^2 = x^3 + 59x - 59, P = (1, 1) \in E$$

$$A = -59 \quad B = 59.$$

and $k = 16296$ compute $kP \pmod{n}$ as described in Lenstra's algorithm to find a non-trivial factor of n .

```
In[91]:= fxy[xy1_, xy2_] := Module[{x1 = First[xy1], y1 = Part[xy1, 2],
  x2 = First[xy2], y2 = Part[xy2, 2], xx, n = 199843247, xdiff = 0, xinv},
  xdiff = GCD[x2 - x1, n];
  If[Not[xdiff == 1], Print[xdiff]];
  xinv = ModularInverse[x2 - x1, n];
  xx = (y2 - y1)^2 xinv^2 - x1 - x2;
  Return[Mod[{xx, -(y2 - y1) xinv xx - (y1 x2 - y2 x1) xinv}, n]]]

In[70]:= fxx[xy_] := Module[{x1 = First[xy], y1 = Part[xy, 2], xx, n = 199843247, c = 1},
  c = ModularInverse[(2 y1), n]; xx = (3 x1^2 + 59)^2 c^2 - 2 x1;
  Return[Mod[{xx, (3 x1^2 + 59) c (x1 - xx) - y1}, n]]]

ModularInverse[x_, n_] :=
Module[{inv}, inv = Mod[Part[Part[ExtendedGCD[x, n], 2], 1], n];
Return[inv]]
```