Cryptology, homework sheet 1

Due 15 September 2022, 10:30

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually.
For this exercise you can use your calculator or Pari-GP for basic arithmetic modulo 13 but not for more advanced calculations.

1. Verify that $P_A = (837670, 538535)$ is on the circle $C : x^2 + y^2 = 1$ over $\mathbb{F}_p$ for $p = 1000003$. Solve the discrete logarithm problem with base point $P = (1000, 2)$, i.e., find an integer $0 \leq a < p + 1$ with $P_A = aP$.
   For this exercise you should use some computer algebra system, e.g. `https://www.sagemath.org/`. Hand in your program code along with the solution. | 7 points |

2. Show that $(0, 1)$ is the neutral element with respect to the addition law on an Edwards curve, i.e., that $P + (0, 1) = (0, 1) + P = P$ for any point P on $E : x^2 + y^2 = 1 + dx^2y^2$. Then show that $(0, -1)$ has order 2 and that $(\pm 1, 0)$ have order 4. | 3 points |

3. Show that points of the form $(\pm b, \pm b)$ on $x^2 + y^2 = 1 + dx^2y^2$ have order 8 if they exist.
   Hints:
   - Show that they double to a point of order 4, then argue that this implies order 8.
   - Make sure to check that your denominators are nonzero.

   | 5 points |