Math 116 Spring 2022
Homework 7

Due Friday, May 20th

Sage instructions

You can use `E = EllipticCurve(GF(p), [1, 1])` to set `E` to be the elliptic curve $Y^2 = X^3+X+1$ over $\mathbb{F}_p$. When the underlying ring is not a field, you can use `E = EllipticCurve(Zmod(N), [1, 1])` to set `E` to be the elliptic curve $Y^2 = X^3 + X + 1$ over $\mathbb{Z}/N\mathbb{Z}$. The code `P = E(0,1)` sets `P` to be the point of `E` with coordinates $(0, 1)$. You can use usual addition `P+Q` to add two points `P` and `Q` on `E`, and use the usual multiplication `2*P` to compute `2P`.

You can use a while loop:

```
while some_condition:
    # loop body
```

to repeatedly run the loop body until the `some_condition` is true.

Problem 1. (by hand) Write n = 19 as a sum of positive and negative powers of 2 with at most $\frac{1}{2}\lfloor \log_2 n\rfloor + \frac{3}{2}$ nonzero terms.

Problem 2. (6.14, with Sage) Alice and Bob agree to use elliptic Diffie–Hellman key exchange with the prime, elliptic curve, and point

$$p = 2671, \quad E\colon Y^2 = X^3 + 171X + 853, \quad P = (1980, 431) \in E(F_{2671}).$$

(a) Alice sends Bob the point $Q_A = (2110, 543)$. Bob decides to use the secret multiplier $n_B = 1943$. What point should Bob send to Alice?

(b) What is their secret shared value?

(c) Find n_A by exhaustive search. (Start with `QA_guess = P` and `nA_guess = 1`, then repeatedly add `P` to `QA_guess` in a while loop until you hit a match.)

(d) Alice and Bob decide to exchange a new piece of secret information using the same prime, curve, and point. This time Alice sends Bob only the x-coordinate $x_A = 2$ of her point Q_A. Bob decides to use the secret multiplier $n_B = 875$. What single number modulo p should Bob send to Alice, and what is their secret shared value?

Problem 3. (6.21(a), with Sage) Use the elliptic curve factorization algorithm to factor each of the numbers $N = 589$ using the given elliptic curve $E\colon Y^2 = X^3 + 4X + 9$ and point $P = (2, 5)$.

Problem 4. (Not graded) Read section 6.5 on "The Evolution of Public Key Cryptography."