Math 1580 – Problem Set 7. Due Friday Nov. 4, 4pm

Updated 11/2, 11/3: typos corrected in Problem 3 and 4(e). The constant term in 3 is 853, not 835. Thanks to Anthony for catching this.

Problem 1. Let E be the elliptic curve $E : Y^2 = X^3 - 2X + 4$ over the rational numbers and let $P = (0, 2)$ and $Q = (3, -5)$.
(a) Compute $P \oplus Q$.
(b) Compute $P \oplus P$ and $Q \oplus Q$.
(c) Compute $P \oplus P \oplus P$ and $Q \oplus Q \oplus Q$.

Problem 2. Make an addition table for E over $\mathbb{F}_p$:
(a) $E : Y^2 = X^3 + X + 2$ over $\mathbb{F}_5$.
(b) $E : Y^2 = X^3 + 2X + 3$ over $\mathbb{F}_7$.

Problem 3. Alice and Bob agree to use elliptic Diffie-Hellman key exchange with the prime, elliptic curve, and point

$$p = 2671, \quad E : Y^2 = X^3 + 171X + 853, \quad P = (1980, 431) \in E(\mathbb{F}_{2671})$$

(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 secred shared value?

Problem 4. Let E and F be events in a probability space $(\Omega, \mathbb{P})$.
(a) Prove that $\mathbb{P}(E|E) = 1$. Explain in words why this is reasonable.
(b) If E and F are disjoint, prove that $\mathbb{P}(F|E) = 0$. Explain why this is reasonable.
(c) Let $F_1, \ldots, F_n$ be events satisfying $F_i \cap F_j = \emptyset$ for all $i \neq j$. We say that $F_1, \ldots, F_n$ are *pairwise disjoint.* Prove that

$$\mathbb{P}\left(\bigcup_{i=1}^{n} F_i\right) = \sum_{i=1}^{n} \mathbb{P}(F_i)$$

(d) Let $F_1, \ldots, F_n$ be pairwise disjoint as above, and assume further that

$$F_1 \cup \cdots \cup F_n = \Omega$$

where Ω is the entire sample space. Prove that

$$\mathbb{P}(E) = \sum_{i=1}^{n} \mathbb{P}(E|F_i)\mathbb{P}(F_i).$$

(e) Let $F_1, \ldots, F_n$ satisfy the conditions of part (d). Prove the general version of Bayes's formula

$$\mathbb{P}(F_i|E) = \frac{\mathbb{P}(E|F_i)\mathbb{P}(F_i)}{\mathbb{P}(E|F_1)\mathbb{P}(F_1) + \mathbb{P}(E|F_2)\mathbb{P}(F_2) + \cdots + \mathbb{P}(E|F_n)\mathbb{P}(F_n)}.$$