MATH 1025: Introduction to Cryptography

Midterm 2 Review

Problem 1.

(a) Compute the index of coincidence for the word $s =' \texttt{coincidence}'$.

(b) Compute the mutual index of coincidence for the words $s =' \texttt{trust}'$ and $t =' \texttt{truth}'$.

Problem 2.

(a) Give an example of a string s with $\text{IndCo}(s) = \text{MutIndCo}(s, s)$.

(b) Give an example of a string s with $\text{IndCo}(s) < \text{MutIndCo}(s, s)$.

(c)* Show that for any string s $\text{IndCo}(s) \leq \text{MutIndCo}(s, s)$.

Problem 3. Let $\mathbb{k} = \mathbb{F}_7$.

(a) Find a polynomial $f(x)$ of degree 3 over $\mathbb{k}$, which has no zeros.

(b) Compute the discriminant of $f(x)$.

(c) Is the elliptic curve E given by equation $y^2 = f(x)$ smooth?

Problem 4. Find the maximal prime number p, such that any elliptic curve over $\mathbb{F}_p$ has at most 64 points.

Problem 5. How many point addition operations will the double-and-add algorithm require in order to find the point $38P$ for some point P on elliptic curve E?

Problem 6. Let G be a group and $g \in G$ an element of order 1000. Suppose we would like to solve the DLP for g and h, that is, find a positive integer s such that $h = g^s$ using the collision algorithm. What is the minimal size of the lists (assume the lists are of the same size), so that the lower bound on the probability of collision is 90%?

Problem 7. Let P be a point on a smooth elliptic curve over $\mathbb{R}$. Suppose that P is not the point at infinity.

(a) Give a geometric condition that is equivalent to P being a point of order 2.

(b) Give a geometric condition (justify your answer) that is equivalent to P being a point of order 3.

Problem 8. Let E be a smooth elliptic curve over $\mathbb{R}$.

(a) Find the equation $\psi(x)$ that the x-coordinate of a point (element) satisfies if and only if it has order 3?[1] (justify your answer)

[1] **Hint:** hopefully, you found out that the answer in 7(b) is 'inflection points'. That means a point $P = (P_x, P_y)$ has order 3 iff $y''(P) = \dfrac{d^2y}{dx^2} = 0$. Find the second derivative using implicit differentiation of $y^2 = x^3 + ax + b$, the defining equation of E, twice. Then use the defining equation of E again to get rid of the y terms.

(b) Let's pick a concrete example with $b = 0, a = 1$, i.e. the defining equation of E is $y^2 = x^3 + x$. Find the inflection points (give both coordinates).