MATH 1025: Introduction to Cryptography

Midterm 2 Review

Solutions

Problem 1.

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

Solution: there are 11 characters in s, character 'c' appears 3 times, characters 'e', 'i' and 'n' appear 2 times each, the remaining characters appear at most once in s:
$\text{IndCo}(s) = \frac{\binom{3}{2} + 3 \cdot \binom{2}{2}}{\binom{11}{2}} = \frac{6}{55}$.

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

Solution: both strings have length 5, character 't' appears twice in both s and t, characters 'r' and 'u' appear once:
$\text{MutIndCo}(s,t) = \frac{2 \cdot 2 + 1 \cdot 1 + 1 \cdot 1}{5 \cdot 5} = \frac{6}{25}$.

Problem 2.

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

Solution: let ξ be any character and $s =' \xi\xi\ldots\xi'$, then $\text{IndCo}(s) = \text{MutIndCo}(s,s) = 1$.

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

Solution: any other string.

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

Solution: let F_i be the number of times that i^{th} character appears in string s of length ℓ. Then $\text{IndCo}(s) = \frac{\sum_{i=1}^{26} F_i(F_i-1)}{\ell(\ell-1)}$, while $\text{MutIndCo}(s,s) = \frac{\sum_{i=1}^{26} F_i^2}{\ell^2}$. As each of the differences $\mathcal{D}_i := \frac{F_i(F_i-1)}{\ell(\ell-1)} - \frac{F_i^2}{\ell^2} = \frac{\ell F_i(F_i-1) - (\ell-1)F_i^2}{\ell^2(\ell-1)}$ is a fraction with positive denominator and nonpositive numerator $\ell F_i(F_i-1) - (\ell-1)F_i^2 = \ell F_i^2 - \ell F_i - \ell F_i^2 + F_i^2 = F_i(F_i-\ell) \le 0$, it follows that $\text{IndCo}(s) - \text{MutIndCo}(s,s) = \sum_{i=1}^{26} \mathcal{D}_i \le 0$. Notice that the equality occurs when one of the F_i's is equal to ℓ (ξ is any character and $s =' \xi\xi\ldots\xi'$), confirming the observation in (a).

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

(a) Find a polynomial $f(x)$ of degree 3 over $\Bbbk$, which has no zeros.

Solution: the image of the map $\varphi : \mathbb{F}_7 \to \mathbb{F}_7$ given by $\varphi(x) = x^3 - x$ consists of elements $\{0, 1, 3, 4, 6\}$. Hence the polynomials $x^3 - x - 2$ and $x^3 - x - 5$ do not have zeros over $\mathbb{F}_7$.

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

Solution: let's pick $f(x) = x^3 - x - 2$, then $D_f = 4 \cdot (-1)^3 + 27 \cdot (-2)^2 \equiv 3 \pmod 7$.

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

Solution: $D_f \neq 0$, so the curve is smooth.

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

Solution: Hasse's theorem asserts that the number of points N on such a curve is bounded from above by $p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2$, hence p needs to satisfy the inequality $(\sqrt{p} + 1)^2 \leq 64$, which simplifies to $\sqrt{p} + 1 \leq 8 \Leftrightarrow \sqrt{p} \leq 7$ or $p \leq 49$. We conclude that $p = 47$.

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?

Solution: $38 = 2^5 + 2^2 + 2^1$, five operations to find $32P$ and two more operations to compute $32P \oplus 4P \oplus 2P$, the total number of operations is equal to 7.

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%?

Solution: as the lower bound on the probability of collision is given by $1 - e^{-\frac{n^2}{1000}}$, we need to solve the inequality $1 - e^{-\frac{n^2}{1000}} \geq 0.9$. The latter is equivalent to $e^{-\frac{n^2}{1000}} \leq 0.1$ or $\frac{n^2}{1000} \geq -\ln(0.1)$, which, approximately, gives $n^2 \geq 2303$, hence, $n \geq 48$.

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.

Solution: the tangent line to E at P is vertical, hence these are the points of intersection of the graph of E with the x-axis (the graph of E is symmetric w.r.t. the x-axis and, as $\ominus P$ is the reflection of P w.r.t. the x-axis, $P = \ominus P$ only for P on the x-axis).

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

Solution: such a point P satisfies $P \oplus P \oplus P = \mathcal{O}$ or $P \oplus P = \ominus P$, which implies that the third point of intersection of the tangent line to E at P with the graph of E is P. Let $F_\ell(x)$ be the restriction of the defining polynomial of E to the tangent line to E at P. Then $F_\ell(x)$ vanishes at P with multiplicity 3, meaning that $F_\ell(P_x) = F'_\ell(P_x) = F''_\ell(P_x) = 0$ (here P_x is the x-coordinate of P), thus P is an inflection point.

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)

Solution: using implicit differentiation, we find $2y\frac{dy}{dx} = 3x^2 + a$, thus, $\frac{dy}{dx} = \frac{3x^2+a}{2y}$. Differentiating implicitly one more time gives

$$\frac{d^2y}{dx^2} = \frac{d\left(\frac{3x^2+a}{2y}\right)}{dx} = \frac{6x\cdot 2y - 2\frac{dy}{dx}(3x^2+a)}{4y^2} = \frac{12xy^2 - (3x^2+a)^2}{4y^3} = \frac{12x(x^3+ax+b) - (3x^2+a)^2}{4y^3},$$

so $\psi(x) = 12x(x^3+ax+b) - (3x^2+a)^2 = 3x^4 + 6ax^2 + 12bx - a^2$.

(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).

Solution: we have $\psi(x) = 3x^4 + 6x^2 - 1$ and using the substitution $t = x^2 \geq 0$, get the quadratic equation $\psi(t) = 3t^2 + 6t - 1$, which has the zeros $t_{1,2} = \frac{-6\pm 4\sqrt{3}}{6}$. Notice that $t_2 = \frac{-6-4\sqrt{3}}{6}$ is less than 0, while $t_1 = \frac{-6+4\sqrt{3}}{6} = \frac{-3+2\sqrt{3}}{3}$ is greater. Notice that the domain of E is $x \geq 0$, hence, the only possible value of the x- coordinate is $\sqrt{\frac{-3+2\sqrt{3}}{3}}$. The inflection points are

$$P_1 = \left(\sqrt{\frac{-3+2\sqrt{3}}{3}}, \frac{2\sqrt{-3+2\sqrt{3}}}{3}\right)$$
$$P_2 = \left(\sqrt{\frac{-3+2\sqrt{3}}{3}}, -\frac{2\sqrt{-3+2\sqrt{3}}}{3}\right).$$

[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 $y''(P) = \frac{d^2y}{dx^2} = 0$. 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.