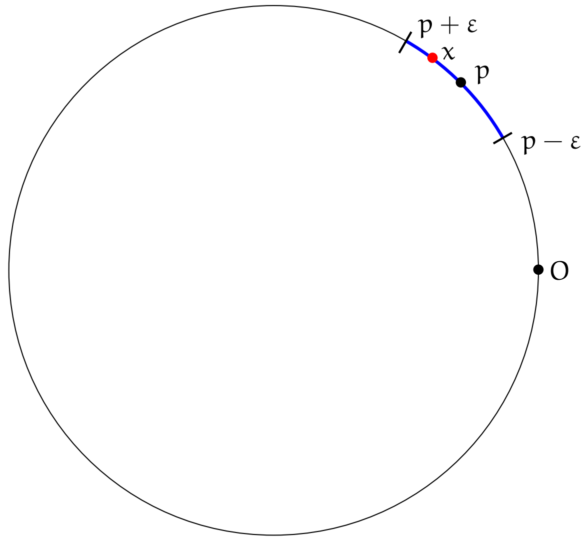
MATH 1800: Quantum Information Theory with Applications to Cryptography

Take-Home Exam

Definition 1. A subset $X \subset S^1$ is called **dense** if for any $\varepsilon > 0$ and any point $p \in S^1$ there is a point $x \in X$ on the open arc of length 2ε centered at p.



Problem 1. *Let* $\lambda := e^{i\varphi} \in S^1$ *be a point on the unit circle and consider the subset of points* $X_\lambda := \{\lambda^n\}_{n\in\mathbb{Z}} = \{\dots, \lambda^{-2}, \lambda^{-1}, 1, \lambda, \lambda^2, \dots\} \subset S^1$.

(a) *(5 pts) Show that* X_λ *is finite if and only if* $\varphi = \dfrac{p}{q}\pi$ *with* $p, q \in \mathbb{Z}$.[1]

(b) *(10 pts) Show that if the set* X_λ *is infinite, then for any* $\varepsilon > 0$, *there exist two points* $x_1, x_2 \in X_\lambda$ *with the distance* $d(x_1, x_2) < \varepsilon$.[2]

[1] **Hint:** $e^{in_1\varphi} = e^{in_2\varphi} \Leftrightarrow e^{i(n_1-n_2)\varphi} = 1 = e^{2k\pi i}\dots$

[2] **Hint:** what is the maximal number of points on the unit circle with the distance between any pair at least ε?

(c) *(10 pts) Show that if X_λ is infinite, then it is a dense subset of S^1.*[3]

Characters and DFT

Definition 2. Let G be a finite abelian group and $\mathbb{C}^* = \{z \in \mathbb{C} \mid z \neq 0\}$ the multiplicative group of nonzero complex numbers. A **character** of G is a homomorphism $\chi : G \to \mathbb{C}^*$. Recall, that a map χ is a group homomorphism provided $\chi(gh) = \chi(g)\chi(h)$.

Henceforth in this section we assume $G = \mathbb{Z}/n\mathbb{Z}$. Let $\omega = e^{2\pi i/n}$ be the primitive n^{th} root of unity and χ_j the character given by $\chi_j(1) = \omega^j$.

Problem 2. *Define a Hermitian inner product on characters via*

$$\langle \chi_i, \chi_j \rangle := \frac{1}{G} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)}.$$

(a) *(5 pts) Let χ be a character. Show that*[4]

$$\frac{1}{G} \sum_{g \in G} \chi_j(g) = \begin{cases} 1, & j = 0 \\ 0, & j \neq 0. \end{cases}$$

(b) *(5 pts) Verify that*

$$\langle \chi_i, \chi_j \rangle = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

[3]**Hint:** let $x_1 = \lambda^{n_1}, x_2 = \lambda^{n_2} \in X_\lambda$ be two points with $d(x_1, x_2) < \varepsilon$, then the point $\lambda^{n_1 - n_2}$ is on distance at most ε from $O = \lambda^0 = (1, 0)$. Now let $t = n_1 - n_2$ and take a look at the subset $\{\ldots, \lambda^{-2t}, \lambda^{-t}, 1, \lambda^t, \lambda^{2t}, \ldots\} \subset X_\lambda \subset S^1$.

[4]**Hint:** let $h \in G$ be an element and notice the equality of sets $\{hg\}_{g\in G} = \{g\}_{g \in G} = G$, in other words action by h on the left is a bijective map from G to itself (explain why it is true). Now $\frac{1}{G} \sum_{g\in G} \chi_i(g) = \frac{1}{G} \sum_{g \in G} \chi_j(hg) = \ldots$

(c) *(5 pts) Let* $\delta_g : G \to \mathbb{C}$ *be the delta function of element* $g \in G$, *i.e.*

$$\delta_g(h) = \begin{cases} 1, & h = g \\ 0, & h \neq g. \end{cases}$$

Check that $\mathsf{DFT}(\delta_i) = \chi_i$.

(d) *(5 pts) Let* $\mathbb{C}[G]$ *be the space of functions on* G. *A natural basis is given by the delta functions* $\{\delta_g \mid g \in G\}$. *Show that the character functions* $\{\chi_i \mid i \in \mathbb{Z}/n\mathbb{Z}\}$ *form an orthonormal basis in* $\mathbb{C}[G]$ *with respect to the inner product* $\langle \cdot, \cdot \rangle$ *defined in the beginning of this problem.*[5]

Remark 3. The group G naturally acts on its space of functions. Let $f \in \mathbb{C}[G]$ be a function and $h \in G$ an element, then the action of h on f is given via

$$(h \cdot f)(g) := f(h^{-1}g).$$

Problem 3. *(10 pts) Show that each character* χ_i *is an eigenvector with respect to this action. In other words*

$$(h \cdot \chi_i)(g) = \lambda(h)\chi_i(g)$$

for some $\lambda(h) \in \mathbb{C}^*$.

[5]**Hint:** use that DFT is invertible together with the results in (c) and (b).

Group structure on elliptic curve

Let $\mathbb{P}^2$ be the set of all one-dimensional subspaces (lines through the origin) in a three-dimensional vector space. The points on $\mathbb{P}^2$ are defined by three coordinates up to simultaneous rescaling and denoted by $p = [x : y : z]$. As $[x : y : z] \sim [tx : ty : tz]$ give rise to the same point in $\mathbb{P}^2$ (define the same line through the origin) for any $t \neq 0$, it only makes sense to work with homogeneous polynomials (all monomials have the same degree) in x, y and z. Let $E : \{[x : y : z] \in \mathbb{P}^2 \mid y^2 z = x^3 + axz^2 + bz^3\} \subset \mathbb{P}^2$ be an elliptic curve.

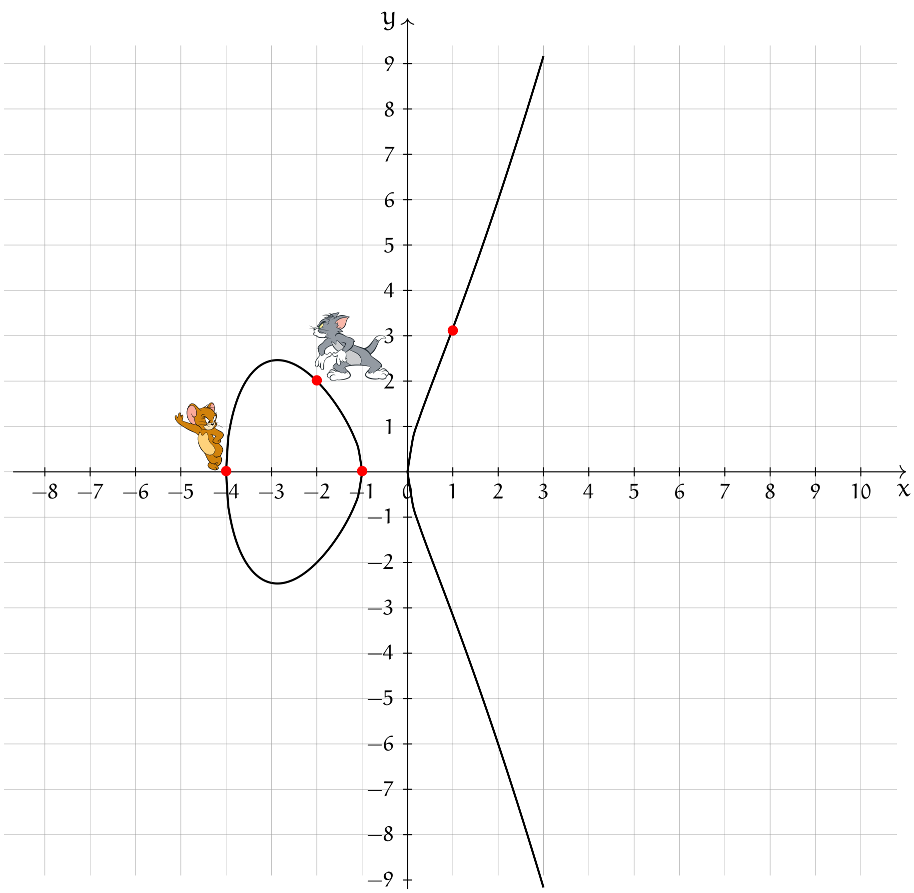
Remark 4. In class (see 'LecturesOnEllipticCurves.pdf' file) we 'looked' at the elliptic curve away from the line $\{z = 0\} \subset \mathbb{P}^2$, i.e. on the open subset $U_{z\neq 0} = \mathbb{P}^2 \setminus \{z = 0\}$. As each point $[x : y : z] \in U_{z\neq 0}$ is equivalent to $\frac{1}{z}[x : y : z] = [\frac{x}{z} : \frac{y}{z} : 1]$, the defining equation of E becomes $y^2 = x^3 + ax + b$ (we simply put $z = 1$).

Remark 5. The set $\mathbb{P}^2$ is called a **projective plane**. Analogously one can define a projective space of any dimension.

Next consider the set of **finite** expressions (formal sums) $\mathcal{P} := \{\sum_{P\in E} n_P P \mid n_p \in \mathbb{Z}\}$ with a free abelian group structure.

Definition 6. A formal sum $D = \sum_{P\in E} n_p P \in \mathcal{P}$ as above is called a **divisor**. The **degree** of a divisor D is the integer $\deg(D) = \sum n_p$.

Example 7. Let P, Q, R, S be some points on E and consider the divisors $D_1 = 2P - 3Q + 4S$ and $D_2 = P + R - 3S$. Then the divisor $D_3 = 2D_2 - D_1$ is $D_3 = 2D_2 - D_1 = 2P + 2R - 6S - (2P - 3Q + 4S) = 2R - 10S + 3Q$ and the degree of D_1 is $\deg(D_1) = 2 - 3 + 4 = 3$.



Problem 4. *We will work with the elliptic curve* $E : Y^2 = X(X+1)(X+4)$. *Let*  $= (-4, 0)$ *and*  $= (-2, 2)$ *be two points on* E.

(a) *(5 pts) Consider the divisors* $D_1 = 3$  -5  $+ 3(-1, 0)$ *and* $D_2 = 2$  $+$  $- 2(1, \sqrt{10})$ *and find*

(1) $D_1 + 2D_2 =$

(2) $3D_1 - D_2 =$

(b) (5 pts)

(1) $deg(D_1) =$

(2) $deg(D_2) =$

(3) $deg(D_1 + 2D_2) =$

(4) $deg(3D_1 - D_2) =$

(c) (5 pts) Show that in general for any two divisors $D, D' \in \mathcal{P}$ *one has* $deg(D + D') = deg(D) + deg(D')$. *In other words, the map*

$$deg : \mathcal{P} \to \mathbb{Z}$$

is a group homomorphism.

We will work with the subset $\mathcal{P}^0 \subset \mathcal{P}$, which consists of degree 0 elements.

Remark 8. Notice that $\mathcal{P}^0$ is the kernel of the homomorphism deg, hence, a subgroup of $\mathcal{P}$.

Let $\sim$ be an equivalence relation on $\mathcal{P}^0$ generated by

$$P_1 + P_2 + P_3 \sim Q_1 + Q_2 + Q_3$$

iff $P_1, P_2, P_3 \in \ell_1$ and $Q_1, Q_2, Q_3 \in \ell_2$ for some lines ℓ_1 and ℓ_2.
Let $\mathcal{O}$ be the point $[0 : 1 : 0]$.

Remark 9. This is the 'mysterious' point that we did not explicitly define in class, since it is 'hidden' on the line $\{z = 0\} \subset \mathbb{P}^2$, which we did not 'see' on $U_{z \neq 0}$.

Problem 5. *(5 pts) Show that the line $z = 0$ intersects E only at $\mathcal{O}$, but with multiplicity 3.* [6]

Problem 6. *Let* $D = \sum_{P \in E} n_p P \in \mathcal{P}^0$.

(a) *(5 pts) Show that* $D \sim \widetilde{D} = \left(\sum_{Q \in E} n_q Q \right) - m\mathcal{O}$ *with* $n_q \in \mathbb{Z}_{>0}$ *and* $m = -\sum n_q$.[7]

(b) *(10 pts) Show by induction on* $n = \sum n_q$ *that* $\widetilde{D} \sim P - \mathcal{O}$. [8]

Remark 10. Let G_E be the group $\mathcal{P}^0/_\sim$. We have established a surjection of sets

$$\varphi : E \longrightarrow G_E$$
$$\varphi(P) = P - \mathcal{O}.$$

It can be shown that φ is one-to-one[9] and, thus an isomorphism. Therefore the elliptic curve has a group structure G_E.

[6]**Hint:** let $f(x)$ be the restriction of the defining equation of E to the line $z = 0$ and check that $f(0) = f'(0) = f''(0) = 0$.

[7]**Hint:** if $n_P < 0$, consider the line ℓ through the points P and $R = \ominus P$, then $P + R + \mathcal{O} \sim 3\mathcal{O}$...

[8]**Hint:** for the induction step, draw a line ℓ through two points Q_1 and Q_2 with nonzero coefficients in $\widetilde{D}$ (or a tangent line to a point Q with $n_Q \geq 2$) and use that $Q_1 + Q_2 + R \sim R + (\ominus R) + \mathcal{O}$ (or $2Q + R \sim R + (\ominus R) + \mathcal{O}$), where R is the third point in $E \cap \ell$.

[9]Not so hard to show, but requires a bit of knowledge in Algebraic Geometry, so we will skip that part.

Use the programs at http://tsvboris.pythonanywhere.com/IntrotoCryptography to solve problems in the next two sections.

MV-ElGamal cryptosystem

Problem 7. *We will work with the MV-ElGamal cryptosystem (see page* 4 *of 'Lecture* 19*' notes).*

(a) *(*10 *pts) Sherlock knows the elliptic curve* E *and the ciphertext values* $C_1 = \alpha_1 S_x^{AB}$ *and* $C_2 = \alpha_2 S_y^{AB}$*. Show how he can use this knowledge to write down a polynomial equation (modulo* p*) that relates the two parts of the plaintext message (*α_1 *and* α_2*).*

(b) *(*10 *pts) Alice and Bob exchange a message using MV-ElGamal cryptosystem with elliptic curve* $E : y^2 = x^3 + 7x - 3$ *over* $\mathbb{F}_{1223}$*, with the chosen point* $P = (11, 216)$*. They use the correspondence* $A \leftrightarrow 1, B \leftrightarrow 2, \ldots, Z \leftrightarrow 26$ *to transform their text message into a plaintext* $m \in \mathbb{F}_{1223}$*. Sherlock intercepts the message* $(Q_B, C_1, C_2) = ((1086, 292), 37, 681)$ *that Bob sent to Alice. Moreover, Watson has found out and told Sherlock that the first part of the plaintext is* $\alpha_1 \equiv 89 \leftrightarrow$ *HI. Use your answer to part* (a) *to recover the second part* α_2 *of the plaintext and the whole message* $m = m_1 || m_2$*.*

Elliptic Curve Digital Signature Algorithm (ECDSA)

The **Elliptic Curve Digital Signature Algorithm** (ECDSA) is presented below (Samantha signs a document and Victor verifies the signature):

Step 1. **Public Parameter Creation**

A trusted party chooses a finite field $\mathbb{F}_p$, an elliptic curve $E/\mathbb{F}_p$, and a point $P \in E(\mathbb{F}_p)$ of large prime order q, i.e. $qP = \mathcal{O}$, where $\mathcal{O}$ is the identity element.

Step 2. **Key Creation**

Samantha chooses a secret signing key $1 < n_S < q - 1$, computes $V = n_S P \in E(\mathbb{F}_p)$ and publishes the verification key V.

Step 3. **Signing**

Samantha chooses a document, i.e. a number $D \pmod q$ and an ephemeral key $e \pmod q$. Then she computes $eP \in E(\mathbb{F}_p)$, followed by

$s_1 \equiv x(eP) \pmod q$ and

$s_2 \equiv (D + n_S s_1)e^{-1} \pmod{q}$.

Samantha publishes the signature (s_1, s_2).

Step 4. **Verification**

Victor finds $v_1 \equiv D s_2^{-1} \pmod{q}$ and $v_2 \equiv s_1 s_2^{-1} \pmod{q}$. He computes $v_1 P + v_2 V \in E(\mathbb{F}_p)$ and verifies that $x(v_1 P + v_2 V) \equiv s_1 \pmod{q}$.

Problem 8. *(10 pts) Prove that ECDSA works, i.e., check that the verification step succeeds in verifying a valid signature.*[10]

Problem 9. *This problem asks you to compute some numerical instances of ECDSA described above for the public parameters* $E : Y^2 = X^3 + 231X + 473, p = 17389, q = 1321, P = (11259, 11278) \in E(\mathbb{F}_p)$. *You should begin by verifying that* P *is a point of order* q *in* $E(\mathbb{F}_p)$.

(a) *(10 pts) Samantha's private signing key is* $s = 542$. *What is her public verification key* V? *What is her digital signature* (s_1, s_2) *on the document* $d = 644$ *using the ephemeral key* $e = 847$?

(b) *(10 pts) Tabitha's public verification key is* $V = (11017, 14637)$. *Is* $(s_1, s_2) = (907, 296)$ *a valid signature on the document* $d = 993$?[11]

A bit more on elliptic curves

Definition 11. Let p be an odd prime number. An integer k is a **quadratic residue** modulo p if it is congruent to a perfect square modulo p (there exists $1 \le a \le p-1$ with $k \equiv a^2 \pmod{p}$) and is a quadratic nonresidue modulo p otherwise. The **Legendre symbol** is a function of k and p defined as

$$\left(\frac{k}{p}\right) := \begin{cases} 1, k \text{ is a quadratic residue modulo } p \\ -1, k \text{ is a quadratic nonresidue modulo } p \\ 0, k \equiv 0 \pmod{p}. \end{cases}$$

[10] **Hint:** you need to check that $x(v_1 P + v_2 V) \equiv s_1 \bmod q$, which is straightforward: $x(v_1 P + v_2 V) \equiv x(D s_2^{-1} P + s_1 s_2^{-1} n_S P) \equiv \ldots$

[11] **Hint:** see Step 4.

An equivalent definition (Legendre's original way) is

$$\left(\frac{k}{p}\right) \equiv k^{(p-1)/2} \pmod{p}.$$

The Legendre symbol is a multiplicative function with respect to its top argument:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Problem 10. *(a) (5 pts) Use Legendre's definition to show that*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, p \equiv 1 \ (\textit{mod}\ 4) \\ -1, p \equiv 3 \ (\textit{mod}\ 4) \end{cases}$$

(b) (10 pts) Show that there are $p+1$ points on the elliptic curve over $\mathbb{F}_p$ given by $y^2 = x^3 - x$ with $p \equiv 3$ (mod 4).[12]

Problem 11. *Let E be an elliptic curve with the equation $y^2 = x^3 + ax + b$.*

(a) (10 pts) Show that if the equation $x^3 + ax + b$ splits into linear factors modulo p (in other words $x^3 + ax + b \equiv (x-\alpha)(x-\beta)(x-\gamma)$ (mod p) for some α, β and $\gamma \in \mathbb{F}_p$), then the group $G(E)$ is not cyclic.

(b) (5 pts) If the cubic polynomial $x^3 + ax + b$ has a root modulo p, then the number of elements on E over $\mathbb{F}_p$ is even.

[12]**Hint:** let $f(x) = x^3 - x$ and $a \in \mathbb{F}_p^*$, compare the Legendre symbols $\left(\frac{f(a)}{p}\right)$ and $\left(\frac{f(-a)}{p}\right)$.

Grover's algorithm

Problem 12. *Let* $f : \mathbb{B}^2 \to \mathbb{B}$ *be the function given by*

$$f(|x_1x_2\rangle) = \begin{cases} |0\rangle, & |x_1x_2\rangle \neq |11\rangle \\ |1\rangle, & |x_1x_2\rangle = |11\rangle. \end{cases}$$

(a) *(5 pts) Using* NOT, CNOT, CCNOT *gates, draw a circuit for the oracle* $\mathcal{O}_f$ *with* $\mathcal{O}_f(|i\rangle|-\rangle) = (-1)^{f(i)}|i\rangle|-\rangle$ *(the input state is* $|x_1\rangle, |x_2\rangle, |-\rangle$*).*

(b) *(5 pts) Let* R *be the reflection with respect to* $|00\rangle$ *i.e.*

$$R(|i\rangle|-\rangle) = \begin{cases} |i\rangle|-\rangle, & i \neq 00 \\ -|00\rangle|-\rangle, & i = 00. \end{cases}$$

Using NOT *and* CCNOT *gates, draw a circuit for* $-R$.[13]

(c) *(5 pts) Draw a circuit for Grover diffusion operator* $\mathcal{G} = H^{\otimes 2}(-R)H^{\otimes 2}\mathcal{O}_f$ *(the operators in the circuit are applied from left to right).*

[13] It is easier to construct a circuit for $-R$. As the images of the same state vector after application of R and $-R$ differ by a global phase change (multiplication by -1 in this case), such vectors are equivalent.

(d) *(5 pts) Draw a complete circuit realizing Grover's algorithm (starting with all qubits and ancilla qubits in state* $|0\rangle$*) with* $m = 1$ *iteration and find the resulting state vector prior to the measurement (show steps).*