Quantum Computation & Cryptography
Pre-workshop Questions

Note: For questions of the form "*What is x?*" you should only be able to give a qualitative answer, not a precise mathematical definition (if you also know the precise mathematical definition, that's even better).

Complex Numbers

1. What is a complex number? What is the complex conjugate? What is the polar (Euler) representation of complex numbers? What is the absolute value (modulus) of a complex number?

2. Let $z_1 = 1 + i$, $z_2 = 3 - 2i$. What is the polar form of z_1? What are the values of $\overline{z}_1$ and $\overline{z}_2$ (where $\overline{z}$ denotes the complex conjugate of z)? What are the values of $|z_1|$, $|z_2|$, $|z_1 + z_2|$, $|z_1 - z_2|$ (where $|\cdot|$ denotes absolute value)?

3. What are the fifth roots of unity? (i.e. find those z's such that $z^5 = 1$)

4. Let z_i, with $i \in \{0...k-1\}$, denote the k'th roots of unity. What is the value of $\sum_{i=0}^{k-1} z_i$?

5. Suppose we have z_1 and z_2 such that $|z_1|^2 + |z_2|^2 = 1$. Let $z_1' = e^{i\phi_1} z_1$ and $z_2' = e^{i\phi_2} z_2$. Is it also true that $|z_1'|^2 + |z_2'|^2 = 1$ for any $\phi_1, \phi_2 \in [0, 2\pi]$? Why/why not?

Linear Algebra

1. What is a vector space? What is a basis of a vector space? What is an orthonormal basis?

2. Consider the vectors:

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad v_2 = \begin{pmatrix} -2 \\ 3 \\ 2 \end{pmatrix} \quad v_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

   What is the inner product (standard Euclidian dot product) of v_1 and v_2? What about v_2 and v_3? Do these three vectors form a basis for $\mathbb{R}^3$? Why/why not?

3. Consider the matrix:

$$M = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 0 & 2 \\ -3 & 4 & 2 \end{pmatrix}$$

Compute the following quantities:

$$Mv_1; \quad v_2^T M; \quad v_3^T M v_2; \quad M^2 v_3; \quad v_1^T M^T M v_1$$

Where v_1, v_2, v_3 are the vectors from the previous question and $\cdot^T$ denotes the transpose operation.

4. What are eigenvalues and eigenvectors?

5. Consider the following matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \; Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

What are the eigenvalues and eigenvectors of these matrices?

Probability Theory

1. What is a discrete probability distribution? What is a discrete random variable?

2. Suppose we have a random variable X, defined as:

$$X = \begin{cases} 1 & \text{with probability } 1/3 \\ 2 & \text{with probability } 1/3 \\ 3 & \text{with probability } 1/2 \end{cases}$$

Is this a valid random variable? Why/why not?

3. Suppose X denotes the random variable of outcomes from tossing a *fair* six-sided dice. What would X look like? What is the expectation value of X, denoted $E(X)$? What is the variance of X, denoted $Var(X)$?

4. Let X and Y represent the random variables associated with the outcomes of two independent fair coin tosses. Suppose we associate the value $+1$ to *heads* and -1 to *tails*, i.e.:

$$X = \begin{cases} +1 & \text{with probability } 1/2 \\ -1 & \text{with probability } 1/2 \end{cases} \qquad Y = \begin{cases} +1 & \text{with probability } 1/2 \\ -1 & \text{with probability } 1/2 \end{cases}$$

Compute the following distributions: $Pr(X = x|Y = y)$, $Pr(Y = y|X = x)$, $Pr(X = x, Y = y)$. What is $E(XY)$?

5. Now assume X and Y, from the previous question, are perfectly *correlated*, i.e. it is always the case that $X = Y$. What will the three distributions and $E(XY)$ be in this case? What if X and Y are perfectly *anti-correlated*, i.e. it is always the case that $X = -Y$?