Forget this world and all its troubles and if possible its multitudinous Charlatans– everything in short but the Enchantress of Numbers.
– Ada Lovelace

Problem Set 10

PCMI USS, Summer 2023

1. (a) Prove the following proposition:

   Proposition 1 *Let n be a natural number and suppose that x and y are integers such that $x^2 \equiv y^2 \pmod{n}$, but $x \not\equiv y \pmod{n}$ and $x \not\equiv -y \pmod{n}$. Then both $\gcd(x+y, n)$ and $\gcd(x-y, n)$ are both nontrivial factors of n.*

   (b) Suppose you wish to factor $n = 713$. We are assuming that you can quickly find the order of any number modulo n, and we wish to factor n. So consulting your order-finding oracale, you find that the number $a = 3$ has order $r = 330$ modulo n. You now compute $a^{r/2} = 3^{165}$, and find the answer

   $$3^{165} \equiv 185 \pmod{713}.$$

   Let $x = 185$. Explain how you know that $x^2 \equiv 1 \pmod{n}$ without further computation.

   (c) Explain why this implies that 713 must be composite.

   (d) Use the Proposition and your value of x to find a nontrivial factor of n.

2. Let $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ be our favorite EPR pair.

   (a) Consider the measurable Z_1Z_2, which can also be written as $Z \otimes Z$. Suppose that this measurement is performed on $|\psi\rangle$. Intuitively, what do you think the expected value will be? Confirm your guess by computing the expression $\langle\psi|Z_1Z_2|\psi\rangle$.

   (b) Repeat for X_1X_2. Again, first see if you can intuit the answer, and then make the rigourous compuation.

   (c) Now try Z_1X_2.

   (d) Let $Q = Z_1$. This can also be written as $Q = Z \otimes I$. Explain why this corresponds Alice measuring in the computational basis (the Q measurement from the Bell paradox.)

   (e) Now consider the observable $S = \frac{1}{\sqrt{2}}(X_2 + Z_2)$. Show that S defines the measurement called S in Bell's paradox—that is, a measurement of Bob's qubit in the $\pi/8$ basis.

   (f) Use your results to rigorously show that the expected value of QS is $\frac{1}{\sqrt{2}}$. (which was critical for our analysis of Bell's paradox).

3. Let n be a natrual number. How many square roots of 1 are there modulo n? That is, how many elements $x \in \mathbb{Z}_n$ satisfy the $x^2 = 1$ in $\mathbb{Z}_n$? [You might try looking cases, such as when n is prime, n is the product of distinct primes, n is power of a prime, etc.]

4. (a) Let p be prime. What is the probability that a randomly chosen element of $\mathbb{Z}_p^*$ is a primitive root.

   (b) Say you're given a large prime p and you want to find a primitive root. Does your answer to (a) seem like good news or bad news?

   (c) Unfortunately, checking to see whether a given element of $a \in \mathbb{Z}_p^*$ is a primitive root is not easy. Suppose, however, that you know the factorization of $p - 1$. Explain now how you can efficiently check whether a given $a \in \mathbb{Z}_p^*$ is a primitive root.

   (d) Rudy asks you for a 1000-digit prime p together with a primitve root $a \in \mathbb{Z}_p^*$. Can you help Rudy out?

5. Let p be prime. How many square roots of -1 are there modulo p? That is, how many elements $x \in \mathbb{Z}_p$ satisfy the $x^2 = -1$ in $\mathbb{Z}_p$? Generalize to arbitrary n?

6. **(Bell, the Board Game)**

   (a) Design and make physical pieces which fit together like the measurements Q, R, S, T in the Bell paradox. Alice's pieces Q and R might be one color and Bob's pieces S and T another. Each piece could in one of two orientations, say up or down. Pieces Q and S would fit together somehow if they were both up or both down, but not if one was up and one was down. Similarly for the pair R, S—they fit together if they're both up or both down. And same for the pair R and T. But the pieces Q and T should fit together only in the case that one is up and the other is down. It would be cool if they were somehow symmetrical or appealing in some other way.

   (b) Start a business producing and selling your pieces. Come up with a clever name. Cut your idea guy in for 10%.

7. Come up with a magic trick or some other type of demonstration based on Bell's paradox. If Alice and Bob do not actually share entanglement, in what ways can they use "magic" (i.e., cheat) to fool the audience into thinking that they are violating Bell's inequality? (This is related to an important question that the experimentalists had to consider to rule out silly reasons that might explain the Bell violations.)

   Once the physical pieces Q, R, S, T are created, I could imagine a dramatization where someone playing Unice places each piece up or down, and then distributes the red pieces to Alice and the two blue pieces to Bob. Alice and Bob flip coins and each pick one of their pieces. And then magically, time after time, their pieces fit together. Such is impossible without "magic," since our Bell inequality for the expected value was at most $1/2$. (And it's impossible quantumly too btw, since the $\sqrt{2}/2$ we found is optimal.)