Ma/CS 6a: Problem Set 7*

Due noon, Friday, November 21

1. A group is *Abelian* or *commutative* if for every $x, y \in G$, we have $xy = yx$. For each of the following groups, either prove that it is commutative or give a counterexample.

(i) The cyclic group C_m.
(ii) The group of symmetries of the square.
(iii) Any group G that satisfies $(ab)^2 = a^2 b^2$ for every $a, b \in G$.

2. In class we proved that if $\mathrm{GCD}(m, n) = 1$, then $C_m \times C_n = C_{mn}$. Prove that if $\mathrm{GCD}(m, n) \neq 1$, then $C_m \times C_n$ is not cyclic.

3. (NO COLLABORATION) Prove or disprove:

(i) If G is a finite group of an even order, then G contains an odd number of elements of order two (hint: inverse elements).
(ii) The alternating group A_4 is isomorphic to the group of symmetries of the regular hexagon.

4. In class we proved the claim $|G| = |Gx| \cdot |G_x|$ by using the *double counting* technique. In this problem you will use this technique to prove a very different result.

Let $t(j)$ denote the number of elements in $\{1, 2, 3, \ldots, j\}$ that divide j. Also, let $\bar{t}(n) = \frac{1}{n}\sum_{j=1}^{n} t(j)$. That is, $\bar{t}(n)$ is the average value of $t(j)$ over all possible values of $1 \leq j \leq n$. Prove that for every n, we have $\bar{t}(n) \leq \ln(n) + 1$. (hint: recall the *harmonic series* and the bounds on its size. There is no need to prove these bounds).[1]

5. In Lecture 4, we saw the following *Fermat primality testing.* To test whether a number $a \in \mathbb{N}$ is prime, we choose $q \in \{1, 2, 3, \ldots, a-1\}$ and check whether $q^a \equiv q \mod a$. If this congruence does not hold, then a is not prime by Fermat's little theorem.

We also saw that if $\gcd(a, q) = 1$, then we can cancel one q from each side of the congruence, obtaining $q^{a-1} \equiv 1 \mod a$. We assume that a is very large, so the probability of choosing $q \in \{1, 2, 3, \ldots, a-1\}$ such that $\gcd(a, q) \neq 1$ is a small number ε. Thus, we use the condition $q^{a-1} \equiv 1 \mod a$, instead of the original one.

Carmichael numbers are the composite numbers which always pass this test. Let a be a composite number which is not a Carmichael number. Prove that the probability that the test fails to discover that a is composite when using a uniformly chosen $q \in \{1, 2, 3, \ldots, a-1\}$ is at most $1/2 + \varepsilon$ (hint: start with the set of elements of $\{1, 2, 3, \ldots, a-1\}$ that have an inverse under multiplication $\mod a$, and show that it is a group under this operation. Also show that any *bad* q is in this group).

*The awesome students who helped correcting this assignment: Évariste Galois, Tim Holland, Leon Ding, and Grace Lee.

[1] You might be interested to know that this bound is close to being tight for every n. Thus, by using a simple double counting, we can get powerful results.