Ma/CS 6a: Problem Set 7*

Due noon, Thursday, November 20

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 $(ab)^2 = a^2b^2$ for every $a, b \in G$.

2. In class we proved that if $\text{GCD}(m, n) = 1$, then $C_m \times C_n = C_{mn}$. Prove that if $\text{GCD}(m, n) \neq 1$, 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 $t(n, j)$ denote the number of elements in $\{1, 2, 3, \ldots, n\}$ that are divisible by j. For example, we have

$$t(8, 1) = 8,\ t(8, 2) = 4,\ t(8, 3) = t(8, 4) = 2,\ t(8, 5) = t(8, 6) = t(8, 7) = t(8, 8) = 1.$$

We set $\bar{t}(n) = \frac{1}{n}\sum_{j=1}^{n} t(n, j)$. That is, $\bar{t}(n)$ is the average value of $t(n, j)$ over all possible values of j. Prove that for every n, we have $\bar{t}(n) \leq \log(n) + 1$. (hint: recall the *harmonic series* and the bounds on its size. There is no need to prove these bounds). You might solve the question without noticing that what you did is considered as double counting. If this happens, try to frame your solution using a table, looking at its rows and columns as we did in class.[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 a 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 awesome students who helped correcting this assignment: Évariste Galois, Tim Holland, and Leon Ding.

[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.

the test fails for a when using a uniformly chosen $q \in \{1, 2, 3, \dots, a-1\}$ is at most $1/2 + \varepsilon$ (hint: start with a standard group whose elements are $\{1, 2, 3, \dots, a-1\}$ and consider the elements for which the congruence holds).