Homework #4, to be completed by Thursday, Sep 29.

Reading:

1. For this homework assignment: Chapters 5 and 6

2. For the next week's classes (Sep 27,29): 7.1-7.4.

Note: Most of the problems below come from homeworks 5 and 6 in Spring 2014.

Problems:

1. Let n, m be positive integers and $d = gcd(m, n)$. Prove that

$$\phi(mn)\phi(d) = \phi(m)\phi(n)d$$

(where ϕ is the Euler function).

2. In this question we investigate the following question: given $n \in \mathbb{N}$, how many solutions can the equation $\phi(x) = n$ have?

(a) Read about Fermat primes in Chapter 2. Let $F_n = 2^{2^n} + 1$ be the n^{th} Fermat number. It is easy to verify directly that F_n is prime for $0 \le n \le 4$, and it is known that F_n is composite for $5 \le n \le 32$. Use these facts to compute the number of solutions to the equation $\phi(x) = 2^{2016}$.

(b) Let $n = 2pq$ where p and q are distinct odd primes. Prove that the equation $\phi(x) = n$ has a solution if and only if at the least one of the following holds: $q = 2p+1$, $p = 2q+1$ or $2pq+1$ is prime. Also prove that the number of solutions is equal to 0, 2 or 4.

3. Let R and S be commutative rings with 1, and let $\phi : R \to S$ be a surjective ring homomorphism satisfying $\phi(1_R) = 1_S$.

(a) Prove that $\phi(R^\times) \subseteq S^\times$ and the restricted map $\phi : R^\times \to S^\times$ is a group homomorphism.

(b) Give an example showing that $\phi(R^\times)$ may be strictly smaller than $S^\times$.

(c) Assume now that ϕ is a ring isomorphism. Prove that $\phi(R^\times) = S^\times$ and the restricted map $\phi : R^\times \to S^\times$ is a group isomorphism. (This result was stated as Lemma 7.1 in class)

4. Use the structure of the groups U_n to find the number of reduced solutions to the congruence $x^3 \equiv 1 \mod n$.

5.

(a) Let $G_1, \ldots, G_k$ be finite groups. Prove that

$$\exp(G_1 \times \ldots \times G_k) = lcm(\exp(G_1), \ldots, \exp(G_k)),$$

where as usual $\exp(G)$ denotes the exponent of G.

(b) Give an example showing that if G is finite, but non-abelian, then $exp(G)$ may not equal to $o(g)$ for any $g \in G$.

6. Determine whether 67 is a primitive root mod 3^{2016}.

7. Let $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Find the order of the element $[67]_n \in U_n$. **Hint:** if you use a correct approach, you can solve this problem almost without computations.

8. Find all $n \in \mathbb{N}$ for which the group U_n has exponent 4.