Homework #5. Due Wednesday, February 19th, in class

Reading:

1. For this homework assignment: Chapter 5.
2. For the next two classes: Chapter 6.

Problems:

1. Let $n \geq 2$ be an even integer. Prove that for any $a \in \mathbb{Z}$ the congruence $x^2 + 3x + a \equiv 0 \mod n$ always has an even number of reduced solutions (possibly zero solutions).

2. 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).

3. 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 $0 \leq n \leq 4$, and it is known that F_n is composite for $5 \leq n \leq 32$. Use these facts to compute the number of solutions to the equation $\phi(x) = 2^{2013}$.

(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.

4. 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 8.1 in class)

5. For a natural number k let $U_k = \mathbb{Z}_k^\times$, the group of units of $\mathbb{Z}_k$ (this notation is standard; we will start using it in class next week). Now fix $m, n \in \mathbb{N}$ where $m \mid n$, and define $f : U_n \to U_m$ by $f([x]_n) = [x]_m$ (we verified in class that such f is well defined). Prove that f is surjective, that is,

$$f(U_n) = U_m.$$

Hint: First consider the case when n is a prime power, in which case the result can be proved using an explicit description of U_n and U_m as subsets of $\mathbb{Z}_n$ and $\mathbb{Z}_m$, respectively (similar to what we used in the proof of Theorem 8.5(1) in class). In the general case write $n = p_1^{a_1} \dots p_k^{a_k}$ (where $p_1, \dots, p_k$ are distinct primes and each $a_i \geq 1$) and $m = p_1^{b_1} \dots p_k^{b_k}$ and consider the diagram

$$\begin{array}{ccc} U_n & \xrightarrow[f_1]{} & U_{p_1^{a_1}} \times \ldots \times U_{p_k^{a_k}} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ U_m & \xrightarrow{f_2} & U_{p_1^{b_1}} \times \ldots \times U_{p_k^{b_k}} \end{array} \tag{1}$$

where the maps f_1, f_2 and g are defined by

$$f_1([x]_n) = ([x]_{p_1^{a_1}}, \dots, [x]_{p_k^{a_k}})$$
$$f_2([x]_m) = ([x]_{p_1^{b_1}}, \dots, [x]_{p_k^{b_k}})$$
$$g([x_1]_{p_1^{a_1}}, \dots, [x_k]_{p_k^{a_k}}) = ([x_1]_{p_1^{b_1}}, \dots, [x_k]_{p_k^{b_k}})$$

Note that this diagram is commutative, that is, $gf_1 = f_2 f$ as maps. Use what you already know about f_1, f_2 (from class) and g to prove that f is surjective.

Hint for Problem 1. Start with the case $n = 2$, then consider the case when n is a power of 2 and finally prove the result for an arbitrary even n.

Hint for Problem 2. Use an explicit formula for the Euler function. The solution will be considerably simpler if you pick the right version of the formula.