Homework #5. Due Wednesday, February 20th, in class

Reading:

1. For this homework assignment: Chapter 5 and Sections 6.1 - 6.2.

2. For the next two classes: Chapter 6.

Problems:

1. Let p be a prime. For a nonzero integer x, denote by $ord_p(x)$ the largest integer a s.t. p^a divides x (if $p \nmid x$, we set $ord_p(x) = 0$). We also put $ord_p(0) = \infty$, so that we get a function $ord : \mathbb{Z} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ Prove the following properties of the ord function:

(i) $ord_p(xy) = ord_p(x) + ord_p(y)$

(ii) $ord_p(x + y) \geq \min\{ord_p(x), ord_p(y)\}$

(iii) $ord_p(x + y) = \min\{ord_p(x), ord_p(y)\}$ whenever $ord_p(x) \neq ord_p(y)$

2. 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 solutions.

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

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

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

(a) Prove that for any $n \in \mathbb{N}$, the equation $\phi(x) = n$ has only finitely many solutions.

(b) 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 $\phi(x) = 2^{2013}$.

(c) 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.

5. Let $R_1, \ldots, R_k$ be commutative rings with 1 and $R = R_1 \times \ldots \times R_k$ be their direct product.

(a) Prove that $R^\times = R_1^\times \times \ldots \times R_k^\times$ as subsets of R, that is, an element $(r_1, \ldots, r_k) \in R$ lies in $R^\times$ if and only if $r_i \in R_i^\times$ for each i.

(b) Prove that $R^\times$ and $R_1^\times \times \ldots \times R_k^\times$ are isomorphic as groups. **Hint:** there is not much to prove.

6. 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 $\phi(R^\times) \subseteq S^\times$

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

7. Keeping the notations of Problem 4, assume that $R = \mathbb{Z}_n$ and $S = \mathbb{Z}_m$ where $m \mid n$, and $\phi : R \to S$ is defined by $\phi([x]_n) = [x]_m$ (we verified in class that such ϕ is well defined). Prove that

$$\phi(U_n) = U_m.$$

Hint: First consider the case when n is a prime power. In the general case write $n = p_1^{a_1} \ldots p_k^{a_k}$ (where $p_1, \ldots, p_k$ are distinct primes and each $a_i \geq 1$) and $m = p_1^{b_1} \ldots p_k^{b_k}$ and consider the diagram

$$\begin{array}{ccc} U_n & \xrightarrow[f_1]{} & U_{p_1^{a_1}} \times \ldots \times U_{p_k^{a_k}} \\ {\scriptstyle f_3}\downarrow & & \downarrow{\scriptstyle f_4} \\ U_m & \xrightarrow{f_2} & U_{p_1^{b_1}} \times \ldots \times U_{p_k^{b_k}} \end{array} \tag{1}$$

where the maps f_1, f_2, f_3 and f_4 are defined by

$$\begin{aligned} f_1([x]_n) &= ([x]_{p_1^{a_1}}, \ldots, [x]_{p_k^{a_k}}) \\ f_2([x]_m) &= ([x]_{p_1^{b_1}}, \ldots, [x]_{p_k^{b_k}}) \\ f_3([x]_n) &= [x]_m \\ f_4([x]_{p_1^{a_1}}, \ldots, [x]_{p_k^{a_k}}) &= ([x]_{p_1^{b_1}}, \ldots, [x]_{p_k^{b_k}}) \end{aligned}$$

Note that this diagram is commutative, that is, $f_4 f_1 = f_2 f_3$ as maps. Use what you already know about f_1, f_2 and f_4 to prove that f_3 is surjective (which is what you need to show).

8. In this problem you can use the following result which will be proved at the beginning of class on Monday, February 18:

Proposition 10.1: *Let p be an odd prime, $a \geq 2$ an integer and $m = p^{a-2}(p-1)$. Then for any $x \in \mathbb{Z}$ either $x^m \not\equiv 1 \mod p^a$ or $(x+p)^m \not\equiv 1 \mod p^a$.*

Now let $x \in \mathbb{Z}$, and assume that x is a primitive root mod p.

(i) Prove that the orders of elements $[x]_{p^a}$ and $[x+p]_{p^a}$ of U_{p^a} are both divisible by $p-1$.

(ii) Use (i) and Proposition 10.1 to prove that at least one of the elements x and $x+p$ is a primitive root mod p^a (this result is proved in a different way in the book).