Homework #4. Solutions to selected problems.

For solutions to the remaining problems see Solutions to HW#5 and HW#6 on Spring 2014 webpage.

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 $0 \leq n \leq 4$, 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 $\phi(x) = 2^{2016}$.

Solution: Let $x = \prod_{i=1}^{k} p_i^{a_i}$ be the prime factorization of x. Then $\phi(x) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1)$. Since $\phi(x) = 2^{2016}$, each prime p_i is equal to 2 or has the form $2^m + 1$ for some $m \in \mathbb{N}$, and $a_i = 1$ unless $p_i = 2$

If m is divisible by an odd prime, then $2^m + 1$ cannot be prime because of the identity $x^s + 1 = (x+1)(\sum_{i=0}^{s-1}(-1)^i x^i)$ which holds for any odd s (if s is an odd prime divisor of m, we can apply this formula to $x = 2^{m/s}$). Thus, each p_i is 2 or $F_n = 2^{2^n} + 1$ for some $n \in \mathbb{Z}_{\geq 0}$. Since F_n is not prime for $5 \leq n \leq 32$ and clearly $F_n - 1 > 2^{2016}$ for $n \geq 33$, the only possibilities for p_i are $2, F_0 = 3, F_1 = 5, F_2 = 17$ and $F_3 = 257$ and $F_4 = 65537$.

Hence x must be of the form $x = 2^a \prod_{i=0}^{4} F_i^{a_i}$ where each $a_i = 0$ or 1. Then $\phi(x) = 2^{a-1+a_0+2a_1+4a_2+8a_3+16a_4}$, so $\phi(x) = 2016 \iff a-1+a_0+2a_1+4a_2+8a_3+16a_4 = 2016$. Clearly for any choice of $a_0, a_1, a_2, a_3, a_4 \in \{0, 1\}$ this equation has unique solution for a, namely, $a = 2017 - (a_0 + 2a_1 + 4a_2 + 8a_3 + 16a_4)$, and this solution is positive! Hence the number of solutions is equal to $2^5 = 32$.

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)

Solution: (a) Take any $r \in R^\times$. By definition there exists $u \in R$ such that $ru = 1_R$. Since $\phi(1_R) = 1_S$, we have $\phi(r)\phi(u) = \phi(ru) = \phi(1_R) = 1_S$, so by definition $\phi(r) \in S^\times$. Therefore $\phi(R^\times) \subseteq S^\times$. The fact that $\phi : R^\times \to S^\times$ is a group homomorphism is clear since $\phi : R \to S$ respects multiplication (by assumption). Note that surjectivity of ϕ is actually not needed for this part (the point of mentioning surjectivity was to make part (b) interesting).

(b) Let $R = \mathbb{Z}$, $S = \mathbb{Z}_5$ and define $\phi : R \to S$ by $\phi(x) = [x]_5$. Then ϕ is a surjective homomorphism, but the restricted map $\phi : R^\times \to S^\times$ is not surjective since $\phi(R^\times) = \phi(\{1, -1\}) = \{[1]_5, [4]_5\}$ while $S^\times = \{[1]_5, [2]_5, [3]_5, [4]_5\}$.

(c) By (a) we have $\phi(R^\times) \subseteq S^\times$. Since ϕ is a ring isomorphism, the inverse map $\phi^{-1} : S \to R$ is well defined and also an isomorphism. Hence, applying the result of (a) to ϕ^{-1}, we get $\phi^{-1}(S^\times) \subseteq R^\times$, and now applying ϕ to both sides of the inclusion, we get $S^\times \subseteq \phi(R^\times)$. Combining this with the opposite inclusion $\phi(R^\times) \subseteq S^\times$, we conclude that $\phi(R^\times) = S^\times$.

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

Solution: First note that any $x \in \mathbb{Z}$ satisfying $x^3 \equiv 1 \mod n$ must be coprime to n, so the number of reduced solutions to this congruence is equal to the number of solutions to the equation $g^3 = [1]$ in $\mathbb{Z}_n$. As usual, it suffices to consider the case when n is a prime power $n = p^a$.

Suppose first that p is an odd prime. Then U_n is cyclic, let g be a generator of U_n, and let $m = o(g) = |U_n| = \phi(n) = p^{a-1}(p-1)$.

Take any $x \in U_n$ and write it as $x = g^i$ for some $0 \leq i \leq m-1$ (this can be done uniquely). Note that $x^3 = [1] \iff g^{3i} = [1] \iff m \mid 3i$.

Case 1: $3 \mid m$. Then m is coprime to 3, so by the Coprime Lemma $m \mid 3i \iff m \mid i$. Since $0 \leq i \leq m-1$, the only i that works is $i = 0$, so the equation has one solution.

Case 2: $3 \nmid m$. Then $\frac{m}{3}$ is an integer, and $m \mid 3i \iff 3i = mt$ for some $t \in \mathbb{Z} \iff i = \frac{m}{3}t$ for some $t \in \mathbb{Z}$. Since $0 \leq i \leq m-1$, we have exactly three values of i that work, namely $i = 0, \frac{m}{3}, \frac{2m}{3}$, so the equation has three solutions.

Since $m = p^{a-1}(p-1)$, it is clear that $3 \mid m \iff p \equiv 1 \mod 3$ or $p = 3$ and $a \geq 2$. This finishes the analysis in the case when p is an odd prime.

If $p = 2$, we claim that the equation $x^3 = [1]$ has exactly one solution.

Indeed, $x = [1]$ is always a solution. Any other solution must be an element of order 3 in U_n. But if n is a power of 2, $|U_n|$ is also a power of 2, so $3 \nmid |U_n|$, and therefore $|U_n|$ has no elements of order 3 by Lagrange theorem.

We can now state the final answer. Let s_n denote the number of reduced solutions to $x^3 \equiv 1 \mod n$. We proved that if p is a prime, then $s_{p^a} = 3$ if $p \equiv 1 \mod 3$ or ($p = 3$ and $a \geq 2$) and $s_{p^a} = 1$ otherwise. Since $s_{p_1^{a_1} \ldots p_k^{a_k}} = s_{p_1^{a_1}} \ldots s_{p_k^{a_k}}$ (where $p_1, \ldots, p_k$ are distinct primes), the final answer is as follows:

Let t be the number of (distinct) prime factors of n of the form $3i + 1$. Then $s_n = 3^t$ if n is not divisible by 9 and $s_n = 3^{t+1}$ if n is divisible by 9.