Homework #5. Solutions to selected 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).

Solution: Let $f(x) = x^2 + 3x + a$. Below we denote by s_n the number of reduced solutions to $f(x) \equiv 0 \mod n$.

First consider the case $n = 2$. The number $x^2 + 3x = x(x+3)$ is always even (since x is even or $x+3$ is even). So, if a is even, the congruence $f(x) \equiv 0 \mod 2$ always holds (hence $s_2 = 2$), and if a is odd, $f(x) \equiv 0 \mod 2$ never holds (hence $s_2 = 0$). In either case, s_2 is even.

Now suppose that $n = 2^e$ for some $e \in \mathbb{N}$. Since $f'(x) = 2x + 3$ is never divisible by 2, by Lifting Theorem we know that $s_{2^e} = s_2$ (and thus s_{2^e} is always even).

Finally, consider the general case. As proved in class, if $k, l \in \mathbb{N}$ are coprime, then $s_{kl} = s_k s_l$. Given any even n, we can write $n = 2^e m$ where $e > 0$ and m is odd. Then $s_n = s_{2^e} s_m$ is even since we just proved that s_{2^e} is even.

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).

Solution: Given a positive integer k, denote by $P(k)$ the set of primes dividing k, and let

$$C(k) = \prod_{p \in P(k)} (1 - \frac{1}{p}).$$

One of the formulas for the Euler function can be written as

$$\phi(k) = kC(k).$$

Therefore, $\phi(mn)\phi(d) = mndC(mn)C(d)$ and $\phi(m)\phi(n)d = mndC(m)C(n)$, and to prove the desired formula we just need to show that

$$C(mn)C(d) = C(m)C(n) \qquad (***)$$

To prove (***) we will argue that for each prime p, the expression $1-\frac{1}{p}$ appears on both sides of (***) with the same multiplicity. We consider three cases.

Case 1: $p \nmid m$ and $p \nmid n$. In this case, $p \nmid d$ and $p \nmid nm$ either, so $1-\frac{1}{p}$ does not appear on either side of (***).

Case 2: p divides n or m, but not both. In this case, $p \nmid d$, but $p \mid nm$. Hence the factor $1-\frac{1}{p}$ appears with multiplicity 1 in both sides of (***) (it comes from $C(mn)$ on the left and either $C(m)$ or $C(n)$, but not both, on the right).

Case 3: p divides n and m. Then p also divides nm and d. Hence $1-\frac{1}{p}$ appears in each of the four products $C(mn), C(d), C(m), C(n)$ and hence appears in both sides of (***) with multiplicity two.

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.

Solution to (b): First of all, recall that $\phi(m)$ is even for any $m > 2$. This fact will play a key role in the argument below.

Let x be such that $\phi(x) = 2pq$, and let $x = p_1^{a_1} \dots p_k^{a_k}$ be a prime factorization of x. We first claim that there exists at most one i such that $p_i^{a_i} > 2$. Indeed, if there exist $i \neq j$ such that $p_i^{a_i} > 2$ and $p_j^{a_j} > 2$, then $\phi(p_i^{a_i})$ and $\phi(p_j^{a_j})$ are both even, whence $\phi(x)$ is divisible by 4, a contradiction since $\phi(x) = 2pq$ and p and q are odd.

Thus, the only possibilities for x are $x = p_1^{a_1}$ or $x = 2p_1^{a_1}$ (and in the latter case p_1 is odd).

Case 1: $x = p_1^{a_1}$. If $a_1 \geq 3$, then $\phi(x)$ is divisible by p_1^2, a contradiction, so $x = p_1$ or p_1^2. If $x = p_1$, $\phi(x) = p_1 - 1$, so $x = 2pq + 1$. Moreover, $x = 2pq+1$ is a solution if and only if $2pq+1$ is prime (since we assume that p_1 is prime).

If $x = p_1^2$, $\phi(x) = p_1(p_1 - 1)$. Since p_1 is prime, the equality $p_1(p_1 - 1) = 2pq$ holds if and only if one of the following holds:

(i) $p_1 = 2$ and $p_1 - 1 = pq$

(ii) $p_1 = p$ and $p_1 - 1 = 2q$

(iii) $p_1 = q$ and $p_1 - 1 = 2p$

Clearly, case (i) is impossible, case (ii) occurs if and only if $p = 2q + 1$ and (iii) occurs if and only if $q = 2p + 1$. It is also clear that (ii) and (iii) cannot hold simultaneously.

Overall, we get that the number of solutions of the form $x = p_1^{a_1}$ is equal to $0, 1$ or 2, and for any such solution p_1 is odd (as $p_1 = p, q$ or $2pq + 1$)

Case 2: $x = 2p_1^{a_1}$ with p_1 odd. Then $\phi(x) = \phi(2)\phi(p_1^{a_1}) = \phi(p_1^{a_1})$, so $\phi(2p_1^{a_1}) = n$ if and only if $\phi(p_1^{a_1}) = n$. Hence every solution found in case 1 yields the corresponding solution in case 2 (obtained by multiplication by 2), and there are no other solutions in case 2.

Thus, the total number of solutions is twice the number of solutions found in case 1, hence is equal to $0, 2$ or 4, and by the argument in case 1, solutions exist if and only if $p = 2q + 1$, $q = 2p + 1$ or $2pq + 1$ is prime.