Solutions to Homework 6

Tim Smits

February 18, 2022

1. Solve the following systems of congruences. Your answer should be a single congruence class in each case: $x \equiv \_ \bmod \_$.

(a)
$$\begin{cases} x \equiv 6 \bmod 8 \\ x \equiv 3 \bmod 9 \\ x \equiv 8 \bmod 11 \\ x \equiv 7 \bmod 13 \end{cases}$$

(b)
$$\begin{cases} x \equiv 10 \bmod 12 \\ x \equiv 4 \bmod 15 \\ x \equiv 14 \bmod 50 \end{cases}$$

Note: the moduli here are *not* pairwise coprime, so you'll have to do something different than usual. *(Hint: factor each modulus and turn each single congruence into a system of congruences. Then you can eliminate the redundant ones.)*

(c) Show that the system below does *not* have a solution.
$$\begin{cases} x \equiv 6 \bmod 12 \\ x \equiv 9 \bmod 15 \\ x \equiv 22 \bmod 50 \end{cases}$$

Combined with the previous part, this demonstrates that the moduli not being pairwise coprime may or may not result in solutions to systems.

Solution:

(a) First, we solve the first two congruences. Saying $x \equiv 6 \bmod 8$ means we can write $x = 6 + 8k$ for some integer k. Plugging into the second congruence, we find $6 + 8k \equiv 3 \bmod 9$. This says $8k \equiv 6 \bmod 9$, and since 8 is it's own inverse mod 9, multiplying through yields $k \equiv 3 \bmod 9$. This says $k = 3 + 9\ell$ for some ℓ, so plugging in says $x = 6 + 8(3 + 9\ell) = 30 + 72\ell$, so $x \equiv 30 \bmod 72$. Similarly, the solution to $x \equiv 8 \bmod 11$ and $x \equiv 7 \bmod 13$ is given by $x \equiv 85 \bmod 143$, and the solution to these two remaining congruences is $x \equiv 7950 \bmod 10296$.

(b) Since $12 = 4 \cdot 3$, saying $x \equiv 10 \bmod 12$ is the same as saying $x \equiv 2 \bmod 4$ and $x \equiv 1 \bmod 3$. Similarly, $x \equiv 4 \bmod 15$ means $x \equiv 1 \bmod 3$ and $x \equiv 4 \bmod 5$, while $x \equiv 14 \bmod 50$ means $x \equiv 0 \bmod 2$ and $x \equiv 14 \bmod 25$. Of the 6 congruences, only three of them are relevant: $x \equiv 0 \bmod 2$ says x is even, which is already covered by $x \equiv 2 \bmod 4$, while

$x \equiv 14 \bmod 25$ already means that $x \equiv 4 \bmod 5$. Therefore, we wish to solve $x \equiv 2 \bmod 4$, $x \equiv 1 \bmod 3$, and $x \equiv 14 \bmod 25$. Solving these three congruences as in the previous part yields $x \equiv 214 \bmod 300$.

(c) Saying $x \equiv 9 \bmod 15$ means, in particular, that $x \equiv 4 \bmod 5$. Similarly, $x \equiv 22 \bmod 50$ means $x \equiv 2 \bmod 5$, and these obviously cannot both simultaneously be satisfied. Therefore, the system has no solution.

2. Prove for integers $m, n > 1$ that $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$ where $d = \gcd(m, n)$.

Solution: Write $\varphi(m) = m\prod_{p|m}(1 - \frac{1}{p})$, $\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$, $\varphi(mn) = mn\prod_{p|mn}(1 - \frac{1}{p})$, and $\varphi(d) = d\prod_{p|d}(1 - \frac{1}{p})$ using the formula for the φ function. Therefore, we wish to prove that $\varphi(d)\varphi(mn) = \varphi(m)\varphi(n)d$, which after plugging in and canceling is equivalent to proving $\prod_{p|mn}(1 - \frac{1}{p})\prod_{p|d}(1 - \frac{1}{p}) = \prod_{p|m}(1 - \frac{1}{p})\prod_{p|n}(1 - \frac{1}{p})$. The product in the right hand side counts the primes that divide both m and n *twice*, however, because the primes dividing mn are precisely the primes that divide m or n and the primes dividing d are precisely the primes that divide both m and n from our formula on HW 4, the products on both sides contain the same terms and we're good.

3.

(a) Find, with proof, all solutions to $\varphi(n) = 6$.

(b) Prove there is no solution to $\varphi(n) = 14$.

Solution:

(a) If $p \mid n$ then $p - 1 \mid \varphi(n)$ from the multiplicativity of the φ function. This says the only possible prime divisors of n must be the primes p such that $p - 1 \mid 6$, which leaves $p \in \{2, 3, 7\}$. Write $n = 2^a3^b7^c$ for some integers a, b, c. By multiplicativity, we must have $6 = \varphi(n) = \varphi(2^a)\varphi(3^b)\varphi(7^c)$. We now just need to figure out restrictions on the exponents. For $c \geq 2$ we have $\varphi(7^c) > 6$, so $c \leq 1$. For $b \geq 3$ we have $\varphi(3^b) > 6$, and for $a \geq 3$ we have $4 \mid \varphi(2^a)$. This yields $0 \leq a \leq 2$, $0 \leq b \leq 2$, and $0 \leq c \leq 1$. If $c = 1$, then $\varphi(7) = 6$, so $b = 0$ and $a = 0, 1$. This gives $n = 7, 14$. Otherwise, $c = 0$, so $n = 2^a3^b$. If $b = 2$, then we must have $a = 0, 1$ so we get the two solutions $n = 9, 18$. We cannot actually have $b = 1$, because this would mean $\varphi(2^a) = 3$, and $\varphi(n)$ is always even for integers bigger than 2. This leaves $b = 0$ as the last possibility so $n = 2^a$, but clearly no a in our range actually works. Therefore, there are only the four solutions we found: $n = 7, 9, 14, 18$.

(b) Again, note that if $p \mid n$ then $p - 1 \mid \varphi(n)$ so p must be a prime such that $p - 1 \mid 14$. This leaves $p \in \{2, 3\}$. Thus, $n = 2^a3^b$, from which we see that $\varphi(n)$ is never divisible by 7, so it can never equal 14. Therefore, there are no solutions.

4. Let $p > 2$ be prime and $k \geq 1$. Prove that $x^2 \equiv 1 \bmod p^k$ if and only if $x \equiv \pm 1 \bmod p^k$.

Solution: If $x \equiv \pm 1 \bmod p^k$, then clearly we have $x^2 \equiv 1 \bmod p^k$. Now suppose that $x^2 \equiv 1 \bmod p^k$. This says $p^k \mid (x^2 - 1) = (x + 1)(x - 1)$. We'd like to show that either $p^k \mid (x + 1)$ or $p^k \mid (x - 1)$. In other words, we need to show that all powers of p go into a single factor. Suppose otherwise, that $p \mid (x + 1)$ and $p \mid (x - 1)$. Then p must divide their difference, which is 2. However, p is odd, so this isn't possible. Therefore, p^k divides one of the factors and we are done.

5.

(a) What are the solutions to $x^2 \equiv 1 \bmod 2$? $x^2 \equiv 1 \bmod 4$? $x^2 \equiv 1 \bmod 8$?

(b) Prove that for $k \geq 3$, $x^2 \equiv 1 \bmod 2^k$ has exactly four solutions: $x \equiv \pm 1 \bmod 2^k$, $x \equiv \pm 1 + 2^{k-1} \bmod 2^k$. *(Hint: prove this by induction on k. If $x^2 \equiv 1 \bmod 2^k$, note that $x^2 \equiv 1 \bmod 2^{k-1}$.)*

Solution:

(a) $x \equiv 1 \bmod 2$, $x \equiv \pm 1 \bmod 4$, $x \equiv \pm 1, \pm 3 \bmod 8$.

(b) The case of $k = 3$ was done above, so suppose for some integer k that the only solutions to $x^2 \equiv 1 \bmod 2^k$ are $x \equiv \pm 1 \bmod 2^k$ and $x \equiv \pm 1 + 2^{k-1} \bmod 2^k$. We wish to show there are exactly four solutions to $x^2 \equiv 1 \bmod 2^{k+1}$, given by $x \equiv \pm 1 \bmod 2^{k+1}$ and $x \equiv \pm 1 + 2^k \bmod 2^{k+1}$. Suppose that $x^2 \equiv 1 \bmod 2^{k+1}$, then in particular, we must have $x^2 \equiv 1 \bmod 2^k$. By assumption, this means $x \equiv \pm 1 \bmod 2^k$ or $x \equiv \pm 1 + 2^{k-1} \bmod 2^k$. To handle all possible cases simultaneously, we write $x = \pm 1 + 2^{k-1}\ell + 2^k m$ for some integers ℓ, m, where $\ell = 0$ or 1. Squaring says $x^2 = (\pm 1 + 2^{k-1}\ell + 2^k m)^2 = 1 + 2^{2k-2}\ell^2 + 2^{2k}m^2 \pm 2^k\ell \pm 2^{k+1}m + 2^{2k}m\ell$. Since $2k - 2 \geq k + 1$ and $2k \geq k + 1$, reducing mod 2^{k+1} says $x^2 \equiv 1 + 2^k\ell \bmod 2^{k+1}$, which forces $\ell = 0$. This says $x = \pm 1 + 2^k m$ for some m. If m is even, then $x \equiv \pm 1 \bmod 2^{k+1}$ and if m is odd, then $x \equiv \pm 1 + 2^k \bmod 2^{k+1}$. This says these are the only *possible* solutions, and it's easy to see that they all indeed work, so there are precisely four solutions as desired.

6.

(a) Let $m, n > 1$ be relatively prime integers. Prove the map $f : S_{mn} \to S_m \times S_n$ given by $f([x]_{mn}) = ([x]_m, [x]_n)$ is a bijection. *(Hint: you'll want to use the Chinese Remainder Theorem to show the map is surjective!)*

(b) Let $N = 2^e p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of N. Set $N_2 = |S_{2^e}|$ and $N_{p_i} = |S_{p_i^{e_i}}|$. Write down a formula for the number of solutions to $x^2 \equiv 1 \bmod N$ in terms of N_2 and N_{p_i}, and use your formula to compute the number of solutions to $x^2 = [1]$ in $\mathbb{Z}/N\mathbb{Z}$ for $N = 60, 4410, 10!$.

(c) Find all solutions to $x^2 \equiv 1 \bmod 39188$. *(Much like with the proof of the Chinese Remainder Theorem, your proof of part (a) will tell you how to do this!)*

Solution:

(a) The proof that f is injective is the same as in the proof of the Chinese Remainder Theorem, so all we really have to do is check that f is surjective. Choose $([a]_m, [b]_n) \in S_m \times S_n$. By the Chinese Remainder Theorem, we can find $[x]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$ such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$. We'd then like to say that $f([x]_{mn}) = ([a]_m, [b]_n)$ so that f is surjective, but before we can do that we must check that this congruence class we have constructed lives in S_{mn}, i.e. that $x^2 \equiv 1 \bmod mn$. Since $x \equiv a \bmod m$, this means $x^2 \equiv a^2 \equiv 1 \bmod m$ and similarly $x^2 \equiv 1 \bmod n$. This says $m \mid x^2 - 1$ and $n \mid x^2 - 1$, so because m and n are relatively prime we get that $mn \mid x^2 - 1$, so $x^2 \equiv 1 \bmod mn$. Therefore $[x]_{mn} \in S_{mn}$, so we're good. Therefore, f is a bijection as desired.

(b) Writing $N = 2^e p_1^{e_1} \cdots p_k^{e_k}$ and repeatedly applying the above bijection says there is a bijection between S_N and $S_{2^e} \times S_{p_1^{e_1}} \times \ldots \times S_{p_k^{e_k}}$. Taking cardinalities then says $|S_N| = |S_{2^e} \times S_{p_1^{e_1}} \times \ldots \times S_{p_k^{e_k}}| = |S_{2^e}| \cdot |S_{p_1^{e_1}}| \cdots |S_{p_k^{e_k}}| = N_2 N_{p_1} \cdots N_{p_k}$. Problem 4 tells us that

$N_{p_i} = 2$ and N_2 is either $1, 2, 4$ depending on if $e = 1, 2, \geq 3$. We have $60 = 2^2 \cdot 3 \cdot 5$, so $|S_{60}| = |S_4| \cdot |S_3| \cdot |S_5| = 2 \cdot 2 \cdot 2 = 8$. Similarly, we have $4410 = 2 \cdot 3^2 \cdot 5 \cdot 7^2$ so $|S_{4410}| = 1 \cdot 2 \cdot 2 \cdot 2 = 8$. Finally, $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$ so $S_{10!} = 4 \cdot 2 \cdot 2 \cdot 2 = 32$.

(c) We have $39188 = 2^2 \cdot 97 \cdot 101$, so by part (b) there are $2 \cdot 2 \cdot 2 = 8$ solutions to $x^2 \equiv 1 \bmod 39188$. Each of the congruence $x^2 \equiv 1 \bmod 4$, $x^2 \equiv 1 \bmod 97$, and $x^2 \equiv 1 \bmod 101$ have as their only solutions $x \equiv \pm 1 \bmod 4, x \equiv \pm 1 \bmod 97, x \equiv \pm 1 \bmod 101$. This gives rise to 8 possible systems of three equations, and each system glues to a solution modulo 39188 by the Chinese Remainder Theorem. For example, $x \equiv 1 \bmod 4$, $x \equiv -1 \bmod 97$, $x \equiv 1 \bmod 101$ can be solved using the method of problem 1 and yields the solution $x \equiv 4849 \bmod 39188$. If you solve all 8 systems you'll find the 8 solutions are $x \equiv 1, 4849, 14745, 19593, 19595, 24443, 34339, 39187 \bmod 39188$.