CSE 311 HW5

Rohan Mukherjee

February 8, 2023

1. Let $P(n) = 5 \mid 9^n - 4^n$.

   Base case: $9^2 - 4^2 = 81 - 16 = 65 = 5 \cdot 13$, so clearly $5 \mid 9^2 - 4^2$, which is $P(2)$ so the base case holds.

2. (a) Given any arbitrary integer $n > 3$, I claim that the $n - 3$ satisfies the conditions on b. First we have to show that $1 \leqslant n - 3 \leqslant n$. As n is an integer strictly greater than 3, we know that $n \geqslant 4$, and from here we can subtract 3 from both sides to get $n - 3 \geqslant 1$. Similarly, as $-3 \leqslant 0$, we can add n to both sides to get that $n - 3 \leqslant n$, which shows that n is in the right bounds. Now, given any $a \in \mathbb{Z}$, we wish to show that $a + 3 + (n - 3) \equiv a \pmod{n}$. This statement is equivalent to showing that $n \mid (a + 3 + (n - 3) - a)$, and as $n \cdot 1 = (a + 3 + (n - 3) - a) = (3 + n - 3) = n$, so we see that this statement holds true. As n was arbitrary, we have concluded that for any integer $n > 3$, there exists a b so that b undoes 3 $\pmod{n}$.

   (b) Let the domain of discourse be integers. The statement in predicate logic is $\forall n \forall b \forall b'((\mathtt{Greater}(n, 3) \wedge \mathtt{Undoes3}(b, n) \wedge \mathtt{Undoes3}(b', n)) \to b \equiv b' \pmod{n})$. Given any arbitrary integer $n > 3$, and any arbitrary $b, b' \in \mathbb{Z}$, suppose that b and b' undo 3 for $\pmod{n}$ addition. Note that given any $a \in \mathbb{Z}$, we know that $n \mid (a + 3 + b - a) \iff n \mid 3 + b$ by the definition of undoing 3 for $\pmod{n}$ addition. Then $3 + b = kn$ for some $k \in \mathbb{Z}$. Similarly, given any $c \in \mathbb{Z}$, we know that $n \mid (c + 3 + b' - c) \iff n \mid 3 + b'$, so $3 + b' = ln$ for some $l \in \mathbb{Z}$. Then $b - b' = 3 + b - (3 + b') = 3k - 3l = 3(k - l)$, by plugging in what we learned above. As $k - l$ is an integer, this statement says that $3 \mid b - b'$, so we have concluded that $b \equiv b' \pmod{n}$. Finally, as b, b', and n were arbitrary, we have proven our statement.

3. (a) No. If we take $x = y = z = 2$, we see that $x \mid y$, as $2 \mid 2$, and that $y \mid z$, as again $2 \mid 2$. But clearly as $xy = 4$, $z = 2$, and as $4 \nmid 2$, we see that $xy \nmid z$. So we have disproven this claim by finding a counterexample.

   (b) Yes. We prove this by using the definition of divides. As $x \mid y$, we can say that $y = kx$ for some $k \in \mathbb{Z}$. As $y \mid z$, we can say that $z = ly$ for some $l \in \mathbb{Z}$. Plugging in the value for y, we see that $z = lkx$, and as lk is the product of integers, it too is an integer, so this statement says that $x \mid z$.

EC. (a) Note: because $\gcd(a, n) = 1$, there exists integers $s, t \in \mathbb{Z}$ so that $ba + tn = 1$, which tells us that $b = a^{-1} \pmod{n}$. So clearly now $r = a^{-1}ar \pmod{n}$, which gives us the first inclusion. Second, given any $ax \in aR$, first simply reduce ax to be between 0 and $n-1$. It suffices to show that $\gcd(ax, n) = 1$. We know that there exists u, v so that $ux + vn = 1$. Note that $1 = 1 \cdot 1 = (ux + vn)(ba + tn) = uxba + uxtn + vnba + vntn = (ub)xa + n(uxt + vba + vtn)$, so xa also has an inverse mod n. By letting $d = \gcd(ax, n)$, we see that $d \mid 1$, which means that $d = 1$, which gives the reverse inclusion.

(b) As the elements are the same, if we list the elements of R as $\{r_1, \cdots, r_{\varphi(n)}\}$, we can say that

$$r_1 \cdots r_{\varphi(n)} = ar_1 \cdots ar_{\varphi(n)}$$

Now, as each element of r has an inverse mod n, we can cancel all the r_i's, and we see that $a^{\varphi(n)} \equiv 1 \pmod{n}$.

(c) By the division algorithm, we see that there exists q so that $b = q\varphi(n) + b\%\varphi(n)$. Then, as exponents work the same in $\mathbb{Z}/n$, we see that $a^b = a^{q\varphi(n)+b\%\varphi(n)} = a^{q\varphi(n)} \cdot a^{b\%\varphi(n)} = 1^q \cdot a^{b\%\varphi(n)} = a^{b\%\varphi(n)}$ (where equality is in $\mathbb{Z}/n$).

(d) What is known is that $ed \equiv 1 \pmod{\varphi(n)}$. Next, as $\left(a^b\right)^c = a^{bc}$ in $\mathbb{Z}/n$, we see that $y^d \equiv x^{ed} \equiv x^1 \equiv x \pmod{n}$, as the power is reduced mod $\varphi(n)$.

(e) For the first part, we see that for any n, $\gcd(n, 1) = 1$, as the largest divisor of 1 is 1. For any prime p, and given any $1 \leqslant n \leqslant p-1$, we see that $n \nmid p$, as p is prime, as well as $p \nmid n$, as $n < p$. These facts together show that p is not a common divisor of n and p, and as p only has two positive divisors, where we know that p isn't a common divisor, the greatest common divisor between n and p must be 1. So $\varphi(p) = p - 1$. Note that $(a), (b)$ are comaximal ideals of the ring $\mathbb{Z}$, as there exists s, t so that $as + bt = 1$, which means that the sum would contain every multiple of 1–the entire ring. Also, $(a) \cap (b) = (ab)$, as the elements of the left set are multiples of both a and b. By the chinese remainder theroem for rings, we see that $\mathbb{Z}/(a) \times \mathbb{Z}/(b) \cong \mathbb{Z}/(a) \cap (b) \cong \mathbb{Z}/(ab)$. It suffices to show that the group of units of the RHS is indeed $(\mathbb{Z}/a)^\times \times (\mathbb{Z}/b)^\times$. If (a, b) is a unit, then there exists (s, t) so that $(c, d) \cdot (s, t) = (cs, dt) = (1, 1)$. This shows that c is a unit in $\mathbb{Z}/c$, and that d is a unit in $\mathbb{Z}/d$. The reverse inclusion is trivial. Finally note that $|(\mathbb{Z}/n)^\times| = \varphi(n)$, because the only numbers with an inverse mod n are going to be those that have gcd 1 with n (else, you could show its a zero divisor by multiplying with $n/\gcd(a, n) < n$ if $\gcd(a, n) \neq 1$. As the rings are isomorphic, their groups of units are isomorphic, which finally tells us that there is a bijection between their group of units, which tells us that their group of units have the same order–which tells us that $\varphi(ab) = \varphi(a)\varphi(b)$. Maybe this is a little overkill, but I think its cool. Here is a diagram of what's going on:

$$\begin{tikzcd}
\mathbb{Z}/(a) \cap (b) \arrow[d, tail, two heads] \arrow[dr, tail, two heads] & \\
\mathbb{Z}/(ab) \arrow[r, tail, two heads] & \mathbb{Z}/(a) \times \mathbb{Z}/(b)
\end{tikzcd}$$

Where the arrows here are ring homomorphisms.

4. Let $P(n) = 4 \mid (9^n - 1)$. Our proof is by induction on n.

   Base case: $0 \cdot 4 = 0 = 1 - 1 = 9^0 - 1$, so $4 \mid 9^0 - 1$, and therefore $P(0)$ is true.

   Inductive Hypothesis: Suppose $P(k)$ is true for an arbitrary integer $k \geqslant 0$.

   Inductive step: Notice that $9^{k+1} - 1 = 9^{k+1} - 9 + 9 - 1 = 9(9^k - 1) + 8$, where I added a smart 0 and then factored out a 9. By the inductive hypothesis, $9^k - 1 = 4l$ for some $l \in \mathbb{Z}$, so $9(9^k - 1) + 8 = 9 \cdot 4l + 8$. Factoring out the 4, we see that $9 \cdot 4l + 8 = 4(9l + 2)$, and as $9l + 2$ is an integer, this statement shows that $4 \mid 9^{k+1} - 1$, which was $P(k + 1)$.

   So $P(n)$ is true for all integer $n \geqslant 0$ by the principle of induction.

5. Let $P(n) = Mystery(n) = 21 \cdot 2^n + 9 \cdot (-1)^n$. We proceed by strong induction on n.

   Base cases: n=0, n=1 We see that $Mystery(0) = 30$, as it would go into the second if statement, and clearly $30 = 21 \cdot 2^0 + 9 \cdot (-1)^0 = 21 + 9 = 30$, which shows $P(0)$. We also see that $Mystery(1) = 33$, as it would go into the third if statement, and clearly $33 = 21 \cdot 2^1 + 9 \cdot (-1)^1 = 42 - 9 = 33$, which shows $P(1)$.

   Inductive Hypothesis: Suppose $P(0) \wedge P(1) \wedge \cdots \wedge P(k)$ for an arbitrary integer $k \geqslant 1$.

   Inductive Step: Looking at the definition of $Mystery(k+1)$, we see that as $k+1 \geqslant 2$, it is in particular not 0 or 1, so we will be in the last return statement and $Mystery(k+1) = Mystery(k) + 2 \cdot Mystery(k-1)$. By our inductive hypothesis, we know that the RHS is equal to $21 \cdot 2^k + 9 \cdot (-1)^k + 2 \cdot \left(21 \cdot 2^{k-1} + 9 \cdot (-1)^{k-1}\right)$. Now,

$$\begin{aligned} 21 \cdot 2^k + 9 \cdot (-1)^k + 2 \cdot \left(21 \cdot 2^{k-1} + 9 \cdot (-1)^{k-1}\right) &= 21 \cdot 2^k + 9 \cdot (-1)^k + 21 \cdot 2^k + 9 \cdot 2 \cdot (-1)^{k-1} \\ &= 21 \cdot 2^{k+1} + 9((-1)^k + 2 \cdot (-1)^{k-1}) \end{aligned}$$

   For the final equal sign, I combined the two $21 \cdot 2^k$'s, and I factored a 9 out of the other two terms. Therefore, it suffices to show that $(-1)^k + 2 \cdot (-1)^{k-1} = (-1)^{k+1}$. This requires a simple trick, i.e. multiplying by 1:

$$\begin{aligned} (-1)^k + 2 \cdot (-1)^{k-1} &= (-1)^k + 2 \cdot (-1)^{k-1} \cdot \frac{-1}{-1} \\ &= (-1)^k - 2 \cdot (-1)^k \\ &= -(-1)^k \\ &= (-1)^{k+1} \end{aligned}$$

   Where on the second line we have brought one of the -1's to the front of the two, and the second one we added to the power of the $(-1)^{k-1}$. So using this result, we see that

$$21 \cdot 2^{k+1} + 9((-1)^k + 2 \cdot (-1)^{k-1}) = 21 \cdot 2^{k+1} + 9(-1)^{k+1}$$

   Which is precisely what $P(k+1)$ asserts. By the principle of strong induction, we may conclude that $P(n)$ holds for all $n \geqslant 0$.

6. This assignment took me around 1.5 hours to complete, and around 1.5 hours to review. I knew a lot of the number theory coming into the course, so it didn't take long to figure out the problems. The longest problem was 5, as I would say it is the most challenging on this homework assignment, utilizing at least two tricks. I do not have any other feedback.