# WRITTEN HW #4 SOLUTIONS

(1) (10 points) For each of the following numbers, compute the ones digit of that number in its decimal expansion. Your answer should not require any electronic computational tools.
  (a) (2 points) $7^{2375}$
  (b) (3 points) $\sum_{n=1}^{15} n!$
  (c) (5 points) $3 \uparrow\uparrow n$, for $n \geq 3$, where $a \uparrow\uparrow n$ means a power tower of $a$ with size $n$: for instance, $2 \uparrow\uparrow 3 = 2^{2^2} = 2^4$, while $2 \uparrow\uparrow 4 = 2^{2^{2^2}} = 2^{2^4} = 2^{16}$. (Remember that towers of exponentials are evaluated from the top down, not the bottom up, so for instance $3^{3^3} = 3^{27}$, not $(3^3)^3 = 27^3$, which is a much smaller number than $3^{27}$.) Your answer should be in terms of $n$.

**Solution.** Notice $7^4 \equiv 1 \bmod 10$, and $2375 \equiv 3 \bmod 4$, so $7^{2375} \equiv 7^3 \equiv 3 \bmod 10$. So $7^{2375}$ ends in a 3.

Notice many of the terms in the sum of $n!$ have a 0 at the end; namely, any term with $n \geq 5$, because for those terms $10 \mid n!$. So the ones digit of this number is the same as the ones digit of $1! + 2! + 3! + 4! = 33$, which is 3.

First, notice that $3^4 \equiv 1 \bmod 10$, so to determine the ones digit of $3 \uparrow\uparrow n$, it suffices to determine the residue class of $3 \uparrow\uparrow (n-1) \bmod 4$. However, notice that $3^2 \equiv 1 \bmod 4$, so the residue class of $3 \uparrow\uparrow (n-1) \bmod 4$ is determined by the residue class of $3 \uparrow\uparrow (n-2) \bmod 2$; ie, $3 \uparrow\uparrow (n-2) \bmod 2$ whether is odd or even. If $n \geq 3$, this is always an odd number, so this means $3 \uparrow\uparrow (n-1) \equiv 3 \bmod 4$, so $3 \uparrow\uparrow n \equiv 7 \bmod 10$. $\square$

(2) (10 points) Find all solutions (modulo the appropriate modulus) to the following linear congruences. Explain why your answer is correct.
  (a) $2x \equiv 7 \bmod 5$
  (b) $5x \equiv 3 \bmod 15$
  (c) $x^2 + 1 \equiv 0 \bmod 13$
  (d) $x^2 + 1 \equiv 0 \bmod 19$
  (e) $244x \equiv 32 \bmod 75$

**Solution.**
  (a) $2x \equiv 7 \bmod 5$ has exactly one solution mod 5, because $\gcd(2,5) = 1 \mid 7$, and trial and error (or whatever technique you prefer) shows this solution is $x \equiv 1 \bmod 5$.
  (b) $5x \equiv 3 \bmod 15$ has no solutions, because $\gcd(5,15) = 5 \nmid 3$.
  (c) $x^2 + 1 \equiv 0 \bmod 13$ has either 0, 1, or 2 solutions, because $x^2 + 1$ is a quadratic polynomial and 13 is prime. Inspection shows that $x \equiv \pm 5 \bmod 13$ are the two solutions.

(d) $x^2 + 1 \equiv 0 \bmod 19$ has either 0, 1, or 2 solutions, for the same reason as the previous problem.

(e) $244x \equiv 32 \bmod 75$ has one solution mod 75, because $\gcd(244, 75) = 1$. Indeed, the Euclidean algorithm yields

$$\begin{aligned} 244 &= 75 \cdot 3 + 19, \\ 75 &= 19 \cdot 3 + 18, \\ 19 &= 18 + 1, \\ 18 &= 1 \cdot 18. \end{aligned}$$

Recall that to solve $244x \equiv 32 \bmod 75$ by hand, we try to find solutions to Bezout's identity $244x + 75y = 1$:

$$\begin{aligned} 1 &= 19 - 18 \\ &= 19 - (75 - 19 \cdot 3) = 75 \cdot -1 + 19 \cdot 4 \\ &= 75 \cdot -1 + (244 - 75 \cdot 3) \cdot 4 = 244 \cdot 4 - 75 \cdot 13. \end{aligned}$$

Therefore $244 \cdot 4 \equiv 1 \bmod 75$. To solve $244x \equiv 32 \bmod 75$, we multiply this previous equation by 32, to get $244(4 \cdot 32) \equiv 32 \bmod 75$, or $x \equiv 53 \bmod 75$. $\square$

(3) (20 points) Let $X$ be a set. A *relation* on $X$ is a subset $R$ of $X \times X = \{(x, y) | x, y \in X\}$. We will write $aRb$ if $(a, b) \in R$. For example, if $X = \mathbb{Z}$, then the subset $R$ consisting of all ordered pairs $(x, 2x), x \in \mathbb{Z}$, is a relation on $\mathbb{Z}$, and we have $1R2, 4R8$, say.

A relation $R$ is called an *equivalence relation* if $aRa$ for all $a \in X$ (ie, if $R$ is *reflexive*), if $aRb$ implies $bRa$ (ie, if $R$ is *symmetric*), and if $aRb$, $bRc$ implies $aRc$ (ie, $R$ is *transitive*). The example relation defined in the last paragraph is not an equivalence relation – it violates each of the three properties an equivalence relation needs to satisfy. On the other hand, recall that the relation $R$ on $\mathbb{Z}$ defined by $aRb$ if and only if $a \equiv b \bmod n$, for some fixed integer $n$, is an equivalence relation.

A *partition* of a set $X$ is a collection of subsets $\{X_i\}$ of $X$, such that each element of $X$ is in exactly one subset $X_i$. For example, if $X = \{1, 2, 3\}$, then $X_1 = \{1, 3\}, X_2 = \{2\}$ is a partition of $X$, whereas $X_1 = \{1, 2\}, X_2 = \{2, 3\}$ is not, nor is $X_1 = \{1\}, X_2 = \{3\}$.

Let $R$ be an equivalence relation. The equivalence class of an element $x \in X$ is defined to be the set of all $y \in X$ such that $xRy$, and is written $[x]$. Show that every element of $X$ is in some equivalence class, and that if $[x], [y]$ have non-empty intersection, then $[x] = [y]$. In particular, conclude that the equivalence classes of $R$ partition $X$.

Conversely, show that a partition $\{X_i\}$ of $X$ induces an equivalence relation on $X$, where $aRb$ if and only if $a, b$ lie in the same subset $X_i$.

**Solution.** We will first show the equivalence classes of $R$ partition $X$. Since $R$ is an equivalence relation, clearly $aRa$ for each $a \in X$, so each element of $X$ is in some congruence class, even if it is the only element of its congruence class.

Now assume we have two congruence classes $[x], [y]$ with nontrivial intersection. Let $a$ be such a common element, so that we have $xRa$, $aRy$ (guaranteed by symmetry). By transitivity, these two relations imply that $xRy$. Now let $c \in [y]$ be arbitrary. Then $xRy, yRc$ implies that $xRc$, so $c \in [x]$. This shows that $[y] \subset [x]$; a symmetric argument shows $[x] \subset [y]$. Therefore $[x] = [y]$ as desired, so all distinct equivalence classes have empty intersection.

Conversely, assume we have some partition $\{X_i\}$ of $X$. Assume we have the relation $R$, where $aRb$ if and only if $a, b$ lie in the same subset $X_i$. Clearly $a$ is in the same subset as itself, so $R$ is reflexive. If $a$ is in the same subset as $b$, then $b$ is in the same subset as $a$, so we have symmetry. Now assume we have $aRb$, $bRc$. This means that $a$ is in the same subset as $b$ and that $b$ is in the same subset as $c$, so $a$ and $c$ must be in the same subset, hence we do have $aRc$, i.e. $R$ is transitive. □

(4) (10 points) Recall that we said addition and multiplication of congruences classes was well-defined $\bmod n$, since we proved that if $a \equiv a' \bmod n, b \equiv b' \bmod n$, then $a + b \equiv a' + b' \bmod n, ab \equiv a'b' \bmod n$. Show that exponentiation of congruences classes is not well-defined in general, by exhibiting specific $a, a', b, b', n$ such that $a \equiv a' \bmod n, b \equiv b' \bmod n$, but $a^b \not\equiv a'^{b'} \bmod n$.

**Solution.** There are lots of counterexamples for this problem. One such example is $a = a' = 2$, $b = 10$, $b' = 20$, $n = 10$. If we check this, we see that $a^b = 2^{10} \equiv 4 \pmod{10}$, but $a^{b'} = 2^{20} \equiv 6 \pmod{10}$. □