WRITTEN HW #4, DUE OCT 24 2011

Remember to write clearly and to justify all your claims in your solutions. Please staple your assignment before turning it in.

(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.

(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) $244x \equiv 32 \bmod 75$

(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.

(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 $a^b \not\equiv a'^{b'} \bmod n$.