15-151 Homework 8

Please submit in class at 8:00am on Tuesday 1st August

Exercises

In the following exercises, the notation $[n]$, for $n \in \mathbb{N}$, refers to the set $\{k \in \mathbb{N} \mid 1 \leq k \leq n\}$.

1. For each $a \in [14]$ coprime to 14, find a multiplicative inverse for a modulo 14 and the order of a modulo 14. **[4 points]**

2. The parts of this question form a proof of Fermat's little theorem. Throughout this question, p is a prime modulus and a is an integer not divisible by p.

   (a) Explain why each element of $[p-1]$ is coprime to p. **[1 points]**

   (b) Prove that, for each $x \in [p-1]$, there exists an element of $\{a, 2a, \ldots, (p-1)a\}$ which is congruent to x modulo p. **[3 points]**

   (c) Prove that, for all $k, \ell \in [p-1]$, if $ka \equiv \ell a \bmod p$, then $k = \ell$. **[3 points]**

   (d) Use parts (b) and (c) to prove that $(p-1)! \equiv a^{p-1}(p-1)!$. **[3 points]**
   Hint: $a^{p-1}(p-1)! = a \times 2a \times \cdots \times (p-1)a$.

   (e) Explain why this implies that $a^{p-1} \equiv 1 \bmod p$. **[2 points]**

3. Find the last two digits of $7^{7^{7^{7^{7^{7^{7}}}}}}$. **[6 points]**

   Hint: recall from class that $7^4 \equiv 1 \bmod 100$.

4. For each of the following functions, determine (with proof) whether it is injective and whether it is surjective.

   (a) $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(m,n) = 2^m(2n+1)$ for all $(m,n) \in \mathbb{N} \times \mathbb{N}$. **[5 points]**

   (b) $q : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ defined by $q(a,b) = \dfrac{a}{b}$ for all $(a,b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. **[5 points]**

Project milestone

Complete the questionnaire located at the following URL:

`https://goo.gl/forms/1CX86soJ3Kauki9A3` **[3 points]**