Assignment 5

Tuesday June 12, 2012

1 Algebra

This section is intended to completed on Friday June 11th.

Let p be a prime number for the following two problems. Recall for every a where $a \not\equiv 0 \mod p$, there is an inverse; ie. there is some b such that $a \cdot b \equiv 1 \mod n$. This result will come in handy for the next two problems.

Problem 1. Fix p a prime number, and a such that $0 < a < p$.

1. Argue by contradiction that all the following are in distinct equivalence classes mod p:

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$$

2. Recall there are p congruence classes mod p. Use this and the previous part to argue that

$$a \cdot (2a) \cdot (3a) \cdot \cdots \cdot ((p-1)a) \equiv (p-1)! \mod p$$

3. This does not use the previous parts of the problem. Argue that

$$a \cdot (2a) \cdot (3a) \cdot \cdots \cdot ((p-1)a) \equiv a^{p-1}(p-1)! \mod p$$

4. Argue that $a^{p-1} \equiv 1 \mod p$ using the previous two parts.

You just proved **Fermat's Little Theorem**

Problem 2. Let p be a prime number larger than 2

1. Take $a \in \mathbb{Z}$ such that $a \not\equiv 0 \mod p$. By the handy result above, a has an inverse. Prove that this inverse is unique. *Hint: Suppose it had two inverses; show they are equal*

   As inverses are unique, we can make a notation for them: call the inverse of a, whenever a is nonzero, a^{-1}. So for nonzero a, we have $a \cdot a^{-1} \equiv 1 \mod n$.

2. Prove that $(a^{-1})^{-1} = a$; that is the inverse of a's inverse is a.

3. Note that $a^2 - 1 \equiv (a+1)(a-1) \mod p$. Prove that $a^2 \equiv 1 \mod p$ if and only if $(a \equiv 1 \mod p)$ or $(a \equiv -1 \mod p)$.

4. Prove that

$$(p-1)! \equiv (p-1) \mod p$$

   Hint: Look at $2 \cdot 3 \cdot \cdots \cdot p-2$. *Everything on this list has an inverse. Use the previous results to show that the inverse is on this list, cannot be itself, and that its inverse's inverse is itself. So what is this product congruent to mod p?*

You just prove **Wilson's Theorem**

2 Relations

This section is intended to be completed on Friday June 11th.

Problem 3. Consider the following theorem and proof:

> **Theorem 1.** *If R is a symmetric and transitive relation on A, then R is reflexive.*
>
> *Proof.* Take $a \in A$. We want to show that aRa. Well, as aRb then we have by symmetry bRa. We have aRb and bRa, so by transitivity we have aRa. Thus R is reflexive. □

Give the error of this proof.

3 Basic Functions

This section is intended to be completed on Monday June 11th.

Problem 4. Tell me if the following relations are functions; if they are then give the range.

1. $\{ (0,1), (5,6), (2,2) \}$
2. $\{ (0,2), (5,3), (0,3), (1,2) \}$

Problem 5. For each of the following rules, decide whether they are well-defined functions. Explain why.

1. $f : \mathbb{Q} \to \mathbb{Q}$ defined by
$$f\left(\frac{a}{b}\right) = a$$
2. $f : \mathbb{Q} \to \mathbb{Q}$ defined by
$$f\left(\frac{a}{b}\right) = \frac{b}{a}$$
3. $g : Z_3 \to Z$
$$g([x]_3) = x + 2$$
4. $k : \mathbb{Z} \to \mathbb{Z}_7$
$$k(n) = 7n$$

Problem 6. Give the range of the following functions:

1. $f : \mathbb{N} \to \mathbb{N}$ defined by
$$f(x) = 2x + 3$$
2. $f : \mathbb{R} \to \mathbb{R}$ defined by
$$f(x) = \sqrt{2} \cdot x$$

Problem 7. Fix $f : \mathbb{R} \to \mathbb{R}$ by
$$f(x) = 2x + 1$$
And $g : \mathbb{R} \to \mathbb{R}$ by
$$g(x) = \sin(x)$$
Determine the following

1. $f[(0,1)]$
2. $f^{-1}[(0,1)]$
3. $g[[0, \frac{\pi}{2}]]$
4. $g^{-1}[[-1,1)]$

4 A Preview of Cardinality

This section is intended to be completed on Monday June 11th. Here we will just try to preview what we will do with the rest of our week.

Problem 8. Write down a function from $\mathbb{N}$ to $\mathbb{Z}$ such that for every $y \in \mathbb{Z}$.

$$f^{-1}[\{y\}] \neq \emptyset$$