MATH 441; EXAM # 1, 100 points, February 22, 2005 (R.A.Brualdi)

TOTAL SCORE (5 problems; 100 points possible):

Name: SOLUTIONS

1. [20 points] Let $\equiv$ be an equivalence relation on a set S. Let a, b be two elements in S.

Prove that if the equivalence classes containing a and b have a nonempty intersection, that is, $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$.

Suppose that $c \in [a] \cap [b]$. Let $x \in [a]$. By properties of an equivalence relation (reflexive,symmetric, transitive) we have $x \equiv a \equiv c \equiv b$ and so $x \equiv b$. Thus $[a] \subseteq [b]$ and in a similar way one concludes that $[b] \subseteq [a]$. Hence $[a] = [b]$.

2. [20 points] determine the least nonnegative residue of the following (**calculator answer not acceptable**):

- 8^{101} mod 9.

  We have $8 \equiv -1$ mod 9, and so $8^{101} \equiv (-1)^{101} = -1 \equiv 8$ mod 9

- 13^{101} mod 168.

  We have $13^2 = 169 \equiv 1$ mod 168 and so $13^{101} \equiv (13^2)^{50} \cdot 13 \equiv 1^{50} \cdot 13 = 13$ mod 168.

- 12345678987654321 mod 11

  The given number is congruent mod 11 to: $1 - 2 + 3 - 4 + 5 - 6 + 7 - 8 + 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 1$.

- 12345678987654321 mod 8

  The given number is congruent mod 8 to 321, since 1000 is divisible by 8, and 321 is congruent to 1 mod 8.

3. [30 points] Consider the commutative ring with identity, $Z/18Z$.

- What is $\phi(18)$?

  $\phi(18) = 6$

- Determine which elements of $Z/18Z$ are units?

  For $a \in \{1, 2, \ldots, 18\}$ to be a unit, $\text{GCD}(a, 18) = 1$. So we get as units: $1, 5, 7, 11, 13, 17$.

- Pair up the units of $Z/18Z$ so that in each pair $\{a, b\}$, b is the inverse of a. (Of course, some elements might be paired with themselves.)

  1 and 1, 5 and 11, 7 and 13, 17 and 17.

- If possible, solve 5x=7 in $Z/18Z$.

  By above 11 is the inverse of 5 mod 18. So in $Z/18Z$, we have $x = 11 \cdot 7 = 5$.

4. [15 points] Let R be a commutative ring R with identity. Let a and b be elements in R.

- What is the definition of $-a$ in R?

  $-a$ is defined to be the element of R which when added to a, in either order, gives 0.

- Prove that $-(ab) = a(-b)$.

  We have $ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$ by distributive law and a property of 0. Addition in the other order works in a similar way.

5. [15 points] **Prove using mathematical induction** that for $x \neq 1$ (**Be sure to set up the induction carefully**):

$$1 + x + x^2 + \cdots + x^{n-1} = \tfrac{1-x^n}{1-x}, \quad (n \geq 1).$$

We use induction on $n \geq 1$. If $n = 1$, the LHS is 1 and the RHS is $1 - x/1 - x = 1$. Now assume the identity holds for n, and we prove directly that it holds for $n + 1$:

$$\begin{aligned} 1 + x + x^2 + \cdots + x^{n-1} + x^n &= (1 + x + x^2 + \cdots + x^{n-1}) + x^n \\ &= \frac{1 - x^n}{1 - x} + x^n \\ &= \frac{1 - x^n + x^n(1 - x)}{1 - x} \\ &= \frac{1 - x^{n+1}}{1 - x} \end{aligned}$$

which is the identity with n replaced by $n + 1$.

Hence the identity is true for all $n \geq 1$ by induction.