SECOND 347 MIDTERM, FALL 2005
DUE WEDNESDAY 10/26

You are not allowed to discuss these problems with anybody apart from me. You are allowed to use without proof everything that we did in class and everything you proved on former homework assignements or midterms.

If you do not know how to approach a problem, try to use the list from homework number 5. Writing down cleanly what you need to prove, how your proof would start and what exactly you need to show will give you partial credit. For the proof writing questions, never just put formulas and some dots on the paper, write down formal proofs with whole sentences.

(1) Let p and q be prime numbers. Set $n = p \cdot q$ and

$$m = (p-1) \cdot (q-1).$$

Let e be a natural number such that e and m share no common factors. Then there are positive integers d and y such that

$$ed = 1 + my.$$

Let now W be a non-negative integer less then n. Let C be the remainder if W^e is divided by n.

(a) (7 points) In the example $p = 3$ and $q = 5$, compute m, and then find (by trial and error if necessary) possible values for e and d.

(b) (5 points) Stick with the values for e, d and y you chose in part (a). Starting with $W = 8$, compute C and C^d and the remainder of C^d if divided by n. Then do the same for $W = 7$.

(c) (6 points) Let a and k be a natural numbers, and let b be an integer. Prove: if r is the remainder of b modulo a then the remainder of b^k modulo a equals the remainder of r^k modulo a.

(d) (12 points) Use Fermat's little theorem to prove that for any values of p, q and e satisfying the above conditions, the remainder of C^d modulo n is W.

Date: October 20, 2005.

For the following problem you are allowed to use the fact that the natural numbers are unbounded, i.e. that for every real number r there exists a natural number m sch that $m > r$.

(2) (16 points) Let a_n be the sequence

$$a_n := \frac{2n}{n - \frac{1}{2}}.$$

Prove the following statement: for every real number $\varepsilon > 0$ there exists a natural number N such that for every natural number $n \geq N$:

$$|a_n - 2| < \varepsilon$$

This should be easy, once you have exactly understood what there is to do.

(3) What is the largest real number r such that for every real number x with absolute value $|x| < r$ the equation

$$x^2 \leq 3|x|$$

holds?

(a) (3 points) Find r.

(b) (7 points) Write down a formal proof that, with your r from part (a), for every real number x whose absolute value $|x|$ is strictly less then r the equation

$$x^2 \leq 3|x|$$

holds.

(c) (9 points) Prove that your r is the largest real number with this property.

(4) **Bar codes:** Let

$$d_1 \quad d_2 \quad d_3 \quad d_4 \quad d_5 \quad d_6 \quad d_7 \quad d_8 \quad d_9 \quad d_{10} \quad d_{11} \quad d_{12}$$

be the twelve digits of a bar code (also called UPC). Bar codes are always made in such a way that

$$3d_1 + d_2 + 3d_3 + d_4 + 3d_5 + d_6 + 3d_7 + d_8 + 3d_9 + d_{10} + 3d_{11} + d_{12}$$

is a multiple of 10. (Check this in the supermarket!) This helps to prevent errors when the number is communicated.

(a) (3 points) Which of the following is a correct UPC?

0 71734 00021 8

0 70734 00021 8

0 70743 00021 8

(b) (4 points) Find the covered digit of the following UPC:

$$0 \quad 28500 \quad 11070 \quad \square$$

(c) (5 points) Find the covered digit of the following UPC:

$$0 \quad 48001 \quad 26\square 04 \quad 2$$

(d) (4 points) A UPC number for a product is

$$0 \quad 51000 \quad 02526 \quad 5.$$

Explain why the errors in the following misread version of this UPC would not be detected by this way of checking it:

$$0 \quad 51000 \quad 02625 \quad 5$$
$$0 \quad 50000 \quad 05526 \quad 5$$

(5) You might want to compare this problem to Definition 1.39 of the book (page 16).

Consider the set $\mathbb{Q} \times \mathbb{Q}$ of ordered paires of rational numbers. For such pairs, define $+$ and $\times$ by

$$(a, b) + (c, d) := (a + b, c + d) \quad \text{and}$$
$$(a, b) \times (c, d) := (ac + 2bd, ad + bc).$$

For example

$$\left(\frac{1}{2}, \frac{2}{3}\right) \times \left(-5, \frac{9}{2}\right) = \left(\frac{19}{6}, -\frac{13}{12}\right).$$

(a) (6 points) Prove that $+$ and $\times$ are commutative, associative and distributive. You are allowed to use that addition and multiplication of rational numbers is commutative, associative and distributive.

For example $+$ is commutative: Let $a, b, c, d \in \mathbb{Q}$ be arbitrary. Sice addition of rational numbers is commutative, we know that $a + c = c + a$ and $b + d = d + b$. Therefore

$$(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b).$$

(b) (4 points) Show that there exists a pair $(a_0, b_0) \in \mathbb{Q} \times \mathbb{Q}$ such that for every pair $(a, b) \in \mathbb{Q} \times \mathbb{Q}$,

$$(a_0, b_0) + (a, b) = (a, b).$$

Show that there exists a pair $(a_1, b_1) \in \mathbb{Q} \times \mathbb{Q}$ such that for every pair $(a, b) \in \mathbb{Q} \times \mathbb{Q}$,

$$(a_1, b_1) \times (a, b) = (a, b).$$

(c) (2 points) With the (a_0, b_0) you found above, show that for every pair $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ there exists a pair "$-(a, b)$" in $\mathbb{Q} \times \mathbb{Q}$ such that $(a, b) + (-(a, b)) = (a_0, b_0)$.

(d) (7 points) With the (a_1, b_1) you found above, show that for every pair $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ such that $(a, b) \neq (a_0, b_0)$, there exists a pair "$(a, b)^{-1}$" in $\mathbb{Q} \times \mathbb{Q}$ such that $(a, b) \times (a, b)^{-1} = (a_1, b_1)$.