MAT 312/AMS 351
Midterm exam #1 with SOLUTIONS
Tuesday 10/8/02

1. Prove by induction that for all positive integers n,

$$\sum_{i=1}^{n} i(i-1) = \frac{n(n^2-1)}{3}.$$

SOLUTION: The base case $n = 1$ is true since both sides of the equality to be established produce 0. So assume that $k \in \mathbb{Z}_{>1}$ and that the equality is valid for $n = k - 1$. Then

$$\sum_{i=1}^{k} i(i-1) = \sum_{i=1}^{k-1} i(i-1) + k(k-1) = \frac{(k-1)((k-1)^2-1)}{3} + \frac{3k(k-1)}{3}$$

$$= \frac{(k-1)((k-1)^2-1+3k)}{3} = \frac{(k-1)(k^2-2k+1-1+3k)}{3} = \frac{(k-1)(k^2+k)}{3}$$

$$= \frac{k(k-1)(k+1)}{3} = \frac{k(k^2-1)}{3}.$$

Hence the equality is also valid for $n = k$ and by induction for all $n \in \mathbb{Z}_{>0}$.

The next question dealt with the issue of dividing an integer b by an integer a to obtain a quotient q and a remainder r. Since the textbook calls this procedure "the division algorithm," it could have been misinterpreted to deal with the algorithm for obtaining the gcd of a and b. Both interpretation were considered legitimate. The answers under the second interpretation are marked as ALTERNATE SOLUTION.

2. (a) Let a and b be positive integers. State the Euclidean algorithm for dividing b by a.
SOLUTION: Let a and $b \in \mathbb{Z}_{>0}$. There exist unique integers q and $r \in \mathbb{N}$ such that

$$0 \leq r < a$$

and

$$b = qa + r.$$

ALTERNATE SOLUTION: There exist unique integers q_i and $r_i \in \mathbb{N}$, $1 \leq i \leq n$, such that

$$b = q_1 a + r_1, 0 < r_1 < a,$$
$$a = q_2 r_1 + r_2, 0 < r_2 < r_1,$$
$$r_1 = q_3 r_2 + r_3, 0 < r_3 < r_2,$$
$$\ldots,$$
$$r_{n-2} = q_n r_{n-1} + r_n, 0 < r_n < r_{n-1},$$
$$r_{n-1} = q_{n+1} r_n,$$

and hence

$$(b, a) = r_n.$$

(b) Apply the Euclidean algorithm to $a = 6$ and $b = 25$.
SOLUTION:

$$25 = 4 \cdot 6 + 1.$$

ALTERNATE SOLUTION:

$$25 = 4 \cdot 6 + 1,$$
$$6 = 6 \cdot 1,$$

and hence

$$(25, 6) = 1.$$

(c) Apply the Euclidean algorithm to $a = -6$ and $b = -25$.
SOLUTION:

$$-25 = 5 \cdot (-6) + 5.$$

ALTERNATE SOLUTION:

$$-25 = 5 \cdot (-6) + 5,$$
$$-6 = -2 \cdot 5 + 4,$$
$$5 = 1 \cdot 4 + 1,$$
$$4 = 4 \cdot 1,$$

and hence

$$(-25, -6) = 1.$$

3. This problem involves arithmetic modulo 16. All answers should only involve expressions of the form $[a]_{16}$, with a an integer and $0 \leq a < 16$.
(a) Compute $[4]_{16} + [15]_{16}$.
SOLUTION:

$$[4]_{16} + [15]_{16} = [4]_{16} + [-1]_{16} = [3]_{16}.$$

(b) Compute $[4]_{16}[15]_{16}$.
SOLUTION:

$$[4]_{16}[15]_{16} = [4]_{16}[-1]_{16} = [-4]_{16} = [12]_{16}.$$

(c) Compute $[15]_{16}^{-1}$.
SOLUTION:

$$[15]_{16}^{-1} = [-1]_{16}^{-1} = [-1]_{16} = [15]_{16}.$$

(d) List the units in $\mathbb{Z}_{16}$.
SOLUTION:

$$\{[1]_{16}, [3]_{16}, [5]_{16}, [7]_{16}, [9]_{16}, [11]_{16}, [13]_{16}, [15]_{16}\}.$$

(e) List the zero-divisors in $\mathbb{Z}_{16}$.
SOLUTION:

$$\{[2]_{16}, [4]_{16}, [6]_{16}, [8]_{16}, [10]_{16}, [12]_{16}, [14]_{16}\}.$$

4. In this problem you will use the Chinese remainder theorem (CRT) to solve for all integers x that satisfy

$$2x \equiv 4 \mod 8,$$
$$6x \equiv 18 \mod 30$$

and

$$3x \equiv 12 \mod 21.$$

(a) Transform each of the above equations to equivalent equations of the form

$$x \equiv a \mod m.$$

SOLUTION: Let $ax \equiv b \mod n$ be a congruence equation. If $d = (a, n)|b$, then this equation is equivalent to $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{n}{d}$. Thus our three equations translate to

$$x \equiv 2 \mod 4,$$

$$x \equiv 3 \mod 5$$

and

$$x \equiv 4 \mod 7.$$

(b) What conditions do the three resulting moduli m have to satisfy in order to apply CRT?
SOLUTION: They must be pairwise relatively prime.
(c) Solve simultaneously the three congruences. Express your answer as a single congruence class.
SOLUTION: The solution is of the form $[a]_M$ and $M = 4 \cdot 5 \cdot 7 = 140$. To find the smallest positive a, we note that the three equations have respective positive solutions given by

$$\{2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46..., \},$$

$$\{3, 8, 13, 18, ..., 48, 53, ..., \}$$

and

$$\{4, 11, 18, 25, 32, 39, 46, 53, 60, 67, 74, 81, ..., \}.$$

We are looking for the smallest integer to be found in all three sets: 18. Thus our solution is

$$x \equiv 18 \mod 140.$$

We can get the the same result in a different way. We form

$$M_1 = \frac{M}{4} = 35, M_2 = \frac{M}{5} = 28, M_3 = \frac{M}{7} = 20,$$

and then

$$y_1 \in [35]_4^{-1} = [3]_4^{-1} = [3]_4, y_2 \in [28]_5^{-1} = [3]_5^{-1} = [2]_5, y_3 \in [20]_7^{-1} = [6]_7^{-1} = [6]_7.$$

Then

$$x \equiv 2 \cdot 3 \cdot 35 + 3 \cdot 2 \cdot 28 + 4 \cdot 6 \cdot 20 = 858 \equiv 18 \mod 140.$$

5. (a) State Euler's theorem.
SOLUTION: Let n be an integer ≥ 2 and a an integer that is relatively prime to n. Then

$$a^{\varphi(n)} \equiv 1 \mod n.$$

(b) Compute $\varphi(100)$.
SOLUTION:

$$\varphi(100) = \varphi(2^2 5^2) = \varphi(2^2)\varphi(5^2) = (4-2)(25-5) = 40.$$

(c) Use Euler's theorem to compute $7^{2962} \mod 100$.
SOLUTION:

$$7^{2962} = 7^{40 \cdot 74 + 2} \equiv 7^2 = 49 \mod 100.$$