

# MIDTERM

7 November 2013

**No calculators, no books, no notes.**

There are 5 questions, for a total of 100 points.

For credit you need to write clearly and fully justify everything you write down. If you use theorems proved in class, or in the book, or elsewhere, in the course of a proof, make clear what result you are using. We will grade only what is written on the page and marked as part of the solution (e.g. not crossed out).

Do not get hung up on one problem. Make sure you get to work on all of them.

1. (10 points) Compute  $\phi(25000)$ .
2. (20 points) Find all positive integers less than 1000 that leave the remainder 1 when divided by each of 2, 3, 5 and 7.
3. (15 points) Factor the following polynomial into linear factors (mod 13) or show that it is irreducible (mod 13).

$$X^2 + 4X - 3$$

4. (20 points) Show that  $(n^2 + n) \equiv 0 \pmod{2}$  for any integer  $n$ .
5. (a) (10 points) Let  $a$  and  $n$  be relatively prime positive integers. Using what you know about gcd, show that  $a$  has an inverse  $b \pmod{n}$ , i.e.  $ab \equiv 1 \pmod{n}$ .
  - (b) (10 points) Show that  $b$  is relatively prime to  $n$ .
  - (c) (15 points) Show that  $\text{ord}_n(a) = \text{ord}_n(b)$ .

Question:	1	2	3	4	5	Total
Points:	10	20	15	20	35	100
Score:						

Good luck! ☺