

Due: October 26

Collaborative – Collaboration Allowed

All the usual instructions apply. I decided to make this test collaborative so that you can use Thursday 25 to meet.

Do **four** of the following five problems. If you do more than four, please be clear about which four you wish to count.

- (1) (a) Prove that  $38(7^{2n+1}) - 13(16^{2n})$  is divisible by 23 for all  $n \geq 0$ . (Hint: use congruences!)
- (b) Is  $3333^{4444} + 4444^{3333}$  divisible by 77? Hint: This will be easier if you notice that a number is divisible by 77 if and only if it is divisible by both 7 and 11.
- (2) (a) Let  $a, b, n$  be integers with  $n \geq 0$ . Use induction and the result of problem 5(b) from Test #3 to prove the *Binomial Theorem*:

$$\begin{aligned}(a+b)^n &= a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{i}a^{n-i}b^i + \cdots + \binom{n}{n-1}ab^{n-1} + b^n \\ &= \sum_{i=0}^n \binom{n}{i}a^{n-i}b^i.\end{aligned}$$

- (b) Prove that if  $p$  is prime then  $\binom{p}{i} \equiv 0 \pmod{p}$  for  $1 \leq i \leq p-1$ .
- (c) Let  $p$  be a prime and  $a, b$  integers. Prove *The Freshman's Dream*:

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

(Yes, I *am* making fun of freshmen!)

- (3) Here are a couple more divisibility tests for you:
  - (a) Prove that the remainder upon dividing an integer by 9 is the same as the remainder upon dividing the sum of its digits by 9.
  - (b) Let  $n$  be a 7 digit number and  $d_6d_5d_4d_3d_2d_1d_0$  its base 10 representation. Prove that  $n$  is divisible by 7 if and only if  $d_0 + 3d_1 + 2d_2 - d_3 - 3d_4 - 2d_5 + d_6$  is divisible by 7.
- (4) (a) In a homework problem, we showed that the usual cancellation law does not hold for congruences. That is, if  $ab \equiv ac \pmod{m}$  and  $a \not\equiv 0 \pmod{m}$ , it is not necessarily the case that  $b \equiv c \pmod{m}$ . However, cancellation law does hold when the modulus (i.e., the integer  $m$  above) is prime. Prove this fact.
- (b) Can you generalize part (a) in some fashion? That is, suppose  $ab \equiv ac \pmod{m}$  (where  $m$  is not necessarily prime anymore). Under what conditions can you cancel  $a$  from both sides of the congruence? Do a few examples and then make a conjecture. (Hint: examine the cases  $m = 8$  and  $m = 10$  thoroughly. Your generalization might use gcds in some way.)
- (5) (a) Let  $p$  be an odd prime. Prove that  $p \equiv 1 \pmod{4}$  or  $p \equiv 3 \pmod{4}$ .
- (b) Let  $n$  be a positive integer such that  $n \equiv 3 \pmod{4}$ . Prove that  $n$  is divisible by some prime  $p$  such that  $p \equiv 3 \pmod{4}$ .
- (c) Prove there are infinitely many primes which are congruent to 3 modulo 4. (Hint: Try to mimic Euclid's proof on page 35 of your notes. You may want to evaluate an expression of the form  $(p_1^2 p_2^2 \cdots p_k^2 + 2) \% 4$ .)

**Statement of Sources:** Give a list of all people with whom you discussed the problems on this test. Also, if you used any references besides the class notes, list them as well.