

MATH 580/780I MIDTERM 2 SOLUTIONS, FALL 2006

NIGEL BOSTON

1. (a)  $n = y^2 + 1$  where  $y = x^2$ . If prime  $p$  divides  $n$ , then  $y^2 \equiv -1 \pmod{p}$  has a solution, so  $p$  is not  $4k + 3$ .

(b) The values of  $x^4 \pmod{5}$  are 1 or 0, never  $-1$ . The values of  $x^4 \pmod{13}$  are 1, 3, 9 or 0, never  $-1$ .

2. (a) Since the  $\gcd(10, 25) = 5$ , which does not divide 37, there are no solutions.

(b) By the Chinese Remainder Theorem, since  $\gcd(6, 11) = 1$ , there is a unique solution  $\pmod{66}$ . The integers that are 3  $\pmod{11}$  are 3, 14, 25, 36, 47, ..., so we find 47 that is 5  $\pmod{6}$ . So the answer is all integers that are 47  $\pmod{66}$ .

3. (a)  $10! = 10 \cdot 9 \cdot 8 \cdots 5 \cdots 2 \cdot 1$  is divisible by 100 so the last two digits are 00.

(b)  $1 + 3 + 5 + 7 + 9 = 25$  whereas  $2 + 4 + 6 + 8 = 20$ . These are not congruent  $\pmod{11}$  so it fails the test for divisibility by 11. So the answer is no.

4. (a) By Bertrand, if  $n$  is even and  $n/2 \geq 2$ , i.e.  $n \geq 4$ , then there is a prime  $p$  such that  $n/2 < p < n$ , i.e.  $p < n < 2p$ . If  $n$  is odd, say  $2k - 1$  ( $k \geq 2$ ), there is a prime  $p$  such that  $k < p < 2k$ , i.e.  $(n+1)/2 < p \leq n$ , so  $p \leq n < 2p - 1 < 2p$ . This leaves  $n = 2$ , for which  $p = 2$  does the job.

(b) Take prime  $p$  as in part (a). Then of the integers  $1, 2, 3, \dots, n$ , only  $p$  is divisible by  $p$ . Thus,  $n!$  contains  $p$  to the power 1, so is not a square.

5. (a) State as in the book.

(b) By Fermat,  $2^p \equiv 2 \pmod{p}$ , so  $n \equiv 1 \pmod{p}$ , say  $n = kp + 1$ . Since  $n = 2^p - 1$ ,  $2^p \equiv 1 \pmod{n}$ , so  $2^{kp} \equiv 1 \pmod{n}$ , so  $2^n = 2^{kp+1} \equiv 2 \pmod{n}$ .