

MATH 580/780I FINAL SOLUTIONS, FALL 2006

NIGEL BOSTON

1. (a)  $(a + b)^n = a^n + \binom{n}{1}a^{n-1}b + \dots + \binom{n}{r}a^{n-r}b^r + \dots + b^n$   
 (b)  $\binom{n}{4} = n(n-1)(n-2)(n-3)/24$  is an integer.
2.  $72 = 2 * 30 + 12, 30 = 2 * 12 + 6, 12 = 2 * 6 + 0$ , so  $\gcd(30, 72) = 6$ .  $6 = 30 - 2 * 12 = 30 - 2 * (72 - 2 * 30) = 5 * 30 - 2 * 72$ .
3. Dividing by 4,  $4x + 5y = 50$ . One solution is  $(0, 10)$ , so general solution is  $x = 5t, y = 10 - 4t$ . These are positive when  $t > 0$  and  $t < 5/2$ , so  $t = 1$  or  $2$ , leading to  $(5, 6)$  and  $(10, 2)$ .
4. (a)  $\gcd(a, b) = 2^4 3^3$ ; (b)  $\text{lcm}(a, b) = 2^5 3^5 5^2 7^3$ ; (c)  $a + b = 3^3(2^5 5^2 + 2^4 3^2 7^3)$  is divisible by  $3^3$  but not  $3^4$ , since the number in brackets is not divisible by 3.
5. (a) If  $n > 3$ ,  $n! - 1 \equiv 3 \pmod{4}$ , so not a square.  $3! - 1 = 5$  is not a square. [Alternatively,  $n! = x^2 + 1$  contradicts  $x^2 + 1$  having no prime factors of the form  $4k + 3$  such as 3.]  
 (b)  $4p + 1 = n^2$  implies  $4p = n^2 - 1 = (n - 1)(n + 1)$ . By unique factorization,  $\{n - 1, n + 1\} = \{1, 4p\}$  or  $\{2, 2p\}$  or  $\{4, p\}$ . So  $n - 1$  or  $n + 1$  is at most 4, so  $n \leq 5$ . A finite check gives  $p = 2$ . [Alternatively, if  $p$  is odd, then  $4p + 1 \equiv 5 \pmod{8}$ , which squares never are.]
6. (a)  $987654321 \equiv 21 \pmod{100}$ . Powers of 21  $\pmod{100}$  are 21, 41, 61, 81, 1 so period 5.  $123456789 \equiv 4 \pmod{5}$  so  $987654321^{123456789} \equiv 81 \pmod{100}$ . Ans: 81.  
 (b) Sum of digits =  $7 + X + Y \equiv 0 \pmod{9}$  and  $3 + Y \equiv X + 4 \pmod{11}$ .  $X = 5, Y = 6$  works.
7.  $2x \equiv 5 \pmod{7}$  implies  $x \equiv 6 \pmod{7}$ .  $2x \equiv 2 \pmod{10}$  implies  $x \equiv 1 \pmod{5}$ . One solution is 6 and the Chinese Remainder Theorem says the solution is unique  $\pmod{35}$ . Ans:  $x \equiv 6 \pmod{35}$ .
8. (a)  $a^{\phi(n)} \equiv 1 \pmod{n}$  if  $\gcd(a, n) = 1$ .  
 (b) Certainly  $2^n \equiv 1 \pmod{2^n - 1}$ . If  $k < n$ , then  $2^k \not\equiv 1 \pmod{2^n - 1}$  since  $2^k - 1 < 2^n - 1$ . So the order is  $n$ . By Euler, the order divides  $\phi$  of the modulus.
9. Let  $p$  be 3, 11, or 17. If  $\gcd(a, p) = 1$ ,  $a^{p-1} \equiv 1 \pmod{p}$  (Fermat). Since each  $p - 1$  divides 560,  $a^{560} \equiv 1 \pmod{p}$ , so  $a^{561} \equiv a \pmod{p}$ . If  $\gcd(a, p) \neq 1$ , then  $a, a^{561} \equiv 0 \pmod{p}$  so  $a^{561} \equiv a \pmod{p}$ . Since  $a^{561} - a$  is divisible by 3, 11 and 17, it is divisible by  $3 * 11 * 17 = 561$ .
10. (a)  $f(mn) = f(m)f(n)$  whenever  $\gcd(m, n) = 1$ .  
 (b) Since 1 and  $n$  are divisors of  $n$ ,  $\sigma(n) \geq n + 1 > n$ . Since the divisors of  $n$  are a proper subset of  $\{1, 2, 3, \dots, n\}$ ,  $\tau(n) < n$ .

Typeset by  $\mathcal{A}\mathcal{M}\mathcal{S}$ -TEX