

MA312 Assignment #1

#2/ (e)  $\gcd: pq^2$   
 $\text{lcm}: p^2q^3$

#4/  $1 = 7s + 11t$   
 $1 = 7(-3) + 11(2)$

#6/ assume:  $a|c, b|c, \gcd(a,b)=1$  prove:  $ab|c$

proof: By assumption  $c = am = bn$  for some  $m, n \in \mathbb{Z}$ .  $\exists s, t$  s.t.  $as + bt = 1$ .  
 Mult. by  $c$ :  $cas + cbt = c$ . Using the assumptions we get  
 $bnas + amt = c$ . Now factor,  
 $ab(ns + mt) = c$ . Thus  $ab|c$ .

If  $a, b$  not rel. prime:  $a|b, b|b$  but  $a \cdot b \nmid b$ .

#9/ Let  $n \in \mathbb{Z}^+$ . If  $a \bmod n = a', b \bmod n = b'$ , prove  $(a+b) \bmod n = (a'+b') \bmod n$   
 $ab \bmod n = a'b' \bmod n$

(1)  $n|a-a' \wedge n|b-b' \Rightarrow n|a-a'+b-b' \Rightarrow a+b \bmod n = a'+b' \bmod n$   
 $\Rightarrow n|a+b - (a'+b') \Rightarrow$

(2) proof: since  $a = nq_1 + a', b = nq_2 + b'$  it follows that  
 $a+b = a - nq_1 + b - nq_2 + nq_3$  for some  $q_3 \in \mathbb{Z}$ .  
 modding out by  $n$  on both sides gives  $a'+b' \bmod n = a+b \bmod n$

(this part is similar)

#11/ Let  $n, a \in \mathbb{Z}^+, d = \gcd(a, n)$  Show  $ax \bmod n = 1$  has sol'n  $\Leftrightarrow d=1$ .

$\Rightarrow$  If  $ax \bmod n = 1$  has sol'n then  $\exists y$  s.t.  $ay \bmod n = 1$ . Thus,

$ay + 1 = nq$  or  $ay' + nq = 1$  w/  $y', q \in \mathbb{Z}$ , implying  $d=1$ .

$\Leftarrow$  If  $d=1$  then  $\exists s, t \in \mathbb{Z}$  s.t.  $as + nt = 1$  or  $as + 1 = n(-t)$  implying  $(as) \bmod n = 1$   
 So  $s$  is a sol'n to the given.

#14/  $p, q, r$  primes  $\neq 3$ . Show  $3 \mid p^2 + q^2 + r^2$ . There are initially 3 possibilities:  $p=3k, p=3k+1, p=3k+2$ .

$$\left. \begin{array}{l} p=3k+1 \text{ or } p=3k+2 \text{ for } k \in \mathbb{Z}. \\ q=3l+1 \text{ or } q=3l+2 \quad l \in \mathbb{Z} \\ r=3s+1 \text{ or } r=3s+2 \quad s \in \mathbb{Z} \end{array} \right\} \text{ Because if } p=3k \text{ then } p \text{ is not prime or } p=3.$$

Either way  $p \equiv \pm 1 \pmod{3}$   
 $q \equiv \pm 1 \pmod{3}$   
 $r \equiv \pm 1 \pmod{3}.$

$$\begin{aligned} \text{So } p^2 + q^2 + r^2 &= (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 \pmod{3} \\ &= 1 + 1 + 1 \pmod{3} \\ &= 3 \pmod{3} = 0. \end{aligned}$$

$$\text{So } 3 \mid p^2 + q^2 + r^2.$$

$$\begin{aligned} \#16/ \quad 7^{1000} \pmod{6} &= (7 \pmod{6})^{1000} = 1 \\ 6^{1001} \pmod{7} &= (-1)^{1001} \pmod{7} = -1 \pmod{7} = 6 \end{aligned}$$

$$\#18/ \quad 402 \pmod{5} = 3^{402} \pmod{5} = (3^2)^{201} \pmod{5} = 9^{201} \pmod{5} = (-1)^{201} \pmod{5} = -1 \pmod{5} = 4$$

#20/ Let  $p_1, p_2, \dots, p_n$  be primes. Show  $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$  is divisible by none of the  $p_i$ .

$$\text{Set } n = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$$

$$n \bmod p_i = 1 \text{ for each } i \in 1, \dots, n.$$

If  $p_i \mid n$  then  $n = p_i q$  implying  $n \bmod p_i = 0$ . QED.

#21/ There are  $\infty$  primes.

Proof: Proceed by contradiction. Assume there are only a finite # of primes,  $p_1, p_2, \dots, p_n$ . Let  $n = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ .

By #20  $n$  is not divisible by any of the  $p_i$ . Since these are all the primes this means  $n$  is not divisible by any other prime.

By def'n  $n$  must be prime. But  $n$  is not on the list (if it were then we'd have  $p_i \mid n$  for some  $i$ ). Thus the  $p_i$  are not the only primes & we conclude there must be an  $\infty$  # of primes.