

## MATH 4400, SOLUTIONS TO THE MIDTERM EXAM

1) Find the last two digits of  $3^{125}$ .

Solution: The question is: What is  $3^{125}$  modulo 100? Since 3 is relatively prime to 100, we can apply the theorem of Lagrange to the group  $(\mathbb{Z}/100\mathbb{Z})^\times$ . The order of this group is  $\varphi(100) = \varphi(4)\varphi(25) = 2 \cdot 20 = 40$ . It follows that  $3^{40} \equiv 1 \pmod{100}$  and

$$3^{125} = 3^{3 \cdot 40 + 5} \equiv 3^5 \equiv 43 \pmod{100}.$$

2) Solve the system of congruences  $x \equiv 4 \pmod{55}$  and  $x \equiv 11 \pmod{69}$ .

Solution: The first equation implies  $x = 4 + k \cdot 55$ . Substituting into the second equation gives  $k \cdot 55 \equiv 7 \pmod{69}$ . The inverse of 55 modulo 69 is  $-5$ . Thus  $k \equiv -35$ .

3) Prove that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Solution:  $10^k \equiv 1 \pmod{9}$  for all integers  $k$ . If  $a_m, \dots, a_0$  are decimal digits of an integer  $n$ , then

$$n = a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_0 \equiv a_m + a_{m-1} + \dots + a_0 \pmod{9}.$$

4) Let  $G$  be a group and  $g$  an element in  $G$  of order 9. What is the order of  $g^3$ ? What is the order of  $g^2$ ? Justify your answers.

Solution: Since the order of  $g$  is 9,  $g^9, g^{18}, g^{27}, g^{36}, \dots$  are all powers of  $g$  equal to the identity element in  $G$ . Thus the order of  $g^k$  is the smallest integer  $m$  such that  $km$  is a multiple of 9. If  $k = 3$  then  $m = 3$ , if  $k = 2$  then  $m = 9$ .

5) Let  $S = \{p_1, \dots, p_n\}$  be a set of odd primes. Let  $m = 3p_1 \cdots p_n + 2$ . Show that  $m$  is divisible by an odd prime  $q \equiv 2 \pmod{3}$  not in the set  $S$ . Conclude that there are infinitely many primes congruent to 2 modulo 3.

Solution: Let  $m = q_1 \cdot q_2 \cdots q_s$  be a factorization into primes. Since  $m$  is odd the primes factors  $q_i$  are also odd. If  $q_i = p_j \in S$ , then  $q_i = p_j$  divides 2, a contradiction since  $q_i = p_j$  is odd. Thus all  $q_i$  are not in  $S$ . Since  $m$  is not divisible by 3,  $q_i \equiv 1 \pmod{3}$  or  $q_i \equiv 2 \pmod{3}$  for every  $i$ . If  $q_i \equiv 1 \pmod{3}$  for all  $i$  then  $m \equiv 1 \pmod{3}$ . But  $m \equiv 2 \pmod{3}$ , thus  $q_i \equiv 2 \pmod{3}$  for at least one prime  $q_i$ .

6) Let  $G$  be a group. Assume that  $a = a^{-1}$  for every  $a$  in  $G$ . Show that  $G$  is commutative, i.e.  $ab = ba$  for all  $a$  and  $b$  in  $G$ .

Solution:  $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ .