MATH 4400, SOLUTIONS TO THE MIDTERM EXAM

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

Solution: The question is: What is 3^{101} modulo 100? Since 3 is relatively prime to 100, we can use Euler's theorem modulo 100. Since $\varphi(100) = \varphi(4)\varphi(25) = 2 \cdot 20 = 40$, it follows that $3^{40} \equiv 1 \pmod{100}$ and

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

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 $k \cdot 55 = 7 \pmod{69}$. The inverse of 55 modulo 69 is -5. Thus $k = -35$.

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 $a_m, \ldots, a_0$ are decimal digits of an integer n, then

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

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, $g^9, g^{18}, g^{27}, g^{36}, \ldots$ 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) Find the inverse of $2 + 5i$ modulo 31. Is there an inverse of $2 + 5i$ modulo 29?

Solution: We are looking for $x + yi$ such that $(2 + 5i)(x + yi) = 1$. This leads to a pair of linear equations $2x - 5y = 1$ and $5x + 2y = 0$. Modulo 31 there is a unique solution, $x = 2/29$ and $y = -5/29$. The inverse of 29 modulo 31 is 15, so $30 + 18i$ is the inverse modulo 31. Modulo 29 the system has no solution: the determinant of the system is $29 \equiv 0 \pmod{29}$, so the two lines are parallel, but they do not coincide, since $(0, 0)$ is a solution to only one of the two equations. Alternatively, observe that $(2 + 5i)(2 - 5i) \equiv 0 \pmod{29}$, so $2 + 5i$ is a zero divisor, and thus it cannot be invertible.

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