Mathematics 100A Homework 5
Due: Wednesday 4 November 2020

Instructions: Please write clearly and fully explain your solutions. It is OK to work with others to solve the problems, but if you do so, you should write your solutions up separately. Copying solutions from your peers or a solutions manual will be deemed academic misconduct. Please feel free to reach out to me or the TA if you have any questions.

1. Chapter 2, exercise 9.3

Proof. If an integer \( a \) has decimal digits \( d_r d_{r-1} \cdots d_1 d_0 \) then \( a = \sum_k d_k 10^k \). But \( 10 \equiv 1 \pmod{9} \), so \( 10^k \equiv 1 \equiv 1 \pmod{9} \). Thus \( a \equiv \sum_k d_k \pmod{9} \), as desired. \( \square \)

2. Chapter 2, exercise 9.5

Proof. The answer is every odd integer. To see this, we first prove that if \( n \) is even, then there aren’t solutions to this congruence. To see this, one can reduce modulo 2 (because \( n \) is even!) to obtain \( -y \equiv 1 \pmod{2} \) and \( y \equiv 0 \pmod{2} \). But these two congruences are inconsistent, so there is not any solution.

Now suppose \( n \) is odd. Set \( x = n + 1 \), which is an integer because \( n \) is odd. Set \( y = 0 \). One verifies by substitution that these \( x, y \) solve the congruences. \( \square \)

3. Chapter 2, exercise 9.7

Proof. One verifies by computation that \( A^3 \equiv 1_2 \pmod{3} \). Thus the order of \( A \) is three, because the order is not 1, as \( A \) is not the identity modulo 3.

We claim that the order of \( B \) is 8. To see this, first compute that \( B^4 \equiv -1_2 \pmod{3} \). Then \( B^8 \equiv 1_2 \pmod{3} \). Therefore, the order of \( B \) divides 8, so is 1, 2, 4 or 8. But the order cannot be 1, 2, or 4 because \( B^4 \) is not congruent to 1 modulo 3. \( \square \)

4. This question has two parts.

(a) Suppose \( p \) is a permutation in \( S_n \), and that \( p = (12 \cdots k) \) for some \( k \leq n \). That is, \( p(1) = 2, p(2) = 3, \cdots, p(k) = 1 \) and \( p(j) = j \) if \( k + 1 \leq j \leq n \). Prove that \( sgn(p) = (-1)^{k-1} \). \textbf{Hint:} Induct on \( k \).

(b) Suppose \( n_1, n_2, \cdots, n_k \) are distinct integers between 1 and \( n \) inclusive. Let \( q \) be the permutation of \( S_n \) with cycle decomposition \( q = (n_1 n_2 \cdots n_k) \). Prove that \( q \) is conjugate to \( p \). Deduce that \( sgn(q) = (-1)^{k-1} \). \textbf{Hint:} Let \( g \) be any permutation in \( S_n \) with \( g(1) = n_1, g(2) = n_2, \ldots, g(k) = n_k \). Consider \( gpg^{-1} \).

Proof. There are two parts:

(a) We induct on \( k \), the case \( k = 1 \) being trivial. Now, recall the homomorphism \( L : S_n \to \text{GL}_n(\mathbb{R}) \) so that \( sgn(p) = \det(L(p)) \). Denote by \( p' \) the permutation \( (12 \cdots (k - 1)) \). By interchanging the \( k \) and \( (k - 1)'s \)t columns of \( L(p) \), one obtains \( L(p') \). Because interchanging columns multiplies the determinant by \( -1 \), one obtains \( \det(L(p')) = (-1) \det(L(p')) \). This gives the induction.

1
(b) Let \( g \) be any permutation of \( S_n \) with \( g(1) = n_1, g(2) = n_2, \ldots, g(k) = n_k \); it is clear that such a \( g \) exists because the \( n_1, n_2, \ldots, n_k \) are distinct. Set \( g' = g p q^{-1} \). We will verify that \( g' = q \). To do this, we evaluate \( g' \) on every integer \( \ell \), first if \( \ell \in \{n_1, n_2, \ldots, n_k\} \) and next if \( \ell \) is not in that set. For the first case, we have 
\[
q'(n_j) = (g p q^{-1})(g(j)) = gp = g(j + 1) = n_{j+1}
\]
if \( 1 \leq j < k \), and similarly \( q'(n_k) = n_1 \). For the second case, we have \( \ell = g(j) \) for some integer \( j \) with \( k < j \leq n \). Then
\[
q' (\ell) = (g p q^{-1})(g(j)) = gp = g(j) = \ell.
\]
Thus \( q'(\ell) = q(\ell) \) for all integers \( \ell \) with \( 1 \leq \ell \leq n \), so \( q' = q \).

Because \( sgn \) is a homomorphism to an abelian group \( \{\pm 1\} \), we obtain
\[
sgn(q) = sgn(g p q^{-1}) = sgn(g) sgn(p) sgn(q^{-1}) = sgn(p).
\]
Thus \( sgn(q) = (-1)^{k-1} \) as desired.

5. Chapter 2, exercise 10.2

Proof. The exercise has two parts:

(a) Suppose that \( xH \cap yK \) is nonempty, and contains some element \( z \). Then \( z \in xH \), so \( xH = zH \). Similarly, \( z \in yK \), so \( yK = zK \). Thus \( xH \cap yK = zH \cap zK \). Because left-multiplication by \( z \) is a bijection on \( G \), \( zH \cap zK = z(H \cap K) \). This is a single \( (H \cap K) \)-coset, as desired.

(b) Suppose \( [G : H] = m \) and \( [G : K] = n \) with \( G = x_1 H \cup \cdots \cup x_m H \) and \( G = y_1 K \cup \cdots \cup y_n K \). There are at most \( mn \) non-empty sets \( (x_j H) \cap (y_k K) \). From part (a), every such set is an \( (H \cap K) \)-coset. Moreover, every \( (H \cap K) \)-coset occurs in this list, because \( z(H \cap K) = (zH) \cap (zK) \). Thus \( [G : H \cap K] \leq mn \) and in particular is finite.

6. Chapter 2, exercise 12.4

Proof. The cosets of \( H = \{\pm 1, \pm i\} \) in \( G = C^\times \) consist of the sets \( \{z, iz, -z, -iz\} \) for \( z \in C^\times \). Geometrically, these complex numbers are related to each other by rotating the complex plane by a multiple of \( \pi/2 \). They are the four corners of a square.

One has that \( G/H \) is isomorphic to \( G \). Indeed, the map \( \varphi : G \rightarrow G \) given by \( \varphi(z) = z^4 \) has kernel exactly \( H \). Moreover, it is surjective because every nonzero complex number has a nonzero fourth root in \( C \). Thus, by the first isomorphism theorem, \( \varphi \) induces an isomorphism \( G/H \rightarrow G \).