Applied Algebra, MAT312/AMS351
Practice Problems for the Final: Solutions

(1) Find the greatest common divisor of $12n + 1$ and $30n + 2$.

Solution: Using the Euclidean algorithm, we find that

$$\gcd(30n + 2, 12n + 1) = \gcd(12n + 1, 6n) = \gcd(6n, 1) = 1.$$

(2) Prove that the product of three consecutive natural numbers is always divisible by 6.

Solution: If the first of the three integers is even, then the product is even. If it is odd, then the second of the three integers is even; thus the product is even in any case. A similar argument using the possible congruence classes of the first integer modulo 3 shows that the product is divisible by 3. Since 2 and 3 are relatively prime, the result follows by unique factorization of primes.

(3) Solve the following linear congruences
(a) $26x \equiv 8 \mod 44$;
(b) $24x \equiv 9 \mod 40$.

Solution: (a) Since the greatest common divisor of 26 and 44 is 2, which divides 8, this congruence–which is equivalent to $13x \equiv 4 \mod 22$–has a solution, namely $x = [13]_{22}^{-1}[4]_{22}$. Computing $[13]_{22}^{-1}$ by either running the Euclidean algortihm backwards or by the matrix method, we find $[13]_{22}^{-1} = [-5]_{22}$. Thus $x = [2]_{22}$.

(b) Since the greatest common divisor of 40 and 24 (i.e. 8) does not divide 9, this congruence has no solution.

(4) Solve the following system of linear congruences:

$$\begin{cases} x \equiv 4 \mod 25 \\ 3x \equiv 6 \mod 39 \end{cases}$$

Solution: This is equivalent to the system

$$\begin{cases} x \equiv 4 \mod 25 \\ x \equiv 2 \mod 13 \end{cases}$$

which, by the Chinese Remainder Theorem, has a solution. Since $25\cdot(-1)+13 \cdot (2) = 1$, the solution is $x \equiv (4 \cdot 13 \cdot 2) + (2 \cdot 25 \cdot (-1)) = 54 \mod 325$.

(5) Show that the equation $5x^7 - x^4 = 23$ has no integer solutions.

Solution: If we reduce this equation mod 2, it becomes $x^7 + x^4 \equiv 1 \mod 2$, which has no solution (direct check for all cogruence classes mod 2).

(6) Recall that the Fibonacci sequence is defined as $F_1 = 1, F_2 = 1$, and then for every $n > 2$, $F_n = F_{n-1}+F_{n-2}$. Prove that for every n, $F_2+F_4+\cdots+F_{2n} = F_{2n+1} - 1$.

Solution: We proceed by induction on n. When $n = 1$, the assertion amounts to $F_2 = F_3 - 1$; since $F_1 = 1$, this is immediate from the definition of the Fibonacci sequence. Now assume that it is true for k. We then have

$$\begin{aligned} F_2 + F_4 + \cdots + F_{2(k+1)} =& (F_2 + F_4 + \cdots + F_{2k}) + F_{2k+2} \\ =& (F_{2k+1} - 1) + F_{2k+2} \\ =& F_{2k+3} - 1 = F_{2(k+1)+1} - 1. \end{aligned}$$

(7) Find the last two digits of the number 3333^{4444}.

Solution: Since 3333 is relatively prime to 100, we may use Euler's Theorem. We have that $\phi(100) = 40$ and $3333 \equiv 33 \mod 100$, so $3333^{4444} \equiv 33^4 = 3^4 \cdot 11^4 = 81 \cdot 121 \cdot 121 \equiv 81 \cdot 21 \cdot 21 \equiv 1701 \cdot 21 \equiv 1 \cdot 21 = 21 \mod 100$.

(8) Let G be a group and $C = \{a \in G : ax = xa \text{ for all } x \in G\}$. Prove that C is a subgroup of G.

Solution: It suffices to show that for all $a, b \in C, ab \in C$ and $a^{-1} \in C$. Let $a, b \in C$ and x be any element of G. Then $(ab)x = a(bx) = (bx)a = (xb)a = x(ba) = x(ab)$. Also, since a commutes with every element of G, it commutes with x^{-1} in particular, i.e. $ax^{-1} = x^{-1}a$. Taking inverses of both sides gives $xa^{-1} = a^{-1}x$.

(9) Let R be a relation on $\mathbb{Q}^\times$ (nonzero rational numbers) defined by:

aRb if and only if ab is a square of a rational number.

Prove that R is an equivalence relation.

Solution: (Reflexivity) For all $a \in \mathbb{Q}^\times$, $aa = a^2$. (Symmetry) Observe that multiplication of rationals is commutative. (Transitivity) Let $a, b, c, q, r \in \mathbb{Q}^\times$ be such that $ab = q^2$ and $bc = r^2$. Then $(qrb^{-1})^2 = (ab)(bc)(b^{-2}) = ac$.

(10) Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 4 & 2 \end{pmatrix}$.

(a) Compute $(145)\pi$.
(b) Determine the order of π.
(c) Determine the sign of π.

Solution: First note that π may be written in cycle notation as $(13)(46)(257)$.
(a) $(145)\pi = (145)(13)(46)(257) = (1346572)$.
(b) $o(\pi) = \text{lcm}(o((13)), o((46)), o((257))) = 6$ (this works since the cycles in question are disjoint).
(c) $\text{sign}(\pi) = \text{sign}((13)) \cdot \text{sign}((46)) \cdot \text{sign}((257)) = 1$. (Alternative solution: count inverstions in π.)

(11) (a) What is the order of the group $S(4)$?
(b) What are the possible orders of elements in a group of order 24?
(c) What are the possible orders of permutations in the group $S(4)$?

Solution: (a) The order of $S(4)$ is $4! = 24$. (b) By Lagrange's Theorem, the only possible orders of an element in a group of order 24 are 1,2,3,4,6,8,12, and 24. (c) An element of $S(4)$ which is not the identity can be written as either a 2-cycle, a 3-cycle, a 4-cycle, or a product of two disjoint 2-cycles. Thus the possible orders of an element of $S(4)$ are 1,2,3, and 4.

(12) Let a, b, c be elements of some group G. Solve the equation $(ax)(bc) = e$ in G. Justify every step.

Solution: $(ax)(bc) = e \Rightarrow ax = (bc)^{-1}$ (existence of inverses) $\Rightarrow ax = c^{-1}b^{-1}$ (by the formula for the inverse of the product) $\Rightarrow x = a^{-1}c^{-1}b^{-1}$ (can drop parentheses by associativity) .

(13) (a) Let H be the subgroup of G_{15} generated by $[4]_{15}$. List all elements of H.
(b) List all cosets of H in G_{15}.

Solution: (a) Since $([4]_{15})^2 = [1]_{15}$, $H = \{[1]_{15}, [4]_{15}\}$.
(b) The cosets are

$$\begin{aligned} H &= \{[1]_{15}, [4]_{15}\} \\ [2]_{15} \cdot H &= \{[2]_{15}, [8]_{15}\} \\ [7]_{15} \cdot H &= \{[7]_{15}, [13]_{15}\} \\ [11]_{15} \cdot H &= \{[11]_{15}, [14]_{15}\} \end{aligned}$$

(14) Let $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Show that R, equipped with ordinary addition and multiplication of real numbers, is a ring . Is R a field?

Solution: To show that R is an additive abelian group, we show that it is a subgroup of the (abelian!) additive group of real numbers. It suffices to check that the difference of any two elements of R is in R. Indeed, given $a + b\sqrt{2}, c + d\sqrt{2} \in R$, $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$; since $a - c, b - d \in \mathbb{Q}$ we are done.

Then we only need to show that R is closed under multiplication, since associativity of multiplication and distributivity properties are "inherited" from the reals. Indeed, given $a+b\sqrt{2}, c+d\sqrt{2} \in R$, $(a+b\sqrt{2}) \cdot (c+d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. Thus R is a ring as claimed.

Furthermore the multiplication in R is commutative and R contains a unit element ($1 = 1 + 0\sqrt{2}$).

Finally, we show that R is a field, i.e. that $R^\times$ is an abelian group. The only group axiom that needs checking is the existence of inverses. If $a+b\sqrt{2}$ is an element of $R^\times$, that is, $a, b \in \mathbb{Q}$ are not both zero, "rationalizing the denominator" tells us that $(a + b\sqrt{2}) \cdot (\frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}) = 1$. (Note that this is valid because $\sqrt{2}$ is irrational.)

(15) Let $f : B^3 \to B^5$ be a coding function given by $f(abc) = a\bar{a}b\bar{b}c$, where $\bar{a} = 1$ if $a = 0$ and $\bar{a} = 0$ if $a = 1$. What is the minimal distance between two distinct codewords in B^5? How many errors can this code detect? How many errors can this code correct?

Solution: Note that f, while not a linear code, is given by first applying the generating matrix

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and then adding 01010 to the result. For all $v, w \in B^3$, $(vA + 01010) - (wA+01010) = vA-wA$, so it suffices to work with the linear code given by A instead. The minimum weight of a nonzero codeword of this linear code is 1 (look at the third row of A), so the minimum distance between distinct codewords of f is also 1. It follows that the code can neither correct nor detect any errors.

(16) Write down the two-column decoding table for the code given by the generator matrix

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Use this table to correct the message

010101 101010 001101 100101.

Solution: First, we compute the parity-check matrix associated to B. This is

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We choose the zero vector, all 6 unit vectors (corresponding to rows of H), and 100001 (corresponding to $111 = 110 + 001$) to be coset leaders. The table is then

syndrome	**coset leader**
000	000000
001	000001
010	000010
100	000100
011	001000
101	010000
110	100000
111	100001

The syndrome of 010101 is 000, so it is a codeword. The syndromes of 101010, 001101, and 100101 are 111, 110, and 011, respectively. Adding the appropriate coset leaders gives the "corrected" message

010101 001011 101101 101101.