QUEEN'S UNIVERSITY
FACULTY OF ARTS AND SCIENCE
DEPARTMENT OF MATHEMATICS & STATISTICS
MATH 210
MIDTERM
MARCH 2023

- This test is 120 minutes in length.
- Calculators, data sheets, or other aids are **not** permitted.
- Each question is worth 10 points.
- Answers will be evaluated based on their clarity and correctness.
  Please show all work.
- Answers are to be recorded on the question paper.

1. For all nonnegative integers n, prove by induction that

$$\sum_{k=0}^{n} k\,2^k = (n-1)\,2^{n+1} + 2\,.$$

Solution. We proceed by induction on n. When $n = 0$, we have

$$\sum_{k=0}^{n} k\,2^k = (0)2^0 = 0 = -2+2 = (0-1)2^{0+1} + 2\,,$$

so the base case holds. Assume that $\sum\limits_{k=0}^{n} k\,2^k = (n-1)\,2^{n+1} + 2$. It follows that

$$\begin{aligned}
\sum_{k=0}^{n+1} k\,2^k &= \left(\sum_{k=0}^{n} k\,2^k\right) + (n+1)\,2^{n+1} \\
&= \big((n-1)\,2^{n+1} + 2\big) + (n+1)\,2^{n+1} \\
&= (n-1+n+1)\,2^{n+1} + 2 \\
&= (2n)\;2^{n+1} + 2 = \big((n+1)-1\big)2^{n+2} + 2
\end{aligned}$$

which completes the induction. $\square$

2. **(i)** Use the Euclidean Algorithm to calculate $\gcd(210, 48)$.

Solution. The Euclidean Algorithm involves repeatedly dividing the dividend by the remainder until one reaches 0:

$$\begin{aligned} 210 &= (4)(48) + 18 \\ 48 &= (2)(18) + 12 \\ 18 &= (1)(12) + 6 \\ 12 &= (2)(6) + 0 \end{aligned}$$

Since the final nonzero remainder is the greatest common divisor, we see that $\gcd(210, 48) = 6$. □

(ii) For Euler's totient function ϕ, compute $\phi(24)$.

Solution. Euler's totient function $\phi(24)$ counts the positive integers up to 24 that are coprime to 24. Using sieve methods, we have

$$\phi(24) = \left| \left\{ \begin{matrix} 1, & \cancel{2}, & \cancel{3}, & \cancel{4}, & 5, & \cancel{6}, & 7, & \cancel{8}, \\ \cancel{9}, & \cancel{10}, & 11, & \cancel{12}, & 13, & \cancel{14}, & \cancel{15}, & \cancel{16}, \\ 17, & \cancel{18}, & 19, & \cancel{20}, & \cancel{21}, & \cancel{22}, & 23, & \cancel{24} \end{matrix} \right\} \right| = 8\,. \qquad \square$$

3. Define a relation on $\mathbb{R}^2$ as follows: $(x_1,x_2) \sim (y_1,y_2)$ if and only if $x_1^2+x_2^2 = y_1^2+y_2^2$.

(i) Demonstrate that $\sim$ is an equivalence relation.

Solution. We verify the three defining properties of an equivalence relation:

(Reflexive) Consider any (x_1,x_2) in $\mathbb{R}^2$. Since $x_1^2+x_2^2 = x_1^2+x_2^2$, we see that $(x_1,x_2) \sim (x_1,x_2)$, so the relation is reflexive.

(Symmetric) Suppose that we have the relation $(x_1,x_2) \sim (y_1,y_2)$. By definition, we have $x_1^2+x_2^2 = y_1^2+y_2^2$. We see that $y_1^2+y_2^2 = x_1^2+x_2^2$ and $(y_1,y_2) \sim (x_1,x_2)$, so the relation is symmetric.

(Transitive) Suppose that $(x_1,x_2) \sim (y_1,y_2)$ and $(y_1,y_2) \sim (z_1,z_2)$. By definition, we have $x_1^2+x_2^2 = y_1^2+y_2^2$ and $y_1^2+y_2^2 = z_1^2+z_2^2$. We deduce that $x_1^2+x_2^2 = z_1^2+z_2^2$ and $(x_1,x_2) \sim (z_1,z_2)$, so the relation is transitive.

We conclude that this relation $\sim$ on $\mathbb{R}^2$ is an equivalence relation. $\square$

(ii) Describe the set of equivalence classes.

Solution. For any pair $(x_1,x_2) \in \mathbb{R}^2$, we have $x_1^2+x_2^2 \geqslant 0$. For each nonnegative real number r, the equivalence class $\{(x_1,x_2) \in \mathbb{R}^2 \mid x_1^2+x_2^2 = r^2\}$ consists of all points in the real plane lying on a circle of radius r centred at the origin. Since each pair (x_1,x_2) lies on the unique circle of radius $\sqrt{x_1^2+x_2^2}$, the interval $[0,\infty)$ forms a system of distinct representatives. $\square$

4. **(i)** Establish that, for any integer m, we have $m^2 \equiv 0, 1, \text{ or } 4 \mod 8$.

Solution. Since $\{0,1,2,3,4,5,6,7\}$ is a system of distinct representatives modulo 8 and

$$\begin{aligned} 0^2 &\equiv 0 \mod 8 & 4^2 &\equiv 16 \equiv 0 \mod 8 \\ 1^2 &\equiv 1 \mod 8 & 5^2 &\equiv 25 \equiv 1 \mod 8 \\ 2^2 &\equiv 4 \mod 8 & 6^2 &\equiv 36 \equiv 4 \mod 8 \\ 3^2 &\equiv 9 \equiv 1 \mod 8 & 7^2 &\equiv 49 \equiv 1 \mod 8 \end{aligned}$$

we conclude that, for any integer m, we have $m^2 \equiv 0, 1, \text{ or } 4 \mod 8$. □

(ii) Confirm that the equation $x^2 + y^2 + z^2 = 8007$ has no integer solutions.

Solution. If the given equation had integer solutions, then it would have also have solutions modulo 8. Reducing modulo 8 gives $x^2 + y^2 + z^2 \equiv 7 \mod 8$. Using part (i), we know that $m^2 \equiv 0, 1, \text{ or } 4 \mod 8$. To have $x^2 + y^2 + z^2 \equiv 7 \mod 8$, an odd number of the 3 squares must be congruent to 1 modulo 8. When all 3 are congruent to 1 modulo 8, we have $x^2 + y^2 + z^2 \equiv 3 \not\equiv 7 \mod 8$. When 1 square is congruent to 1 modulo 8, we have $x^2 + y^2 + z^2 \equiv 0 \text{ or } 5 \not\equiv 7 \mod 8$. We conclude that $x^2 + y^2 + z^2 \not\equiv 7 \mod 8$, so there are no integer solutions. □

Remark. One can enumerate the 10 possible cases:

$$x^2 + y^2 + z^2 \equiv \begin{cases} 0 \mod 8 & \text{if } x^2, y^2, z^2 \text{ are all congruent to 0 modulo 8, or two} \\ & \text{ are congruent to 4 and the other is congruent to 0} \\ 1 \mod 8 & \text{if one of } x^2, y^2, z^2 \text{ is congruent to 1 modulo 8} \\ & \text{and the other two are both congruent to 0 or 4} \\ 2 \mod 8 & \text{if two of } x^2, y^2, z^2 \text{ are congruent to 1 modulo 8} \\ & \text{and the other is congruent to 0} \\ 3 \mod 8 & \text{if } x^2, y^2, z^2 \text{ are all congruent to 1 modulo 8} \\ 4 \mod 8 & \text{if one of } x^2, y^2, z^2 \text{ are congruent to 4 modulo 8} \\ & \text{and the other two are both congruent to 0 or 4} \\ 5 \mod 8 & \text{if one of } x^2, y^2, z^2 \text{ is congruent to 0 modulo 8, one} \\ & \text{is congruent to 1, and the other is congruent to 4} \\ 6 \mod 8 & \text{if two of } x^2, y^2, z^2 \text{ are congruent to 1 modulo 8,} \\ & \text{and the other is congruent to 4} \end{cases}$$

Having enumerated all possibilities,

5. Let $\mathbb{F}_3 := \mathbb{Z}/\langle 3 \rangle$ be the field with 3 elements. Consider the two polynomials $f := x^4 + 2x^3 + x^2 + 2$ and $g := x^3 + 2x$ in the polynomial ring $\mathbb{F}_3[x]$.

(i) Find the quotient and remainder for the division of f by g.

Solution. We have

$$\begin{array}{r|l} & x+2 \\ \cline{2-2} x^3+2x & x^4+2x^3+x^2+0x+2 \\ & x^4+0x^3+2x^2 \\ \cline{2-2} & 2x^3+2x^2+0x+2 \\ & 2x^3+0x^2+x+0 \\ \cline{2-2} & 2x^2+2x+2 \end{array}$$

so the quotient is $f \,//\, g = x+2$ and the remainder is $f \,\%\, g = 2x^2+2x+2$. $\square$

(ii) Does the polynomial f have a multiple root in $\mathbb{F}_3$? Explain your reasoning.

Solution. Since $\{0,1,2\}$ is a system of distinct representatives modulo 3 and

$$\begin{aligned} f([0]_3) &= [2]_3 \\ f([1]_3) &= [1]_3 + [2]_3 + [1]_3 + [2]_3 = 0 \\ f([2]_3) &= [1]_3 + 2[2]_3 + [1]_3 + [2]_3 = [2]_3 \end{aligned}$$

it follows that $[1]_3$ is the only root of polynomial f. Observe that

$$D(f) = 4x^3 + 6x^2 + 2x = x^3 + 2x = g$$

and $g([1]_3) = [1]_3 + 2[1]_3 = [0]_3$. Hence, $[1]_3$ is a root of f having multiplicity greater than 1. $\square$

Remark. One can verify that $f = (x+2)^2(x^2+x+2)$.

6. Consider the following subset of real (2×2)-matrices

$$R := \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}.$$

(i) Let $\mathrm{M}_2(\mathbb{R})$ be the ring of all real (2×2)-matrices. Prove that R is a subring of $\mathrm{M}_2(\mathbb{R})$.

Solution. For any real numbers a, b, c, and d, we have

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} - \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} (a-c) & (b-d) \\ -(b-d) & (a-c) \end{bmatrix} \in R,$$
$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{bmatrix} \in R,$$

and setting $a = 1$ and $b = 0$ implies $\mathbf{I}_2 \in R$. Thus, the subset R is a subring of $\mathrm{M}_2(\mathbb{R})$. □

(ii) Prove that R is a commutative ring.

Solution. Since $\mathbb{R}$ is a commutative ring, we have

$$\begin{bmatrix} c & d \\ -d & c \end{bmatrix} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

which shows that the ring R is also commutative. □

(iii) Is R a field? Provide a proof or counterexample.

Solution. When $(a,b) \neq (0,0)$, we have $a^2 + b^2 \neq 0$ and

$$\frac{1}{a^2+b^2} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \frac{1}{a^2+b^2} \begin{bmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I}_2 .$$

Hence, every nonzero element in R is a unit and R is a field. □

Remark. One verifies that $R \cong \mathbb{C}$.

Space for additional work. If you want this work to be graded, then clearly indicate which problem you are continuing on both this page and the page with the original problem.