

Midterm Examination
Time Limit: 50 Minutes

October 30 2020

This examination document contains 5 pages, including this cover page, and 4 problems. You must verify whether there are any pages missing, in which case you should let the instructor know. **Write in your full name and student ID** on the top of every page. The solutions **must be submitted to Gradescope by 10:00am**. The Gradescope window *will* close sharply at 10:00am.

You may *not* use your books, notes, the Internet, or any calculator on this exam.

You are required to show your work on each problem on this exam. The following rules apply:

- (A) **If you use a lemma, proposition or theorem which we have seen in the class or in the book, you must indicate this:** state clearly what the result says, and explain why it may be applied.
- (B) **Organize your work**, in a reasonably neat and coherent way, in the space provided. Work scattered all over the page without a clear ordering will receive little credit. For each solution, make sure to show all of your work.
- (C) **Mysterious or unsupported answers will not receive full credit.** A correct answer, unsupported by calculations, explanation, or algebraic work will receive little credit; an incorrect answer supported by substantially correct calculations and explanations will receive partial credit.

Problem	Points	Score
1	25	
2	25	
3	25	
4	25	
Total:	100	

The table to the right shows the point distribution for the four problems. The highest score is 100.

1. (25 points) Show that there are infinitely primes of the form $3k + 2$, for $k \in \mathbb{N}$.

Solution. Let us argue by contradiction. Suppose that there are only finitely many primes $A = \{p_1, \dots, p_N\}$ of the form $3k + 2$, with $k \in \mathbb{N}$. Then consider the natural odd number

$$P = 3(p_1 \cdot \dots \cdot p_N) - 1 \in \mathbb{N}.$$

First, let us show that none of the $p_i \in A$ divide P , for any $1 \leq i \leq N$. By contradiction again, suppose there exists an $i \in \mathbb{N}$ such that $p_i | P$, then

$$p_i | P - 4(p_1 \cdot \dots \cdot p_N),$$

since p_i divides each summand. However $P - 3(p_1 \cdot \dots \cdot p_N) = -1$ and thus p_i divides -1 , which is a contradiction since p_i is prime for $1 \leq i \leq N$. In consequence, none of the primes $p_i \in A$ divide P , and in particular $P \notin A$.

Second, either P is a prime itself or it is not.

In the former case, since P is of the form $3k - 1$, equivalently of the form $3k + 2$, we get a contradiction with the fact that A contained all primes of the form $3k - 2$, since it does not contain P .

In the later case, where P is not a prime, we claim that P is divisible by at least one prime $\rho \in \mathbb{N}$ of the form $3k + 2$. Indeed, if all prime factors in the decomposition of P were of the form $3k$ or $3k + 1$, then P itself would be of the form $3k$ or $3k + 1$, as the product of numbers of the form $3k$ and $3k + 1$ is of the form $3k$ or $3k + 1$. Since P is of the form $3k + 2$, it must contain at least a prime factor ρ of the form $3k + 2$. This is also a contradiction since ρ is a prime of the form $3k + 2$ but $\rho \notin A$, since ρ divides P .

We have thus reached a contradiction, and our initial assumption that there are only finitely many primes of the form $3k + 2$ must have been incorrect. Hence, there are infinitely many primes of the form $3k + 2$, as required. \square

2. (25 points) Solve the following two parts:

(a) (15 points) Show that for all $n \in \mathbb{N}$ the following inequality holds:

$$2^{n-1} \leq n!$$

Solution: Let us prove this by induction on $n \in \mathbb{N}$.

The base case is $n = 1$. It is true since $2^0 \leq 1!$ is the correct inequality $1 \leq 1$.

For the induction step, let us assume that the inequality $2^{n-1} \leq n!$ holds, and we want to prove that $2^n \leq (n+1)!$. Indeed,

$$2^n = 2 \cdot 2^{n-1} \leq 2 \cdot n! \leq (n+1) \cdot n! = (n+1)!,$$

where in the first inequality we use the induction step $2^{n-1} \leq n!$ and in the second we use $2 \leq (n+1)$, which is true for all $n \in \mathbb{N}$. \square

(b) (10 points) Prove that for all $n \in \mathbb{N}$ the following equality holds:

$$\sum_{k=0}^n \binom{n}{k} 8^k = 9^n.$$

Solution: The Binomial Theorem states that for any $a, b \in \mathbb{N}$

$$\sum_{k=0}^n \binom{n}{k} a^k b^{n-k} = (a+b)^n.$$

By substituting $a = 8$ and $b = 1$ we obtain the desired equality. \square

3. (25 points) Suppose (x_n) , $n \in \mathbb{N}$, is a sequence that satisfies the recursion

$$x_{n+1} = x_n + 12x_{n-1}, \quad \text{with } x_1 = 1 \text{ and } x_2 = 25.$$

(a) (10 points) Write down the terms x_1, x_2, x_3, x_4, x_5 and x_6 .

Solution: The values $x_1 = 1$ and $x_2 = 25$ are given to us. Then we use recursion to compute the next few values:

$$x_3 = x_2 + 12x_1 = 25 + 12 = 37, \quad x_4 = x_3 + 12x_2 = 37 + 12 \cdot 25 = 337,$$

$$x_5 = x_4 + 12x_3 = 337 + 12 \cdot 37 = 781, \quad x_6 = x_5 + 12x_4 = 781 + 12 \cdot 337 = 4825.$$

Hence we get the values:

$$x_1 = 1, \quad x_2 = 25, \quad x_3 = 37, \quad x_4 = 337, \quad x_5 = 781, \quad x_6 = 4825.$$

□

(b) (15 points) Find a closed formula for the n th term x_n .
(Show all of your work.)

Solution: The characteristic polynomial of the recursion $x_{n+1} = x_n + 12x_{n-1}$ is

$$p(r) = r^2 - r - 12.$$

Its two distinct zeroes $r_1, r_2 \in \mathbb{Z}$ are $r_1 = -3$ and $r_2 = 4$. Thus, the general expression for the n th term x_n is of the form

$$x_n = C \cdot (-3)^n + D \cdot 4^n.$$

It suffices to determine C and D from the initial conditions. By inserting $x_1 = 1$ and $x_2 = 25$ in the above expression we get the equations

$$1 = C \cdot (-3) + D \cdot 4,$$

$$25 = C \cdot (-3)^2 + D \cdot 4^2$$

which have the unique solution $C = 1$ and $D = 1$. Hence the closed formula for the n th term of the sequence (x_n) is

$$x_n = (-3)^n + 4^n.$$

□

4. (25 points) Solve the following two problems:

(a) (10 points) Find the last digit of 19^{31} .

Solution: This is asking for a representative k of the equivalence class of 19 under the equivalence relation *modulo* 10, with $0 \leq k \leq 9$. Let us work modulo 10, where we then have

$$19 \equiv (-1) \pmod{10},$$

and thus $19^{31} \equiv (-1)^{31} \equiv -1 \equiv 9 \pmod{10}$. The answer is thus 9. \square

(b) (15 points) Show that there do not exist two integers $x, y \in \mathbb{Z}$ such that

$$x^2 + 4x + 1 = 4y^2.$$

Solution: We will work with modular arithmetic *modulo* 4. For that, consider the equation

$$x^2 + 4x + 1 = 4y^2,$$

modulo 4, where it becomes

$$x^2 + 1 \equiv 0 \pmod{4}.$$

Now, any equivalence class $x \pmod{4}$ satisfies either

$$x^2 \equiv 0 \pmod{4}, \quad \text{or} \quad x^2 \equiv 1 \pmod{4},$$

if $x \in \mathbb{N}$ is either even or odd. This is verified directly by plugging the values $x = 0, 1, 2, 3$ modulo 4 and squaring them. In consequence, the above equation reads

$$1 \equiv 0 \pmod{4}, \quad \text{or} \quad 2 \equiv 0 \pmod{4},$$

which is impossible, and so no solution can exist. This concludes the proof.

An alternative solution would be to argue that the left hand side of

$$x^2 + 4x + 1 = 4y^2,$$

is never divisible by 4, whereas the right hand side is divisible by 4. Hence no solution can exist since this would lead to a contradiction. \square