UECM1304 Tutorial 3: Elementary Number Theory and Methods of Proof

4 hours

§3.1 Formal Characterisation of Numbers

1. Assuming that m and n are particular integers, use the definitions of even, odd, prime and composite to answer the following questions.
   (a) If $m > n > 0$, is $m^2 - n^2$ composite?
   (b) Is $6m + 10n$ even?
   (c) Is $10mn + 13$ odd?
   (d) If $m > 0$ and $n > 0$, is $m^2 + 2mn + n^2$ composite?
2. (a) Assume that $a \neq 0$ and $b \neq 0$ are both integers. Is $(b - a)/(ab^2)$ a rational number?
   (b) Assume that a and $b > 0$ are both integers. Is $(5a + 12b)/4b$ a rational number?
3. Suppose a, b, c and d are integers and $a \neq c$. Suppose also x is a real number that satisfies the equation $\dfrac{ax + b}{cx + d} = 1$. (**) Is x rational?
4. Is the following argument valid?

   Any sum of two rational numbers is rational.
   The sum $r + s$ is rational.
   ___
   Therefore the numbers r and s are both rational.

§3.2 Methods of Proof

Direct Proof

5. Use the rules of inference and real number axioms to prove that $/ \therefore \forall x(3 < x \rightarrow 25 < x^2 + 5x + 2)$.
6. Prove the following existential statements:
   (a) There are distinct integers m and n such that $1/m + 1/n$ is an integer.
   (b) There are real numbers a and b such that $\sqrt{a + b} \neq \sqrt{a} + \sqrt{b}$.
   (c) There is an integer n such that $2n^2 - 5n + 2$ is prime.
7. Prove the following universal statement by using method of exhaustion.

   For each integer n with $1 \leq n \leq 10$, $n^2 - n + 11$ is a prime number.
8. Prove the following universal statements:
   (a) For all integers n, if n is odd then n^2 is odd.
   (b) If n is any odd integer, then $(-1)^n = -1$.
9. Suppose m, n and d are integers and $m \mod d = n \mod d$.
   (a) Does it necessarily follow that $m = n$?
   (b) Prove that $m - n$ is divisible by d.

10. Show that the square of any integer has the form $3k$ or $3k+1$ for some integer k. [Hint: Adapt from Final 2024 Q3(b), related Quotient-Remainder Theorem]
11. Prove that for any integer a, one of the integers a, $a+2$, $a+4$ is divisible by 3. [Hint: Adapt from Final 2024 Q3(b), related Quotient-Remainder Theorem]
12. Prove that $\dfrac{a(a^2+2)}{3}$ is an integer for all integers $a \geq 1$. [Hint: Adapt from Final 2024 Q3(b), related Quotient-Remainder Theorem]

Contrapositive Proof

13. Prove the following statements by contraposition.
    (a) If a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.
    (b) If a sum of two real numbers is less than 50, then at least one of the numbers is less than 25.

Proof by Contradiction

14. Use proof by contradiction to prove the following statements:
    (a) There is no greatest even integer.
    (b) For all real numbers x and y, if x is irrational and y is rational then $x-y$ is irrational.
15. Use proof by contradiction to prove the following statements:
    (a) For all integers n, $3n+2$ is not divisible by 3.
    (b) For any integer n, n^2-2 is not divisible by 4.
16. Show that $\log_2 5$ is an irrational number.

§3.3 Disproving Statements

17. Disprove the following existential statement:

    There exists an integer n such that $6n^2+27$ is prime.

18. Prove or disprove the following statements:
    (a) Every positive integer is the sum of the squares of three integers.
    (b) There are 100 consecutive positive integers that are not perfect squares (an integer which can be written as s^2 for some integer s).
19. Disprove the following universal statements:
    (a) For all real numbers a and b, if $a < b$, then $a^2 < b^2$.
    (b) For all integers m and n, if $2m+n$ is odd, then m and n are both odd.
20. Consider the following existential statement:

    There exists an integer x with $x \geq 4$ such that $2x^2-5x+2$ is prime. (*)

    (a) Give a negation of the statement (*).
    (b) Prove that the statement (*) is false by showing that its negation is true.
21. Determine whether the statement is true or false. Justify your answer with a proof or a counterexample, as appropriate.
    (a) The product of any two even integers is even.
    (b) For all integers m, if $m > 2$, then m^2-4 is composite.
    (c) For all integers n and m, if $n-m$ is even, then n^3-m^3 is even.
    (d) For all integers n, n^2-n+11 is a prime number.
    (e) The quotient of any two rational numbers is a rational number.

(f) If r and s are any two rational numbers, then $\frac{r+s}{2}$ is rational.

§3.4 Mathematical Induction

22. Prove that $\sum_{i=1}^{n-1} i(i+1) = \dfrac{n(n-1)(n+1)}{3}$ for all integers $n \geq 2$.
23. Show that $\sum_{i=1}^{n+1} i \cdot 2^i = n \cdot 2^{n+2} + 2$ for all integers $n \geq 0$.
24. Prove that $n^3 - 7n + 3$ is divisible by 3, for each integer $n \geq 0$.
25. Show that $7^n - 2^n$ is divisible by 5 for integer $n \geq 1$.
26. $2^n < (n+1)!$, for all integers $n \geq 2$.
27. $5^n + 9 < 6^n$, for all integers $n \geq 2$.
28. A sequence $a_1, a_2, a_3, \cdots$ is defined by letting $a_1 = 3$ and $a_k = 7a_{k-1}$ for all integers $k \geq 2$. Show that $a_n = 3(7^{n-1})$ for all integers $n \geq 1$.
29. Prove that for any real number $x > -1$ and any positive integer n, $(1+x)^n \geq 1 + nx$.
30. Let the "Tribonacci sequence" be defined by $T_1 = T_2 = T_3 = 1$ and $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ for $n \geq 4$. Prove that $T_n < 2^n$ for all $n \in \mathbb{Z}^+$.

§3.5 Divisibility

31. Let n and k be integers. If $n = 4k + 3$, does 8 divides $n^2 - 1$?
32. Use the unique factorisation theorem to write the following integers in standard factored form.
    (a) 5377 .... [ ]
    (b) 3675 .... [ ]
    (c) 1330 .... [ ]
    (d) 211 .... [ ]
    (e) 19683 .... [ ]
    (f) 15! .... [ ]
33. If x and y are integers and $10x = 9y$, does $10|y$? does $9|x$? Explain.
34. Determine whether some of the following numbers

$$72, 21, 15, 36, 69, 81, 9, 27, 42, 63$$

can be add up to 100. [Hint: This is related to GCD discussed in class]

35. Suppose that in standard factored form $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where k is a positive integer; $p_1, p_2, \cdots, p_k$ are prime numbers; and $e_1, e_2, \cdots, e_k$ are positive integers.
    (a) What is the standard factored form for a^2?
    (b) Find the least positive integer n such that $2^5 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot n$ is a perfect square.
36. Find integers q and r such that $n = dq + r$ and $0 \leq r < d$.
    (a) $n = 36$, $d = 40$ .... [ ]
    (b) $n = -27$, $d = 8$ .... [ ]
37. When an integer a is divided by 7, the remainder is 4. What is the remainder when $5a$ is divided by 7?
38. Without evaluating the expression, use floor notation to express 259 div 11 and 259 mod 11.

§3.6 Modular Arithmetic

39. Based on the Fermat Little Theorem, mathematicians have developed a "test" for primality called the "Fermat's primality test": Pick $a \in \{2, ..., n-1\}$ randomly, if $a^{n-1} \not\equiv 1 \pmod{n}$, n is **composite**, else n is "probably prime". Use Fermat's primarity test with $a = 347$ to test if 5377 is prime or composite (compare your result to Question 32(d)).
40. Use Fermat's primarity test with $a = 16$ to test if 211 is prime (compare your result to Question 32).
41. Use Euler Theorem to compute $2^{1000000} \mod 77$.

    [Euler Theorem: A generalisation of the Fermat's Little Theorem] If $\gcd(a, n) = 1$,then $a^{\phi(n)} \equiv 1 \pmod{n}$. Here ϕ is the Euler phi function.

Euclidean Algorithm

42. Use the extended Euclidean algorithm to find the $\gcd(4158, 1568)$ and prove that the statement $\exists u \exists v (4158u + 1568v = \gcd(4158, 1568))$ is true in the **integer** domain.

§3.8 Application: Cryptography

43. Use the Caesar cipher to encrypt the message `WHERE SHALL WE MEET`.
44. Use the Caesar cipher to decrypt the message `LQ WKH FDIHWHULD`.
45. Generate the translation table for the affine cipher with $a = 5$ and $b = 8$ by writing and executing a program.
46. Encipher "AFFINE CIPHER" using an affine cipher with $a = 5$ and $b = 8$.
47. Use the RSA cipher with public key $n = 713 = 23 \cdot 31$ and $e = 43$.
    (a) Encode the message `HELP` into numeric equivalents and encrypt them.
    (b) Decrypt the ciphertext `675 89 89 48` and find the original messages.

Discussion of June 2024 Final Exam Q3

(a) Use induction to prove that $5|(7^n - 2^n)$ for all $n \geq 1$. (12 marks)

Remember the steps of "mathematical inducation":

predicate + base case + induction.

Proof: Predicate $P(n) = 5|(7^n - 2^n)$.

Base case: We look for $n \geq 1$. The 1 is the base. So we need to prove

$$P(1) = 5|(7^1 - 2^1)$$

This is the proof: Since $7^1 - 2^1 = 7 - 2 = 5 = 5 \times 1$. Therefore, $5|5 = 7^1 - 2^1$, i.e. $P(1)$ is true.

Induction case: We assume $P(k)$ is true for $k \geq 1$. We need to prove $P(k + 1)$ using $P(k)$.

Writing down $P(k + 1)$ is not useful. We look at part of $P(k + 1)$, i.e

$$7^{k+1} - 2^{k+1} \qquad (\dagger)$$

We need to understand $P(k)$, i.e. what $5|(7^k - 2^k)$ means. It means

$$7^k - 2^k = 5m \qquad (*)$$

where m is some integer.

The **formula** (†) is related to (*) in the following way:

$$7^{k+1}-2^{k+1} = 7^k\times 7-2^k\times 2 = 7^k\times(5+2)-2^k\times 2 = 7^k\times 5+2(7^k-2^k) = 7^k\times 5+2\times 5m = 5\times(7^k+2m)$$

Since $7^k + 2m$ is some integer, therefore

$$5|(7^{k+1} - 2^{k+1}).$$

This means that $P(k+1)$ can be derived from $P(k)$.

The difficulty one may face is the breaking down of 7 to $5 + 2$ and also the understanding of the notion of divisibility $m|n$, which means we can find some integer k such that $n = mk$.

(b) Prove that any product of two consecutive integers have the form $3k$ or $3k + 2$ for some integer k.

Two consecutive integers can be written as n and $n + 1$ but $n(n + 1) = n^2 + n$ is not helping us to get the answer.

So we need to try to think about writing n as $3m$, $3m + 1$ or $3m + 2$. They are all possibilities of integer n because when n is divided by 3, the remainders are 0, 1 or 2.

Now, we can try to write out a proof.

Proof: When $n = 3m$, $n + 1 = 3m + 1$,

$$n(n + 1) = 9m^2 + 3m = 3k$$

where $k = 3m^2 + m$.

When $n = 3m + 1$, $n + 1 = 3m + 2$,

$$n(n + 1) = 9m^2 + 9m + 2 = 3k + 2$$

where $k = 3m^2 + m$.

When $n = 3m + 2$, $n + 1 = 3m + 3$,

$$n(n + 1) = 3(m + 1)(3m + 2) = 3k$$

where $k = (m + 1)(3m + 2)$.