UECM1303 Tutorial 3: Elementary Number Theory

May 2021

Divisibility

1. Let n and k be integers. If $n = 4k + 3$, does 8 divides $n^2 - 1$?

2. 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! ....

3. If x and y are integers and $10x = 9y$, does $10|y$? does $9|x$? Explain.

4. 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]

5. 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.

6. Find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

   (a) $n = 36$, $d = 40$ ....

   (b) $n = -27$, $d = 8$ ....

7. When an integer a is divided by 7, the remainder is 4. What is the remainder when $5a$ is divided by 7?

8. Without evaluating the expression, use floor notation to express 259 div 11 and 259 mod 11.

Modular Arithmetic

9. 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 2).

10. Use Fermat's primarity test with $a = 16$ to test if 211 is prime (compare your result to Question 2).

11. 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

12. Use the extended Euclidean algorithm to find the $\gcd(4158, 1568)$ and express it as a linear combination of the two numbers.

13. (a) Find an inverse for 210 modulo 13.
    (b) Find a positive inverse for 210 modulo 13.

Linear Congruence & Chinese Remainder Theorem

14. Find all solutions to the system of congruences.

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

Application of Number Theory in Cryptography
(Not coming out in test / final)

15. Use the Caesar cipher to encrypt the message `WHERE SHALL WE MEET`.

16. Use the Caesar cipher to decrypt the message `LQ WKH FDIHWHULD`.

17. Generate the translation table for the affine cipher with $a = 5$ and $b = 8$ by writing and executing a Racket program.

18. Encipher "AFFINE CIPHER" using an affine cipher with $a = 5$ and $b = 8$.

19. 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.

Methods of Proof
Direct Proof

20. 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.

21. Use the quotient-remainder theorem to show that the square of any integer has the form $3k$ or $3k + 1$ for some integer k.

22. Prove that for any integer a, one of the integers a, $a + 2$, $a + 4$ is divisible by 3.

23. Prove that $\dfrac{a(a^2 + 2)}{3}$ is an integer for all integers $a \geq 1$.

Proof by Contradiction

24. 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.

25. Show that $\log_2 5$ is an irrational number.

Mathematical Induction

26. Prove that $\displaystyle\sum_{i=1}^{n-1} i(i+1) = \frac{n(n-1)(n+1)}{3}$ for all integers $n \geq 2$.

27. Show that $\displaystyle\sum_{i=1}^{n+1} i \cdot 2^i = n \cdot 2^{n+2} + 2$ for all integers $n \geq 0$.

28. Prove that $n^3 - 7n + 3$ is divisible by 3, for each integer $n \geq 0$.

29. For each integer $n \geq 1$, $7^n - 2^n$ is divisible by 5.

30. $2^n < (n+1)!$, for all integers $n \geq 2$.

31. $5^n + 9 < 6^n$, for all integers $n \geq 2$.

32. 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 $n \geq 1$.

33. Prove that for any real number $x > -1$ and any positive integer n, $(1+x)^n \geq 1 + nx$.

34. 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 $n \in \mathbb{Z}^+$.