MATH2081: Math for Computing
Lecturer: Dr. Nguyen Hieu Thao
Email: thao.nguyenhieu@rmit.edu.vn

RMIT UNIVERSITY

Tutorials 7 - Number Theory

(2024A, Week 8)[13]

1. Find the prime factorization of 11!.
2. Find the greatest common divisor of $32 \cdot 11$ and $23 \cdot 5 \cdot 7$.
3. Let a, b and c be integers. Show that if $a \mid b$ and $b \mid c$, then $a \mid c$.
4. How many bits are needed to represent each integer?
   (a) 128
   (b) 2^{1000}
   (c) 3^{481}
   (d) $6.87 \cdot 10^{48}$
5. Express the binary number 11111111 in decimal.
6. Express the decimal number 1024 in binary.
7. Add the binary numbers $110110 + 101101$.
8. Express each hexadecimal number in decimal and in binary.
   (a) $3A$
   (b) $A03$
9. Add the hexadecimal numbers $4A + B4$.
10. Express the octal number 7643 in decimal.
11. Consider the base 6 number system using the six symbols A, B, C, D, E and F, which represent the values 0, 1, 2, 3, 4 and 5, respectively.
    (a) Convert the base 6 number BAF to a decimal number.
    (b) Convert the decimal number 137 to a base 6 number.

[13] Most of the content of this document is taken from the book [1].

12. Let S be the set of all nonempty strings on the alphabet $\{0, 1\}$, each of which represents a binary number. Consider the function $f : S \to S$ given by

$$w \mapsto f(w) = w01, \quad \text{for every string } w \in S,$$

where $w01$ is the concatenation of the two strings w and 01.

(a) Compute the string value $f(0101010)$. What is the decimal value of the binary number represented by $f(0101010)$?

(b) Is f an injective and/or a surjective? Justify your answers.

13. Consider the key defined as character

$$\_ABCDEFGHIJKLMNOPQRSTUVWXYZ$$

replaced by

$$EIJFUAXVHWP\_GSRKOBTQYDMLZNC.$$

(a) Encrypt the message 'COOL'.

(b) Decrypt the message 'UTWR'.

14. Assume that for an RSA public-key crptosystem, we choose primes $p = 17$, $q = 23$ and $e = 31$. Refer to the notation system in Lecture Notes 7.

(a) Compute n.

(b) Compute $\phi(n)$.

(c) Compute d.

(d) Encrypt 101 using the public key (e, n).

(e) Decrypt 250 using the private key (d, n).

References

1. Johnsonbaugh, R.: Discrete Mathematics - Eighth Edition. *Pearson Education*, New York (2018).