Homework 3.

- The file name of your homework (in PDF) should be in the format: "學號-作業編號.pdf". For example: 00957999-hw3.pdf
- Please submit your homework to Tronclass **before 23:59, December 8 (Sunday), 2024.**

(可以用 word 檔寫完後轉成 pdf 檔上傳，或是手寫後拍照後存成 pdf 檔上傳)

1. (21%) Find
   (a) 11^{644} mod 645
   (Sol.) 1
   (b) 3^{2003} mod 99
   (Sol.) 27
   (c) 123^{1001} mod 101
   (Sol.) 22
   (d) 7^{121} mod 13.
   (Sol.) 7
   (e) 23^{1002} mod 41
   (Sol.) 37
   (f) gcd(1529, 14039)
   (Sol.) 139
   (g) gcd(1111, 0)
   (Sol.) 1111
2. (21%) Expansion conversion
   (a) Convert 97644 to a binary expansion.
   (Sol.) $(1\ 0111\ 1101\ 0110\ 1100)_2$

   (此大題因為答案不會混淆，可以不加下標)

   (b) Convert $(10\ 1011\ 0101)_2$ to a decimal expansion.
   (Sol.)
   693
   (c) Convert $(423)_8$ to a binary expansion.
   (Sol.) $(1\ 0001\ 0011)_2$
   (d) Convert $(1010\ 1010\ 1010)_2$ to an octal expansion.
   (Sol.) $(5252)_8$
   (e) Convert $(135AB)_{16}$ to an octal expansion.
   (Sol.) $(232653)_8$
   (f) Convert $(BADFACED)_{16}$ to an octal expansion.

(Sol.) $(27267726355)_8$

(g) Convert $(1011\ 0111\ 1011)_2$ to an octal expansion.

(Sol.) $(5573)_8$

3. (12%) Find the sum and the product of each of these pairs of numbers. Express your answers as the same base.

(a) $(100\ 0111)_2$, $(111\ 0111)_2$

(Sol.) $(1011\ 1110)_2$, $(10\ 0001\ 0000\ 0001)_2$

(此大題因為答案不會混淆，可以不加下標)

(b) $(112)_3$, $(210)_3$

(Sol.) $(1022)_3$, $(101220)_3$

(c) $(763)_8$, $(147)_8$

(Sol.) $(1132)_8$, $(144305)_8$

(d) $(1AE)_{16}$, $(BBC)_{16}$

(Sol.) $(D6A)_{16}$, $(13B5C8)_{16}$

4. (6%) Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \le c \le 12$ such that

(a) $c \equiv 11b \pmod{13}$.

(Sol.) 8

(b) $c \equiv 2a + 3b \pmod{13}$.

(Sol.) 9

(c) $c \equiv a^3 - b^3 \pmod{13}$.

(Sol.) 11

5. (8%) Find each of these values.

(a) $(177 \bmod 31 \cdot 270 \bmod 31) \bmod 31$

(Sol.) 19

(b) $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$

(Sol.) 13

(c) $(32^3 \bmod 13)^2 \bmod 11$

(Sol.) 9

(d) $(99^2 \bmod 32)^3 \bmod 15$

(Sol.) 9

6. (10%) Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

(a) 117, 213

(Sol.) $3 = 11 \cdot 213 - 20 \cdot 117$

(b) 124, 323

(Sol.) $1 = 43 \cdot 323 - 112 \cdot 124$

7. (12%) Find **all** solutions (寫出通式):

(a) $4x \equiv 5 \pmod 9$

(Sol.) $8 + 9k, k \in \mathbb{Z}$

(b) $34x \equiv 77 \pmod{89}$

(Sol.) $52 + 89k, k \in \mathbb{Z}$

(c) $15x^2 + 19x \equiv 5 \pmod{11}$

(Hint: Show the congruence is equivalent to the congruence $15x^2 + 19x + 6 \equiv 0 \pmod{11}$.)

(Sol.) $3 + 11k, k \in \mathbb{Z}$ or $6 + 11k, k \in \mathbb{Z}$

(d) Find all solutions, if any, to the system of congruences $x \equiv 5 \pmod 6$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.

(Sol.) $23 + 30k, k \in \mathbb{Z}$

8. (10%)

(a) Show that for every positive integer n,

$$1 \cdot 2 + 2 \cdot 3 + \cdots \ldots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

(Sol.) Prove by mathematical induction. Let P(n) be "$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = n(n+1)(n+2) / 3$."

Basis step: P(1) is true because $1 \cdot 2 = 2 = 1(1+1)(1+2) / 3$.

Inductive step: Assume that P(k) is true. Then $1 \cdot 2 + 2 \cdot 3 + \cdots + k(k+1) + (k+1)(k+2) = [k(k+1)(k+2) / 3] + (k+1)(k+2) = (k+1)(k+2)[(k / 3) + 1] = (k+1)(k+2)(k+3) / 3$.

(b) Find the flaw with the following "proof" that $a^n = 1$ for all nonnegative integers n, whenever a is a nonzero real number.

Basis Step: $a^0 = 1$ is true by the definition of a^0.

Inductive Step: Assume that $a^j = 1$ for all nonnegative integers j with $j \leq k$. Then we can get

$$a^{k+1} = \frac{a^k \cdot a^k}{a^{k-1}} = \frac{1 \cdot 1}{1} = 1$$

(Sol.)

The flaw comes in the inductive step, where we are implicitly assuming that $k \geq 1$ in order to talk about a^{k-1} in the denominator (otherwise the exponent is not a nonnegative integer, so we cannot apply the inductive hypothesis).

$$a^{k+1} = \frac{a^k \cdot a^k}{a^{k-1}} = \frac{1 \cdot 1}{1} = 1$$

Our basis step was $n = 0$, so we are not justified in assuming that $k \geq 1$ when we try to prove the statement for $k + 1$ in the inductive step. Indeed, it is precisely at n = 1 that the proposition breaks down.