Chuyên đề: **ĐỒNG DƯ THỨC**

A. Tóm tắt các kiến thức cơ bản :

I/ Định nghĩa : Cho m là số nguyên dương. Hai số nguyên a và b được gọi đồng với nhau theo module m, nếu a - b chia hết cho m (a - b)| m hay m\(a - b)

Ký hiệu : $a \equiv b \pmod m$ được gọi là một đồng dư thức.

Ví dụ : $3 \equiv -1 \pmod 4$

$5 \equiv 17 \pmod 6$

$18 \equiv 0 \pmod 6$

Điều kiện $a \equiv 0 \pmod m$ có nghĩa là bội của a ⋮ m (a | m) hay m là ước của a (m \ a) .

Nếu a - b không chia hết cho m, ta viết $a \not\equiv b \pmod m$

II/ Các tính chất cơ bản :

1) Với mọi số nguyên a, ta có $a \equiv a \pmod m$

2) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$

3) $a \equiv b \pmod m$ và $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

**Chứng minh* : Ta có : $a \equiv b \pmod m \Rightarrow a - b ⋮ m$ (m \ (a - b))

và $b \equiv c \pmod m \Rightarrow b - c ⋮ m$ (m \ (b - c))

Vì a - c = (a - b) + (b - c) => a - c ⋮ m (tính chất chia hết của tổng) hay

$a \equiv c \pmod m$.

4)) $a \equiv b \pmod m$ và $c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$

**Chứng minh* :

Ta có : $a \equiv b \pmod m \Rightarrow a - b ⋮ m \Rightarrow a - b = m.q_1$ (với $q_1 \in Z$) (1)

$c \equiv d \pmod m \Rightarrow c - d ⋮ m \Rightarrow c - d = m.q_2$ (với $q_2 \in Z$) (2)

Cộng (1) và (2) vế theo vế ta được : $(a - b) + (c - d) = m.(q_1 + q_2)$

$\Leftrightarrow (a + c) - (b + d) = m.(q_1 + q_2) \Rightarrow (a + c) - (b + d) ⋮ m$

Hay $a + c \equiv b + d \pmod m$

Hệ quả : $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ... , $a_n \equiv b_n \pmod m$

$\Rightarrow a_1 + a_2 + a_3 + ... + a_n \equiv b_1 + b_2 + b_3 + ... + b_n \pmod m$

5) $a \equiv b \pmod m$ và $c \equiv d \pmod m \Rightarrow a.c \equiv b.d \pmod m$

**Chứng minh* :

Ta có : $a - b = m.q_1 \Rightarrow a = b + m.q_1$ (với $q_1 \in Z$) (1)

$c - d = m.q_2 \Rightarrow c = d + m.q_2$ (với $q_2 \in Z$) (2)

Nhân (1) và (2) vế theo vế ta được : $a.c = (b + m.q_1)(d + m.q_2)$

$ac = bd + bmq_2 + dmq_1 + m^2q_1q_2 \Leftrightarrow ac - bd = m(bq_2 + dq_1 + mq_1q_2)$

$\Rightarrow ac - bd ⋮ m \Rightarrow ac \equiv bd \pmod m$.

Hệ quả : a) $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ... , $a_n \equiv b_n \pmod m$

$\Rightarrow a_1.a_2.a_3. \;...\; .a_n \equiv b_1.b_2.b_3. \;...\; .b_n \pmod m$

b) $a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$ - với mọi $n \in N$

+Nhận xét :

a) * $a \equiv 1 \pmod 2$ và $b \equiv 1 \pmod 2 \Rightarrow a + b \equiv 2 \pmod 2$

Mà $2 \equiv 0 \pmod 2$ => $a + b \equiv 0 \pmod 2$

* $a \equiv 1 \pmod 2$ và $b \equiv 1 \pmod 2$ => $a.b \equiv 1 \pmod 2$

Điều này có nghĩa : Tổng của hai số lẻ là một số chẵn, tích của hai số lẻ là một số lẻ.

b)$a \equiv 3 \pmod 7$ => $a^2 \equiv 9 \pmod 7 \equiv 2 \pmod 2$

Điều này có nghĩa : Nếu một số chia 7 dư 3 thì bình phương số đó chia 7 dư 2.

+Chú ý :

a)Không được chia hai vế của một đồng dư thức .

Ví dụ : * $2 \equiv 12 \pmod{10}$ nhưng $1 \not\equiv 6 \pmod{10}$.

b) $a \not\equiv 0 \pmod m$ và $b \not\equiv 0 \pmod m$, nhưng a.b có thể đồng dư với 0 theo module m.

Ví dụ : $2 \equiv 0 \pmod{10}$ và $5 \equiv 0 \pmod{10}$, nhưng $2.5 = 10 \equiv 10 \pmod{10}$.

Như vậy để phép chia hai vế của đồng thức đòi hỏi phải kèm theo một số điều kiện .

6) Nếu $a \equiv b \pmod m$ và d là ước chung của a, b sao cho $(d, m) = 1$

thì : $a : d \equiv b : d \pmod m$ ($\frac{a}{d} \equiv \frac{b}{d} \pmod m$)

Chứng minh :

Ta có $a \equiv b \pmod m$ => $a - b \,\vdots\, m$ => $a - b = mq$ (1)

Chia hai vế của (1) cho d (vì d là ước chung của a, b => $d \neq 0$)

$\frac{a-b}{d} = \frac{m.q}{d}$ <=> $\frac{a}{d} - \frac{b}{d} = \frac{m.q}{d}$ là số nguyên (vì d là ước của a, b.

Do đó $\frac{a}{d} - \frac{b}{d}$ là số nguyên). => $mq \,\vdots\, d$, mà $(d, m) = 1$ => $q \,\vdots\, d$

Vậy $\frac{a}{d} - \frac{b}{d} \,\vdots\, m$ hay $\frac{a}{d} \equiv \frac{b}{d} \pmod m$

7)Nếu $a \equiv b \pmod m$ và d là số nguyên là ước chung của ba số a, b, m

thì $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

Chứng minh :

Vì Nếu $a \equiv b \pmod m$ => $a - b \,\vdots\, m$ => $a - b = mq$ (1)

Và d là ước chung của a, b, m => $d \neq 0$. Chia cả hai vế (1) cho d

$\frac{a-b}{d} = \frac{m.q}{d}$ <=> $\frac{a}{d} - \frac{b}{d} = \frac{m}{d}.q$ => $\frac{a}{d} - \frac{b}{d} \,\vdots\, \frac{m}{d}$ hay $\frac{m}{d}$ là ước của $\frac{a}{d} - \frac{b}{d}$

Vậy : $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

8)Nếu $a \equiv r \pmod m$ với $0 \leq r < m$, thì r chính là số dư trong phép chia a cho m.

Chứng minh : Ta có $a \equiv r \pmod m$ => $a - r = m.q$ => $a = m.q + r$ (với $0 \leq r < m$)

B/Áp dụng :

I.Các ví dụ :

Dạng 1 : Tìm số dư của phép chia

Bài 1 : Tìm số dư trong phép chia 2004^{2004} cho 11

Sử dụng dấu hiệu chia hết cho 11 : *Một số được gọi là chia hết cho 11 khi và chỉ khi hiệu giữa các tổng chữ số ở hàng lẻ và tổng các chữ số hàng chẵn kể từ trái sang phải chia hết cho 11.*

Ví dụ : Xét xem số 5016 có chia hết cho 11 ?

Ta có (5 + 1) - (0 + 6) = 0. Vì 0 $\vdots$ 11 => 5016 $\vdots$ 11

Giải :

Ta có 2002 $\vdots$ 11 => 2004 - 2 $\vdots$ 11 => $2004 \equiv 2 \pmod{11}$

=> $2004^{2004} \equiv 2^{2004} \pmod{11}$, mà $2^{10} \equiv 1 \pmod{11}$ (vì 1024 - 1 $\vdots$ 11)

=> $2004^{2004} = 2^4.2^{2000} = 2^4.(2^{10})^{200} \equiv 2^4 \equiv 5 \pmod{11}$

Vậy 2004^{2004} chia 11 dư 5.

Bài 2 : Tìm số dư khi chia A = 1944^{2005} cho 7

Giải :

Ta có : $1944 \equiv -2 \pmod 7$ => $1944^{2005} \equiv (-2)^{2005} \pmod 7$

Mà $(-2)^3 \equiv -1 \pmod 7$ => $(-2^3)^{668} \equiv 1^{668} \pmod 7$ hay $(-2^3)^{668} \equiv 1 \pmod 7$

=> $(-2^3)^{668}.(-2) \equiv -2 \pmod 7$ hay $(-2)^{2005} \equiv -2 \pmod 7$

Vậy 1944^{2005} cho 7 dư 5.

Bài 3 : Chứng minh rằng các số A = $6^{1000} - 1$ và B = $6^{1001} + 1$ đều là bội số của 7

Giải :

Ta có $6 \equiv -1 \pmod 7$ => $6^{1000} \equiv 1 \pmod 7$ => $6^{1000} - 1 \vdots 7$

Vậy A là bội của 7

Từ $6^{1000} \equiv 1 \pmod 7$ => $6^{1001} \equiv 6 \pmod 7$, mà $6 \equiv -1 \pmod 7$

=> $6^{1001} \equiv -1 \pmod 7$ => $6^{1001} + 1 \vdots 7$

Vậy B là bội của 7

Bài 4 : Tìm số dư trong phép chia $1532^5 - 1$ cho 9

Giải :

Ta có $1532 \equiv 2 \pmod 9$ => $1532^5 \equiv 2^5 \pmod 9$, mà $2^5 \equiv 5 \pmod 9$

=> $1532^5 \equiv 5 \pmod 9$ => $1532^5 - 1 \equiv 4 \pmod 9$

Vậy 1532^5 - 1 chia cho 9 dư là 4.

Bài 5 : Chứng minh rằng A = $7.5^{2n} + 12.6^n$ chia hết cho 19

Giải :

Ta có A = A = $7.5^{2n} + 12.6^n$ = A = $7.25^n + 12.6^n$

Vì $25 \equiv 6 \pmod{19}$ => $25^n \equiv 6^n \pmod{19}$

=>$7.25^n \equiv 7.6^n \pmod{19}$ => $7.25^n + 12.6^n \equiv 7.6^n + 12.6^n \equiv 19.6^n \equiv 0 \pmod{19}$. *Điều này chứng tỏ A chia hết cho 19.*

Bài 6 : Tìm dư trong phép chia 3^{2003} cho 13.

Giải :

Ta có $3^3 \equiv 1 \pmod{13}$ mà 2003 = 3.667 + 2 => $3^{2003} = (3^3)^{667}.3^2$

$3^3 \equiv 1$ => $(3^3)^{667} \equiv 1^{667}$ => $(3^3)^{667}.3^2 \equiv 1.3^2 \pmod{13}$ $(3^3)^{667}.3^2 \equiv 9$

=> $3^{2003} \equiv 9 \pmod{13}$.

Vậy 3^{2003} chia cho 13 dư 9 .

Bai 7 : Chứng minh rằng 2^{2002} - 4 chia hết cho 31

Giải :

Ta có $2^5 \equiv 1 \pmod{31}$, mà 2002 = 5.400 + 2

Nên $2^{2002} = (2^5)^{400}.2^2$

Vì $2^5 \equiv 1 \pmod{31} \Rightarrow (2^5)^{400} \equiv 1^{400} \pmod{31} \Rightarrow (2^5)^{400}.2^2 \equiv 1.2^2 \pmod{31}$

=> $2^{2002} \equiv 4 \pmod{31}$ => *2^{2002} - 4 chia hết cho 31*

Bài 8 : Chứng minh rằng : $2222^{5555} + 5555^{2222}$ chia hết cho 7

Giải :

Ta có $2222 + 4 \vdots 7 \Rightarrow 2222 \equiv -4 \pmod{7} \Rightarrow 2222^{5555} \equiv (-4)^{5555} \pmod{7}$

$5555 - 4 \vdots 7 \Rightarrow 5555 \equiv 4 \pmod{7} \Rightarrow 5555^{2222} \equiv 4^{2222} \pmod{7}$

$\Rightarrow 2222^{5555} + 5555^{2222} \equiv (-4)^{5555} + 4^{2222} \pmod{7}$

Mà $4^{2222} = (-4)^{2222} \Rightarrow (-4)^{5555} + 4^{2222} = (-4)^{2222}.4^{3333} + 4^{2222}$

$= (-4)^{2222}.4^{3333} - (-4)^{2222} = (-4)^{2222}(4^{3333} - 1) \equiv (4^3) - 1 \pmod{7}$ (1)

Ta lại có : $4^3 \equiv 1 \pmod{7} \Rightarrow 4^3 - 1 = 63 \vdots 7 \Rightarrow 4^3 - 1 \equiv 0 \pmod{7}$ (2)

Nên $(-4)^{5555} + 4^{2222} \equiv 0 \pmod{7}$

Từ (1) và (2) => $2222^{5555} + 5555^{2222}$ chia hết cho 7.

Bài 9 : Tìm dư trong phép chia $5^{70} + 7^{50}$ cho 12

Giải :

Ta có $5^2 \equiv 1 \pmod{12} \Rightarrow (5^2)^{35} \equiv 1 \pmod{12}$ hay $5^{70} \equiv 1 \pmod{12}$ (1)

$7^2 \equiv 2 \pmod{12} \Rightarrow (7^2)^{25} \equiv 1 \pmod{12}$ hay $7^{50} \equiv 1 \pmod{12}$ (2)

Từ (1) và (2) => $5^{70} + 7^{50}$ chia cho 12 dư 2.

Bài 10 : Tìm số dư của A = $776^{776} + 777^{777} + 778^{778}$ khi chia cho 3 và khi chia cho 5?

Giải :

+Ta có $776 \equiv -1 \pmod{3} \Rightarrow 776^{776} \equiv -1 \pmod{3} \Rightarrow 776^{776} \equiv 1 \pmod{3}$

$777 \equiv 0 \pmod{3} \Rightarrow 777^{777} \equiv 0 \pmod{3}$

$778 \equiv 1 \pmod{3} \Rightarrow 778^{778} \equiv 1 \pmod{3}$

=> $776^{776} + 777^{777} + 778^{778}$ khi chia cho 3 dư 2.

+Ta có $776 \equiv 1 \pmod{5} \Rightarrow 776^{776} \equiv 1 \pmod{5}$

$777 \equiv -3 \pmod{5} \Rightarrow 777^{777} \equiv -3^{777} \pmod{5}$

$778 \equiv 3 \pmod{5} \Rightarrow 778^{778} \equiv 3^{778} \pmod{5}$

$\Rightarrow 776^{776} + 777^{777} + 778^{778} \equiv 1 - 3^{777} + 3^{778} \pmod{5}$

Hay $776^{776} + 777^{777} + 778^{778} \equiv 1 + 3.3^{777} - 3^{777} \pmod{5}$

$776^{776} + 777^{777} + 778^{778} \equiv 1 + 3^{777}(3 - 1) \pmod{5}$

$776^{776} + 777^{777} + 778^{778} \equiv 1 + 2.3^{777}$

Mà $3^2 \equiv -1 \pmod{3} \Rightarrow (3^2)^{388}.3 \equiv 3 \pmod{5}$

Vậy A = $776^{776} + 777^{777} + 778^{778} \equiv 1 + 2.3 \equiv 2 \pmod{5}$

Vậy A chia cho 5 dư 2.

Bài 11 : Tìm số dư của A = $3^{2005} + 4^{2005}$ khi chia cho 11 và khi chia cho 13 ?

Giải :

+Ta có : $3^5 \equiv 1 \pmod{11} \Rightarrow (3^5)^{401} \equiv 1 \pmod{11}$

Và $4^5 \equiv 1 \pmod{11} \Rightarrow (4^5)^{401} \equiv 1 \pmod{11}$

=> $A = 3^{2005} + 4^{2005} \equiv 2 \pmod{11}$

=> *A chia cho 11 dư 2*

+Ta có : $3^3 \equiv 1 \pmod{13} \Rightarrow (3^3)^{668}.\,3 \equiv 1.3 \pmod{13} \Rightarrow 3^{2005} \equiv 3 \pmod{13}$

Và $4^3 \equiv -1 \pmod{13} \Rightarrow (4^3)^{668}.4 \equiv 1.4 \pmod{13} \Rightarrow 4^{2005} \equiv 4 \pmod{13}$

=> $A = 3^{2005} + 4^{2005} \equiv 7 \pmod{13}$

=> *A chia cho 13 dư 7* .

Bài 12 : Giả sử m là số nguyên dương. Chứng minh rằng : Nếu $ac_1 \equiv ac_2 \pmod{m}$ và (a, m) = 1 thì $c_1 \equiv c_2 \pmod{m}$

Giải :

Ta có : $ac_1 \equiv ac_2 \pmod{m} \Rightarrow m \setminus ac_1 - ac_2 \Rightarrow m \setminus a(c_1 - c_2)$

Vì (a, m) = 1 => $m \setminus c_1 - c_2 \Rightarrow c_1 \equiv c_2 \pmod{m}$

Bài 13 :

Chứng minh rằng : Nếu p là một số nguyên tố và không là ước của số nguyên a thì $a^{p-1} \equiv 1 \pmod{p}$

Giải :

Xét dãy số 1; 2; 3; ... ; p - 1. Tất cả các số này đôi một không đồng dư với nhau theo môđun p. Do đó các số a, 2a, 3a, ... ; (p - 1)a cũng đôi một không đồng dư với nhau rtheo môđun p. Bởi vì ngược lại nếu có $r_1a \equiv r_2a \pmod{p}$ mà (a, p) = 1 => $r_1 \equiv r_2 \pmod{p}$ - với r_1, r_2 là hai số nào đó của dãy số 1, 2, 3, ... , p - 1 (vô lí)

Hơn nửa mõi một số của dãy a, 2a, 3a, ... , (p - 1)a đồng dư với đúng một trong các số 1, 2, 3, ... , p - 1 theo môđun p

=> a.2a.3a. ... .(p- 1)a ≡ 1.2.3. ... (p - 1) (mod p) hay $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.

Vì (p, (p - 1)!) = 1 => $a^{p-1} \equiv 1 \pmod{p}$

Bài 14 : Chứng minh rằng : Nếu c là số nguyên dương : $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{c.m}$

Giải :

$a \equiv b \pmod{m} \Rightarrow a - b = m.q \Rightarrow ac - bc = mc.q \Rightarrow ac \equiv bc \pmod{c.m}$

*Định lý nhỏ Fermat : ***Giả sử p là số nguyên tố bất kỳ, khi đó với mọi số tự nhiên n ta có n^p - n chia hết cho p.***

Giải :

Ta có $n^p - n = n(n^{p-1} - 1)$

Nếu n chia hết cho p => định lý được chứng minh.

Nếu n không chia hết cho p thì (n, p) = 1, nên $n^{p-1} \equiv 1 \pmod{p}$

=>$(n^{p-1} - 1)$ chia hết cho p.

Bài 15 :

Bạn Thắng học sinh lớp 6A đã viết một số có hai chữ số mà tổng các chữ số của nó là 14. Bạn Thắng đem số đó chia cho 8 thì được số dư là 4, nhưng khi chia cho 12 thì được số dư là 3.

a)Chứng minh rằng bạn Thắng đã làm sai ít nhất một phép tính chia.

b)Nếu phép chia thứ nhất cho 8 là đúng thì phép chia thứ hai cho 12 có ó dư là bao nhiêu ? Hãy Tìm số bị chia.

Giải :

a)Gọi số đó là $n = \overline{ab}$

Vì n chia cho 8 dư 4, nên n = 8p + 4

Và n chia cho 12 dư 3, nên n = 12q + 3

=> 8p + 4 = 12q + 3 (Mà 8p + 4 là số chẵn, còn 12q + 3 là số lẻ). Do vậy bạn Thắng đã làm sai một phép chia.

b)Vì a + b = 14 => $ab \equiv 2 \pmod 3$ => $4ab \equiv 8 \pmod{12}$ (1)

Nếu $ab \equiv 0 \pmod 4$ => $3ab \equiv 0 \pmod{12}$ (2)

Từ (1) và (2) => $ab \equiv 8 \pmod{12}$ => n chia cho 12 dư 8

Do n = 8p + 4 là số chẵn mà n = ab => $b \in \{0; 2; 4; 6; 8\}$

Nếu b = 0 => a = 14 (loại - vì a là số có một chữ số khác 0)

b = 2 => a = 12 (loại)

b = 4 => a = 10 (loại)

b = 6 => a = 8

b = 8 => a = 6

=> Số cần tìm là 86 hoặc 68 => Số bị chia là 68.

Dạng 2 : Tìm chữ số tận cùng của một số

a)Tìm một chữ số tận cùng của a^n :

-Nếu a có chữ số tận cùng là 0; 1; 5 hoặc 6 thì a^n lần lượt có chữ số tận cùng lần lượt là 0; 1; 5 hoặc 6.

-Nếu a có chữ số tận cùng là 2, 3 hoặc 7, ta vận dụng nhận xét sau với $k \in Z$

$2^{4k} \equiv 6 \pmod{10}$

$3^{4k} \equiv 1 \pmod{10}$

$7^{4k} \equiv 1 \pmod{10}$

Do đó để tìm chữ số tận cùng của a^n với a có chữ số tận cùng là 2; 3; 7 ta lấy n chia cho 4. Giả sử n = 4k + r với $r \in \{0; 1; 2; 3\}$

Nếu $a \equiv 2 \pmod{10}$ thì $a^n \equiv 2^n = 2^{4k+r} \equiv 6.2^r \pmod{10}$

Nếu $a \equiv 3 \pmod{10}$ hoặc $a \equiv 7 \pmod{10}$ thì $a^n \equiv a^{4k+r} \equiv a^r \pmod{10}$

Ví dụ 1 : Tìm chữ số cuối cùng của các số :

a) 6^{2009} , b) 9^{2008} , c) 3^{2009} , d) 2^{2009}

Giải :

a) 6^{2009} có chữ số tận cùng là 6 (vì 6 khi nâng lên luỹ thừa với số mũ tự nhiên khác 0 vẫn bằng chính số 6)

b) $9^{2008} = (9^2)^{1004} = 81^{1004} = \ldots 1$ có chữ số tận cùng là 1

$9^{1991} = 9^{1990}.9 = (9^2)^{995}.9 = 81^{995}.9 = (\ldots 1).9 = \ldots 9$ có chữ số tận cùng là 9

Nhận xét : Số có chữ số tận cùng là 9 khi nâng lên luỹ thừa với số mũ tự nhiên chẵn khác 0 nào thì chữ số tận cùng là 1, khi nâng lên luỹ thừa với số mũ tự nhiên lẻ thì có số tận cùng là 9.

c) $3^{2009} = (3^4)^{502}.3 = 81^{502}.3 = (\ldots 1).3 = \ldots 3$ có chữ số tận cùng là 3.

d) $2^{2009} = 2^{2008}.2 = (2^4)^{502}.2 = 16^{502}.2 = (\ldots 6).2 = \ldots 2$ có chữ số tận cùng là 2

Ví dụ 2 : Tìm chữ số tận cùng của các số sau :

a) 4^{21} , b) 3^{103} , c) 8^{4n+1} $(n \in N)$ d) $14^{23} + 23^{23} + 70^{23}$

Giải :

a) $4^{30} = 4^{2.15} = (4^2)^{15} = 16^{15} = \ldots 6$ có chữ số tận cùng là 6

$4^{21} = 4^{20+1} = (4^2)^{10}.4 = 16^{10}.4 = (\ldots 6).4 = \ldots 4$ có chữ số tận cùng là 4

Nhận xét : Số nào có số tận cùng là 4 thì khi nâng lên luỹ thừa với số mũ tự nhiên chẵn thì có số tận cùng là 6, khi nâng lên với số mũ tự nhiên lẻ có số tận cùng là 4)

b) $3^{103} = 3^{102}.3 = (3^2)^{51}.3 = 9^{51}.3 = (\ldots 9).3 = \ldots 7$ có chữ số tận cùng là 7

c) $8^{4n+1} = 8^{4n}.8 = (2^3)^{4n}.8 = 2^{12n}.8 = (2^4)^{3n}.8 = 16^{3n}.8 = (\ldots 6).8 = \ldots. 8$ có chữ số tận cùng là 8

d) $14^{23} = 14^{22}.14 = (\ldots 6).14 = \ldots. 4$

$23^{23} = 23^{22}.23 = (23^2)^{11}.23 = (\ldots 9).23 = \ldots 7$

$70^{23} = \ldots 0$

Vậy : $14^{23} + 23^{23} + 70^{23} = \ldots 4 + \ldots 7 + \ldots 0 = \ldots 1$ có chữ số tận cùng là 1

b)Tìm hai số tận cùng của số a^n :

Ta có nhận xét sau :

$2^{20} \equiv 76 \pmod{100}$

$3^{20} \equiv 01 \pmod{100}$

$6^5 \equiv 76 \pmod{100}$

$7^4 \equiv 01 \pmod{100}$

Mà $76^n \equiv 76 \pmod{100}$ với $n \geq 1$

$5^n \equiv 25 \pmod{100}$ với $n \geq 2$

Suy ra kết quả sau với k là số tự nhiên khác 0.

$a^{20k} \equiv 00 \pmod{100}$ nếu $a \equiv 0 \pmod{10}$

$a^{20k} \equiv 01 \pmod{100}$ nếu $a \equiv 1; 3; 7; 9 \pmod{10}$

$a^{20k} \equiv 25 \pmod{100}$ nếu $a \equiv 5 \pmod{10}$

$a^{20k} \equiv 76$ (mod 100 nếu $a \equiv 2; 4; 6; 8 \pmod{10}$

Vậy để tìm hai chữ số tận cùng của a^n, ta lấy số mũ n chia cho 20

Bài 1 : Tìm hai chữ số tân cùng của 2^{2003}

Giải :

Ta có : $2^{20} \equiv 76 \pmod{100} \Rightarrow 2^{20k} \equiv 76 \pmod{100}$

Do đó : $2^{2003} = 2^3.(2^{20})^{100} = 8.(2^{20})^{100} = (\ldots 76).8 = \ldots 08$

Vậy 2^{2003} có hai chữ số tận cùng là 08.

Bài 2 : Tìm hai chữ số tận cùng của B = $7^{9^{9^9}}$

Giải :