SỞ GIÁO DỤC VÀ ĐÀO TẠO ĐĂK LĂK
TRƯỜNG THPT PHAN ĐÌNH PHÙNG

****

HÀ DUY NGHĨA

MỘT ỨNG DỤNG THÚ VỊ CỦA LÝ THUYẾT ĐỒNG DƯ

CHUYÊN ĐỀ BỒI DƯỠNG HSG

Đăk Lăk -2012

MỤC LỤC

LỜI MỞ ĐẦU

Bộ môn số học là một trong những môn học thú vị, hấp dẫn nhất của toán học, bởi nó rất gần gũi trong cuộc sống trong mỗi con người. Ngay từ lớp 6 các em học sinh đã được tiếp cận và học, nhưng đến những năm học cấp 3 các em không được tiếp tục học và từ đó bộ môn này hầu như không được nhắc đến và có lẽ đi vào quên lãng. Do đó, bài viết này tôi muốn giới thiệu đến quý thầy cô giáo, các em học sinh một ứng dụng thú vị của lí thuyết đồng dư nhằm gợi lại cảm hứng nghiên cứu học tập cho quý thầy cô giáo cũng như các em học sinh về bộ môn này.

Bài viết gồm hai phần, phần đầu tôi giới thiệu sơ lược lại lý tuyết đồng dư và nêu lên các tính chất cần thiết bổ sung cho phần sau. Phần thứ 2 tôi giới thiệu các quy luật đi tìm dấu hiệu chia hết của các số nguyên tố cũng như một số ví dụ về các bài toán chia hết.

Bài viết tuy ngắn nhưng không tránh khỏi thiếu sót, rất mong được sự đóng góp ý kiến của bạn đọc.

Tác giả

LÝ THUYẾT ĐỒNG DƯ VÀ ÁP DỤNG

1.1 Đồng dư thức

Định nghĩa 1.1.1. Cho a, b, m là các số nguyên, $m \neq 0$. Số a được gọi là *đồng dư* với b theo môđun m nếu m là ước của $(b - a)$. Nếu a đồng dư với b theo môđun m thì viết $a \equiv b \pmod{m}$. Ngược lại, nếu a không đồng dư với b theo môđun m thì ta viết $a \not\equiv b \pmod{m}$.

Ví dụ $2 \equiv 5 \pmod{3}$ vì $3|(5 - 2)$.

Nếu $a \equiv b \pmod{m}$ thì b gọi là một *thặng dư* của a theo môđun m.

Nếu $0 \leq b \leq m - 1$ thì b gọi là một thặng dư bé nhất của a theo môđun m.

Mệnh đề 1.1.2. *Cho a, b, c, m là những số nguyên $m \neq 0$. Khi đó, ta có*

(i) $a \equiv a \pmod{m}$,

(ii) Nếu $a \equiv b \pmod{m}$ *thì* $b \equiv a \pmod{m}$,

(iii) Nếu $a \equiv b \pmod{m}$ *và* $b \equiv c \pmod{m}$ *thì* $a \equiv c \pmod{m}$.

Chứng minh. Mệnh đề $(i), (ii)$ là hiển nhiên, ta chứng minh mệnh đề (iii). Thật vậy, ta có $a \equiv b \pmod{m}, b \equiv c \pmod{m}$ suy ra $m|(b - a)$ và $m|(c - b)$. Do đó $m|(b - a + c - b)$, hay $m|(c - a)$. Vậy $a \equiv c \pmod{m}$. □

Tiếp theo, ký hiệu $\overline{a}$ là tập hợp tất cả các số nguyên đồng dư với a theo môđun m, $\overline{a} = \{n \in \mathbb{Z} | n \equiv a \pmod{m}\}$. Nói cách khác, $\overline{a}$ là tập hợp các số nguyên có dạng $\{a + km\}$. Từ đó, ta có định nghĩa sau.

Định nghĩa 1.1.3. Một tập gồm các phần tử dạng $\overline{a} = \{a + km, k \in \mathbb{Z}\}$ gọi là một *lớp đồng dư* của a theo môđun m.

Ví dụ với $m = 2$, ta có lớp $\overline{0}$ là tập các số nguyên chẵn, lớp $\overline{1}$ là tập các số nguyên lẻ.

Mệnh đề 1.1.4. *Cho a, b, m là những số nguyên $m \neq 0$. Khi đó, ta có* *(i)* $\overline{a} = \overline{b}$ *khi và chỉ khi* $a \equiv b \pmod m$,

(ii) $\overline{a} \neq \overline{b}$ *khi và chỉ khi* $\overline{a} \cap \overline{b} = \emptyset$,

(iii) Có đúng m *lớp đồng dư phân biệt theo môđun* m.

Chứng minh. (i) Giả sử $\overline{a} = \overline{b}$, ta xét $a \in \overline{a} = \overline{b}$. Do đó, $a \equiv b \pmod m$. Ngược lại, nếu $a \equiv b \pmod m$ thì $a \in \overline{b}$. Ngoài ra, nếu $c \equiv a \pmod m$ thì $c \equiv b \pmod m$. Điều này chứng tỏ rằng $\overline{a} \subseteq \overline{b}$. Hơn nữa, từ $a \equiv b \pmod{m}$ ta suy ra $b \equiv a \pmod m$, hay $\overline{b} \subseteq \overline{a}$. Từ đó suy ra $\overline{a} = \overline{b}$.

(ii) Dễ thấy rằng, nếu $\overline{a} \cap \overline{b} = \emptyset$ thì $\overline{a} \neq \overline{b}$. Ngược lại, ta cần chứng tỏ rằng nếu $\overline{a} \cap \overline{b} \neq \emptyset$ thì $\overline{a} = \overline{b}$. Thật vậy, giả sử $\overline{a} \cap \overline{b} \neq \emptyset$ gọi $c \in \overline{a} \cap \overline{b}$. Khi đó, ta có $c \equiv a \pmod m$ và $c \equiv b \pmod m$. Điều này suy ra $a \equiv b \pmod m$. Do đó, theo (i) ta suy ra $\overline{a} = \overline{b}$.

(iii) Để chứng minh phần này, ta chứng minh tập $\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ là m lớp đồng dư phân biệt theo môđun m. Thật vậy, giả sử tồn tại $0 \leq k < l < m$ sao cho $\overline{k} = \overline{l}$. Khi đó, theo (i) ta có $k \equiv l \pmod{m}$, hay $m|(l-k)$. Điều này mâu thuẫn với giả thiết $0 < l - k < m$. Do đó, $\overline{k} \neq \overline{l}$. Ngoài ra, với mỗi $a \in \mathbb{Z}$ luôn tồn tại cặp số nguyên q, r sao cho $a = qm + r, 0 \leq r < m$, suy ra $a \equiv r \pmod m$ hay $\overline{a} = \overline{r}$. □

Định nghĩa 1.1.5. Tập gồm m phần tử $\{A = a_1, a_2, ..., a_m\}$ gọi là một *hệ thặng dư đầy đủ* theo môđun m nếu $\{B = \overline{a_1}, \overline{a_2}, \overline{a_3}, ..., \overline{a_m}\}$ là tập gồm m lớp đồng dư phân biệt theo môđun m.

Từ định nghĩa ta thấy rằng, hệ thặng dư đầy đủ theo môđun m là không duy nhất. Ví dụ các tập $\{0, 1, 2, 3\}, \{4, 9, 14, -1\}, \{0, 1, -2, -1\}$ là những hệ thặng dư đầy đủ theo môđun 4.

Mệnh đề 1.1.6. *Nếu* $a \equiv c \pmod{m}$ *và* $b \equiv d \pmod{m}$ *thì* $a + b \equiv c + d \pmod m$ *và* $ab \equiv cd \pmod m$.

Chứng minh. Dễ dàng suy ra từ định nghĩa. □

Mệnh đề 1.1.7. *Cho* a, b, c, m *là các số nguyên,* $m > 0, ac \equiv bc \pmod m$ *và* $d = (c, m)$. *Khi đó, ta có*

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

Chứng minh. Giả sử $ac \equiv bc \pmod m$. Ta có $m|(bd-ac)$, suy ra tồn tại số nguyên k sao cho $c(b-a)=km$. Khi đó, chia hai vế cho d ta được $\frac{c}{d}(b-a)=k\frac{m}{d}$. Ngoài ra, theo giả thiết ta có $d=(c,m)$, suy ra $\left(\frac{c}{d},\frac{m}{d}\right)=1$. Do đó, ta có $\frac{m}{d}|(b-a)$ hay

$$a \equiv b \pmod{\frac{m}{d}}.$$ □

Mệnh đề 1.1.8. *Cho* $a, b, m_1, ..., m_k$ *là các số nguyên,* $m_1, ..., m_k > 0, a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, ..., a \equiv b \pmod{m_k}$. *Khi đó, ta có*

$$a \equiv b \pmod{[m_1...m_k]},$$

trong đó $[m_1m_2...m_k]$ *là bội chung nhỏ nhất của* $m_1, m_2..., m_k$.

Chứng minh. Suy ra trực tiếp từ định nghĩa. □

Mệnh đề 1.1.9. *Nếu* $a \equiv b \pmod n$ *thì* $a^n \equiv b^n \pmod{n^2}$.

Chứng minh. Từ $a \equiv b \pmod n$ suy ra $a = b + nq$. Do đó, theo công thức khai triển nhị thức ta có

$$\begin{aligned} a^n - b^n &= (b+nq)^n - b^n \\ &= \binom{n}{1} b^{n-1}qn + \binom{n}{2} b^{n-2}q^2n^2 + \cdots + \binom{n}{n} q^n n^n \\ &= n^2 \left(b^{n-1}q + \binom{n}{2} b^{n-2}q^2 + \cdots + \binom{n}{n} q^n n^{n-2} \right). \end{aligned}$$

Từ đó suy ra $a^n \equiv b^n \pmod{n^2}$.
Điều ngược lại không đúng, ví dụ như $3^4 \equiv 1^4 \pmod{4^2}$ nhưng $3 \not\equiv 1 \pmod 4$. □

Mệnh đề 1.1.10. *Nếu* a, b *là các số nguyên và* p *là số nguyên tố thì*

$$(a+b)^p \equiv a^p + b^p \pmod p$$

Chứng minh. Theo công thức khai triển nhị thức ta có

$$(a+b)^p = a^p + b^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} a.b^{p-1}.$$

Do đó, để chứng minh mệnh đề ta chỉ cần chứng minh $p|\binom{p}{k}, (1 \le k \le p-1)$. Thật vậy, ta có

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

suy ra

$$k\binom{p}{k} = \frac{p!}{(k-1)!(p-k)!}$$
$$= p\frac{(p-1)!}{(k-1)!(p-k)!} = p\binom{p-1}{k-1}.$$

Từ đó, $p|k\binom{p}{k}$. Ngoài ra, do ƯCLN$(p,k) = 1$ nên $p|\binom{p}{k}$. □

1.2 Ứng dụng của lý thuyết đồng dư để tìm dấu hiệu chia hết

Ví dụ 1.2.0.1. Tìm dấu hiệu chia hết cho $2^k, 3, 5^k, 7, 11, 13, 37$.

Lời giải: Xét số tự nhiên $a = \overline{a_n.a_{n-1}...a_0}$. Tức là a được viết dưới dạng

$$a = a_n.10^n + \cdots + a_1.10 + a_0, (0 \leq a_i \leq 9).$$

- *Dấu hiệu chia hết cho* 2^k.

  Vì $10 \equiv 0 \pmod 2$ nên $10^k \equiv 0 \pmod{2^k}$. Từ đó suy ra

  $$a \equiv a_{k-1}.10^{k-1} + \cdots + a_0 \pmod{2^k}.$$

  Do đó, số a chia hết cho 2^k khi số $b = a_{k-1}.10^{k-1} + \cdots + a_0 \equiv 0 \pmod{2^k}$, tức là b chia hết cho 2^k. Nói cách khác, số tự nhiên a chia hết cho 2^k khi số tự nhiên b được lập từ k chữ số tận cùng của a chia hết cho 2^k.

  Tương tự, ta cũng có $10 \equiv 0 \pmod 5$ và $10^k \equiv 0 \pmod{5^k}$. Do đó, số a chia hết cho 5^k khi số b lập từ k chữ số tập cùng của a chia hết cho 5^k.

- *Dấu hiệu chia hết cho* 3 *và* 9.

  Ta có $10 \equiv 1 \pmod 3$ suy ra $10^k \equiv 1 \pmod 3$. Do đó $a_i.10^k \equiv a_i \pmod 3$. Từ đó suy ra $a = a_n.10^n + \cdots + a_1.10 + a_0 \equiv a_n + \cdots + a_0 \pmod 3$. Vậy, số a chia hết cho 3 khi tổng các chữ số của nó chia hết cho 3.

  Tương tự ta cũng có $10 \equiv 1 \pmod 9$ và $a_i.10^k \equiv a_i \pmod 9$. Vậy, số a chia hết cho 9 khi tổng các chữ số của nó chia hết cho 9.

- *Dấu hiệu chia hết cho* 7

  Ta có

$$\begin{aligned}
&a_0 \equiv a_0 \pmod 7 && \Rightarrow a_0 \equiv a_0 \pmod 7\\
&10 \equiv 3 \pmod 7 && \Rightarrow 10a_1 \equiv 3a_1 \pmod 7\\
&10^2 \equiv 2 \pmod 7 && \Rightarrow 10^2a_2 \equiv 2a_2 \pmod 7\\
&10^3 \equiv -1 \pmod 7 && \Rightarrow 10^3a_3 \equiv -1a_3 \pmod 7\\
&\dots
\end{aligned}$$

  Từ đó, ta có bảng đồng dư theo môđun 7 tương ứng như sau

a_0	$10a_1$	10^2a_2	10^3a_3	10^4a_4	10^5a_5	10^6a_6	10^7a_7	10^8a_8	10^9a_9	$10^{10}a_{10}$	$10^{11}a_{11}$	...	$10^{6t-1}a_{6t-1}$
a_0	$3a_1$	$2a_2$	$-a_3$	$-3a_4$	$-2a_5$	a_6	$3a_7$	$2a_8$	$-a_9$	$-3a_{10}$	$-2a_{11}$	...	$-2a_{6t-1}$

Bảng 1.1:

  Do đó, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 7 khi tổng dạng

  $(a_0+3a_1+2a_2)-(a_3+3a_4+2a_5)+(a_6+...)+...-(a_{6t-3}+3a_{6t-2}+2a_{6t-1}) \equiv 0 \pmod{7}$

  Ngoài ra, với mọi số x, y, z ta đều có

$$x + 3y + 2z \equiv 100z + 10y + x \pmod 7 \equiv \overline{zyx} \,(\mathrm{mod}\ 7.)$$

  Từ đó suy ra, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 7 khi tổng dạng

$$\overline{a_2a_1a_0} - \overline{a_5a_4a_3} + \overline{a_8a_7a_6} - \overline{a_{11}a_{10}a_9} + ..., \text{ chia hết cho } 7$$

- *Dấu hiệu chia hết cho* 11

  Tương tự dấu hiệu chia hết cho 7, ta cũng có

$$\begin{aligned}
&a_0 \equiv a_0 \pmod{11} && \Rightarrow a_0 \equiv a_0 \pmod{11}\\
&10 \equiv -1 \pmod{11} && \Rightarrow 10a_1 \equiv -a_1 \pmod{11}\\
&10^2 \equiv 1 \pmod 7 && \Rightarrow 10^2a_2 \equiv a_2 \pmod{11}\\
&10^3 \equiv -1 \pmod{11} && \Rightarrow 10^3a_3 \equiv -1a_3 \pmod{11}\\
&\dots
\end{aligned}$$

a_0	$10a_1$	10^2a_2	10^3a_3	10^4a_4	10^5a_5	10^6a_6	10^7a_7	10^8a_8	10^9a_9	$10^{10}a_{10}$	$10^{11}a_{11}$	...	$10^{2t-1}a_{2t-1}$
a_0	$-a_1$	a_2	$-a_3$	a_4	$-a_5$	a_6	$-a_7$	a_8	$-a_9$	a_{10}	$-a_{11}$	...	$-a_{2t-1}$

Bảng 1.2:

Do đó, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 11 khi tổng dạng

$$a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 + ... - a_{2t-1} \equiv 0 \pmod{11}$$

Nói cách khác, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 11 khi tổng đan dấu

$$a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 + ... - a_{2t-1} \text{ chia hết cho } 11$$

- *Dấu hiệu chia hết cho* 13

Ta có

$$\begin{aligned}
&a_0 \equiv a_0 \pmod{13} && \Rightarrow a_0 \equiv a_0 \pmod{13}\\
&10 \equiv -3 \pmod{13} && \Rightarrow 10a_1 \equiv -3a_1 \pmod{13}\\
&10^2 \equiv -4 \pmod{13} && \Rightarrow 10^2a_2 \equiv -4a_2 \pmod{13}\\
&10^3 \equiv -1 \pmod{13} && \Rightarrow 10^3a_3 \equiv -1a_3 \pmod{13}\\
&\dots
\end{aligned}$$

Tương tự ta cũng có bảng các lớp đồng dư theo môđun 13 (Bảng 1.3)

a_0	$10a_1$	10^2a_2	10^3a_3	10^4a_4	10^5a_5	10^6a_6	10^7a_7	10^8a_8	10^9a_9	$10^{10}a_{10}$	$10^{11}a_{11}$	...	$10^{6t-1}a_{6t-1}$
a_0	$-3a_1$	$-4a_2$	$-a_3$	$3a_4$	$4a_5$	a_6	$-3a_7$	$-4a_8$	$-a_9$	$3a_{10}$	$4a_{11}$	...	$4a_{6t-1}$

Bảng 1.3:

Từ bảng 1.3 ta suy ra rằng, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 13 khi tổng dạng

$$(a_0 - 3a_1 - 4a_2) - (a_3 - 3a_4 - 4a_5) + ... - (a_{6t-3} - 3a_{6t-2} - 4a_{6t-1}) \equiv 0 \pmod{13}$$

Ngoài ra, với mọi số x, y, z ta đều có

$$x - 3y - 4z \equiv 100z + 10y + x \pmod{13} \equiv \overline{zyx} \pmod{13.}$$

Từ đó suy ra, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 13 khi tổng dạng

$$\overline{a_2a_1a_0} - \overline{a_5a_4a_3} + \overline{a_8a_7a_6} - \overline{a_{11}a_{10}a_9} + ... \text{ chia hết cho } 13.$$

- *Dấu hiệu chia hết cho* 33

  Ta có

$$\begin{aligned}
a_0 &\equiv a_0 \pmod{33} & &\Rightarrow a_0 \equiv a_0 \pmod{33}\\
10 &\equiv 10 \pmod{33} & &\Rightarrow 10a_1 \equiv 10a_1 \pmod{33}\\
10^2 &\equiv 1 \pmod{33} & &\Rightarrow 10^2a_2 \equiv a_2 \pmod{33}\\
10^3 &\equiv 10 \pmod{33} & &\Rightarrow 10^3a_3 \equiv 10a_3 \pmod{33}\\
&\ldots
\end{aligned}$$

a_0	$10a_1$	10^2a_2	10^3a_3	10^4a_4	10^5a_5	10^6a_6	10^7a_7	10^8a_8	10^9a_9	$10^{10}a_{10}$	$10^{11}a_{11}$	...	$10^{2t}a_{2t}$
a_0	$10a_1$	a_2	$10a_3$	a_4	$10a_5$	a_6	$10a_7$	a_8	$10a_9$	a_{10}	$10a_{11}$	...	a_{2t}

Bảng 1.4:

Từ bảng 1.4 ta suy ra rằng, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 33 khi tổng dạng

$$(a_0 + a_2 + \cdots + a_{2t}) + 10(a_1 + a_3 + \cdots + a_{2t+1}) \equiv 0 \pmod{33}$$

Ngoài ra, với mọi số x, y ta đều có

$$x + 10y \equiv 10y + x \pmod{33} \equiv \overline{yx} \,(\mathrm{mod}\ 33.)$$

Từ đó suy ra, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 33 khi tổng dạng

$$\overline{a_1a_0} + \overline{a_3a_2} + \overline{a_5a_4} + \overline{a_6a_5} + \text{...chia hết cho 33.}$$

Ngoài ra, ta có $33 = 11.3$ nên ta suy ra được một dấu hiệu khác nữa của số chia hết cho 11; 3 là tổng dạng

$$\overline{a_1a_0} + \overline{a_3a_2} + \overline{a_5a_4} + \overline{a_6a_5} + ..., \text{chia hết cho } \ 11;\ 3.$$

- *Dấu hiệu chia hết cho* 37

  Ta có

$$\begin{aligned}
a_0 &\equiv a_0 \pmod{37} & &\Rightarrow a_0 \equiv a_0 \pmod{37}\\
10 &\equiv 10 \pmod{37} & &\Rightarrow 10a_1 \equiv 10a_1 \pmod{37}\\
10^2 &\equiv -11 \pmod{37} & &\Rightarrow 10^2a_2 \equiv 11a_2 \pmod{37}
\end{aligned}$$

$$
\begin{aligned}
&10^3 \equiv 1 \pmod{37} &&\Rightarrow 10^3 a_3 \equiv 1 a_3 \pmod{37}\\
&10^4 \equiv 10 \pmod{37} &&\Rightarrow 10^4 a_3 \equiv 10 a_3 \pmod{37}\\
&10^5 \equiv -11 \pmod{37} &&\Rightarrow 10^4 a_3 \equiv -11 a_3 \pmod{37}\\
&\dots
\end{aligned}
$$

a_0	$10a_1$	10^2a_2	10^3a_3	10^4a_4	10^5a_5	10^6a_6	10^7a_7	10^8a_8	10^9a_9	$10^{10}a_{10}$	$10^{11}a_{11}$	...	$10^{2t}a_{3t}$
a_0	$10a_1$	$-11a_2$	a_3	$10a_4$	$-11a_5$	a_6	$10a_7$	$-11a_8$	a_9	$10a_{10}$	$-a_{11}$	...	$-11a_{3t}$

Bảng 1.5:

Từ bảng 1.5 ta suy ra rằng, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 37 khi tổng dạng

$(a_0+a_3+\cdots+a_{3t})+10(a_1+a_4+\cdots+a_{3t+1})-11(a_2+a_5\cdots+a_{3t+2}) \equiv 0 \pmod{37}$

Ngoài ra, với mọi số x, y, z ta đều có

$$x + 10y - 11z \equiv 100z + 10y + x \pmod{37} \equiv \overline{zyx}\,(\mathrm{mod}\ 37.)$$

Từ đó suy ra, số $a = \overline{a_n.a_{n-1}...a_1a_0}$ chia hết cho 37 khi tổng dạng

$$\overline{a_2a_1a_0} + \overline{a_5a_4a_3} + \overline{a_8a_7a_6} + \cdots, \text{chia hết cho 37.}$$

Ví dụ 1.2.0.2. Chứng minh rằng

a) $4^{4021} + 3^{2012}$ chia hết cho 13,

b) $6^{2023} + 8^{2023}$ chia hết cho 49,

c) $220^{119^{69}} + 119^{69^{220}} + 69^{220^{119}}$ chia hết cho 102,

d) $2222^{5555} + 5555^{2222}$ chia hết cho 7.

Lời giải a)Ta có

$$
\begin{aligned}
4^{4021} + 3^{2012} &= 4.16^{2010} + 9.3^{2010}\\
&\equiv 4(16^{2010} - 3^{2010}) \pmod{13}\\
&\equiv (16-3)(16^{2009} + 16^{2008}3 + ... + 3^{2009}) \pmod{13}\\
&\equiv 0 \pmod{13}.
\end{aligned}
$$

Vậy, $4^{4021} + 3^{2012}$ chia hết cho 13.

b) Ta có $6^{2023} + 8^{2023} = (6+8)(6^{2022} - 6^{2021}8 + 6^{2020}8^2 + \cdots + 8^{2022}) = 14M$, trong đó

$$M = (6^{2022} - 6^{2021}8 + 6^{2020}8^2 + \cdots + 8^{2022}).$$

Hơn nữa, $M \equiv \underbrace{(-1)^{2022} + 1^{2021} - \cdots + 1^{2022}}_{2023 \text{ số hạng}} \equiv 2023 \equiv 0 \pmod 7$, hay $7|M$. Từ đó suy ra, $49|14M$ hay $6^{2023} + 8^{2023}$ chia hết cho 49.

c) Ta có

$$220 \equiv 0 \pmod 2 \Rightarrow 220^{119^{69}} \equiv 0 \pmod 2,$$
$$119 \equiv 1 \pmod 2 \Rightarrow 119^{220^{69}} \equiv 1 \pmod 2,$$
$$69 \equiv 1 \pmod 2 \Rightarrow 69^{220^{119}} \equiv 1 \pmod 2.$$

Do đó, $A = 220^{119^{69}} + 119^{69^{220}} + 69^{220^{119}}$ chia hết cho 2.

Tương tự ta cũng chứng minh được A chia hết cho $3, 17$. Vì các số $\{2, 3, 17\}$ là những số đôi một nguyên tố cùng nhau nên ta suy ra A chia hết cho 102.

d) Ta có $2222 \equiv 3 \pmod 7, 3^2 \equiv 2 \pmod 7, 3^3 \equiv -1 \pmod 7$. Do đó

$$2222^{5555} \equiv 3^{3.1851+2} \equiv -2 \pmod 7.$$

Tương tự, ta cũng có $5555 \equiv 4 \pmod 7, 4^3 \equiv 1 \pmod 7, 4^2 \equiv 2 \pmod 7$ nên

$$5555^{2222} \equiv 4^{3.740+2} \equiv 2 \pmod 7.$$

Từ đó suy ra, $2222^{5555} + 5555^{2222} \equiv 0 \pmod 7$ hay $2222^{5555} + 5555^{2222} \vdots 7$.

Ví dụ 1.2.0.3. Tìm số dư của số 1234356789^4 khi chia cho 8.

Lời giải: Vì $8 = 2^3$ nên số dư của phép chia 1234356789^4 cho 8 cũng chính là số dư của 789^4 khi chia cho 8. Do đó, ta có

$$1234356789^4 \equiv 789^4 \equiv 5^4 \equiv 1 \pmod 8.$$

Từ đó suy ra số dư của phép chia 1234356789^4 cho 8 là 1.

TÀI LIỆU THAM KHẢO

A.Tiếng Việt

1. Hà Huy Khoái (2004), *Chuyên đề bồi dưỡng học sinh giỏi toán phổ thông Số học*, Nhà xuất bản Giáo dục.

2. Hà Huy Khoái (2003), *Số học và thuật toán: Cơ sở lý thuyết và tính toán thực hành*, Nhà xuất bản Đại học Quốc Gia Hà Nội.

3. Nguyễn Tiến Quang (2007),*Bài tập số học*, Nhà xuất bản Giáo dục.

B.Tiếng Anh

4. Cohen, H. (2007), *Number Theory Volume I:Tools and Diophantine Equations,* Springer Science+Business Media, LLC.

5. Ireland K. ,Rosen M. (1990) *A Classical Introduction to Modern Number Theory,* Springer-Verlag, Berlin.

6. Andreeescu, Titu (2006) *104 Number theory Problems From the Training of the USA IMO Team,* Birkhauser.

7. Chau, Le Hai (2010), *Selected Problems of the Vietnamese Mathematical Olympiad (1962-2009),* Singapore.

8. Dušan Djukić (2009),*The IMO Compendium A Collection of Problems Suggested for the International Mathematical Olympiad:1959-2009,* Springer.

C. Một số tài liệu khác trên mạng Internet