

Đa thức

Đa thức là một trong những khái niệm trung tâm của toán học. Trong chương trình phổ thông, chúng ta đã làm quen với khái niệm đa thức từ bậc trung học cơ sở, từ những phép cộng, trừ, nhân đa thức đến phân tích đa thức ra thừa số, dùng sơ đồ Horner để chia đa thức, giải các phương trình đại số.

Bài giảng này sẽ hệ thống hoá lại những kiến thức cơ bản nhất về đa thức 1 biến, các dạng toán thường gặp về đa thức. Ở cuối bài sẽ đề cập 1 cách sơ lược nhất về đa thức nhiều biến.

1. Đa thức và các phép toán trên đa thức

1.1. Định nghĩa. Đa thức trên trường số thực là biểu thức có dạng

$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, trong đó $a_i \in \mathbb{R}$ và $a_n \neq 0$.
 a_i được gọi là các *hệ số* của đa thức, trong đó a_n được gọi là *hệ số cao nhất* và a_0 được gọi là *hệ số tự do*.

n được gọi là *bậc* của đa thức và ký hiệu là $n = \deg(P)$. Ta quy ước bậc của đa thức hằng $P(x) = a_0$ với mọi x là bằng 0 nếu $a_0 \neq 0$ và bằng $-\infty$ nếu $a_0 = 0$.

Để tiện lợi cho việc viết các công thức, ta quy ước với đa thức $P(x)$ bậc n thì vẫn có các hệ số a_k với $k > n$, nhưng chúng đều bằng 0.

Tập hợp tất cả các đa thức 1 biến trên trường các số thực được ký hiệu là $\mathbb{R}[x]$. Nếu các hệ số được lấy trên tập hợp các số hữu tỷ, các số nguyên thì ta có khái niệm *đa thức với hệ số hữu tỷ*, *đa thức với hệ số nguyên* và tương ứng là các tập hợp $\mathbb{Q}[x]$, $\mathbb{Z}[x]$.

1.2. Đa thức bằng nhau

Hai đa thức $P(x) = \sum_{k=0}^m a_k x^k$, $Q(x) = \sum_{k=0}^n b_k x^k$ bằng nhau khi và chỉ khi $m = n$ và $a_k = b_k$ với mọi $k=0, 1, 2, \dots, m$.

1.3. Phép cộng, trừ đa thức.

Cho hai đa thức $P(x) = \sum_{k=0}^m a_k x^k$, $Q(x) = \sum_{k=0}^n b_k x^k$. Khi đó phép cộng và trừ hai đa thức $P(x)$ và $Q(x)$ được thực hiện theo từng hệ số của x_k , tức là

$$P(x) \pm Q(x) = \sum_{k=0}^{\max\{m,n\}} (a_k \pm b_k) x^k$$

Ví dụ: $(x^3 + 3x^2 - x + 2) + (x^2 + x - 1) = x^3 + 4x^2 + 1$.

1.4. Phép nhân đa thức.

Cho hai đa thức $P(x) = \sum_{k=0}^m a_k x^k$, $Q(x) = \sum_{k=0}^n b_k x^k$. Khi đó $P(x).Q(x)$ là một đa thức có bậc $m+n$ và có các hệ số được xác định bởi

$$c_k = \sum_{i=0}^k a_i b_{k-i}.$$

Ví dụ: $(x^3 + x^2 + 3x + 2)(x^2 + 3x + 1) = (1.1)x^5 + (1.3 + 1.1)x^4 + (1.1 + 1.3 + 3.1)x^3 + (1.1 + 3.3 + 2.1)x^2 + (3.1 + 2.3)x + (2.1) = x^5 + 4x^4 + 7x^3 + 12x^2 + 9x + 1.$

1.5. Bậc của tổng, hiệu và tích của các đa thức

Từ các định nghĩa trên đây, dễ dàng suy ra các tính chất sau đây

Định lý 1. Cho $P(x)$, $Q(x)$ là các đa thức bậc m , n tương ứng. Khi đó

a) $\deg(P \pm Q) \leq \max\{m, n\}$ trong đó nếu $\deg(P) \neq \deg(Q)$ thì dấu bằng xảy ra. Trong trường hợp $m = n$ thì $\deg(P \pm Q)$ có thể nhận bất cứ giá trị nào $\leq m$.

b) $\deg(P.Q) = m + n$.

1.6. Phép chia có dư.

Định lý 2. Với hai đa thức $P(x)$ và $Q(x)$ bất kỳ, trong đó $\deg(Q) \geq 1$, tồn tại duy nhất các đa thức $S(x)$ và $R(x)$ thoả mãn đồng thời các điều kiện:

i) $P(x) = Q(x).S(x) + R(x)$

ii) $\deg(R) < \deg(Q)$

Chứng minh. Tồn tại. Ta chứng minh bằng quy nạp theo $m = \deg(P)$. Nếu $\deg(P) < \deg(Q)$ thì ta có thể chọn $S(x) \equiv 0$ và $R(x) = P(x)$ thoả mãn đồng thời các điều kiện i) và ii). Giả sử $m \geq n$ và định lý đã được chứng minh với các đa thức có bậc nhỏ hơn m . Ta chứng minh định lý đúng với các đa thức bậc m . Giả sử

$$P(x) = \sum_{k=0}^m a_k x^k, \quad Q(x) = \sum_{k=0}^n b_k x^k$$

Xét đa thức

$$H(x) = P(x) - \frac{a_m}{b_n} x^{m-n} Q(x)$$

$$= (a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0) - \frac{a_m}{b_n} x^{m-n} (b_n x^n + \dots + b_0)$$

$$= \left(a_{m-1} - \frac{a_m b_{n-1}}{b_n} \right) x^{m-1} + \dots$$

Do hệ số của x^m ở hai đa thức bị triệt tiêu nên bậc của $H(x)$ không vượt quá $m-1$.

Theo giả thiết quy nạp, tồn tại các đa thức $S^*(x)$, $R^*(x)$ sao cho

$$H(x) = S^*(x).Q(x) + R^*(x)$$

Nhưng khi đó

$$P(x) = H(x) + \frac{a_m}{b_n} x^{m-n} Q(x) = \left(\frac{a_m}{b_n} x^{m-n} + S^*(x) \right) + R^*(x)$$

Vậy đặt $S(x) = (a_m/b_n)x^{m-n} + S^*(x)$ và $R(x) = R^*(x)$ ta được biểu diễn cần tìm cho $P(x)$.

Duy nhất. Giả sử ta có hai biểu diễn $P(x) = S(x).Q(x) + R(x)$ và $P(x) = S^*(x).Q(x) + R^*(x)$ thoả mãn điều kiện ii). Khi đó $Q(x).(S(x)-S^*(x)) = R^*(x) - R(x)$. Ta có, theo điều kiện ii) và định lý 1 thì $\deg(R^*(x) - R(x)) < \deg(Q)$. Mặt khác, nếu $S(x) - S^*(x)$ không đồng nhất bằng 0 thì $\deg(Q(x).(S(x)-S^*(x))) = \deg(Q(x)) + \deg(S(x)-S^*(x)) \geq \deg(Q)$. Mâu thuẫn vì hai vế bằng nhau.

Theo ký hiệu của định lý thì $S(x)$ được gọi là thương số và $R(x)$ được gọi là dư số trong phép chia $P(x)$ cho $Q(x)$.

Phép chứng minh nói trên cũng cho chúng ta thuật toán tìm thương số và dư số của phép chia hai đa thức, gọi là *phép chia dài* (long division) hay *sơ đồ Horner*.

Ví dụ: Thực hiện phép chia $3x^3 - 2x^2 + 4x + 7$ cho $x^2 + 2x$

$$\begin{array}{r|l} 3x^3 - 2x^2 + 4x + 7 & x^2 + 2x \\ 3x^3 + 6x^2 & 3x - 8 \\ \hline -8x^2 + 4x + 7 & \\ -8x^2 + 16 & \\ \hline 20x + 7 & \end{array}$$

Vậy ta có $3x^3 - 2x^2 + 4x + 7$ chia $x^2 + 2x$ được $3x - 8$, dư $20x + 7$.

1.7. Sự chia hết. Ước và bội.

Trong phép chia $P(x)$ cho $Q(x)$, nếu dư số $R(x)$ đồng nhất bằng 0 thì ta nói rằng đa thức $P(x)$ *chia hết cho* đa thức $Q(x)$. Như vậy, $P(x)$ chia hết cho $Q(x)$ nếu tồn tại đa thức $S(x)$ sao cho $P(x) = Q(x).S(x)$. Trong trường hợp này ta cũng nói $Q(x)$ *chia hết* $P(x)$, $Q(x)$ là *ước* của $P(x)$ hoặc $P(x)$ là *bội* của $Q(x)$. Ký hiệu tương ứng là $Q(x) \mid P(x)$ và $P(x) : Q(x)$.

Cho $P(x)$ và $Q(x)$ là các đa thức khác 0. *Ước chung lớn nhất* của $P(x)$ và $Q(x)$ là đa thức $D(x)$ thoả mãn đồng thời các điều kiện sau:

- i) $D(x)$ là đa thức đơn khởi, tức là có hệ số cao nhất bằng 1
- ii) $D(x)$ là ước chung của $P(x)$ và $Q(x)$, tức là $D(x) \mid P(x)$ và $D(x) \mid Q(x)$
- iii) Nếu $D'(x)$ cũng là ước chung của $P(x)$ và $Q(x)$ thì $D(x)$ cũng là ước của $D'(x)$.

Tương tự, ta có khái niệm bội chung nhỏ nhất của hai đa thức.

Cho $P(x)$ và $Q(x)$ là các đa thức khác 0. *Bội chung lớn nhất* của $P(x)$ và $Q(x)$ là đa thức $M(x)$ thỏa mãn đồng thời các điều kiện sau:

- iv) $M(x)$ là đa thức đơn khởi, tức là có hệ số cao nhất bằng 1
- v) $M(x)$ là bội chung của $P(x)$ và $Q(x)$, tức là $P(x) \mid M(x)$ và $Q(x) \mid M(x)$
- vi) Nếu $M'(x)$ cũng là bội chung của $P(x)$ và $Q(x)$ thì $M'(x)$ cũng là bội của $M(x)$.

Ký hiệu UCLN và BCNN của hai đa thức $P(x)$, $Q(x)$ là $\text{GCD}(P(x), Q(x))$, $\text{LCM}(P(x), Q(x))$ hay đơn giản hơn là $(P(x), Q(x))$, $[P(x), Q(x)]$.

Hai đa thức $P(x)$, $Q(x)$ được gọi là nguyên tố cùng nhau nếu $(P(x), Q(x)) = 1$.

1.8. Thuật toán Euclide

Để tìm ước chung lớn nhất của hai đa thức $P(x)$, $Q(x)$, ta sử dụng thuật toán Euclide sau đây:

Định lý 3. Giả sử có hai đa thức $P(x)$, $Q(x)$, trong đó $\deg(P) \geq \deg(Q)$. Thực hiện phép chia $P(x)$ cho $Q(x)$ được thương số là $S(x)$ và dư số là $R(x)$. Khi đó

Nếu $R(x) = 0$ thì $(P(x), Q(x)) = q^{*-1}Q(x)$, trong đó q^* là hệ số cao nhất của đa thức $Q(x)$

Nếu $R(x) \neq 0$ thì $(P(x), Q(x)) = (Q(x), R(x))$

Chứng minh. Nếu $R(x) = 0$ thì $P(x) = Q(x).S(x)$. Khi đó đa thức $q^{*-1}Q(x)$ rõ ràng thỏa mãn tất cả các điều kiện của UCLN.

Nếu $R(x) \neq 0$, đặt $D(x) = (P(x), Q(x))$, $D'(x) = (Q(x), R(x))$. Ta có $D(x) \mid P(x) - Q(x).S(x) = R(x)$, suy ra $D(x)$ là ước chung của $Q(x)$, $R(x)$, theo định nghĩa của $D'(x)$, ta có $D'(x)$ là ước của $D(x)$. Mặt khác $D'(x) \mid Q(x)S(x) + R(x) = P(x)$, suy ra $D'(x)$ là ước chung của $P(x)$, $Q(x)$, theo định nghĩa của $D(x)$, ta có $D(x)$ là ước của $D'(x)$. Từ đây, do D và D' đều là các đa thức đơn khởi, ta suy ra $D = D'$.

Định lý trên giải thích cho thuật toán Euclide để tìm UCLN của hai đa thức theo như ví dụ dưới đây:

Ví dụ: Tìm ước chung lớn nhất của hai đa thức $x^5 - 5x + 4$ và $x^3 - 3x^2 + 2$.

Ta lần lượt thực hiện các phép chia

$$x^5 - 5x + 4 \text{ cho } x^3 - 3x^2 + 2 \text{ được } x^2 + 3x + 9 \text{ dư } 25x^2 - 11x - 14$$

$$x^3 - 3x^2 + 2 \text{ cho } 25x^2 - 11x - 14 \text{ được } (25x - 64)/625, \text{ dư } (354/625)(x-1)$$

$$25x^2 - 11x - 14 \text{ cho } x-1 \text{ được } 25x + 14 \text{ dư } 0$$

Vậy $(x^5 - 5x + 4, x^3 - 3x^2 + 2) = x - 1$.

Lưu ý, trong quá trình thực hiện, ta có thể nhân các đa thức với các hằng số khác 0. Ví dụ trong phép chia cuối cùng, thay vì chia $25x^2 - 11x - 14$ cho $(354/625)(x-1)$ ta đã chia cho $x-1$.

1.9. Tính chất của phép chia hết

Nhắc lại, hai đa thức $P(x)$, $Q(x)$ được gọi là nguyên tố cùng nhau nếu $(P(x), Q(x)) = 1$. Ta có định lý thú vị và có nhiều ứng dụng sau về các đa thức nguyên tố cùng nhau:

Định lý 4. (Bezout) Hai đa thức $P(x)$ và $Q(x)$ nguyên tố cùng nhau khi và chỉ khi tồn tại các đa thức $U(x)$, $V(x)$ sao cho $P(x).U(x) + Q(x).V(x) = 1$.

Chứng minh. Giả sử tồn tại các đa thức $U(x)$ và $V(x)$ thỏa mãn điều kiện $P(x).U(x) + Q(x).V(x) = 1$. Đặt $D(x) = (P(x), Q(x))$ thì $D(x) \mid P(x)$, $D(x) \mid Q(x)$ suy ra $D(x) \mid 1 = P(x).U(x) + Q(x).V(x)$. Suy ra $D(x) = 1$.

Ngược lại, giả sử $(P(x), Q(x)) = 1$. Ta chứng minh tồn tại các đa thức $U(x)$ và $V(x)$ sao cho $P(x).U(x) + Q(x).V(x) = 1$. Ta chứng minh bằng quy nạp theo $m = \min\{\deg(P), \deg(Q)\}$.

Nếu $m = 0$ thì điều cần chứng minh là hiển nhiên. Chẳng hạn nếu $\deg(Q) = 0$ thì $Q = q$ là hằng số và ta chỉ cần chọn $U(x) = 0$, $V(x) = q^{-1}$ thì ta được $P(x).U(x) + Q(x).V(x) = 1$.

Giả sử ta đã chứng minh định lý đúng đến m . Xét hai đa thức $P(x)$, $Q(x)$ có $\min\{\deg(P), \deg(Q)\} = m+1$. Không mất tính tổng quát, giả sử $m+1 = \deg(Q)$. Thực hiện phép chia $P(x)$ cho $Q(x)$ được thương là $S(x)$ và dư là $R(x)$. Không thể xảy ra trường hợp $R(x) = 0$ vì khi đó $1 = (P(x), Q(x)) = q^{*1}Q(x)$. Vì vậy, ta có

$$1 = (P(x), Q(x)) = (Q(x), R(x))$$

Lúc này, do $\min(\deg(Q), \deg(R)) = \deg(R) < m+1$ nên theo giả thiết quy nạp, tồn tại các đa thức $U^*(x)$, $V^*(x)$ sao cho $Q(x)V^*(x) + R(x)U^*(x) = 1$. Thay $R(x) = P(x) - Q(x).S(x)$, ta được

$$Q(x)V^*(x) + (P(x) - Q(x)S(x))U^*(x) = 1$$

Hay

$$P(x)U^*(x) + Q(x)(V^*(x) - S(x)U^*(x)) = 1$$

Đặt $U(x) = U^*(x)$, $V(x) = V^*(x) - S(x)U^*(x)$ ta được đpcm.

Tính chất của phép chia hết

i) $Q \mid P$, $Q \mid R$ suy ra $Q \mid P + R$ hay tổng quát hơn $Q \mid P.U + R.V$ với U, V là các đa thức bất kỳ.

- ii) $Q \mid P, P \mid R$ suy ra $Q \mid R$ (tính bắc cầu)
 iii) $Q \mid P, P \mid Q$ suy ra tồn tại số thực khác 0 a sao cho $Q = aP$ (ta gọi P và Q là các đa thức *đồng dạng*)
 iv) Nếu $Q_1 \mid P_1$ và $Q_2 \mid P_2$ thì $Q_1.Q_2 \mid P_1.P_2$.
 v) Nếu $Q \mid P.R$ và $(P, Q) = 1$ thì $Q \mid R$.
 vi) Nếu $Q \mid P, R \mid P$ và $(Q, R) = 1$ thì $Q.R \mid P$

Chứng minh. Các tính chất i-iv) là hiển nhiên xuất phát từ định nghĩa $Q \mid P \Leftrightarrow$ tồn tại S sao cho $P = Q.S$.

Để chứng minh các tính chất v) và vi), ta sẽ áp dụng định Bezout.

v) Từ giả thiết $Q \mid P.R$ và $(P, Q) = 1$ suy ra tồn tại S sao cho $P.R = Q.S$ và U, V sao cho $P.U + Q.V = 1$

Khi đó $R = (P.U + Q.V).R = (P.R)U + Q.V.R = Q.S.U + Q.V.R = Q.(SU + VR)$ suy ra $Q \mid R$.

vii) Từ giả thiết $Q \mid P, R \mid P$ và $(Q, R) = 1$ suy ra $P = Q.S$. Vì $P = Q.S$ chia hết cho R , mà $(Q, R) = 1$ nên theo v) suy ra S chia hết cho R , tức là $S = R.S_1$. Vậy $P = Q.S = (Q.R).S_1$ suy ra P chia hết cho $Q.R$.

1.10. Các ví dụ có lời giải

Bài toán 1. Tìm tất cả các cặp số a, b sao cho $x^4 + 4x^3 + ax^2 + bx + 1$ là bình phương của một đa thức.

Giải: Nếu $x^4 + 4x^3 + ax^2 + bx + 1$ là bình phương của một đa thức thì đa thức đó phải có bậc 2. Giả sử

$$x^4 + 4x^3 + ax^2 + bx + 1 = (Ax^2 + Bx + C)^2$$

$$\Leftrightarrow x^4 + 4x^3 + ax^2 + bx + 1 = A^2x^4 + 2ABx^3 + (2AC + B^2)x^2 + 2BCx + C^2$$

Đồng nhất hệ số hai vế, ta được

$$A^2 = 1, 2AB = 4, 2AC + B^2 = a, 2BC = b, C^2 = 1.$$

Không mất tính tổng quát, có thể giả sử $A = 1$, suy ra $B = 2$. C có thể bằng 1 hoặc -1. Nếu $C = 1$ thì $a = 6, b = 4$. Nếu $C = -1$ thì $a = 2, b = -4$.

Vậy có hai cặp số (a, b) thoả mãn yêu cầu bài toán là $(6, 4)$ và $(2, -4)$.

Bài toán 2. Cho đa thức $P(x)$ và hai số a, b phân biệt. Biết rằng $P(x)$ chia cho $x-a$ dư A , $P(x)$ chia cho $x-b$ dư B . Hãy tìm dư của phép chia $P(x)$ cho $(x-a)(x-b)$.

Giải: Giả sử $P(x) = (x-a)(x-b)Q(x) + Cx + D$. Lần lượt thay $x = a, b$, ta được

$$A = Ca + D, B = Cb + D$$

Từ đó suy ra $C = (A-B)/(a-b), D = A - (A-B)a/(a-b) = (aB - bA)/(a-b)$.

Bài toán 3. Tìm dư trong phép chia x^{100} cho $(x-1)^2$.

Giải: Giả sử $x^{100} = (x-1)^2 Q(x) + Ax + B$. Thay $x = 1$, ta được
 $1 = A + B$.

Lấy đạo hàm hai vế rồi cho $x = 1$, ta được

$$100 = A$$

Từ đó suy ra dư là $100x - 99$.

Bài toán 4. Tìm a, b, c biết rằng đa thức $P(x) = x^3 + ax^2 + bx + c$ chia hết cho $x-2$ và chia $x^2 - 1$ dư $2x$.

Giải: Từ các điều kiện đề bài suy ra $P(2) = 0$, $P(1) = 2$ và $P(-1) = -2$, tức là

$$8 + 4a + 2b + c = 0$$

$$1 + a + b + c = 2$$

$$-1 + a - b + c = -2$$

Từ đó suy ra $b = 1$, $a = -10/3$, $c = 10/3$. Từ đó $P(x) = x^3 - (10/3)x^2 + x + 10/3$.

Bài toán 5. Chứng minh rằng với mọi giá trị của n , đa thức $(x+1)^{2n+1} + x^{n+2}$ chia hết cho đa thức $x^2 + x + 1$.

Giải:

Cách 1. (Quy nạp theo n) Với $n = 0$, điều phải chứng minh là hiển nhiên. Giả sử ta đã có $(x+1)^{2n+1} + x^{n+2}$ chia hết cho $x^2 + x + 1$. Khi đó

$$\begin{aligned}(x+1)^{2n+3} + x^{n+3} &= (x^2 + 2x + 1)(x+1)^{2n+1} + x^{n+3} \\ &\equiv x(x+1)^{2n+1} + x^{n+3} = x((x+1)^{2n+1} + x^{n+2}) \equiv 0 \pmod{x^2 + x + 1}\end{aligned}$$

Cách 2. (Dùng số phức) Đa thức $x^2 + x + 1$ có hai nghiệm là $\alpha = \frac{-1 \pm i\sqrt{3}}{2}$. Để

chứng minh $P(x)$ chia hết cho $x^2 + x + 1$ ta chỉ cần chứng minh $P(\alpha) = 0$. Điều này tương đương với việc chứng minh

$$\left(\frac{1+i\sqrt{3}}{2}\right)^{2n+1} + \left(\frac{-1+i\sqrt{3}}{2}\right)^{n+2} = 0.$$

Chuyển các số phức sang dạng lượng giác rồi dùng công thức Moivre, ta có điều này tương đương với

$$\cos\left(\frac{(2n+1)\pi}{3}\right) + i\sin\left(\frac{(2n+1)\pi}{3}\right) + \cos\left(\frac{(n+2)2\pi}{3}\right) + i\sin\left(\frac{(n+2)2\pi}{3}\right) = 0.$$

Điều này đúng vì $(2n+1)\pi/3 - (n+2)2\pi/3 = \pi$.

Bài toán 6. Tìm tất cả các giá trị n sao cho $x^{2n} + x^n + 1$ chia hết cho $x^2 + x + 1$.

Giải:

Cách 1: Ta nhận thấy $x^3 \equiv 1 \pmod{x^2 + x + 1}$. Do đó

$$x^{2(n+3)} + x^{n+3} + 1 \equiv x^{2n} + x^n + 1 \pmod{x^2 + x + 1}$$

Do đó ta chỉ cần xét với $n = 0, 1, 2$. Rõ ràng

Với $n = 0, 3$ không chia hết cho $x^2 + x + 1$

Với $n = 1, x^2 + x + 1$ chia hết cho $x^2 + x + 1$

Với $n = 2, x^4 + x^2 + 1 \equiv x + x^2 + 1$ chia hết cho $x^2 + x + 1$

Từ đó suy ra $x^{2n} + x^n + 1$ chia hết cho $x^2 + x + 1$ khi và chỉ khi n có dạng $3k+1$ hoặc $3k+2$.

Cách 2: (Số phức) Tương tự như bài 5, ta có $P(x) = x^{2n} + x^n + 1$ chia hết cho $x^2 + x + 1$ khi và chỉ khi $P(\alpha) = 0$. Áp dụng công thức Moivre, ta có điều này tương đương với

$$\cos\left(\frac{4n\pi}{3}\right) + i \sin\left(\frac{4n\pi}{3}\right) + \cos\left(\frac{2n\pi}{3}\right) + i \sin\left(\frac{2n\pi}{3}\right) + 1 = 0$$

Điều này xảy ra khi n không chia hết cho 3.

Bài toán 7. Chứng minh rằng $(x^m - 1, x^n - 1) = x^{(m,n)} - 1$.

Giải: Giả sử $d = (m, n)$ thì rõ ràng $x^m - 1 = (x^d)^{m'} - 1$ chia hết cho $x^d - 1$ và tương tự $x^n - 1$ chia hết cho $x^d - 1$. Suy ra $x^d - 1$ là ước chung của $x^m - 1, x^n - 1$. Giả sử $D(x)$ là một ước chung của $x^m - 1, x^n - 1$. Vì $d = (m, n)$ nên tồn tại các số nguyên dương u, v sao cho $d = mu - nv$. Khi đó $D(x)$ là ước của $(x^{mu} - 1) - (x^{nv} - 1) = x^{nv}(x^d - 1)$. Vì $(x^m - 1, x^{nv}) = 1$ nên $(D(x), x^{nv}) = 1$, suy ra $D(x)$ là ước của $x^d - 1$, suy ra $x^d - 1$ là ước chung lớn nhất của $x^m - 1$ và $x^n - 1$.

1.11. Bài tập

1. Chứng minh rằng mọi đa thức đơn khởi bậc $2n$ đều có thể viết dưới dạng $q^2 + r$ với q, r là các đa thức và $\deg(r) < n$.

2. Tìm dư trong phép chia $x^{100} - 2x^{51} + 1$ cho $x^2 - 1$.

3. Tìm a, b sao cho $(x-1)^2 \mid ax^4 + bx^3 + 1$.

4. Cho $P(x)$ là đa thức với hệ số nguyên. Chứng minh rằng không tồn tại các số nguyên phân biệt a, b, c sao cho $P(a) = b, P(b) = c, P(c) = a$.

5. Cho $P(x)$ là đa thức với hệ số nguyên. Biết rằng $P(2)$ chia hết cho 5 và $P(5)$ chia hết cho 2. Chứng minh rằng $P(7)$ chia hết cho 10.

6. (Rumani 1962) Cho α là số thực thoả mãn điều kiện $\sin(\alpha) \neq 0$. Chứng minh rằng với mọi giá trị $n \geq 2$, đa thức

$P(x) = x^n \sin(\alpha) - x \sin(n\alpha) + \sin(n-1)\alpha$
 chia hết cho đa thức $Q(x) = x^2 - 2x \cos(\alpha) + 1$.

7. (Mỹ 1976) Giả sử $P(x)$, $Q(x)$, $R(x)$ và $S(x)$ thỏa mãn đồng nhất thức

$$P(x^5) + xQ(x^5) + x^2R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x)$$

Chứng minh rằng đa thức $P(x)$ chia hết cho đa thức $x-1$.

8. Với những giá trị nào của n ta có

a) $x^2 + x + 1 \mid (x-1)^n - x^n - 1$

b) $x^2 + x + 1 \mid (x+1)^n + x^n + 1$