ĐỊNH LÍ THẶNG DƯ TRUNG HOA

Prime, Khối THPT Chuyên ĐHSP HN

Hà Nội July 12, 2005

Định lí thặng dư Trung Hoa được coi là một trong những viên kim cương trong số học sơ cấp. Đây có thể coi là một định lí quan trọng lí thuyết đồng dư, trong bài viết này hi vọng trao đổi cùng bạn đọc một số ứng dụng của nó trong việc giải một số bài toán phổ thông.

1 Nội dung định lí và chứng minh:

Định lí. *Định lí thặng dư Trung Hoa được phát biểu như sau: Cho $m_1, \ldots, m_n$ là n số nguyên dương đôi một nguyên tố cùng nhau và $a_1, \ldots, a_n$ là n số nguyên bất kì. Khi đó hệ phương trình đồng dư:*

$$x \equiv a_i \pmod{m_i}$$

Có nghiệm và nghiệm này là duy nhất theo mod $\prod_{i=1}^{n} m_i$

Trước hết ta hãy nhìn lại vấn đề được đặt ra, có hai vấn đề chúng ta cần quan tâm ở đây: thứ nhất là tính giải được của hệ phương trình đồng dư này, thứ hai là tính duy nhất của nghiệm.

Bây giờ ta hãy tiếp cận bài toán, đương nhiên ta chỉ cần chứng mình cho trường hợp $n = 2$, các trường hợp $n > 2$ là hệ quả của trường hợp này. Có rất nhiều cách chứng minh bài toán này, dưới đây là một trong những cách thông dụng:

Trước hết ta sẽ chứng minh bổ đề sau:
Bổ đề Berzout. Cho hai số nguyên m và n sao cho $\gcd(m, n) = 1$. Khi đó luôn tồn tại x và y sao cho $mx + ny = 1$

Chứng minh. Ta xét tập $\{1 - mx\}$, do m và n nguyên tố cùng nhau nên ta có $\{1 - mx\}$ chạy qua một hệ thặng dư đầy đủ $\mod n$. Khi đó ắt tồn tại x sao cho $n \mid 1 - mx$, ta chỉ cần xét $y = \dfrac{1 - mx}{n}$. Bổ đề $Berzout$ được chứng minh xong □

Hệ quả. *Với mọi d nguyên luôn tồn tại u và v sao cho $d = mu + nv$.*
Bây giờ quay lại bài toán của chúng ta, theo lí thuyết đồng dư, tồn tại u, v sao cho:

$$x = a_1 + m_1 u, \ x = a_2 + m_2 v$$

Do đó ta chỉ cần chọn u và v thỏa mãn $a_1 - a_2 = m_2 v - m_1 u$, điều này hiển nhiên theo bổ đề $Berzout$ ở trên. Như vậy tức là tồn tại x thỏa mãn hệ phương trình đồng dư trên. Phép chứng minh hoàn tất cho bài toán tồn tại nghiệm. Bây giờ ta sẽ chứng minh tính duy nhất của nghiệm.

Thật vậy ta hãy xét hai nghiệm x và x' của hệ phương trình đã cho, khi đó ta có

$$x \equiv x' \pmod{m_i} \quad , \forall i = 1, , n$$

Do m_i đôi một nguyên tố cùng nhau nên ta phải có $x \equiv x' \pmod{m_1...m_n}$, ta có khẳng định về tính duy nhất của nghiệm theo $mod\ m_1...m_n$. Có một số chứng minh khác cho bài toán này, tuy nhiên tác giả vẫn thích cách chứng minh này hơn vì nó vẫn có tác dụng cho định lí thặng dư Trung Hoa trong trường hợp tổng quát:
Cho $m_1, .., m_n$ là các số nguyên dương $a_1, .., a_n$ là các số nguyên khi đó hệ phương trình đồng dư:

$$x \equiv a_i \pmod{m_i}$$

có nghiệm khi và chỉ khi $\gcd(m_i, m_j) \mid a_i - a_j, \forall i \neq j$. Khi đó các bạn hãy liên hệ với định lí $Berzout$ ở trên để tự tìm lời giải cho mình coi như là bài tập để hiểu rõ hơn bản chất của vấn đề.

2 Nghiệm của phương trình đồng dư

Định lí. *Nếu ta đặt* $M = \prod_{i=1}^{n} m_i$ *và* $d_i = \dfrac{M}{m_i}$*, hãy chứng minh rằng: với* $x = \sum_{i=1}^{n} a_i (d_i)^{\varphi(m_i)}$

thì $\overline{x}$ *là nghiệm của phương trình đồng dư đã cho.*

Bây giờ ta quan tâm hơn đến việc ứng dụng của định lí Trung Hoa trong lí thuyết đồng dư.
Trước hết ta sẽ nêu lại một số khái niệm cơ bản:
Cho $P(x)$ *là một đa thức hệ số nguyên, việc giải phương trình đồng dư* $P(x) \equiv 0 \pmod{n}$ *là việc tìm tất cả các lớp* $\overline{x}$ *trong* $\mathbb{Z}_n = \{\overline{0}, \overline{1}, .., \overline{n-1}\}$ *mà thỏa mãn* $n \mid P(x)$.

Chẳng hạn xét $P(x) = x^3 - x$, khi đó phương trình đồng dư $P(x) \equiv 0 \pmod{3}$ có 3 nghiệm phân biệt là $\overline{x} = \overline{0}, \overline{1}, \overline{2}$.
Tuy nhiên phương trình đồng dư $P(x) \equiv 0 \pmod{4}$ lại chỉ có 3 nghiệm $\overline{x} = \overline{1}, \overline{x} = \overline{3}, \overline{x} = \overline{0}$.
Định lí sau đây cho phép ta chỉ cần quan tâm đến việc giải các phương trình đồng dư với $n = p^a$ với p là các số nguyên tố.

Định lí 1. Cho $n = \prod_{i=1}^{r} p_i^{a_i}$, khi đó phương trình đồng dư $P(x) \equiv 0 \pmod{n}$ có nghiệm khi và chỉ khi tất cả các phương trình đồng dư $P(x) \equiv 0 \pmod{p_i^{a_i}}$ (*) có nghiệm. Hơn nữa

nếu gọi N_i là số nghiệm của phương trình đó thì phương trình $P(x) \equiv 0 \pmod{n}$ có đúng $N_1...N_r$ nghiệm.

Chứng minh. Chiều thuận của bài toán là hiển nhiên, bởi nếu tồn tại x mà $P(x) \equiv 0 \pmod{n}$ thì hiển nhiên x sẽ thỏa mãn tất cả các phương trình đồng dư $P(x) \equiv 0 \pmod{p_i^{a_i}}$.
Ta xét chiều đảo của bài toán, nhưng trước hết ta chú ý đến một tính chất đơn giản của đa thức hệ nguyên $a - b \mid P(a) - P(b)$.
Bây giờ ta tạm gọi $\overline{x_{p_i}}$ là 1 trong các nghiệm của phương trình đồng dư (*), theo tính chất trên ta chỉ cần xét sự tồn tại của x sao cho: $x \equiv x_{p_i} \pmod{p_i^{a_i}}$
Khi đó câu trả lời là tồn tại theo định lí Trung Hoa. Với ý tưởng này câu sau thực chất là hệ quả, với mỗi 1 cách chọn nghiệm trong N_i nghiệm của các phương trình đồng dư ở trên lại cho ta 1 nghiệm duy nhất $\mod n$, và hiển nhiên các nghiệm này phân biệt theo $\mod n$, từ đó ta có chính xác $N_1 N_r$ nghiệm. Phép chứng minh của ta hoàn tất □

Như vậy như đã nói, việc nghiên cứu nghiệm của phương trình đồng dư $modn$, có thể chuyển về nghien cứu nghiệm trong trường hợp n là lũy thừa của số nguyên tố , và từ đó có thể chuyển về nghiên cứu nghiệm trong trường hợp n là số nguyên tố dựa theo kết quả sau:
Định lí 2. *Giả sử phương trình đồng dư $P(x) \equiv 0 \pmod{p}$ có k nghiệm $\overline{x_1}, .., \overline{x_k}$ đồng thời $\gcd(P'(x_i), p) = 1$ thì với mọi a nguyên dương phương trình $P(x) \equiv 0 \mod p^a$ cũng có đúng k nghiệm theo mod p^a.*
Phép chứng minh của bài toán này dựa vào hệ quả của bổ đề $Helsen$ sau, các bạn có thể tự chứng minh coi như bài tập:

Bổ đề. *Với mọi x và h luôn tồn tại $r(x, h)$ sao cho: $P(x + h) = P(x) + hP'(x) + h^2 r(x, h)$*
áp dụng bổ đề này ta có thể chứng minh được bài toán theo quy nạp. Để hiểu rõ hơn định lí (1) ta sẽ đưa ra một ví dụ minh họa

Bài toán 2.1. *Cho n là số nguyên dương lớn hơn 1, hãy tính số nghiệm của phương trình đồng dư $x(x - 1) \equiv 0 \pmod{n}$.*

Lời giải. Ta viết n dưới dạng phân tích thừa số nguyên tố $n = \prod_{i=1}^{n} a_i$. Khi đó theo định lí 1 ta sẽ quan tâm đến số nghiệm của phương trình đồng dư: $x(x - 1) \equiv 0 \pmod{p_i^{a_i}}$, chú ý rằng x và $x - 1$ nguyên tố cùng nhau nên phương trình đồng dư này chỉ có 2 nghiệm $x \equiv 0 \pmod{p_i^{a_i}}$ hoặc $x \equiv 1 \pmod{p_i^{a_i}}$, từ đó theo định lí 1 phương trình này có tất cả 2^r nghiệm, bài toán được chứng minh xong. □

Bài toán 2.2. *Cho n là số nguyên lẻ có dạng $\prod_{i=1}^{r} p_i^{a_i}$. Khi đó xét a là nguyên bất kì và nguyên tố cùng nhau với n thì phương trình đồng dư $x^2 \equiv a \pmod{n}$ có đúng $\prod_{i=1}^{r}(1+\left(\frac{a}{p_i}\right))$ trong đó $\left(\frac{a}{p_i}\right)$ là kí hiệu Legendre.*

Lời giải. Theo tư tưởng trên ta chỉ cần quan tâm đến việc xét bài toán khi $n = p^a$, ta sẽ chứng minh rằng với mọi k phương trình $x^2 \equiv a \mod p^k$ có đúng $1 + \left(\frac{a}{p}\right)$ nghiệm.
Với $k = 1$ thì kết của của bài toán là hiển nhiên, nếu a là số chính phương $\mod p$ thì phương trình đã cho có đúng 2 nghiệm, nếu a là phi thặng dư chính phương $\mod p$ thì hiển nhiên phương trình vô nghiệm. Vậy ta có kết quả bài toán.
Bây giờ ta hãy xét khi $k > 1$, hiển nhiên ta chỉ cần quan tâm khi mà a là số chính phương $\mod p$. Khi đó gọi x_o là nghiệm của phương trình $P(x) \equiv 0 \pmod{p}$ với $P(x) = x^2 - a$ thì ta có $P(x_o) = 2x_o$, sẽ nguyên tố cùng nhau với p khi p lẻ. Theo định lí (2) ta có kết quả bài toán cho trường hợp $k > 1$. Phép chứng minh của ta hoàn tất. □

Nhận xét. Đương nhiên bài toán này vẫn có thể giải được cho trường hợp n tổng quát, tuy nhiên phép chứng minh này khá dài vì phải chia 1 số trường hợp về lũy thừa của 2, phần này xin dành cho bạn đọc coi như là một bài tìm hiểu nhỏ. Cuối cùng để hiểu hơn ví dụ 1 và ví dụ các bạn hãy thử sức vận dụng để giải bài toán sau đây:

Ví dụ 2.1. *Ta xét $S = \{k \in Z_n | k^2 \equiv 1 \pmod{n}\}$. Hãy tính $\prod_{k\in S} k$ theo $\mod n$.*

Ví dụ 2.2. ***(Tổng quát của định lí Willson)*** *Xét $T = \{k \in Z_n | \gcd(k, n) = 1\}$, hãy tính $\prod_{k\in T} k$ theo $\mod n$.*

Có một gợi ý nhỏ cho hai bài toán này để các bạn tiện theo dõi:
Đầu tiên để ý rằng nếu k thuộc S thì $n - k$ cũng thuộc S, ta có thể phân S thành các cặp số $(k, n - k)$ và chú ý rằng tích các phần từ này đồng dư $-1 \mod n$ do $k^2 \equiv 1 \pmod{n}$, do vậy $\prod_{k\in S} k \pmod{n} = (-1)^{\frac{|S|}{2}}$ chúng ta quay lại ví dụ 1. Tương tự trong T ta cũng chia thành các cặp "nghịch đảo" tuy nhiên cần lưu ý một số phần từ mà nghịch đảo $mod n$ của nó là chính nó, hay chính là thỏa mãn phương trình $k^2 \equiv 1 \pmod{n}$ và chúng ta phải quay lại xét tương tự ví dụ 1 với 1 chút rắc rối hơn. Ta tiếp tục với một ví dụ khá điển hình cho ứng dụng của định lí Trung Hoa:

Bài toán 2.3. *Cho $S = \{p_1, , p_r\}$ là tập r số nguyên tố phân biệt, và P là đa thức hệ số nguyên*

sao cho với mọi n đều tồn tại p_i trong S sao cho $p_i \mid P(n)$. Chứng minh rằng tồn tại i sao cho $p_i \mid P(n), \forall n \in N$.

Lời giải. Ta phản chứng điều ngược lại, tức là với mỗi p_i trong S tồn tại a_i sao cho $p \nmid P(a_i)$, khi đó bằng phép xét x thỏa mãn hệ đồng dư $x \equiv a_i \pmod{p_i}$
Theo định lí Trung Hoa luôn tồn tại x thỏa mãn bài toán, ta suy ra $P(x)$ không có ước nguyên tố trong S và từ đó ta có sự vô lí nghĩa là phải tồn tại p_i thỏa mãn bài toán, đó là điều cần chứng minh. □

Bài toán tổng quát sau đây vẫn đúng nếu ta thay S bằng một tập số nguyên dương bất kì, ý tưởng của bài toán hoàn toàn giống lời giải ơ trên nhưng có cần đôi chút kĩ thuật khéo léo, xin được tiếp tục dành lời giải cho bạn đọc.

Bài toán 2.4 (Đây là một ví dụ khá điển hình cho định lí Trung Hoa)**.** *Chứng minh rằng với mọi số nguyên n ta có thể chọn n số nguyên liên tiếp sao cho tất cả các số đó đều là hợp số.*

Lời giải. Gợi ý: Xét $p_1, .., p_n$ là các số nguyên tố phân biệt sau đó xét hệ đồng dư $x \equiv -k \pmod{p_k^2}$. □

Bài toán 2.5. *Chứng minh rằng với mọi n luôn tồn tại một tập S mà $|S| = n$ sao cho với mỗi tập con T khác rỗng của S thì $\sum_{x \in T} x$ không là luỹ thừa của một số nguyên.*

Lời giải. Với những dạng toán như vậy ta quan tâm nhiều đến số mũ của các thừa số nguyên tố, ta biết rằng một số sẽ là luỹ thừa của một số nguyên nếu như $\gcd(v_{p_i}(n)) > 1$ với p_i là tập các ước nguyên tố của n. Do vậy một mẹo để giải quyết bài toán là tìm cách xác lập một số ước nguyên tố của n mà số mũ của nó trong khai triển của n bằng 1. Điều này gợi ý cho ta bổ đề sau:
Cho $a_1, ..., a_n$ là các số nguyên phân biệt. Khi đó luôn tồn tại x sao cho $x + a_i$ không là số lũy thừa với mọi $i = 1, .., n$. Để chứng minh bổ đề này ta chỉ cần chọn ra n số nguyên tố phân biệt $p_n > ... > p_2 > p_1 > max\{a_1, \ldots, a_n\}$ và xét hệ phương trình đồng dư: $x \equiv p_i - a_i \pmod{p_i^2}$. Khi đó ta có với mọi i từ $1, \ldots, n$ thì $v_{p_i}(x + a_i) = 1$ và ta có kết quả bài toán.
Quay lại ví dụ ta đang xét, bài toán là hệ quả của bổ đề trên thông qua phép quy nạp. Đầu tiên ta dựng cho n. Sau đó chọn số x theo thuật toán trên, bổ sung x vào tập đó ta được tập $n + 1$ phần tử. Và do đó kết thúc bài toán. □

Bài toán 2.6 (Thi vô địch toán Đài Loan)**.** *Ta định nghĩa một hình vuông có 4 đỉnh là các điểm nguyên, đồng thời đoạn thẳng nối tâm O với tất cả các điểm nguyên trên biên và trong hình vuông đó chứa ít nhất một điêm nguyên khác hai đầu mút. Chứng minh rằng với mọi số nguyên dương n, tồn tại một hình vuông tốt dạng $n * n$.*

Lời giải. Bài toán nêu ra vấn đề về đoạn thẳng chứa điểm nguyên, vì vậy buộc ta phải tìm hiểu về tính chất của hai điểm nguyên trên mặt phẳng toạ độ, điều kiện để đoạn thẳng đó chứa điểm nguyên khác hai đầu mút.

Bổ đề 1. *Cho hai điểm $A(a,b)$ và $B(c,d)$ nguyên trên mặt phẳng toạ độ, khi đó đoạn AB chứa ít nhất 1 điểm nguyên khác A và B khi và chỉ khi* $\gcd(a-c, b-d) > 1$.

Phép chứng minh của bổ đề này khá đơn giản với công cụ vector.
Quay lại bài toán ta đang xét, ta gọi đỉnh gần O nhất là (x,y). Khi đó toạ độ các điểm nguyên của hình vuông sẽ là $(x+i, y+j)$ với $i,,j = 0,...,n$. Khi đó ta cần tìm điều kiện để cho với mọi cặp $(i,,j)$ với $i,j \in \{0,...,n\}$ ta luôn có $\gcd(x+i, y+j) > 1$. Điều này gợi ý cho ta sử dụng định lí Trung Hoa để xây dựng điều kiện cho bài toán. Với mỗi cặp (i,j) ta xác định một số nguyên tố p_{ij} sao cho các số p_{ij} phân biệt. Từ đó ta chỉ cần xét x, y thoả mãn hệ:

$$\begin{cases} x \equiv -i \pmod{p_{ij}} \\ y \equiv -j \pmod{p_{ij}} \end{cases}$$

Theo định lí Trung Hoa hệ này có nghiệm x, y, tức là tồn tại một hình vuông $n * n$ thoả mãn bài toán. Bài toán được chứng minh xong. □

Bài toán 2.7. *Cho $f_1, ..., f_n$ là n đa thức khác 0, khi đó chứng minh rằng tồn tại đa thức P hệ nguyên sao cho với mọi $i = 1,..,n$ ta luôn có $P + f_n$ là đa thức bất khả quy.*

Lời giải. Gợi ý: Hãy sử dụng tiêu chuẩn Eistein: Nếu $P(x) = a_n.x^n + ... + a_1x + a_0$ là đa thức hệ số nguyên thoả mãn, tồn tại một số nguyên tố p sao cho:
i) $p \mid a_i, \forall i = 2,...,n$ và $p \nmid a_1$
ii)$p^2 \nmid a_0$
thì $P(x)$ là đa thức bất khả quy. Từ đó xây dựng một đa thức thoả mãn hệ đồng dư phù hợp với hai điều kiện i và ii. □

3 Bài tập

Bài tập 1 (VMO 2009). *Cho $m = 2007^{2008}$, hỏi có tất cả bao nhiêu số tự nhiên $n < m$ sao cho $m|n(2n+1)(5n+2)$*

Bài tập 2 (Bulgaria TST 2003). *Ta gọi một tập C là tốt nếu với mọi k thì tồn tại a, b khác nhau trong C sao cho $\gcd(a+k, b+k) > 1$. Giả sử ta có một tập tốt mà tổng các phần tử trong đó bằng 2003. Chứng minh rằng ta có thể loại đi một phần tử c trong C sao cho tập còn lại vẫn là tập tốt.*

Bài tập 3. *Chứng minh rằng hai khẳng định sau là tương đương:*
1. n không là bội của 4
2. Tồn tại x và y sao cho $p \mid x^2 + y^2 + 1$

Bài tập 4. *Chứng minh rằng phương trình $x^2 - 34y^2 = -1$ không có nghiệm nguyên nhưng với mọi n luôn tồn tại cặp x, y sao cho $n \mid x^2 + 34y^2 + 1$.*

Bài tập 5. *Cho $P(x)$ là đa thức hệ số nguyên, khác hằng. Khi đó với mọi số nguyên M đều tồn tại x sao cho $P(x)$ có ít nhất m số nguyên tố phân biệt.*

Bài tập 6 (Moldova TST 2009). *1. Chứng minh rằng tập các số nguyên có thể phân hoạch thành các cấp số cộng với công sai khác nhau.*
2. Chứng minh rằng tập hợp các số nguyên không thể viết dưới dạng hợp của các cấp số cộng với công sai đôi một nguyên tố cùng nhau.

Bài tập 7 (USA -TST 2009). *Chứng minh rằng tồn tại dãy $\{k_i\}$ tăng thực sự sao cho với mọi n thì $k_1...k_n - 1$ là tích của hai số nguyên liên tiếp.*

Bài tập 8. *Cho S là tập hữu hạn các số nguyên dương, chứng minh rằng tồn tại x sao cho với mọi t thuộc S thì ta có $s.t$ là số lũy thừa.*

Bài tập 9. *Chứng minh rằng với mọi số nguyên n thì tồn tại n số liên tiếp sao cho mỗi sô trong chúng không biểu diễn được dưới dạng tổng hai số chính phương.*
Chú ý: Một số biểu diễn được dưới dạng tổng hai số chính phương khi và chỉ khi $v_p(n)$ chẵn với mọi $p \equiv 3 \pmod 4$