Định lý Chevalley – Warning

Trương Phước Nhân , 31/07/2017

Phát biểu bài toán :

Bài toán 1: (Chevalley – Warning)

Nếu $P_1, P_2, ..., P_k \in \mathbb{Z}_p[x_1, x_2, ..., x_n]$, trong đó p là một số nguyên tố, sao cho $\sum_{i=1}^{k} \deg P_i < n$ thì số các vector $x = (x_1, x_2, ..., x_k) \in \mathbb{Z}_p^n$ sao cho $P_i(x) = 0$ với mọi $1, 2, ..., k$ là một bội số của p .

Chứng minh : Gọi N là số các vector $x = (x_1, x_2, ..., x_k)$ thỏa mãn yêu cầu bài toán thì

$$N \equiv \sum_{x=(x_1,x_2,...,x_k)\in\mathbb{Z}_p^n} \left(1-P_1(x)^{p-1}\right)\left(1-P_2(x)^{p-1}\right)...\left(1-P_k(x)^{p-1}\right) \pmod p$$

(Lưu ý : sử dụng định lý Fermat ta luôn có $a^{p-1} \equiv 1 \pmod p$ với mọi $a \not\equiv 0 \pmod p$ nên số hạng $\left(1-f_1(x)^{p-1}\right)\left(1-f_2(x)^{p-1}\right)...\left(1-f_k(x)^{p-1}\right) \equiv 1 \pmod p$ nếu $f_i(x) = 0$ với mọi $1, 2, ..., k$ và $\equiv 0 \pmod p$ trong trường hợp ngược lại)

Đặt $P(x) = \left(1-f_1(x)^{p-1}\right)\left(1-f_2(x)^{p-1}\right)...\left(1-f_k(x)^{p-1}\right)$. Khi đó $N \equiv \sum_{x=(x_1,x_2,...,x_k)\in\mathbb{Z}_p^n} P(x) \pmod p$ (*).

Khai triển đa thức $P(x)$ ta được một tổ hợp tuyến tính của các đơn thức có dạng $x_1^{t_1}x_2^{t_2}...x_n^{t_n}$. Không làm mất tính tổng quát ta chỉ cần chứng minh hệ thức (*) cho trường hợp $P(x) = x_1^{t_1}x_2^{t_2}...x_n^{t_n}$ với $x = (x_1, x_2, ..., x_n)$

Hiển nhiên $\sum_{x=(x_1,x_2,...,x_k)\in\mathbb{Z}_p^n} x_1^{t_1}x_2^{t_2}...x_n^{t_n} = \prod_{j=1}^{n}\left(\sum_{x_j\in\mathbb{Z}_p} x_j^{a_j}\right)$. (**)

Sử dụng điều kiện từ đầu bài ta suy ra $t_1 + t_2 + ... + t_n \le (p-1)\sum_{i=1}^{k}\deg P_i < (p-1)n$. Do đó ta tìm được một chỉ số i sao cho $t_i < p-1$. Theo một kết quả về đại số thì tập $\mathbb{Z}_p \setminus \{0\}$ là một nhóm cyclic nên tồn tại một số w sao cho $\mathbb{Z}_p \setminus \{0\} = \{1, w, w^2, ..., w^{p-2}\}$ nên $\sum_{x_i\in\mathbb{Z}_p} x_i^{t_i} = \sum_{j=0}^{p-2}(w^{t_i})^j = \frac{(w^{t_i})^{p-1}-1}{w^{t_i}-1} = 0$ (sử dụng định lý Fermat).

Từ điều này kếp hợp với hệ thức (**) ta suy ra điều phải chứng minh. Kết thúc chứng minh của bài toán.

Bài toán 2: (Chevalley)

Giả sử $P_1, P_2, ..., P_k \in \mathbb{Z}_p[x_1, x_2, ..., x_n]$ thỏa mãn $\sum_{i=1}^{k}\deg P_i < n$. Nếu các đa thức $P_1, P_2, ..., P_k$ có một nghiệm chung $x = (x_1, x_2, ..., x_n) \in \mathbb{Z}_p^n$ thì chúng còn có một nghiệm chung khác.

Chứng minh thứ 1: Dễ dàng nhận thấy từ bài toán 1 (định lý Chevalley – Warning) do số các nghiệm chung của các đa thức $P_1, P_2, ..., P_k$ là bội của p và chúng có ít nhất một nghiệm nên số các nghiệm chung phải lớn hơn hoặc bằng 2 và do đó phải tồn tại một nghiệm chung khác.

Chứng minh thứ 2: Giả sử các đa thức $P_1, P_2, ..., P_k$ chỉ có duy nhất một nghiệm chung $(s_1, s_2, ..., s_n)$.

Xét đa thức : $P(x_1, x_2, ..., x_n) = \prod_{i=1}^{m}\left(1-P_i(x_1, x_2, ..., x_n)^{p-1}\right) - c\prod_{j=1}^{n}\prod_{a\in\mathbb{Z}_p\setminus\{s_j\}}(x_j - a)$, trong đó c được chọn sao cho $P(s_1, s_2, ..., s_n) = 0$. Hiển nhiên $c \ne 0$ (nếu ngược lại ta suy ra $P(s_1, s_2, ..., s_n) = 1$, mâu thuẫn với cách chọn c) . Ta sẽ chứng minh $P(x_1, x_2, ..., x_n) = 0$ với mọi $(x_1, x_2, ..., x_n) \in \mathbb{Z}_p^n$. (*)

Thật vậy, nếu $(x_1, x_2, ..., x_n) = (s_1, s_2, ..., s_n)$ thì hệ thức (*) hiển nhiên đúng theo cách chọn c được thỏa mãn, trong trường hợp ngược lại phải tồn tại một đa thức P_i sao cho $P_i(x_1, x_2, ..., x_n) = 0$ (nếu không thì $(x_1, x_2, ..., x_n)$ là một nghiệm chung khác).

Khi đó : $P(x_1, x_2, ..., x_n) = \prod_{i=1}^{m}\left(1-P_i(x_1, x_2, ..., x_n)^{p-1}\right) - c\prod_{j=1}^{n}\prod_{a\in\mathbb{Z}_p\setminus\{s_j\}}(x_j - a) = 0$

(Lưu ý : $1-P_i\left(x_1,x_2,...,x_n\right)^{p-1}=0$ và $\left(x_1,x_2,...,x_n\right)\neq\left(s_1,s_2,...,s_n\right)$ nên $\prod_{j=1}^{n}\prod_{a\in\mathbb{Z}_p\setminus\{s_j\}}\left(x_j-a\right)=0$)

Mặt khác, dễ dàng nhận thấy đa thức $\prod_{i=1}^{m}\left(1-P_i\left(x_1,x_2,...,x_n\right)^{p-1}\right)$ có bậc $\left(p-1\right)\sum_{i=1}^{k}\deg P_i<n\left(p-1\right)$, đa thức $c\prod_{j=1}^{n}\prod_{a\in\mathbb{Z}_p\setminus\{s_j\}}\left(x_j-a\right)$ có bậc $n\left(p-1\right)$ nên đa thức P có bậc $n\left(p-1\right)$. Đồng thời hệ số của số đơn thức $x_1^{p-1}x_2^{p-1}...x_n^{p-1}$ bằng c .

Áp dụng định lý Combinatorial Nullstellensatz (xem thêm về bài viết **"Định lý không điểm tổ hợp"**) trong đó $S_1=S_2=...=S_n=\mathbb{Z}_p$ ta tìm được một bộ $\left(\overline{x_1},\overline{x_2},...,\overline{x_n}\right)\in\mathbb{Z}_p^n$ sao cho $P\left(\overline{x_1},\overline{x_2},...,\overline{x_n}\right)\neq 0$.

Điều mâu thuẫn này kết thúc chứng minh.

Ứng dụng của định lý Chevalley – Warning :

Bài toán : (Erdos – Ginzburg – Ziv)

Cho $n\geq 1$ và $a_1,a_2,...,a_{2n-1}$ là một dãy gồm $2n-1$ số nguyên (không nhất thiết phân biệt).

Chứng minh rằng : Tồn tại một dãy con gồm n số $a_{i_1},a_{i_2},...,a_{i_n}$ sao cho $a_{i_1}+a_{i_2}+...+a_{i_n}\equiv 0\left(\mathrm{mod}\,n\right)$

(xem thêm bài **" Bổ đề Permanet và ứng dụng"** có trình bày một hướng tiếp cận khác cho định lý Erdos – Ginzburg – Ziv)

Chứng minh : Ta chỉ cần chứng minh bài toán cho trường hợp $n=p$ là một số nguyên tố. Giả sử $a_1,a_2,...,a_{2p-1}$ là $2p-1$ số nguyên modulo p. Xét các đa thức

$$P\left(x_1,x_2,...,x_{2p-1}\right)=x_1^{p-1}+x_2^{p-1}+...+x_{2p-1}^{p-1}$$

$$Q\left(x_1,x_2,...,x_{2p-1}\right)=a_1x_1^{p-1}+a_2x_2^{p-1}+...+a_{2p-1}x_{2p-1}^{p-1}$$

Nhận thấy $\deg P+\deg Q\leq 2p-2<2p-1$ và $(0,...,0)$ ($2p-1$) là một nghiệm chung của P và Q. Áp dụng định lý Chevalley – Warning , P và Q phải có một nghiệm chung không tầm thường $\left(s_1,s_2,...,s_n\right)$. Sử dụng định lý Fermat (hoặc sự kiện $\mathbb{Z}_p\setminus\{0\}$ là một nhóm nhân có bậc $p-1$) ta thu được các kết quả sau :

$$P\left(s_1,s_2,...,s_n\right)=s_1^{p-1}+s_2^{p-1}+...+s_{2p-1}^{p-1}=\left|M\right|$$

$$Q\left(s_1,s_2,...,s_n\right)=a_1s_1^{p-1}+a_2s_2^{p-1}+...+a_{2p-1}s_{2p-1}^{p-1}=\sum_{i\in M}a_i$$

trong đó $M=\{i:s_i\neq 0$ trên $\mathbb{Z}_p\}$ (lưu ý do $\left(s_1,s_2,...,s_n\right)$ không tầm thường nên $M\neq\varnothing$) và hiển nhiên $0<\left|M\right|\leq 2p-1$. Theo định nghĩa của bộ $\left(s_1,s_2,...,s_n\right)$ ta suy ra

$$\sum_{i\in M}a_i\equiv 0\ (\mathrm{mod}\ p)\ \text{ và }\ \left|M\right|\equiv 0\ (\mathrm{mod}\ p)\ \text{ hay }\ \left|M\right|=p\ \text{ (theo nhận xét trên)}$$

Từ đây suy ra điều phải chứng minh.

Tài liệu tham khảo :

[1]. Stasys Jukna , Extremal Combinatorics: with Applications in Computer Science,Second Edition.

[2]. Andrei Frimu, Marcel Teleuca, Applications of Combinatorial Nullstellensataz, Gazeta Matematica

[3]. Trương Phước Nhân, Định lý không điểm tổ hợp, 30/07/2017

[4]. Trương Phước Nhân, Bổ đề Permanet và ứng dụng, 30/07/2017