Phi hàm Euler

Trương Phước Nhân, 07/09/2017

Phi hàm Euler $\phi(n)$ được định nghĩa là số các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n, hay nói cách khác $\phi(n)=\left|\left\{k\in[n]:(k,n)=1\right\}\right|$

Kết quả 1: Nếu m,n là hai số nguyên dương nguyên tố cùng nhau thì với mọi số nguyên c tồn tại duy nhất một bộ số (a,b) thỏa mãn $c\equiv ma+nb \pmod{mn}$ với $0\le a\le n-1$ và $0\le b\le m-1$.

<u>Chứng minh :</u> Ta chỉ cần chứng minh rằng tập $\{ma+nb \mid 0\le a\le n-1, 0\le b\le m-1\}$ là một hệ thặng dư đầy đủ modulo mn.

Giả sử $ma_1+nb_1\equiv ma_2+nb_2 \pmod{mn}$ với $0\le a_1;a_2\le n-1$ và $0\le b_1;b_2\le m-1$.

$\Rightarrow ma_1+nb_1\equiv ma_2+nb_2 \pmod{n}$

Suy ra $ma_1\equiv ma_1+nb_1\equiv ma_2+nb_2\equiv ma_2 \pmod{n}$.

Do $(m,n)=1$ suy ra $a_1\equiv a_2 \pmod{n}$ nên $a_1=a_2$ (lưu ý : $0\le a_1;a_2\le n-1$).

Lập luận tương tự ta suy ra $b_1=b_2$. Từ phân tích trên ta suy ra mn số nguyên $ma+nb$ đôi một không đồng dư nhau theo modulo mn, đpcm.

Kết quả 2: $\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_n}\right)$, trong đó $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_m^{\alpha_m}$ với p_i là các số nguyên tố phân biệt và α_i nguyên dương

<u>Chứng minh thứ nhất :</u> Ta cần đến bổ đề sau trong quá trình lập luận

Bổ đề : Số các số nguyên dương nhỏ hơn hoặc bằng n là bội của d là $\left\lfloor \frac{n}{d}\right\rfloor$, trong đó $\lfloor x\rfloor$ là số nguyên lớn nhất không vượt quá x.

Chứng minh bổ đề : Dễ dàng nhận thấy các bội của d mà nhỏ hơn hoặc bằng n là $d,2d,...,\left\lfloor \frac{n}{d}\right\rfloor d$ (bởi vì theo định nghĩa của phần nguyên thì $n<\left(\left\lfloor \frac{n}{d}\right\rfloor+1\right)d$

Trở lại bài toán ban đầu, theo định lý cơ bản của số học ta suy ra $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_m^{\alpha_m}$, trong đó p_i là các số nguyên tố và α_i nguyên dương .

Đặt A_i là tập các số nguyên dương không vượt quá n và chia hết cho p_i.

Khi đó $\bigcup_{i=1}^{m}A_i$ là tập các số nguyên dương không vượt quá n không nguyên tố cùng nhau với n.

Theo định nghĩa của phi hàm Euler thì ta suy ra ngay rằng $\left|\bigcup_{i=1}^{m}A_i\right|=n-\phi(n)$.

Áp dụng nguyên lý bao hàm – loại trừ ta suy ra rằng :

$$\left|\bigcup_{i=1}^{m}A_i\right|=\sum_{i=1}^{m}|A_i|-\sum_{i<j}|A_i\cap A_j|+\sum_{i<j<k}|A_i\cap A_j\cap A_k|-...+(-1)^{m+1}|A_1\cap A_2\cap...\cap A_m|$$

Theo cách ta định nghĩa các tập A_i và dựa vào bổ đề ta suy ra :

$|A_i|=\frac{n}{p_i}$ với mọi $i=\overline{1,m}$; $|A_i\cap A_j|=\frac{n}{p_ip_j}$ $(i<j)$;... và $|A_1\cap A_2\cap...\cap A_m|=\frac{n}{p_1p_2\cdots p_m}$

Kết hợp các tính toán trên lại ta thu được :

$$n-\phi(n)=\sum_{i=1}^{m}\frac{n}{p_i}-\sum_{i<j}\frac{n}{p_ip_j}+\sum_{i<j<k}\frac{n}{p_ip_jp_k}-...+(-1)^{m+1}\frac{n}{p_1p_2\cdots p_m}$$

$$\Rightarrow\phi(n)=n-\sum_{i=1}^{m}\frac{n}{p_i}+\sum_{i<j}\frac{n}{p_ip_j}-\sum_{i<j<k}\frac{n}{p_ip_jp_k}+...+(-1)^{m}\frac{n}{p_1p_2\cdots p_m}$$

$$= n\left(1-\sum_{i=1}^{m}\frac{1}{p_i}+\sum_{i<j}\frac{1}{p_ip_j}-\sum_{i<j<k}\frac{1}{p_ip_jp_k}+\ldots+(-1)^m\frac{1}{p_1p_2\cdots p_m}\right)$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right)$$

<u>Chứng minh thứ hai :</u> Ta cần đến kết quả phụ sau trong quá trình lập luận :

Bổ đề : Nếu m,n là hai số nguyên dương nguyên tố cùng nhau thì $\phi(mn)=\phi(m)\phi(n)$

<u>Chứng minh :</u> Bằng cách áp dụng kết quả 1), ta suy ra rằng với mỗi số nguyên dương $c\in\{1,2,...,mn\}$ ta luôn xác định được duy nhất một bộ số $(a,b)\in\{0,1,...,n-1\}\times\{0,1,...,m-1\}$ sao cho $c\equiv ma+nb \pmod{mn}$.

<u>Nhận xét :</u> $(c,mn)=1$ khi và chỉ khi $(a,m)=(b,m)=1$

Thật vậy, do $(m,n)=1$ nên :

$(c,m)=(ma+nb,m)=(nb,m)=(b,m)$

và $(c,n)=(ma+nb,n)=(ma,n)=(a,n)$

Suy ra : $(c,mn)=1$ khi và chỉ khi $(c,m)=(c,n)=1$ khi và chỉ khi $(a,n)=(b,m)=1$

Do có $\phi(n)$ số $a\in\{0,1,...,n-1\}$ nguyên tố cùng nhau với n và $\phi(m)$ số $b\in\{0,1,...,m-1\}$ nguyên tố cùng nhau với m nên kết hợp với nhận xét trên ta suy ra rằng có $\phi(m)\phi(n)$ số nguyên dương nhỏ hơn mn và nguyên tố cùng nhau với mn. Theo định nghĩa của phi hàm Euler ta suy ra $\phi(mn)=\phi(m)\phi(n)$.

Trở lại với bài toán , bằng cách áp dụng bổ đề vừa chứng minh ta nhận thấy rằng nếu $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_m^{\alpha_m}$ thì $\phi(n)=\phi\left(p_2^{\alpha_2}\right)\phi\left(p_2^{\alpha_2}\right)...\phi\left(p_m^{\alpha_m}\right)$ nên vấn đề của ta là xác định giá trị của $\phi\left(p^{\alpha}\right)$ với p nguyên tố và α nguyên dương. Sử dụng bổ đề phụ trong chứng minh thứ nhất ta suy ra có $p^{\alpha-1}$ số nguyên dương không vượt quá p^{α} nên $\phi\left(p^{\alpha}\right)=p^{\alpha}-p^{\alpha-1}=p^{\alpha}\left(1-\frac{1}{p}\right)$.

Do đó ta suy ra :

$$\phi(n)=p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_n}\left(1-\frac{1}{p_2}\right)...p_n^{\alpha_n}\left(1-\frac{1}{p_n}\right)=p_1^{\alpha_1}p_2^{\alpha_2}...p_m^{\alpha_m}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_n}\right)$$

$$\Rightarrow \phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_n}\right)$$

Tài liệu tham khảo :

[1]. Bài giảng Algebraic Combinatorics của Lionel Levine , 15/02/2011

[2]. Melvyn B. Nathanson, Additive Number Theory – Inverse Problems and the Geometry of Sumsets ,First Edition.

[3]. Trương Phước Nhân, Nguyên lý bao hàm – loại trừ, 28/08/2017