Euler Phi Function

2021.02.21 10:00 KST

Euler Phi Function

$\phi(n)$: 1부터 n까지의 정수 중 n과 서로소인 것의 갯수

n의 소인수가 $p_1, p_2, \ldots, p_k$일 때

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_k})$$

Euler Phi Function

- Bezout’s identity
- 합동식
- Fermat’s little theorem
- Euler’s theorem
- Euler phi function

⚠️ 주의! 저는 수학 알못입니다

Bezout's Identity

Definition

둘 중 하나는 0이 아닌 정수 a, b에 대해 $gcd(a, b) = d$일 때, 다음이 성립한다.

- $|ax + by| = d$를 만족하는 정수 x, y가 존재
- **d는 정수 x, y에 대해 $|ax + by|$로 표현할 수 있는 가장 작은 정수**
- $|ax + by|$로 표현할 수 있는 모든 정수는 d의 배수

Bezout's Identity

0이 아닌 정수 a, b에 대해 $gcd(a, b) = d$일 때, 다음이 성립한다.

- $|ax + by| = d$를 만족하는 정수 x, y가 존재
- **d는 정수 x, y에 대해 $|ax + by|$로 표현할 수 있는 가장 작은 정수**
- $|ax + by|$로 표현할 수 있는 모든 정수는 d의 배수

Proof

$S = \{ax + by > 0 \mid x, y \in Z\}$라 하자.

이 집합은 자연수의 부분집합이고, 공집합이 아니라면 자연수의 정렬성에 의해 가장 작은 어떤 값을 원소로 가진다.

이 때 1) $y = 0$일 때 $|a| \in S$ 가 가능하고, 2) $x = 0$일 때 $|b| \in S$ 가 가능하다. 따라서 S는 공집합이 아니므로 가장 작은 값을 원소로 가지고, 그 값을 z라고 하자.

임의의 정수 k, l에 대해 $z = ak + bl$로 나타낼 수 있다. 또한 S의 임의의 원소를 w라고 했을 때, $w = au + bv$ (u, v는 정수) 로 나타낼 수 있다.

이 때 w가 z의 배수가 아니라고 가정하자. 그러면 $w = zq + r$ $(1 \leq r < z)$ 이고, 이를 r에 대해 나타내면

$r = w - zq = (au + bv) - (ak + bl)q = a(u - kq) + b(v - lq)$ 인데, $(u - kq)$ 와 $(v - lq)$ 역시 정수이고 r은 자연수이므로 $r \in S$ 이다.

그런데, r은 w를 z로 나눈 나머지이므로 z보다 작다. 하지만 z는 S에서 가장 작은 값이므로 모순이다. 따라서 w는 z의 배수이다.

이 때 w는 S의 임의의 원소이므로 S의 모든 원소는 z의 배수이다. 또한 $|a| \in S$, $|b| \in S$ 이므로 z는 a, b의 공약수이다.

$gcd(a, b) = G, a = AG, b = BG$라고 하자.

그러면 $z = ak + bl = AGk + BGl = (Ak + Bl)G$이므로 z는 $gcd(a, b)$의 배수이다.

그런데, a, b의 공약수이면서 $gcd(a, b)$의 배수이려면 $z = gcd(a, b)$여야 한다.

따라서, $z = gcd(a, b)$는 정수 x, y에 대해 $|ax + by|$로 표현할 수 있는 가장 작은 정수이다.

합동식

합동식의 성질

$a \equiv b \mod m$ (a, b, m은 정수): a를 m으로 나눈 나머지와 b를 m으로 나눈 나머지가 같음

$a \equiv b \mod m$이고 c가 정수이면, 다음 성질이 성립한다.

- $a \pm c \equiv b \pm c \mod m$
- $ac \equiv bc \mod m$
- ~~$\frac{a}{c} \equiv \frac{b}{c}$ mod m (c가 a, b의 약수일 때)~~

합동식

합동식에서의 나눗셈

‘어떤 숫자로 나누기’는 그 숫자의 역원이 존재해야 가능하다카더라
ex) 항등식에서 0이 아닌 수의 곱셈에 대한 역원은 존재하지만, 0인 경우 역원이 존재하지 않아 0으로 나눌 수 없음

이를 합동식에 적용하면,
곱셈에 대한 항등원은 임의의 정수 a, m에 대해 $a * 1 \equiv 1 * a \equiv a$ mod m 이므로 1
그러므로 $a * x \equiv x * a \equiv 1$ mod m 인 x가 존재하면 합동식의 양변을 a로 나눌 수 있다.

그런데 베주 항등식에서 $|ax + by|$로 표현 가능한 가장 작은 정수는 $gcd(a, b)$ 이므로 $gcd(a, m) = 1$이다.
따라서 a와 m이 서로소일 때 합동식의 양변을 a로 나눌 수 있다.

Fermat’s Little Theorem

Definition

소수인 p와 p의 배수가 아닌 정수 a에 대해 다음이 성립한다.

- $a^{p-1} \equiv 1 \bmod p$

ex) $a = 14,\ p = 5$일 때 $14^4 = 38416 = 7683 * 5 + 1$

Fermat’s Little Theorem

소수인 p와 p의 배수가 아닌 정수 a에 대해 다음이 성립한다.

- $a^{p-1} \equiv 1 \bmod p$

Proof

집합 $\{1,\ 2,\ ...,\ p-1\}$ 과 이 집합의 모든 원소에 a를 곱한 집합을 $\{a,\ 2a,\ ...,\ (p-1)a\}$이 있을 때,
$\{1,\ 2,\ ...,\ p-1\} \equiv \{a,\ 2a,\ ...,\ (p-1)a\} \bmod p$임을 보이려 한다.

먼저 $\{a,\ 2a,\ ...,\ (p-1)a\} \bmod p$의 원소가 모두 다름을 귀류법을 통해 보이기 위해, $i \neq j$이고 $ia \equiv ja \bmod p$인 i, j $(1 \leq i, j \leq p-1)$이 있다고 가정하면
a와 p가 서로소이므로 합동식의 양변을 a로 나누어 $i \equiv j \bmod p$로 만들 수 있다. 그런데 i, j는 p보다 작은 자연수이므로 $i \neq j$이면서 $i \equiv j \bmod p$일 수는 없다.
따라서 $\{a,\ 2a,\ ...,\ (p-1)a\} \bmod p$의 원소는 모두 다르다.
또한, $\{a,\ 2a,\ ...,\ (p-1)a\}$의 모든 원소는 p와 서로소이고 $\{a,\ 2a,\ ...,\ (p-1)a\} \bmod p$의 모든 원소는 p보다 작기 때문에
$\{a,\ 2a,\ ...,\ (p-1)a\}$와 $\{1,\ 2,\ ...,\ p-1\}$ 은 modular p에 대해 합동인 집합이다.

따라서 각 집합의 모든 원소의 곱 역시 modular p에 대해 합동이다.
이를 식으로 나타내면 $(p-1)! \equiv a^{p-1}(p-1)! \bmod p$이고, $(p-1)!$과 p는 서로소이므로 양변을 $(p-1)!$로 나누면
$a^{p-1} \equiv 1 \bmod p$

Euler's Theorem

Definition

정수 n과 n과 서로소인 정수 a에 대해 다음이 성립한다.

- $a^{\phi(n)} \equiv 1 \bmod n$

이 때 $\phi(n)$를 Euler phi function이라고 부르며, 1부터 n까지의 수 중 n과 서로소인 것의 갯수를 나타낸다.

Euler’s Theorem

정수 n과 n과 서로소인 정수 a에 대해 다음이 성립한다.

- $a^{\phi(n)} \equiv 1$ mod n

이 때 $\phi(n)$를 Euler phi function이라고 부르며, 1부터 n까지의 수 중 n과 서로소인 것의 갯수를 나타낸다.

Proof

Fermat’s little theorem과 유사하게 증명할 수 있다.
1부터 n까지의 수 중 n과 서로소인 것의 집합을 $M = \{p_1, \ldots, p_k\}$라 하고, 모든 원소에 a를 곱한 집합을 $aM = \{ap_1, \ldots, ap_k\}$라 하자.
이 때 $M \equiv aM$ mod n임을 보이려 한다.

먼저 aM의 원소가 모두 다름을 귀류법으로 보이기 위해, $i \neq j$이고 $ia \equiv ja$ mod n인 i, j $(1 \leq i, j \leq n-1)$이 있다고 가정하면
a와 n이 서로소이므로 합동식의 양변을 a로 나누어 $i \equiv j$ mod n를 만들 수 있다. 그러나 i, j는 $n-1$보다 작은 자연수이므로 모순이다.
따라서 aM의 원소는 모두 다르므로 $|M| = |aM|$이다.

다음으로 M과 aM mod n이 같은 집합임을 귀류법으로 보이기 위해, aM의 어떤 원소 ap_i와 M에 속하지 않는 자연수 p' $(1 \leq p' \leq n-1)$에 대해
$ap_i \equiv p'$ mod n인 경우가 존재한다고 가정하자. 그러면 $ap_i = nq + p'$의 형태가 될 것이다.
그런데 n과 p'는 서로소가 아니므로, 두 수의 공약수를 ρ라고 하면 $ap_i = X\rho$가 되어 ap_i와 n은 ρ를 공약수로 갖는다.
그러나 a와 p_i는 모두 n과 서로소이므로 모순이 발생한다. 그러므로 M과 aM mod n은 같은 집합이고, $M \equiv aM$ mod n이다.

그러므로 $p_1 * \ldots * p_k \equiv a^{\phi(n)} * p_1 * \ldots * p_k$ mod n이고, 양변을 n과 서로소인 $p_1 * \ldots * p_k$로 나누면
$a^{\phi(n)} \equiv 1$ mod n

Euler Phi Function

Multiplicative function

정수 n과 n과 서로소인 정수 a에 대해 다음이 성립한다.

- $a^{\phi(n)} \equiv 1 \bmod n$

이 때 $\phi(n)$를 Euler phi function이라고 부르며, 1부터 n까지의 수 중 n과 서로소인 것의 갯수를 나타낸다.
정수 m, n이 서로소일 때, 다음이 성립한다.

- $\phi(mn) = \phi(m)\phi(n)$

Euler Phi Function

$\phi(n)$를 Euler phi function이라고 부르며, 1부터 n까지의 수 중 n과 서로소인 것의 갯수를 나타낸다.

정수 m, n이 서로소일 때, 다음이 성립한다.

- $\phi(mn) = \phi(m)\phi(n)$

Proof

(엄밀한 증명인지는 잘 모르겠음)

$$\begin{bmatrix} 1 & m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & \dots & (n-1)m+2 \\ \dots & \dots & \dots & \dots \\ m & 2m & \dots & nm \end{bmatrix}$$

위 행렬에서 r번째 행은 $\begin{bmatrix} r & m+r & \dots & (n-1)m+r \end{bmatrix}$의 형태로 되어있다.

이 때, 1) m과 r이 서로소가 아니면 그 행의 모든 수도 m과 서로소가 아니고, 2) m과 r이 서로소이면 그 행의 모든 수도 m과 서로소이다.

두 번째 경우에서, 그 행의 모든 수는 modular n에 대해 서로 다르다.

이를 귀류법으로 증명하기 위해, $i \neq j$이고 $im + r \equiv jm + r \bmod n$인 자연수 i, j $(1 \leq i, j \leq n-1)$가 존재한다고 가정하자.

이 때 양변에서 r을 빼고 양변을 n과 서로소인 m으로 나누어주면 $i \equiv j \bmod n$이 되어 모순이 발생한다. 따라서 이 행의 모든 수는 modular n에 대해 서로 다르다.

그리고 각 행의 원소는 n개이므로, $\{r,\ m+r,\ \dots,\ (n-1)m+r\} \equiv \{0,\ 1,\ \dots,\ n-1\} \bmod n$이다.

따라서 이 행 안에는 n과 서로소인 수가 $\phi(n)$개 존재한다. 그런데, 이 행의 모든 수는 m과 서로소라고 하였으므로 이 $\phi(n)$개의 수는 mn과 서로소이기도 하다.

주어진 행렬에서 이러한 행의 갯수는 1부터 m까지의 자연수 중 m과 서로소인 것의 갯수이므로 $\phi(m)$개이다.

따라서 $\phi(mn) = \phi(m)\phi(n)$

Euler Phi Function

$\phi(n)$를 Euler phi function이라고 부르며, 1부터 n까지의 수 중 n과 서로소인 것의 갯수를 나타낸다.
정수 m, n이 서로소일 때, 다음이 성립한다.

- $\phi(mn) = \phi(m)\phi(n)$

임의의 소수 p에 대해 p^k 이하의 수 중 p^k와 서로소가 아닌 수는 항상 p를 인수로 가지며, 이러한 수는 총 $|\{p,\ 2p, \ldots,\ p^{k-1} * p\}| = p^{k-1}$개이다.
그러므로 $\phi(p^k) = p^k - p^{k-1}$이다.

임의의 정수 n을 소인수분해 했을 때 $p_1^{k_1} * p_2^{k_2} * \ldots * p_m^{k_m}$로 나타내어진다면,

$$\phi(n) = \phi(p_1^{k_1} * p_2^{k_2} * \ldots * p_m^{k_m})$$
$$= \phi(p_1^{k_1}) * \phi(p_2^{k_2}) * \ldots * \phi(p_m^{k_m})$$
$$= (p_1^{k_1} - p_1^{k_1-1}) * (p_2^{k_2} - p_2^{k_2-1}) * \ldots * (p_m^{k_m} - p_m^{k_m-1})$$
$$= p_1^{k_1} * p_2^{k_2} * \ldots * p_m^{k_m} * (1 - \frac{1}{p_1}) * (1 - \frac{1}{p_2}) * \ldots * (1 - \frac{1}{p_m})$$
$$= n * (1 - \frac{1}{p_1}) * (1 - \frac{1}{p_2}) * \ldots * (1 - \frac{1}{p_m})$$

따라서 $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_m})$