Eyler funksiyasi

Ta’rif

Eyler funksiyasi $\phi(n)$ (ba’zida $\varphi(n)$ yoki $phi(n)$ orqali ifodalanadi) – bu 1 dan n gacha bo’lgan sonlar oralig’ida n bilan o’zaro tub sonlar sonidir. Boshqacha qilib aytadigan bo’lsak, bu [1;n] oralig’idagi n bilan EKUBi birga teng bo’ladigan sonlar sonidir.

Funksiyaning dastlabki bir nechta qiymati:

$\phi(1) = 1$
$\phi(2) = 1$
$\phi(3) = 2$
$\phi(4) = 2$
$\phi(5) = 4$
$\phi(6) = 2$
$\phi(7) = 6$

Xususiyatlari

Eyler funksiyasining quyidagi uchta xususiyati ixtiyoriy son uchun uning qiymatini hisoblashni o’rganishga yetarli:

- Agar p tub son bo’lsa, $\phi(p) = p - 1$.
  (Ko’rinib turibdi, p ning o’zidan tashqari qolgan barcha son p bilan o’zaro tub.)
- Agar p tub va a natural son bo’lsa, $\phi(p^a) = p^a - p^{a-1}$.
  (p^a bilan o’zaro tub bo’lmaganlar faqatgina $pk(k \in N)$ ko’rinishidagi sonlardir, ya’ni ja’mi $\frac{p^a}{p} = p^{a-1}$ dona).
- Agar a va b o’zaro tub bo’lsa, $\phi(ab) = \phi(a)\phi(b)$ (Eyler funksiyasining “multiplikativlik” xususiyati)
  (Bu fakt xitoycha qoldiqlar teoremasi asosida olingan. $z \leq ab$ tasodifiy sonni ko’raylik. z ni a ga va b ga bo’lgandagi qoldiqni mos ravishda x va y deb belgilab olamiz. Shunda z soni ab bilan o’zaro tub bo’ladi qachonki z soni a bilan ham, b bilan ham alohida ravishda o’zaro tub bo’lsa, yoki, xuddi shuning o’zi, x soni a bilan o’zaro tub va y soni b bilan o’zaro tub bo’lsa. Xitoyning qoldiqlar teoremasi inobatga olinib, ixtiyoriy x va y juftlik ($x \leq a$, $y \leq b$) qaysidir bir z ni ifodalaydi, ya’ni har bir z uchun hosil bo’ladigan x va y juftlik takrorlanmas bo’ladi.)

Bu yerdan ixtiyoriy n soni uchun uning kanonik ko’rinishi (tub ko’paytuvchilari yoyilmasi) orqali Eyler funksiyasini aniqlashimiz mumkin:
agar

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

(barcha p_i lar tub) bo’lsa

$$\begin{aligned}&\phi(n) = \phi(p_1^{a_1}) \cdot \phi(p_2^{a_2}) \cdot \ldots \cdot \phi(p_k^{a_k}) = \\ &= (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \cdot \ldots \cdot (p_k^{a_k} - p_k^{a_k-1}) = \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

Dasturiy ifodalanishi

Eyler funksiyasini hisoblaydigan eng sodda kod, kanonik ko'rinishga keltirish orqali $O(\sqrt{n})$ da hisoblanadi.

```
int phi (int n) {
	int result = n;
	for (int i=2; i*i<=n; ++i)
		if (n % i == 0) {
			while (n % i == 0)
				n /= i;
			result -= result / i;
		}
	if (n > 1)
		result -= result / n;
	return result;
}
```

Eyler funksiyasini hisoblash uchun biz n sonini kanonik ko'rinishidagi tub sonlarni aniqlashimiz kerak. Kanonik ko'rinishni kanonik ko'rinishga keltirishning samarali usullari orqali $O(\sqrt{n})$ dan ham tezkor aniqlash mumkin.

Eyler funksiyasidan ilovalar

Eyler funktsiyasining eng mashhur va muhim xususiyati **Eyler teoremasi**da quyidagicha ifodalanadi:

$$a^{\phi(m)} \equiv 1 \pmod m,$$

Bu yerda a va m o'zaro tub.
m tub bo'lgan holatda Eyler teoremasi **Fermaning kichik teoremasi**ga aylanadi.

$$a^{m-1} \equiv 1 \pmod m$$

Eyler teoremasi amaliy qo'llanmalarda juda keng tarqalgan. Masalan: Modul bo'yicha teskari element.