Mårten Wadenbäck

Eulers Φ-funktion

Vi har sett att vid räkning i $\mathbb{Z}_n$ har ett element $[a] \in \mathbb{Z}_n$ en multiplikativ invers precis då $\operatorname{sgd}(a,n)=1$.

Hur många inverterbara element finns det i $\mathbb{Z}_n$?

Vi definierar Eulers Φ-funktion för att ge svar på den frågan:

$$\Phi(n) = \left|\{a \in \mathbb{Z} : \ 1 \leq a \leq n \ \wedge \ \operatorname{sgd}(a,n)=1\}\right|$$

för alla $n \in \mathbb{Z}_+$.

Vi behöver förstås kunna räkna ut funktionens värden också för att vi skall ha någon nytta av den. Om p är ett primtal är det lätt, eftersom $\operatorname{sgd}(a,p)=1$ för alla $1 \leq a \leq p-1$ och $\operatorname{sgd}(a,p)=p$ för $a=p$. Här är alltså $\Phi(p)=p-1$.

Vi kan utöka detta till följande

Sats: Låt p vara ett primtal och låt k vara ett heltal större än 1. Då är

$$\Phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Bevis: De enda talen som är större än 1 och som delar p^k är precis talen

$$p, 2p, \dots, p^{k-1}p,$$

och dessa är tydligen p^{k-1} stycken, så de resterande $p^k - p^{k-1}$ stycken talen är relativt prima med p^k.

Sats: Om $\operatorname{sgd}(m,n)=1$ så gäller det att $\Phi(mn) = \Phi(m) \cdot I(n)$.

Bevis: Låt $M(k) = \{a \in \mathbb{Z} : 1 \leq a \leq k \wedge \operatorname{sgd}(a,k)=1\}$.

Det satsen säger är då att om $\operatorname{sgd}(m,n)=1$ är $|M(mn)| = |M(m)| \cdot |M(n)|$.

Eftersom det för två mängder A och B gäller att $|A \times B| = |A| \cdot |B|$ kan vi skriva $|M(mn)| = |M(m) \times M(n)|$, och om vi kan hitta en bijektiv funktion från $M(mn)$ till $M(m) \times M(n)$ är vi alltså klara. En sådan funktion är till exempel $x \mapsto (x \bmod m, x \bmod n)$, eftersom Kinesiska restsatsen lovar oss att systemet

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

har precis en lösning $1 \leq x \leq mn$ då $sgd(m,n) = 1$.

Eftersom nu $|M(mn)| = |M(m)| \cdot |M(n)|$, och eftersom $\Phi(k) = M(k)$, blir $\Phi(mn) = \Phi(m) \cdot \Phi(n)$.

Om vi har tillgång till en primtalsfaktorisering av talet n kan vi nu beräkna $\Phi(n)$ med hjälp av de två senaste satserna.

Om $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ blir ju $\Phi(n) = \Phi(p_1^{k_1}) \cdots \Phi(p_r^{k_r})$,

och vi får då

$$\Phi(n) = p_1^{k_1-1}(p_1-1)\, p_2^{k_2-1}(p_2-1) \cdots p_r^{k_r-1}(p_r-1).$$

Exempel: Vad blir

a) $\Phi(18)$? b) $\Phi(100)$?

En formel som eventuellt är lättare att komma ihåg fås genom att bryta ut p_k ur parentes k:

$$\Phi(n) = p_1^{k_1}\left(1-\frac{1}{p_1}\right) p_2^{k_2}\left(1-\frac{1}{p_2}\right) \cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right) =$$

$$= n \cdot \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \cdots \left(1-\frac{1}{p_r}\right).$$

Sats (Eulers sats): Låt $n \geq 2$ och a vara heltal sådana att $\mathrm{sgd}(n,a)=1$. Då är $a^{\Phi(n)} \equiv 1 \mod n$.

Bevis: Låt $m = \Phi(n)$ för att förenkla beteckningarna.

Det finns m heltal $x_1, x_2, \ldots, x_m$ i $\{1, 2, \ldots, n\}$ som är relativt prima med n, och de ger upphov till de m ekvivalensklasserna $[x_1], [x_2], \ldots, [x_m]$. Då $\mathrm{sgd}(a,n)=1$ har $[a]$ en invers i $\mathbb{Z}_n$, så även $[ax_1], [ax_2], \ldots, [ax_m]$ är m olika ekvivalensklasser som har invers i $\mathbb{Z}_n$. Dessa måste alltså vara klasserna $[x_1], \ldots, [x_m]$ fast eventuellt i en annan ordning! Därför är

$$[ax_1]\cdot[ax_2]\cdots[ax_m] = [x_1]\cdot[x_2]\cdots[x_m] \Leftrightarrow$$

$$[a^m x_1 x_2 \cdots x_m] = [x_1 x_2 \cdots x_m] \Leftrightarrow$$

$$[a^m] = [1] \Leftrightarrow a^{\Phi(n)} \equiv 1 \mod n.$$

Exempel: Vi testar att beräkna $5^{\Phi(18)} \mod 18$, och får

$$5^{12} \equiv 25^6 \equiv 7^6 \equiv 49^3 \equiv (-5)^3 \equiv -125 \equiv -35 \equiv 1 \mod 5.$$

Följdsats (Fermats lilla sats): Låt p vara ett primtal. Då är $x^p \equiv x \mod p$ för alla x.

Bevis: Om $p|x$ gäller det säklart. Om $\mathrm{sgd}(x,p)=1$ kan vi multiplicera med inversen till x på båda sidor, och få $x^{p-1} \equiv 1 \mod p$.

Eftersom $\Phi(p) = p-1$ gäller detta enligt Eulers sats.

Eulers sats ligger till grunden för en krypterings- och signeringsteknik som kallas RSA.

Några önskvärda egenskaper som en krypteringsmetod skall uppfylla är

- inverterbar, dvs det skall gå (för mottagaren) att återskapa ursprungsmeddelandet
- det skall vara svårt för andra att göra det
- alla skall kunna kryptera.

RSA-systemet fungerar som följer:

1. Vi väljer två (stora) primtal p och q och beräknar $N = pq$ och $k = \Phi(pq) = (p-1)(q-1)$.
2. Vi väljer ett godtyckligt $e > 1$ sådant att $\mathrm{sgd}(e,k) = 1$, och beräknar d så att $de \equiv 1 \mod k$.

3. Vi publicerar e och N så att alla har tillgång till dem.

4. Den som vill skicka ett hemligt tal M till oss beräknar istället $C \equiv M^e \mod N$ och skickar.

5. Vi dekrypterar genom att beräkna

$$M \equiv C^d \mod N.$$

Varför fungerar detta? Eftersom $de \equiv 1 \mod \Phi(N)$ är ju $de = 1 + r\Phi(N)$. Detta innebär att

$$C^d \equiv M^{de} \equiv M^{1+r\Phi(N)} \equiv M \cdot (M^{\Phi(n)})^r \equiv M \cdot 1^r \equiv M \mod N$$

enligt Eulers sats.

Exempel: Om vi väljer $p = 17$ och $q = 23$ blir

$N = pq = (20-3)(20+3) = 400 - 9 = 391$ och

$k = (p-1)(q-1) = 16 \cdot 22 = 352.$ Eftersom $sgd(352, 25) = 1$

kan vi ta $e = 25$ som publik nyckel, och dess invers i $\mathbb{Z}_k$ som d.

Inversen bestämmer vi som vanligt med

Euklides algoritm:

$$352 = 14\cdot 25 + 2$$
$$25 = 12\cdot 2 + 1$$
$$2 = 2\cdot 1$$

så $1 = 25 - 12\cdot 2 = 25 - 12\cdot(352 - 14\cdot 25) = -12\cdot 352 + 169\cdot 25.$

Här ser vi att $d = 169$ går bra som hemlig nyckel.

Om någon vill skicka det hemliga meddelandet

$M = 16$ krypterar vederbörande detta enligt

$$C \equiv 16^{25} \equiv 16\cdot(16^3)^8 \equiv 16\cdot 4096^8 \equiv 16\cdot 186^8 \equiv$$

$$\equiv 16\cdot 188^4 \equiv 2^4\cdot 188^4 \equiv (2\cdot 188)^4 \equiv 376^4 \equiv (-15)^4 \equiv$$

$$\equiv 225^2 \equiv 186 \mod 391$$

och skickar C.

Vi tar emot C och beräknar

$$M \equiv C^d \equiv 186^{169} \equiv 186\cdot(186^2)^{84} \equiv 186\cdot 188^{84} \equiv$$

$$\equiv 186\cdot 154^{42} \equiv 186\cdot 256^{21} \equiv 186\cdot 256\cdot(256^2)^{10} \equiv$$

$$\equiv 305\cdot 239^{10} \equiv 305\cdot 35^5 \equiv 305\cdot 35\cdot 35^4 \equiv 118\cdot 52^2 \equiv$$

$$\equiv 118\cdot 358 \equiv 16 \mod 391.$$

(Räkningarna görs inte för hand!)