TILLEGG OM EULERS ϕ-FUNKSJON

La ϕ betegne Eulers ϕ-funksjon.

Lemma 1. *La p være et primtall og $r > 0$ et helt tall. Da har vi*

$$\phi(p^r) = p^r - p^{r-1} = p^r(1 - 1/p)$$

Lemma 2. *La n og m være positive hele tall og $\bar{u} \in \mathbb{Z}_m$ og $\bar{v} \in \mathbb{Z}_n$. Da har vi det følgende: $(\bar{u}, \bar{v})$ er enhet i $\mathbb{Z}_m \times \mathbb{Z}_n \Leftrightarrow \bar{u}$ er enhet i $\mathbb{Z}_m$ og $\bar{v}$ er enhet i $\mathbb{Z}_n$.*

Setning 3. *La $m, n > 1$ være hele tall, og anta $\gcd(m, n) = 1$. Da har vi $\phi(mn) = \phi(m)\phi(n)$.*

Proof. Vi har $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$. Antall enheter i $\mathbb{Z}_m$ er $\phi(m)$, og antall enheter i $\mathbb{Z}_n$ er $\phi(n)$. Altså har vi fra Lemma 2 at $\mathbb{Z}_m \times \mathbb{Z}_n$ har $\phi(m)\phi(n)$ enheter. Da $\mathbb{Z}_{mn}$ har $\phi(mn)$ enheter, får vi $\phi(mn) = \phi(m)\phi(n)$. $\square$

Setning 4. *La $n > 1$ i $\mathbb{Z}$, og anta at n er kvadratfritt, dvs. $n = p_1 \cdots p_t$, der $p_1, \ldots, p_t$ er forskjellige primtall. La $a \in \mathbb{Z}$. Da har vi at $a^{\phi(n)+1} \equiv a (\bmod n)$.*

Proof. Det er klart hvis $a = 0$, derfor antar vi at $a \neq 0$. La $d = \gcd(a, n)$. Da er $\gcd(d, n/d) = 1$ og $\gcd(a, n/d) = 1$. Vi har $\phi(n) = \phi(d)\phi(n/d)$ fra Setning 3. Fra Eulers theorem har vi $a^{\phi(n/d)} \equiv 1 (\bmod n/d)$. Så $a^{\phi(n)} \equiv (a^{\phi(n/d)})^{\phi(d)} \equiv 1^{\phi(d)} \equiv 1 (\bmod n/d)$, dvs. $a^{\phi(n)} - 1 = \frac{kn}{d}$, der $k \in \mathbb{Z}$. Siden $d = \gcd(a, n)$ så er $\frac{a}{d}$ et heltall. Dette gir at $a^{\phi(n)+1} - a = k\frac{a}{d}n \in n\mathbb{Z}$, så $a^{\phi(n)+1} \equiv a (\bmod n)$. $\square$

Korollar 5. *La $n > 1$ være et kvadratfritt helt tall, og la $a \in \mathbb{Z}$. Da har vi $a^{k\phi(n)+1} \equiv a (\bmod n)$.*

Proof. Vi bruker induksjon. Merk at tilfellet $k = 1$ følger fra setning 4. Anta derfor at det er sant for k, altså at $a^{k\phi(n)+1} \equiv a (\bmod n)$, og vi ønsker å vise at det er sant for $k + 1$. Vi ser at $a^{(k+1)\phi(n)+1} \equiv a^{\phi(n)} a^{k\phi(n)+1} \equiv a^{\phi(n)} a \equiv a^{\phi(n)+1} \equiv a (\bmod n)$, hvor andre ekvivalens følger fra antagelsen, og fjerde fra setning 4. $\square$

Vi anvender nå teorien på hemmelige koder. **A** velger primtall p, q, og lar $n = pq$. Vi har da $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$. Velg e, der $1 < e < \phi(n)$ og $\gcd(e, \phi(n)) = 1$ (dvs. $\bar{e}$ er enhet i $\mathbb{Z}_{\phi(n)}$). La d være slik at $1 < d < \phi(n)$ og $\bar{d}\bar{e} = \bar{1}$ i $\mathbb{Z}_{\phi(n)}$ (dvs. $\bar{d} = \bar{e}^{-1}$). **A** beholder $\{n, d\}$ (hemmelig nøkkel), og offentliggjør $\{n, e\}$ (offentlig nøkkel).

B vil sende melding M til **A**, der $0 \leq M < n$. **B** beregner N slik at $0 \leq N < n$ og $M^l \equiv N (\bmod n)$, og sender N til **A**. **A** beregner $D(N)$, der $N^d \equiv D(N) (\bmod n), 0 \leq D(N) < n$. Vi har $ed \equiv 1 (\bmod \phi(n))$, dvs. $ed = 1 + k\phi(n)$. Vi får da $D(N) \equiv N^d \equiv M^{ed} \equiv M^{1+k\phi(n)} \equiv M (\operatorname{mod} n)$. Altså har vi $D(N) = M$, så **A** får ut meldingen M.

Poenget er at for store n så er det et problem å skrive n som et produkt av primtall, og dermed vanskelig å finne $\phi(n)$, noe man trenger for å beregne M fra N.

Eksempel. La $p = 47, q = 59$. Da er $n = pq = 2773$, $\phi(n) = 46 \cdot 58 = 2668$. La $d = 157$, så $\gcd(d, \phi(n)) = 1$. Vi finner $e = 17$. Hemmelig nøkkel er $\{2773, 157\}$, og offentlig nøkkel er $\{2773, 17\}$. **B** vil sende $M = 920$. $M^e = 920^{17} \equiv 948 (\operatorname{mod} 2773)$, så **B** sender $N = 948$. **A** beregner $948^d = 948^{157} \equiv 920 (\operatorname{mod} 2773)$.