24/10 - 13

MAT1140

Eulers teorem

Definisjon: Eulers φ-funksjon er funksjonen $\varphi: \mathbb{N} \to \mathbb{N}$ gitt ved

$\varphi(t)$ = antall naturlig tall $n \leq t$ slik at $(n,t)=1$.

Legg merke til at hvis p er et primtall, så er $\varphi(p) = p-1$ siden $1, 2, \ldots, p-1$ er innbyrdes primiske.

Vi er nå klare til å vise Eulers generalisering av Fermats lille teorem.

Eulers teorem: Anta at $(a,t)=1$. Da er

$$\bar{a}^{\varphi(t)} = \bar{1} \ ; \ \mathbb{Z}/(t)$$

Bevis: La $a_1, a_2, \ldots, a_{\varphi(t)}$ være de naturlige tallene mindre enn t som er innbyrdes primiske med t. Da er $aa_1, aa_2, \ldots, aa_{\varphi(t)}$ innbyrdes primiske med t, og siden forkortningsregelen gjelder for a, er $\bar{a}\bar{a}_1, \bar{a}\bar{a}_2, \ldots, \bar{a}\bar{a}_{\varphi(t)}$ forskjellige. Dermed:

$$\{\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{\varphi(t)}\} = \{\bar{a}\bar{a}_1, \bar{a}\bar{a}_2, \ldots, \bar{a}\bar{a}_{\varphi(t)}\}$$

Multiplisera i sammen, får vi

$$\bar{a}_1 \bar{a}_2 \cdots \bar{a}_{\varphi(k)} = \bar{a}\bar{a}_1 \bar{a}\bar{a}_2 \cdots \bar{a}\bar{a}_{\varphi(k)}.$$

Siden forkortningsregelen gjelder for $\bar{a}_1, \bar{a}_2 \ldots, \bar{a}_{\varphi(k)}$, kan vi forkorte og få

$$\bar{a}^{\varphi(k)} = \bar{1}$$

Før vi ser på det neste teorem, trenger vi et lemma:

Lemma: Anta at p er et primtall. Da er $\bar{1}$ og $-\bar{1}$ de eneste elementene i $\mathbb{Z}/(p)$ som er sine egne inverser.

Bevis: Et element $\bar{x}$ er sin egen invers dersom det er en løsning av ligningen $\bar{x}^2 - \bar{1} = \bar{0}$; dvs $(\bar{x}^2 - \bar{1})(\bar{x} + \bar{1}) = \bar{0}$. Siden $\mathbb{Z}/(p)$ ikke har nulldivisorer, betyr dette at vi enten har $\bar{x} = \bar{1}$ eller $\bar{x} = -\bar{1}$.

Wilsons teorem: Hvis p er et primtall, så er

$$\overline{(p-1)!} = -\bar{1} \quad \text{i } \mathbb{Z}/(p).$$

Kommentar: Legg merke til $\bar{1} \cdot \bar{2} \cdots \overline{(p-1)} = \overline{(p-1)!}$ er produktet av alle ikke-null elementer i

i $\mathbb{Z}/(p)$. Dette er et produkt som dukker opp ofte, f.eks i beviset for Fermats lille teorem (Men vi skriver ikke behøver å regne det ut!)

Bevis for Wilsons teorem: For $p = 2$, er $\overline{(p-1)!} = \bar{1} = -\bar{1}$.
For $p > 2$, kan vi skrive $\mathbb{Z}/(p)^*$ som en disjunkt union

$$\{\bar{0}\} \cup \{\bar{1}\} \cup \{-\bar{1}\} \cup \{\bar{x}_1, \bar{x}_1^{-1}\} \cup \{\bar{x}_2, \bar{x}_2^{-1}\} \cup \dots \cup \{\bar{x}_m, \bar{x}_m^{-1}\}$$

der $2m + 3 = p \Rightarrow m = \frac{p-3}{2}$. Ganger vi sammen alle de ikke-null elementene, får vi

$$\bar{1} \cdot (\overline{-1}) \cdot \bar{1} \cdot \bar{1} \cdot \dots \cdot \bar{1} = -\bar{1}$$

På den annen side er produktet av alle ikke-null elementer lik $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{(p-1)}$. Dermed er

$$\overline{(p-1)!} = \bar{1} \cdot \bar{2} \cdots \overline{(p-1)} = -\bar{1}.$$

Kvadratiske rester

Vi antar heretter at p er et primtall. Et element $\bar{a} \in \mathbb{Z}/(p)^*$ kalles en kvadratisk rest dersom det finnes en $\bar{x} \in \mathbb{Z}/(p)^*$ slik at $\bar{x}^2 = \bar{a}$.

Setning: Anta at $p > 2$ er et primtall og at $\bar{a} \neq \bar{0}$ i $\mathbb{Z}/(p)$ er en kvadratisk rest. Da finnes det nøyaktig to elementer i $\mathbb{Z}/(p)$ slik at $\bar{x}^2 = \bar{a}$.

Bevis: Per antagelse finnes det et element $\bar{x}_1$ slik at $\bar{x}_1^2 = \bar{a}$. Da er $(-\bar{x}_1)^2 = \bar{a}$. Siden $\bar{x}_1 \neq -\bar{x}_1$ (hvis ikke er $\bar{2}\bar{x}_1 = \bar{0}$, og det er umulig siden $\mathbb{Z}/(p)$ ikke har nulldivisorer)

For å vise at det ikke finnes flere løsninger, anta at $y^2 = a$. Da er $\bar{0} = \bar{y}^2 - \bar{x}_1^2 = (\bar{y} - \bar{x}_1)(\bar{y} + \bar{x}_1)$, og følgelig er $\bar{y} = \bar{x}_1$ eller $\bar{y} = -\bar{x}_1$.

Setning: Anta at $p > 2$ er et primtall. Da er nøyaktig halvparten av de $p-1$ ikke-null elementene i $\mathbb{Z}/(p)$ kvadratiske rester.

Bevis: Ifølge forrige setning er kvadratene

$$\bar{1}^2, \bar{2}^2, \bar{3}^2, \ldots, (\overline{p-1})^2$$

like to og to, og dermed finnes det $\frac{p-1}{2}$ kvadratiske rester.

Vi er på jakt etter et kriterium for når et element i $\mathbb{Z}/(p)$ er en kvadratisk rest. Først en liten observasjon:

Setning: Anta at $p > 2$ er et primtall og $\bar{a} \in \mathbb{Z}/(p)$, $\bar{a} \neq \bar{0}$. Da er $\bar{a}^{\frac{p-1}{2}}$ lik enten $\bar{1}$ eller $-\bar{1}$.

Bevis: La $\bar{x} = \bar{a}^{\frac{p-1}{2}}$. Ifølge Fermats lille er

$$\bar{x}^2 = \left(\bar{a}^{\frac{p-1}{2}}\right)^2 = \bar{a}^{p-1} = \bar{1}.$$

Dermed er $\bar{x}$ sin egen invers, og dermed er $\bar{x} = \bar{1}$ eller $\bar{x} = -\bar{1}$.

Eulers kriterium: Anta at $p > 2$ er et primtall $p > 2$, og $\bar{a} \in \mathbb{Z}/(p)$, $\bar{a} \neq \bar{0}$. Da er $\bar{a}$ en kvadratisk rest hvis og bare hvis $\bar{a}^{\frac{p-1}{2}} = \bar{1}$.

Bevis: Anta først at $\bar{a}$ er en kvadratisk rest, $\bar{x}^2 = \bar{a}$. Da er

$$\bar{a}^{\frac{p-1}{2}} = (\bar{x}^2)^{\frac{p-1}{2}} = \bar{x}^{p-1} = \bar{1}.$$

Anta så at $\bar{a}$ ikke er en kvadratisk rest. For hver $\bar{x} \in \mathbb{Z}/(p)$, $\bar{x} \neq \bar{0}$, finnes det nøyaktig én $\bar{x}'$, $\bar{x}' \neq \bar{x}$, slik at

$$\bar{x} \cdot \bar{x}' = \bar{a}$$

Dermed kan mengden $\{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ skrives som en disjunkt union

$$\{\bar{x}_1, \bar{x}_1'\} \cup \{\bar{x}_2, \bar{x}_2'\} \cup \dots \cup \{\bar{x}_{\frac{p-1}{2}}, \bar{x}_{\frac{p-1}{2}}'\}$$

Ganger vi sammen, får vi

$$\overline{1 \cdot 2 \cdot \dots \cdot (p-1)} = (\bar{x}_1 \bar{x}_1')(\bar{x}_2 \bar{x}_2'') \dots (\bar{x}_{\frac{p-1}{2}} \bar{x}_{\frac{p-1}{2}}') = \bar{a}^{\frac{p-1}{2}}$$

Siden $\overline{1 \cdot 2 \cdot \dots \cdot (p-1)} = -1$ ved Wilsons teorem, får vi

$$\bar{a}^{\frac{p-1}{2}} = -\underline{1}.$$

Eksempel: Er $\bar{5}$ en kvadratisk rest i $\mathbb{Z}/(11)$.

Vi har $\frac{p-1}{2} = 5$.

$$\bar{5}^5 = \underbrace{(\bar{5} \cdot \bar{5})}_{\bar{3}} \underbrace{(\bar{5} \cdot \bar{5})}_{\bar{3}} \cdot \bar{5} = \bar{9} \cdot \bar{5} = \underline{\bar{1}}$$

Altså er $\bar{5}$ en kvadratisk rest.