## 20. Fermats teorem og Eulers teorem

Fra før: (1) $G$ gruppe med $|G|=n$ $\Rightarrow$ enhver undergr $H \leq G$ må tilfredsstille $|H| \mid n$ (Lagrange). Spesielt, for $g \in G$ må $|\langle g \rangle| \mid n$. Men $|\langle g \rangle| = \min\{t \geq 1 \mid g^t = e\}$, så derfor: $g^n = e \quad \forall g \in G$.

(2) For en ring $R$, la $U(R) = \{a \in R \mid a \text{ er en enhet } (a^{-1} \text{ eksisterer})\}$. Da er $(U(R), \cdot)$ en gruppe. Spesielt, hvis $F$ er en kropp er $U(F) = F \setminus \{0\}$ pr. def, så $(F \setminus \{0\}, \cdot)$ danner en abelsk gr.

<u>Teorem 20.1</u> (Fermats lille teorem). La $a \in \mathbb{Z}$ og $p \in \mathbb{Z}$ et primtall med $p \nmid a$. Da gjelder $a^{p-1} \equiv 1 \pmod p$.

Bevis: Se på kroppen $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ ($\mathbb{Z}_p$ er en kropp ved K. 19.12). Velg $b \in \mathbb{Z}_p$ med $b \equiv a \pmod p$ (det finnes nøyaktig én slik $b$). Da må $b \neq 0$, hvis ikke er $a \equiv 0 \pmod p$, dvs $p \mid a$, umulig. Siden $\mathbb{Z}_p$ er en kropp er $U(\mathbb{Z}_p) = \{1, 2, \ldots, p-1\}$, og fra over gjelder derfor $b^{p-1} = 1$ i $U(\mathbb{Z}_p)$, dvs $b^{p-1} \equiv 1 \pmod p$ (fordi gruppeoperasjonen i $U(\mathbb{Z}_p)$ er $\cdot_p$). Siden $a \equiv b \pmod p$ gjelder $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$ $\square$

<u>Korollar 20.2</u> For et primtall $p$ gjelder $a^p \equiv a \pmod p$ for alle $a \in \mathbb{Z}$.

Bevis: Hvis $p \mid a$ er både $a^p$ og $a$ delelig med $p$, så $a^p \equiv a \pmod p$. Hvis $p \nmid a$ gjelder $a^{p-1} \equiv 1 \pmod p$, multiplisér med $a$ og få $a^p \equiv a \pmod p$. $\square$

Fra før: Se på ringen $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Hvis $a \in \mathbb{Z}_n$ og $a \neq 0$, sier T. 19.3 at

$$a \text{ nulldivisor i } \mathbb{Z}_n \iff \gcd(a,n) \neq 1$$
$$(\exists\, 0 \neq b \in \mathbb{Z}_n \text{ med } a \cdot_n b = 0)$$

Hvis $a \in \mathbb{Z}_n$, $a \neq 0$ og $\gcd(a,n) = 1$, så er $a$ en enhet: se på

$$a, a^2, a^3, \ldots,$$

i $\mathbb{Z}_n$. Siden $a$ ikke er en nulldivisor er $a^t \neq 0$ i $\mathbb{Z}_n$ for alle $t \geq 1$. Siden $|\mathbb{Z}_n \setminus \{0\}| = n-1$ må to av elementene

$$a, a^2, \ldots, a^n$$

være like, dvs $a^t = a^{t+s}$ for en $t \geq 1$ og $s \geq 1$. Da får vi

$$a^t(1 - a^s) = 0$$

i $\mathbb{Z}_n$. Men $a$ ikke nulldiv $\Rightarrow a^t$ ikke nulldiv $\Rightarrow 1 - a^s = 0$, dvs $a^s = 1$. Da er $a$ en enhet: $a^{-1} = a^{s-1}$ (rent ringteoretisk argument). Derfor:

$$U(\mathbb{Z}_n) \overset{\text{def}}{=} \{a \in \mathbb{Z}_n \mid a \text{ enhet}\} = \{a \in \mathbb{Z}_n \mid a \neq 0 \text{ og } \gcd(a,n) = 1\}$$

Def: (Eulers phi-funksjon). For $n \geq 1$ er

$$\phi(n) \overset{\text{def}}{=} \#\{a \mid 1 \leq a \leq n \text{ og } \gcd(a,n)=1\}$$

Eksempler: (1) $\phi(4)=2$ siden 1 og 3 er de eneste tallene i $\{1,2,3,4\}$ som er rel. primiske med 4.

(2) $\phi(10)=4$ siden 1, 3, 7, 9 er de eneste tallene i $\{1,2,\ldots,10\}$ som er rel. pr. med 10.

(3) $\phi(p)=p-1$ $\forall$ primtall $p$.

Merk: Se på $\mathbb{Z}_n$. Har da at enhetene er gitt ved

$$U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \mid a \neq 0 \text{ og } \gcd(a,n)=1\}$$

Derfor er $\boxed{|U(\mathbb{Z}_n)| = \phi(n)}$, dvs $U(\mathbb{Z}_n)$ er en abelsk gr (med $\cdot_n$ som bin.op.) med $\phi(n)$ elementer.

<u>Teorem 20.8</u> (Eulers teorem) La $a,n \in \mathbb{Z}$ med $n \geq 1$ og $\gcd(a,n)=1$. Da gjelder

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

Bevis: Hvis $n=1$ er $x \equiv y \pmod{1}$ gyldig $\forall x,y \in \mathbb{Z}$, så anta $n \geq 2$. Velg $b \in \mathbb{Z}_n$ med $a \equiv b \pmod{n}$. Pr def gjelder $n \mid (a-b)$, dvs

$$a-b = nq$$

for en $q \in \mathbb{Z}$. Siden $\gcd(a,n)=1$ må derfor $\gcd(b,n)=1$. Da vet vi fra over at $b$ er en enhet i $\mathbb{Z}_n$, dvs $b \in U(\mathbb{Z}_n)$. Siden $U(\mathbb{Z}_n)$ er en multiplikativ gr av orden $\phi(n)$, må derfor $b^{\phi(n)}=1$ i $U(\mathbb{Z}_n)$, dvs $b^{\phi(n)} \equiv 1 \pmod{n}$. Siden $a \equiv b \pmod{n}$ fås

$$a^{\phi(n)} \equiv b^{\phi(n)} \equiv 1 \pmod{n} \qquad \square$$

På øving 9: For $m,n$ med $\gcd(m,n)=1$ gjelder $\phi(mn)=\phi(m)\phi(n)$. Vises ved å se på $U(\mathbb{Z}_m)$, $U(\mathbb{Z}_n)$ og $U(\mathbb{Z}_{mn})$.