Lagrange og primtal
– Sjov med endelige grupper

Martin Patrick Speirs

I disse uger oplever mange spirende matematik-unger deres første møde med en af algebraens herligste objekter: grupper! Udover at være en fornøjelse i sig selv, så har gruppeteori et væld af anvendelser inden for en række matematiske discipliner, såvel som i naturvidenskaberne – især i fysik og kemi. Særlig smuk og dyb er konstruktionen af såkaldte symmetrigrupper som f.eks. kan hjælpe med forståelsen af både geometriske objekter og polynomier (Se artikel om Galoisteori).

I denne lille note vil jeg gengive et sjovt bevis for at der er uendeligt mange primtal. Hovedredskabet er *Lagranges sætning*! Hvis G er en (endelig) gruppe og H er en undergruppe i G, så siger Lagrange (og han har skam ret!) at ordenen af H er divisor i ordenen af G. Én måde at se dette på er ved at betragte en meget fin ækvivalensrelation på G, nemlig,

$$a \sim b \iff ab^{-1} \in H$$

(prøv at vise at det *er* en ækvivalensrelation).[3] Det vigtige ved denne ækvivalensrelation er at den giver anledning til en klassedeling af G. I dette tilfælde kan man vise (Gør det! Det er ikke svært) at hver ækvivalensklasse har samme orden som H. Altså består G af en samling ækvivalensklasser, som alle har samme orden som H. Jamen så går ordenen af H jo op i ordenen af G.

Et specialtilfælde af Lagranges sætning opstår når man har et element $g \in G$. Så frembringer g en undergruppe, kaldet $\langle g \rangle$, som altså har en orden som er en divisor i $|G|$.

[3] Der er *ikke* noget underligt ved denne relation. Den minder meget om kongruens på hele tal, altså: $a \equiv b \pmod{m} \iff a - b \in m\mathbb{Z}$

Her er to gode eksempler på endelige grupper: $\mathbb{Z}_q$ og $\mathbb{Z}_q^*$ hvor q er et primtal. Gruppen $\mathbb{Z}_q$ er som bekendt den cykliske gruppe af orden q. Gruppen $\mathbb{Z}_q^*$ består af de elementer i $\mathbb{Z}_q$ som har en *multiplikativ* invers. Da q er et primtal er der netop $q-1$ sådanne elementer. Hvis f.eks. $q = 5$ så er $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ og $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$.

Theorem 1 *Der er uendeligt mange primtal.*

Bevis. Antag for modstrid at der er *endeligt* mange primtal og lad p være det største. Vi ser nu på tallet $2^p - 1$ (et *Mersenne* tal) og finder et primtal som er større end p. Lad q være et primtal som går op i $2^p - 1$ (husk at ethvert tal altid har primdivisorer). Vi har altså at

$$2^p - 1 \equiv 0 \pmod{q} \qquad \text{dvs.} \qquad 2^p \equiv 1 \pmod{q}$$

Vi ser nu på den multiplikative gruppe $\mathbb{Z}_q^*$. Ovenstående kongruens viser at elementet $\overline{2}$ har orden p i $\mathbb{Z}_q^*$ (her er det vigtigt at p er et primtal). Vi har nu fra Lagranges sætning at ordenen af undergruppen $\langle\overline{2}\rangle$ går op i ordenen af $\mathbb{Z}_q^*$. Dvs. $p \mid q - 1$. Men så er $p < q$ og vi har altså fundet et større primtal i modstrid med antagelsen om at p var størst! □

Overstående bevis kommer fra [1] som er en herlig bog at læse i. Bogen findes både på IMF og NAT SUND bibliotekerne og sågar på nettet igennem rex.kb.dk.

God fornøjelse med grupperne!

Litteratur

[1] M. Aigner and G. Ziegler, *Proofs from the Book*, 4th ed. Springer