BOKS (Algebraiske ligninger over endelige tallegemer)

Regning modulo et primtal

Pierre Deligne studerede bl.a. algebraiske ligninger over de reelle tal men også over andre talsystemer, såkaldte *tallegemer*, der har regneoperationer addition og multiplikation som vi kender det fra de reelle tal.
Nogle yderst interessante endelige tallegemer $\boldsymbol{L_p}$ opstår ved i de hele tal at regne *modulo* et primtal *p*. Ved regning modulo *p* anses to tal der afviger fra hinanden med et helt multiplum af *p* som det samme element i $\boldsymbol{L_p}$.
Betragt eksempelvis primtallet 7. Ved regning *modulo* 7 skal to hele tal hvis differens er divisibel med 7 regnes for ens. Vi får derfor kun brug for talsymbolerne {0, 1, 2, 3, 4, 5, 6} ved regning modulo 7 idet tallene 7, 8, 9 i dette tallegeme er ækvivalent med hhv. 0, 1, 2.
Når vi i det underliggende tallegeme for regning modulo 7 betegner addition og multiplikation med hhv. $+_7$ og $\cdot_7$ får vi bl.a. følgende sjove regnestykker

$$3 +_7 4 = 0 \qquad 3 +_7 6 = 2 \qquad 3 \cdot_7 5 = 1 \qquad (3 +_7 6) \cdot_7 5 = 3.$$

De fuldstændige additions- og multiplikationstabeller for regning modulo 7 ser således ud:

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tilsvarende kan vi for ethvert primtal $p = 2, 3, 5, 7, 11, 13, ...$, danne et tallegeme $\boldsymbol{L_p}$ for regning med hele tal modulo *p*.

Hvis vi i andengradsligningen $x^2 + y^2 = 1$ i stedet for reelle tal indsætter variable *x* og *y* fra tallegemet $\boldsymbol{L_p}$ og regner modulo *p*, så svinder d en lukkede cirkelkurve vi kender fra den sædvanlige euklidiske plan ind til en endelig punktmængde $\boldsymbol{C_p}$ i planen. Punkterne $\boldsymbol{C_p}$ i 'cirklen modulo p' svarer netop til løsningerne (*x*, y) til andengradsligningen $x^2 + y^2 = 1$ når vi regner modulo *p*.

For *p* = 2 indeholder $\boldsymbol{C_p}$ kun to punkter: (1,0) og (0,1).
For *p* = 3 indeholder $\boldsymbol{C_p}$ netop fire punkter: (1,0), (0,1), (2,0) og (0,2).
For *p* = 5 indeholder $\boldsymbol{C_p}$ også netop fire punkter: (1,0), (0,1), (4,0) og (0,4).
For *p* = 7 indeholder $\boldsymbol{C_p}$ netop otte punkter: (1,0), (0,1), (2,2), (2,5), (5,2), (5,5), (6,0) og (0,6).

Det er et yderst vanskeligt problem at holde styr på antallet af løsninger til en algebraisk ligning af vilkårlig grad over et vilkårligt tallegeme. Problemet har imidlertid ikke afskrækket Deligne og det er bl.a. på dette område han har ydet de banebrydende bidrag der indbragte ham Abelprisen.