1 INDLEDNING

Tælletallene, som vi skriver $1, 2, 3, \ldots$ og kalder de naturlige tal, menes at være (op)fundet af *sumererne* i den sydlige del af Mesopotamien, landet mellem floderne Eufrat og Tigris i det nuværende Irak, og kort før 2000 f.Kr. kom de med historiens første kendte positions-talsystem.

De ældste skriftlige kilder med tal er lertavler, der er indprægede med kileformede skrifttegn – såkaldt kileskrift. O. Neugebauer og hans medarbejdere afslørede i 1935/37 igennem tydning af et stort antal lertavler, fundet ved byen Babylon, repræsentationen af tælletallene (Neugebauer, 1973).

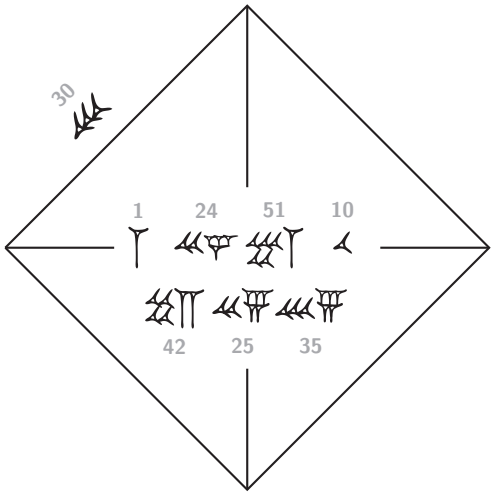
De fandt, at tallene fremstilledes ved hjælp af skrifttegnet 𒁹 for tallet 1 og skrifttegnet 𒌋 for 10 i et *seksagesimalt* positionssystem, hvor cifrene dannedes ud fra tegnene 𒁹 og 𒌋, således at 2 599 801 skrives:

$$\underset{(10+1+1)\times 60^3}{\text{𒌋𒁹𒁹}} \quad + \quad \underset{(1+1)\times 60^2}{\text{𒁹𒁹}} \quad + \quad \underset{10\times 60^1}{\text{𒌋}} \quad + \quad \underset{1\times 60^0}{\text{𒁹}}.$$

YBC 7289 fra Yales babylonske samling er en af de bedst kendte lertavler. Tavlen menes at være fra den første tredjedel af det andet årtusinde f.Kr. og viser et kvadrat med dets diagonaler og nogle kileskriftstegn, se Figur 1.1. På Figur 1.2 læses skrifttegnene i den øverste række til 1 24 51 10 i det seksagesimale

Figur 1.1: Babylonsk lertavle YBC 7289 (Yale) fra den første tredjedel af det andet årtusinde f.Kr. med repræsentation af diagonalen i et kvadrat. Skriften og figuren giver rigtig tolket en god værdi for $\sqrt{2}$.

talsystem, som tolkes til $1+24\times\frac{1}{60}+51\times\frac{1}{60^2}+10\times\frac{1}{60^3} = 1{,}41421259\ldots$ – en temmelig nøjagtig værdi for $\sqrt{2}$, den rigtige værdi er $1{,}41421356\ldots$ I Fowler og Robson (1998) uddybes, hvordan babylonierne faktisk bestemte kvadratrødder.



Figur 1.2: Optegning og kommentering af YBC 7289 fra Figur 1.1. Se Aaboe (1964) for mere information.

Talbegrebet ligger før sproget, og samtlige store verdenskulturer har haft talbegrebet under en eller anden form. I Renæssancen (14. til 17. århundrede) opsamledes og konsolideredes verdens viden til den nu herskende viden; men det var først mod slutningen af 1800-tallet, at man fuldt ud forstod talbegrebet og udmøntede det i Peanos aksiomer, som behandles i Kapitel 2.

Hvor den mesopotamiske kultur fokuserede sin matematik på at udvirke løsninger til problemer, mere end på argumenter eller beviser, var den græske matematiks særkende det matematiske bevis' centrale rolle. Det matematiske bevis – og her især det indirekte bevis (modstridsbeviset) – gjorde det muligt at udtale og begribe, at en bestemt opgave ikke lod sig løse, hvilket er et andet abstraktionsniveau end at eftersøge en løsning, jf. Sørensen (2011).

Primtallene tilhører den eksklusive verden af intellektuelle begreber, der på den ene side har en simpel og elegant beskrivelse og på den anden side fører til ekstrem kompleksitet i detaljen. Et barn kan forstå definitionen af et primtal; men intet menneske har et komplet billede af deres teori og de sammenhænge, de indgår i.

Vi vil ved hjælp af matematisk bevisførelse forstå dele af de naturlige tals multiplikative struktur og primtallenes centrale rolle. Deling eller faktorisering af tal er her det overordnede tema, eksempelvis kan tallet 60 deles eller faktoriseres i $60 = 4 \cdot 15$, som videre deles til:

$$60 = 2 \cdot 2 \cdot 3 \cdot 5,$$

hvorefter yderligere faktorisering er umulig. Dette simple eksempel giver anledning til en række klassiske og forskningsaktuelle spørgsmål, hvis besvarelse også har stor praktisk betydning:

- Kan ethvert tal i lighed med 60 faktoriseres i et produkt af primtal – tal, der ikke kan deles yderligere? Kan en faktorisering kun foretages på én måde?

JA – Aritmetikkens fundamentalsætning, der behandles i afsnit 4.1, præciserer og besvarer begge spørgsmål positivt.

- Er det hurtigt at faktorisere et tal i sine primfaktorer?
  NÆPPE – men der er ikke et definitivt svar. Temaet, der behandles i afsnit 4.1, er helt centralt i moderne kryptografi, jf. afsnit 16.1.
- Er der uendelig mange primtal, tal, der i lighed med 2, 3 og 5 er udelelige?
  JA – bevises i Kapitel 5 på tre forskellige måder.
- Kan man anslå, hvad chancen er for, at et tilfældigt valgt tal er et primtal?
  JA – primtalssætningen, der behandles i Kapitel 6, giver estimater. I nærheden af $n = 1000$ er cirka hvert syvende tal et primtal, og i nærheden af $10\,000\,000\,000$ er omkring 1 ud af 23 tal et primtal.
- Kan man hurtigt afgøre, om et konkret tal er et primtal eller i det mindste med meget stor sandsynlighed afgøre at det er et primtal?
  JA – i afsnit 10.1 beskrives en hurtig gennemførlig test, der fejler mindre end 1 ud af $1\,000\,000\,000\,000\,000\,000$ gange, hvis den erklærer et givet tal for at være et primtal.
- Ved man alt om primtal?
  NEJ – i Kapitel 7 behandles fire klassiske og stadig uløste problemer.
- Kan primtalsfaktorisering anvendes i praksis?
  JA – det er kernen bag sikkerheden i offentlig-nøgle-kryptosystemet RSA, jf. afsnit 16.1.

Hensigten er at uddybe disse spørgsmål og give præcise svar, så vidt det er muligt, belyst såvel igennem den klassiske viden som ved aktuel matematisk forskning. Et yderligere sigte er anvendelsen i moderne kryptografi.

Opgaver

1.1. Forsøg at tolke de øvrige kileskriftsrækker på YBC 7289, jf. Figur 1.2, og sæt dem ind i en sammenhæng med den geometriske figur på lertavlen.