Talteori: Ett historiskt perspektiv

Sebastian Miles

Inledning

Talteori handlar om att undersöka egenskaper av heltalen. Talteori har utvecklats huvudsakligen för att utveckla matematiken som ett ämne utan ändamålet att tillämpas i verkligheten. Trots det har tillämpningar dykt upp som är väsentlig för samhället i stort. Hur har talteorin utvecklats för att åstadkomma tillämpningarna? Vilken roll har andra vetenskaper eller andra grenar inom matematiken för talteori? Inom samhället används talteori för att skicka hemliga meddelanden med kryptografi [1]. Inom teoretisk datorvetenskap har talteori en stor roll. I förordet av *Concrete Mathematics* skriver Donald Knuth [2] (Datorvetenskapsman, matematiker och skaparen av TEX) att under skrivandet av en bokserie kallad *The Art of Computer Programming* insåg han att det saknades matematiska verktyg, matematik som behövdes för att skriva en grundlig bokserie. Matematiken som saknades var bland annat diskret matematik, i vilket talteori ingår.

Tidiga Talteorin

Det tidigaste kända tecken av talteori är den Babyloniska lerplattan *Plimpton 322* (ca 1800 f.kr.) som består av en lista av pythagoreiska tripplar, det är positiva heltal a, b, c som uppfyller $a^2 + b^2 = c^2$. Man tror på grund av antalet tuplar att listan inte var skapad genom slumpmässigt testa tal, utan med någon slags tal-teoretisk metod [3].

Under den antika Grekland (ca 300 f.kr.) levde matematikern och logikern Euklides, han samlade upp det mesta av matematiken som fanns på den tiden och skrev systematiskt ner informationen i 13 böcker, dessa böcker är idag kända som *Euklides Elements*. Böckerna innehåller postulat, propositioner och definitioner, det är ett matematiskt moget verk för dess tid. [4]

Euklides Algoritm

I *Elements* VII presenterar Euklides en algoritm, som idag har fått namnet Euklides algoritm (EUA). I en föreläsning berättar Johan Jonasson vid Chalmers tekniska högskola om just Euklides algoritm. Han börjar först med en hjälpsats som kallas för divisionsalgoritmen: För varje talpar a, b kan man finna en unik kvot q samt en unik rest term r,

$$a = qb + r, \quad 0 < r < b - 1.$$

Vidare för EUA, låt $\text{sgd}(a, b)$ beteckna den största gemensamma nämnaren för de positiva heltalen a, b. Den kan då beräknas genom att successivt tillämpa divisionsalgoritmen enligt processen

$$\begin{aligned}
&a = q_1 b + r_1, \quad 0 < r_1 \leq b - 1 \\
&b = q_2 r_1 + r_2, \quad 0 < r_2 \leq r_1 - 1 \\
&r_1 = q_3 r_2 + r_3, \quad 0 < r_3 \leq r_2 - 1 \\
&\vdots \\
&r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n \leq r_{n-1} - 1 \\
&r_{n-1} = q_{n+1} r_n.
\end{aligned}$$

När resttermen är lika med noll, då är den största gemensamma nämnaren givet av $\text{sgd}(a, b) = r_n$ [5], för ett bevis hänvisas sats 207 i [6].
Jonasson påstår att antal steg i EUA är logaritmisk, det kan visas att den avslutar inom $2 \log_2 b + 1$ steg:

$$\begin{cases} r_{k-1} = q_{k+1} r_k + r_{k+1}, \quad k \geq 1 \\ r_k = q_{k+2} r_{k+1} + r_{k+2} \end{cases} \implies r_{k-1} = q_{k+1}(q_{k+2} r_{k+1} + r_{k+2}) + r_{k+1}$$

$$> q_{k+1} q_{k+2} r_{k+1} + r_{k+1} \geq 2 r_{k+1}$$

Således, har vi den rekursiva olikheten $r_k > 2r_{k+2}$ för $k = 0, 1, \ldots, n$, där $r_0 = b$. Låt sedan $i = \left\lfloor \frac{n}{2} \right\rfloor$, då gäller

$$b > 2r_2 > 4r_4 > \ldots > 2^i r_{2i} \geq 2^i$$
$$\implies \log_2 b > i \geq \frac{n}{2}$$

Nu visar det sig att $2 \log_2 b$ är en övre gräns för n.
Han förklarar även hur man kan utföra EUA baklänges för att lösa den linjära diofantiska ekvationen $ax + bx = \text{sgd}(a, b)$.

Euler $\phi(n)$-funktionen

I Jonassons nästa föreläsning om talteori definierar han Euler $\phi(n)$ funktionen som ger antalet positiva heltal mindre än n som är relativt prima till n:

$$\phi(n) = |\{0 < x < n \mid \text{sgd}(x, n) = 1\}| .$$

Han visar tre egenskaper som funktionen uppfyller:

(a) p är primtal $\implies \phi(p) = p - 1$

(b) $\text{sgd}(a, b) = 1 \implies \phi(ab) = \phi(a)\phi(b)$

(c) p, q är primtal $\implies \phi(pq) = (p - 1)(q - 1)$ (Följer av (a) och (b))

Jonasson bevisar den s.k Eulers sats:
Om $\text{sgd}(a, n) = 1$ då gäller

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

För bevis av ovan nämnda sats hänvisas sats 72 i [6].

Kryptosystemet RSA

För att knyta ihop matematiken till en konkret tillämpning, introducerar Jonasson RSA (Rivest-Shamir-Adleman) kryptosystemet; detta används idag för att skicka krypterade meddelanden. Till exempel, Alice vill skicka ett meddelande till Bob sådan att

(i) Ingen förutom Bob kan läsa det.

(ii) Bob ska veta att det var Alice som skickade det.

(iii) Eve ska inte kunna ändra meddelandet medan det skickas.

Detta är något som RSA kan uppnå. Jonasson förklarar att varje användare måste välja två stora skilda primtal p, q och ett naturligt tal a sådana att

$$\begin{aligned} &\text{sgd}(a, \phi(pq)) = 1 \\ \iff &\text{sgd}(a, (p-1)(q-1)) = 1 \qquad \text{(egenskap (c))} \end{aligned}$$

Talen p, q måste hållas hemligt, dock behöver inte pq och a vara hemliga eftersom primtals faktorisering är väldigt långsamt, sådan att ingen kan beräkna p, q samt $\phi(pq)$ noterar Jonasson. Låt b vara den multiplikativa inversen av a modulo $\phi(pq)$, för att hitta b kan EUA utföras baklänges, detta går snabbt ty det är logaritmisk antal steg.

Antag att Alice vill skicka ett meddelande x till Bob. Om x är ett positivt heltal mindre än p, q, a och b ska Alice skicka

$$y \equiv x^a \mod pq$$

och Bob beräknar

$$z \equiv y^b \mod pq$$

Jonasson motiverar att eftersom b är invers till $a \mod pq$ kan man skriva

$$ab = 1 + t\phi(pq)$$

för något heltal t. Det följer att

$$z \equiv y^b \equiv x^{ab} = x^{1+t\phi(pq)} \pmod{pq}$$

och av Eulers sats fås

$$x \equiv x^{1+t\phi(pq)} \pmod{pq}.$$

Alltså har Bob beräknat det originella meddelandet x som Alice skickade. Jonasson berättar även

om modifieringar som att kryptera två gånger eller använda en hash funktion för att säkerställa att Eve inte har ändrat meddelandet och att det var Alice som var avsändaren [7].

Modern Talteori

Modern talteori syftar på talteori som använder matematik från andra branscher för att formulera satser eller bevis. Algebra kan användas i samband med talteori, i Jonassons första föreläsning visar han den cykliska gruppen $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$, där notationen $[k]$ betyder alla j sådan att $k \equiv j \pmod{n}$ och följer med några satser om gruppen.

Christian Johansson, en matematiker och lektor vid Göteborgs Universitet och Chalmers tekniska högskola talade under My-dagen om vad en matematiker gör och hur matematisk forskning går till. Johansson studerar modern talteori med algebraiska strukturer, särskilt Langlands teorin som är ett tillhör algebraisk talteori. Han säger att Galoisteori ligger centralt, vilket är en teori som kan användas för att visa det finns polynom av minst grad 5 som inte har en exakt lösning [11].

En sats inom analytisk talteori som har fått namnet Primtalssatsen, den påstår att primtalsräknarfunktionen $\pi(x) = \#$ primtal $\leq x$, som räknar antalet primtal upp till x, uppfyller

$$\lim_{x\to\infty} \pi(x) \cdot \frac{\ln x}{x} = 1.$$

Denna sats var först bevisad 1896 genom att använda metoder från komplex analys. Året 1921 skrev G.H Hardy ett brev där han tror att ett bevis som inte är beroende av teorin om funktioner är extraordinärt osannolikt. Trots detta bevisade Paul Erdős och Atle Selberg år 1948 satsen utan komplex analys [8, 9]. Det visar att talteori är inte nödvändigtvis beroende av andra grenar inom matematiken, men har ett stort inflytande. Andra grenar inom matematiken kan även användas för att formulera satser, i detta exempel användes ett gränsvärde från analysen.

I en föreläsning av Martin Hallnäs pratar han om gammafunktionen $\Gamma(x)$—en generalisering av fakultet operatorn för hela $\mathbb{C}$ förutom negativa heltalen. Han berättar om en

tillämpning av gammafunktionen med Riemann zeta-funktionen

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \mathfrak{Re}(s) > 1.$$

Riemannhypotesen handlar om Riemann zeta-funktionens nollställen, det är en av de viktigaste olösta problemen inom matematiken, där en lösning uppger en miljon dollar som pris av Clay Institute. Liknande primtalssatsen har Riemannhypotesen en central betydelse för hur primtalen är fördelade. Hallnäs beskriver bland annat för $\mathfrak{Re}(s) > 1$ håller identiteten

$$\zeta(s)\Gamma(s) = \int_0^{\infty} \frac{t^{s-1}}{e^t - 1} dt,$$

han nämner även den s.k reflektionsformeln

$$\frac{\zeta(s)}{\zeta(1-s)} = 2^s \pi^{s-1} \sin\Big(\frac{\pi s}{2}\Big)\Gamma(1-s)$$

som håller för nästan hela $\mathbb{C}$, detta för främja kopplingen mellan analysen och talteorin [10].

Avslutning

Trots talteori är ren matematisk bransch, en bransch som utvecklas utan den primära tanken att tillämpas till samhället, har den även tillämpningar. Till exempel RSA-kryptosystemet som kan användas för att kryptera och avkryptera meddelanden, som troligtvis kommer att fortsätta att användas flera år i framtiden. Talteori har även en roll inom teoretisk datorvetenskap, för att lösa heltals ekvationer, till exempel för att lösa linjära modulära ekvationen kan man använda utökad Euklides algoritm. Andra grenar inom matematiken har även en roll inom talteori, till exempel analys, det första beviset av primtalssatsen användes komplex analys som ett hjälpmedel, och i exemplet med Riemann zeta-funktionen användes gammafunktionen för att representera den talteoretiska zeta-funktionen. Ett annat exempel algebraisk talteori, där man använder algebraiska strukturer för att generalisera och formulera talteori på nya sätt, med algebraiska terminologi. Här pågår forskning inom till exempel Langlands teori där galoisteori har en väsentlig roll.

References

1. Julius O. Olwenyi Aby Tino Thomas, A. B. *Cryptography in Modern World* `https://cdn.stmarytx.edu/wp-content/uploads/2020/10/Cryptography-in-Modern-World.pdf`. 2020.
2. Graham, R. L., Knuth, D. E. & Patashnik, O. *Concrete Mathematics: A Foundation for Computer Science* 2nd (Addison-Wesley Longman Publishing Co., Inc., 1994).
3. Abdulaziz, A. A. *The Plimpton 322 Tablet and the Babylonian Method of Generating Pythagorean Triples* `https://arxiv.org/abs/1004.0025`. 2010.
4. Waerden, B. L. *Science Awakening I* 1st ed. (Springer Dordrecht, 1975).
5. Jonasson, J. *Heltalsaritmetik del 1* University Lecture. Euklides algoritm och modulär aritmetik. 2022.
6. Hardy, G. H. & Wright, E. M. *An Introduction to the Theory of Numbers* Fourth (Oxford, 1975).
7. Jonasson, J. *Heltalsaritmetik del 2* Universitets föreläsning. Eulers ϕ-funktion och RSA-krypto. 2022.
8. Goldfeld, D. in *The Elementary Proof of the Prime Number Theorem: An Historical Perspective* 179–192 (Springer New York, New York, NY, 2004).
9. Apostol, T. M. *Introduction to Analytic Number Theory* 1st ed. (Springer New York, Ny, 1976).
10. Hallnäs, M. *Gammafunktionen eller varför* $(-1/2)! = \sqrt{\pi}$ Universitets föreläsning. 2022.
11. Johansson, C. *Att Forska i matematik* Universitets föreläsning. 2022.