Stockholms Matematiska Cirkel
Elliptiska kurvor, läsåret 2023-2024

Ludvig Olsson[1] och Lukas Gustafsson[2]

[1] Stockholms universitet
[2] KTH Royal Institute of Technology

Vad ska vi jobba med i år?

Matematiker har en lång historia av att studera kurvor i planet, alltså lösningar till polynomekvationer i 2 variabler. Det visar sig att kurvor av tredje graden har en extra struktur, man kan nämligen definiera en typ av addition av punkter på en elliptisk kurva.
Det här visar sig ha många oväntade konsekvenser. Man kan till exempel enbart definiera additionen på rationella punkter, och får då mycket intressant struktur hos de rationella punkterna av en elliptisk kurva. Man kan till exempel generera nya rationella lösningar genom att addera gamla. Mordells sats säger att man kan nå vilken punkt som helst genom att starta med ett ändligt antal punkter och sedan addera dem, och är slutmålet i årets cirkel.
Man kan även betrakta lösningar till polynomekvationer i situationer som är lite mindre välkända, som exempelvis att undersöka lösningar i $\mathbb{Z}/(p)$. Det här visar sig ha många intressanta användningar inom kryptografi.

Exempel

Betrakta kurvan given av ekvationen

$$y^2 = x^3 + 17.$$

Om vi nu väljer 2 punkter P och Q på kurvan och drar linjen genom dem kommer det att skära kurvan i en tredje punkt. Vi reflekterar den här punkten i x-axeln, och får nu en ny punkt $P+Q$ på kurvan. Det gäller att $P+Q = Q+P$, och att $P + (Q + R) = (P + Q) + R$.
Om vi exempelvis betraktar $P = (-1, 4)$ och $Q = (2, 5)$ kommer linjen genom P och Q ges av ekvationen

$$y = \frac{5-4}{2-(-1)}x + \frac{13}{3} = \frac{1}{3}x + \frac{13}{3}.$$

Linjen möter kurvan igen i

$$\left(\frac{1}{3}x + \frac{13}{3}\right)^2 = x^3 + 17,$$

vilket kan skrivas om som

$$(x+1)(x-2)\left(x + \frac{8}{9}\right).$$

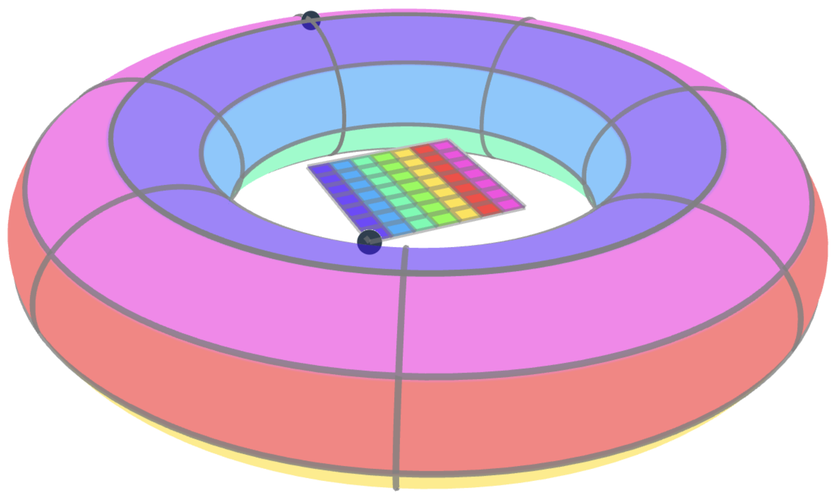
Alltså skär linjen kurvan igen i punkten

$$\left(-\frac{8}{9}, \frac{109}{27}\right).$$

Reflekterar vi i x-axeln får vi

$$\left(-\frac{8}{9}, -\frac{109}{27}\right).$$

Allstå har vi genererat en ny lösning till ekvationen utifrån två enkla lösningar.



Figur 1:Talpplanet modulo 7

Cirkeln

Stockholms matematiska cirkel är en årlig föreläsningsserie för gymnasieelever. Med Cirkeln får du möjligheten att se en annan sida av matematikämnet än den man vanligen får se på gymnasiet.

När och var?

Cirkeln träffas på torsdagar varannan vecka med preliminär start 31:a Augusti. Hälften av träffarna är föreläsningar och hälften övningstillfällen då vi arbetar med övningsuppgifter. Läsåret 2023/2024 kommer Cirkeln att hållas i KTH:s lokaler under hösten och Stockholms Universitets lokaler under våren. Vill du vara med? Alla är välkomna utan att behöva anmäla sig. På många gymnasieskolor kan Cirkeln läsas som en tillvalskurs i matematik. Ta upp det med din gymnasielärare.

Kontakt

Mer information finns på vår hemsida **www.math-stockholm.se/cirkel**
Frågor? Kontakta oss på **cirkel@math-stockholm.se**