De theorie van elliptische krommen

Een elliptische kromme $\mathrm{K}(\mathbb{R})$ wordt gedefiniëerd door alle paren (x, y) in $\mathbb{R}$ die voldoen aan de volgende vergelijking:

$$\mathrm{K}(\mathbb{R}) : y^2 = x^3 + ax + b$$

voor $a, b \in \mathbb{R}$, met als randvoorwaarde dat de discriminant

$$\Delta_{\mathrm{K}} = -16(4a^3 + 27b^2)$$

ongelijk is aan 0. Deze voorwaarde garandeert dat de kromme niet-singulier is. Als conventie wordt vervolgens een afzonderlijk punt in oneindigheid toegevoegd. De punten op deze krommen kunnen nu onderling opgeteld worden, met als resultaat een som van de punten die zich wederom op de kromme bevindt. Evenzo kan een scalaire vermenigvuldiging met dezelfde eigenschap gedefiniëerd worden. Een belangrijke observatie is dat wanneer de punten op de kromme niet langer genomen worden uit $\mathbb{R}$, maar uit een eindig lichaam $\mathbb{F}_p$ van priem orde p, deze eigenschappen behouden blijven. De resulterende grafiek van de kromme zal van aangezicht veranderen en begrensd worden in het vlak. Onder deze restricties is het mogelijk de verzameling punten $\mathrm{K}(\mathbb{F}_p)$ tezamen met de operatie van optelling van punten te nemen om een groep $\mathbf{G} = [\mathrm{K}(\mathbb{F}_p), +]$ te vormen. Merk op dat niet iedere kromme aan de voorwaarden om een welgedefiniëerde groep te vormen hoeft te voldoen, maar de voor cryptografische doeleinden voorgeschreven krommen dit wel doen. Merk tevens op dat, omdat $\mathbf{G}$ priem orde heeft, de groep cyclisch en daardoor abels is. Een opsomming van deze groep is als volgt:

- Voor alle punten P, Q op de kromme $\mathrm{K}(\mathbb{F}_p)$ geldt dat de som $P + Q$ op de kromme ligt. De groep $\mathbf{G}$ is gesloten onder de groepsoperatie.

- De groepsoperatie is associatief. Ofwel, voor $P, Q, R \in \mathbf{G}$ geldt $P + (Q + R) = (P + Q) + R$.

- Het toegevoegde punt in oneindig wordt gerelateerd aan het eenheidselement $e_{\mathbf{G}}$.

- Voor iedere $P \in \mathbf{G}$ bestaat een element $P^{-1} \in \mathbf{G}$ zodat $P + P^{-1} = P^{-1} + P = e_{\mathbf{G}}$.

Deze groepseigenschappen zijn niet vanzelfsprekend, maar behoeven een te uitgebreid bewijs voor dit verslag. Het volstaat te concluderen dat een groep bestaat welke correspondeert met de kromme $\mathrm{K}(\mathbb{R})$.