

Cryptografie met krommen

Reinier Bröker

Universiteit Leiden



Nationale Wiskundedagen
Februari 2006

Cryptografie

Cryptografie gaat over geheimschriften en het versleutelen van informatie.

Voorbeelden.

Klassieke oudheid: Caesarcode. In plaats van wiskunde schrijf ik xjtlvoef.

WO II: Enigma.

Moderne cryptografie gebruikt geavanceerde wiskunde.

Setting

Doel: ik wil mijn creditcardgegevens veilig versturen over internet.

Alle informatie op internet kan afgeluisterd worden.

Ik moet de gegevens dus *versleutelen*.



Voorbeeld

Versturen getal 1234:

Als beide partijen een *geheime sleutel* weten, zeg 7890, dan is het makkelijk.

Verstuur

$$1234 + 7890 = 9124.$$

De ontvanger decodeert

$$9124 - 7890 = 1234.$$

Een buitenstaander ziet enkel 9124 en kan hier niets mee zonder de geheime sleutel.

Afspreken geheime sleutel

Hoe spreek je een geheime sleutel af over internet?

Alle berichten worden onderscheept!

Oplossing: gebruik *elliptische krommen*.

Onderwerpen voor vandaag:

- ◇ wat zijn elliptische krommen?
- ◇ hoe kan ik ze gebruiken voor internet?

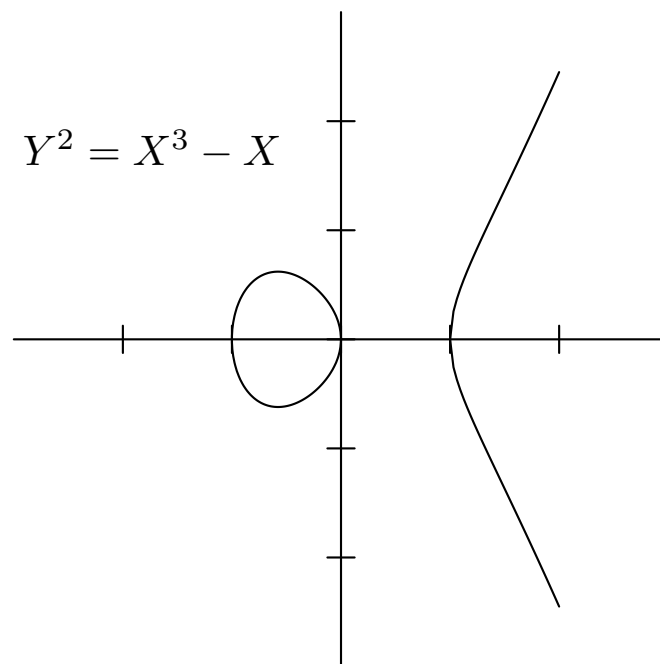
Elliptische kromme

Een elliptische kromme is een vergelijking

$$Y^2 = X^3 + aX + b.$$

Vandaag: $a = -1$, $b = 0$.

Plaatje:



Intermezzo: geschiedenis

In de 17e eeuw zocht men een methode om de booglengte van een ellips te bepalen.

Het blijkt dan te gaan om het berekenen van een *elliptische integraal*.

Elliptische integralen zijn objecten die ‘van nature leven’ op een vergelijking

$$Y^2 = X^3 + aX + b.$$

Elliptische krommen hebben enkel zeer indirect iets met ellipsen te maken!

De naam ‘elliptische kromme’ is meer historisch dan duidelijk...

Elliptische krommen in de 20e eeuw

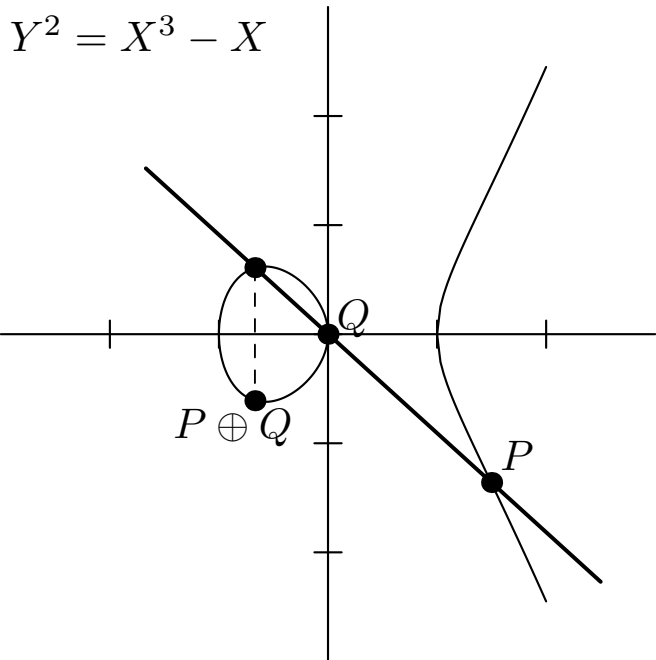
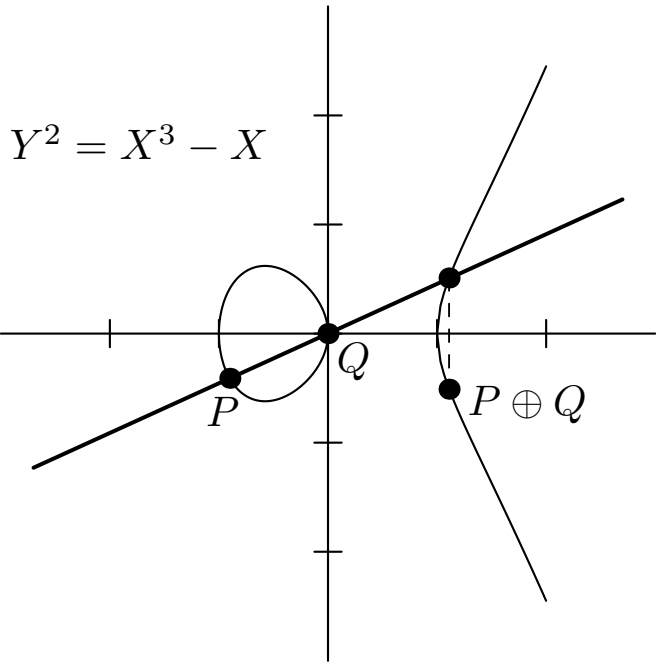
Zoals aangekondigd: elliptische krommen worden nu gebruikt in de *cryptografie*.

Iedere mobiele telefoon bevat nu al een elliptische kromme.

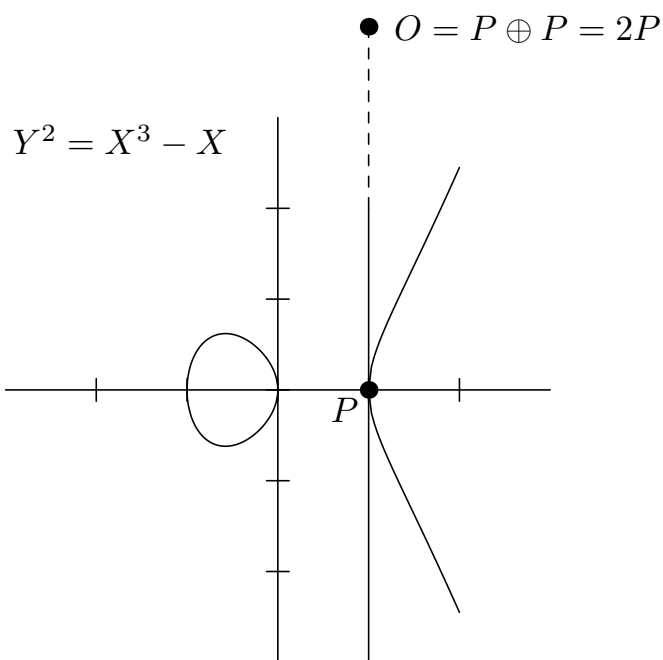
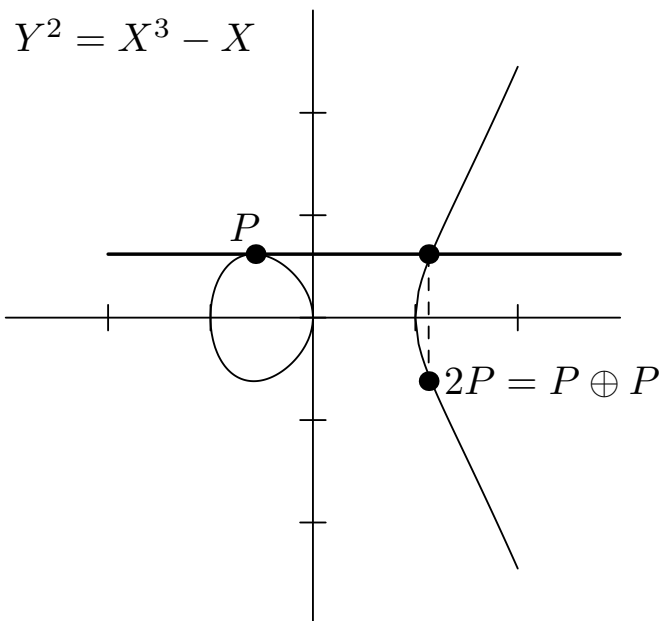
Voornaamste ingrediënt voor cryptografie:
Je kunt punten 'optellen' op een elliptische kromme.

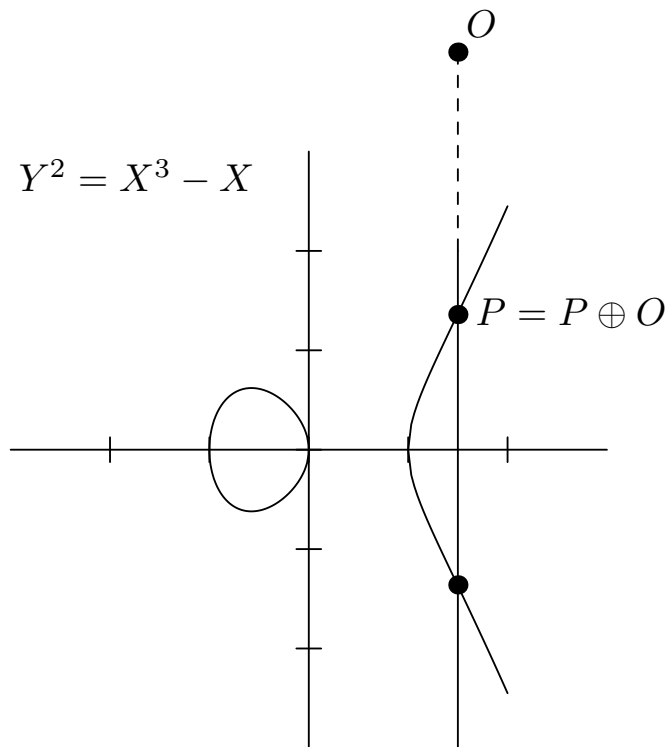


Punten optellen



Punt bij zichzelf optellen





Eigenschappen optelwet:

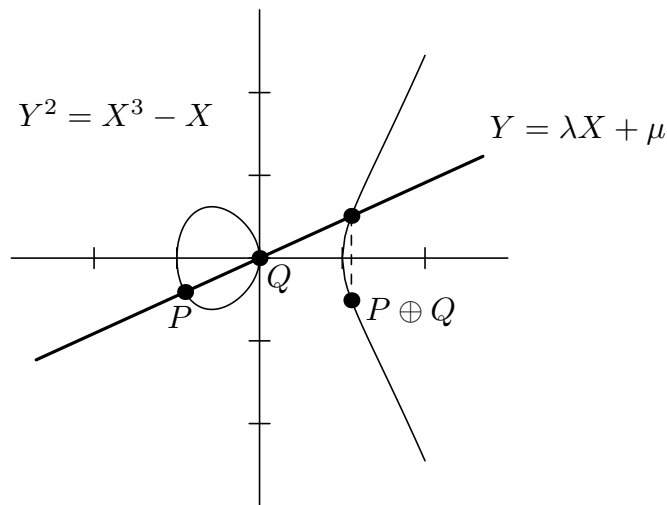
- ◇ $P \oplus Q = Q \oplus P$ voor alle punten P, Q ;
- ◇ $P \oplus O = P$ voor elk punt P ;
- ◇ $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ voor alle punten P, Q, R .

Dit zijn precies de eigenschappen van de gewone optelling op reële getallen!

Intermezzo: gebruik in klas

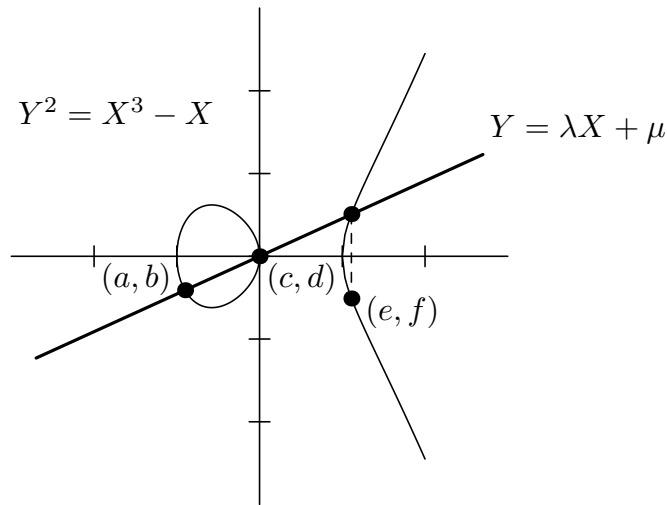
- ◇ geef de elliptische kromme $Y^2 = X^3 - X$
- ◇ geef 2 punten $P = (-0,90; -0,41)$ en $Q = (0, 0)$.
- ◇ vraag: bereken $P \oplus Q$. Met en zonder grafische rekenmachine?

Oplossing:



- ◇ stel vergelijking van de lijn op
- ◇ bereken de snijpunten van de lijn met de kromme.

Formule voor optelwet



Vergelijking lijn (repetitie-opgave?):

$$Y = \frac{b-d}{a-c}X + \frac{ad-bc}{a-c} = \lambda X + \mu.$$

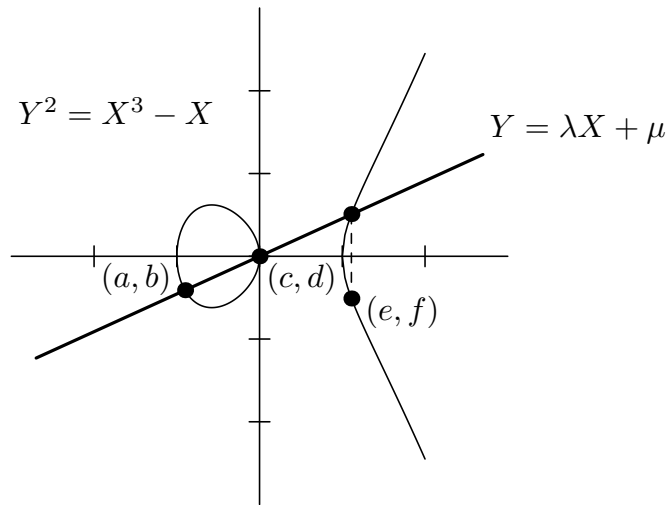
Invullen levert

$$(\lambda X + \mu)^2 = X^3 - X$$

ofwel

$$X^3 - \lambda^2 X^2 + (-2\lambda\mu - 1)X - \mu^2 = 0.$$

Formule voor optelwet, II



We weten:

$$\begin{aligned} X^3 - \lambda^2 X^2 + (-2\lambda\mu - 1)X - \mu^2 \\ \parallel \\ (X - a)(X - c)(X - e). \end{aligned}$$

Bekijk de coëfficiënten van X^2 . Er volgt:

$$\lambda^2 = a + c + e,$$

en dus:

$$\begin{cases} e = \lambda^2 - (a + c) \\ f = -\lambda e - \mu. \end{cases}$$

Terug naar cryptografie

Doel: afspreken van een geheim als *iedereen* meeluistert.

Stap 1. Maak de elliptische kromme $Y^2 = X^3 - X$ en het punt $P = (0,90, -0,41)$ bekend aan *iedereen*.

Stap 2. Ik kies een geheim getal n .

Stap 3. Ik bereken nP en verstuur dit naar de bank.

Stap 4. De bank kiest een geheim getal m .

Stap 5. De bank berekent mP en verstuurt dit naar mij.

Stap 6. Beide berekenen nu het geheim $m(nP) = n(mP) = nmP$.

Versleutelen van informatie

De x -coördinaat van nmP is de *geheime sleutel*.

Voorbeeld.

Voor $nmP = (123456789,70; 987654321,98)$ is de sleutel

$$123456789.$$

Versturen bericht.

Versturen geheim bericht 234098: bereken

$$234098 + 123456789 = 123690887.$$

De bank ontcijfert

$$123690887 - 123456789 = 234098.$$

Zijn elliptische krommen ‘veilig’?

Als de tegenpartij ook het punt nmP weet, is het systeem waardeloos.

De tegenpartij weet:

- ◇ de elliptische kromme
- ◇ het punt P op de kromme
- ◇ het punt nP op de kromme
- ◇ het punt mP op de kromme.

Vraag.

Is hieruit het punt nmP te berekenen?

Antwoord (denkt men).

Enkel als de tegenpartij het getal n of m kan bepalen.

Achterhalen geheime getal n

Idee 1. Bereken $P, 2P, 3P, \dots$ totdat je nP tegenkomt.

Voor cryptografie: $n \approx 10^{60}$.

Stel dat een supercomputer 10^{10} operaties per seconde doet.

Het vinden van n kost dan $\approx 10^{50}$ seconden.

Ter vergelijking: leeftijd heelal is $\approx 10^{18}$ seconden...

NB: We kunnen nP *wel* snel uitrekenen.
Idee berust op

$$256P = (2(2(2(2(2(2(2(2P)))))))).$$

Intermezzo: gebruik in klas

Bewustwording van *grote* getallen.

- Hoeveel inwoners heeft Nederland? ($\approx 10^7$)
- Wat is de lichtsnelheid? ($\approx 10^8$ m/s)
- Hoe hoog is de staatsschuld? ($\approx 10^{11}$ euro)
- Wat is de afstand van de aarde tot de zon?
($\approx 10^{11}$ meter)
- Wat is de leeftijd van het heelal?
($\approx 10^{18}$ seconde)
- Hoeveel 'posities' heeft Rubik's kubus?
($\approx 10^{19}$)
- Hoeveel atomen zijn er in het heelal?
($\approx 10^{80}$)

Achterhalen geheime getal n , II

Idee 2. We weten $nP = (x, y)$.

Uit het aantal cijfers van x kan je wellicht n afleiden?

Dit werkt! Elliptische krommen over *reële getallen* zijn **niet** veilig.

Oplossing: beperk kunstmatig het aantal cijfers: reken modulo N .

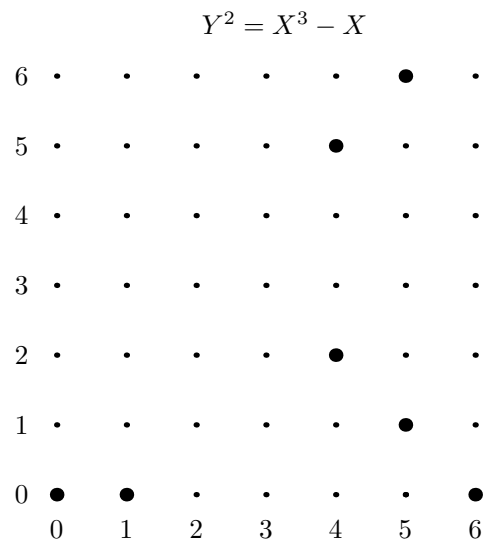
Rekenen modulo N

Twee gehele getallen zijn gelijk modulo N als hun verschil deelbaar is door N .

Voorbeeld.

$(N = 12)$ $17 = 5$, $-1 = 11$. *Klokkijken*

In cryptografie worden elliptische krommen ‘modulo N ’ gebruikt, met N priem.



Plaatjes zijn zinloos, maar de optel*formule* blijft geldig!

Een cryptografische kromme

Neem $N =$

123456789012345678901234567890

654833374525085966737125236501

(priem) en $a =$

788760296979961071205638260948

64556580999965110862558799913.

De elliptische kromme

$$Y^2 = X^3 + 4aX - 8a$$

is geschikt voor cryptografie.

Is dit nu echt veilig?

Elliptische krommen worden sinds 1985 gebruikt.

Iedere mobiele telefoon bevat een elliptische kromme.

Gevoelige informatie over internet wordt beveiligd met elliptische krommen.

Niemand heeft nog een goede ‘aanval’ kunnen bedenken.

Veiligheid berust in zekere zin op de *onkunde* van wiskundigen!

Het systeem kan in principe morgen gekraakt worden door iemand uit Zimbabwe.