Constructing elliptic curves of prescribed order

Bröker, R.

STELLINGEN

behorend bij het proefschrift

Constructing elliptic curves of prescribed order

van Reinier Bröker

1. Er bestaat een algoritme met als invoer een getal $N \in \mathbf{Z}_{\geq 1}$ en de priemfactorisatie van N, en als uitvoer een priemgetal p en een elliptische kromme $E/\mathbf{F}_p$ met $\#E(\mathbf{F}_p) = N$ wanneer een dergelijk paar (p, E) bestaat. Onder heuristische aannames bestaat een paar (p, E) voor alle N en is de verwachte rekentijd van de algoritme

$$O(2^{\omega(N)}(\log N)^{4+\varepsilon})$$

voor iedere $\varepsilon > 0$. Hier is $\omega(N)$ het aantal verschillende priemfactoren van N.

2. Er bestaat een algoritme die bij invoer van een priemgetal p een supersinguliere elliptische kromme geeft over $\mathbf{F}_p$. Als de gegeneraliseerde Riemannhypothese waar is, dan is de rekentijd $O((\log p)^{3+\varepsilon})$ voor iedere $\varepsilon > 0$.

3. Zij $p \geq 5$ een priemgetal, en zij $E/\mathbf{F}_p$ een gewone elliptische kromme. Neem aan dat de ring $\mathbf{Z}[\mathrm{Frob}]$ index 2 heeft in de endomorfismenring $\mathrm{End}(E)$, en dat de discriminant van $\mathrm{End}(E)$ niet deelbaar is door 3 en congruent is met 1 modulo 8. Dan heeft het polynoom

$$(X^{24} - 16)^3 - j(E)X^{24} \in \mathbf{F}_p[X]$$

exact 6 nulpunten in $\mathbf{F}_p$ voor $p \equiv 1 \bmod 3$, en exact 2 nulpunten voor $p \equiv 2 \bmod 3$. Het polynoom

$$(X^{24} + 16)^3 - j(E)X^{24} \in \mathbf{F}_p[X]$$

heeft exact 12 nulpunten in $\mathbf{F}_p$ voor $p \equiv 1 \bmod 3$, en exact 4 nulpunten voor $p \equiv 2 \bmod 3$.

4. Er bestaat een p-adische algoritme om het minimumpolynoom van een klasseninvariant te bepalen. In de praktijk is deze algoritme even snel als de complex-analytische algoritme.

5. Zij n een positief geheel getal. Met kans 1 bestaat er voor een willekeurig polynoom $f \in \mathbf{Z}[X]$ van graad n een priemgetal p zodat $f \bmod p$ irreducibel is.

6. Zij $E/\mathbf{Q}$ de elliptische kromme gegeven door $Y^2 = X^3 - 19$. Dan heeft de verzameling

$$\{p \text{ priem} \mid p \neq 2, 3, 19 \text{ en } E(\mathbf{F}_p) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \text{ met } n \text{ even}\}$$

natuurlijke dichtheid

$$\frac{201}{1292} \prod_{\substack{p \text{ priem} \\ p \equiv 1 \bmod 3}} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p \text{ priem} \\ p \equiv 2 \bmod 3}} \left(1 - \frac{1}{p^2 - 1}\right) \doteq 0{,}0935$$

binnen de verzameling priemgetallen.

7. Met

$$p = 120505190013010118000518001920010120001$$
$$151139038005258381565597004623870095187$$

en

$$a = 455817050190916629929488425728463793 36$$
$$384232274560126266522713072803226558862 \in \mathbf{F}_p,$$

heeft de kromme gegeven door

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

exact

$$120505190013010118000518001920010120001$$
$$618050309051900230120000518001920010120$$

punten over $\mathbf{F}_p$.

8. Er bestaat geen 'huisje' $\overset{\triangle}{\square}$ met zijden van geheeltallige lengte dat de eigenschap heeft dat de oppervlakte van de driehoek gelijk is aan de oppervlakte van het vierkant.

9. Het valt niet mee in de bergen op 5700 meter hoogte een zonsopkomst te fotograferen.

10. Een positief gevolg van de spellingwijziging in 1995 is dat nu zowel $\mathbf{Z}[i]$ als $\mathbf{Z}[\sqrt{-13}]$ een klassengroep hebben.

11. Het lopen van de Nijmeegse Vierdaagse is zowel de snelste als de meest vermoeiende manier een koninklijke onderscheiding te bemachtigen.