Complex multiplication of abelian surfaces

Streng, T.C.

Stellingen

behorend bij het proefschrift
Complex multiplication of abelian surfaces
van Marco Streng

1. Er bestaat een algoritme dat, gegeven een primitief vierdegraads CM-lichaam K, de Igusaklassenpolynomen van K uitrekent in tijd

$$\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2}).$$

   Hierbij is Δ_0 de discriminant van het reële kwadratische deellichaam K_0 van K en Δ_1 de norm van de relatieve discriminant van K over K_0.

2. Zij K een niet-normaal vierdegraads CM-lichaam. Dan is het aantal $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-banen van $\overline{\mathbf{Q}}$-isomorfieklassen van krommen van geslacht 2 met complexe vermenigvuldiging met de maximale orde van K een macht van 2.

3. Zij K een CM-lichaam met maximaal reëel deellichaam K_0 en zij Φ een CM-type van K. Noteer het reflexlichaam van Φ met K^{r} en het reflextype met Φ^{r}. Zij M het lichaam van moduli van een gepolariseerde abelse variëteit met CM van type Φ^{r} met de ring van gehelen van K^{r}.

   Dan is MK/K_0 normaal met Galoisgroep

$$\mathrm{Gal}(MK/K_0) \;\cong\; \mathrm{Gal}(MK/K) \rtimes \mathrm{Gal}(K/K_0),$$

   waarbij $\mathrm{Gal}(MK/K)$ een quotiënt is van de ideaalklassengroep Cl_K van K waarop $\mathrm{Gal}(K/K_0) \cong C_2$ werkt door middel van het nemen van inversen.

4. De complexe hoofdgepolariseerde abelse oppervlakken met een $(2,2)$-isogenie naar zichzelf corresponderen met de punten van één irreducibel Humbertoppervlak en eindig veel andere punten.

5. Zij E een elliptische kromme over een getallenlichaam L en zij $P \in E(L)$ een punt van oneindige orde. Noteer de endomorfismering van E met $\mathcal{O}$. Dan is er voor alle $\mathcal{O}$-idealen $\mathfrak{a}$, op eindig veel na, een priem $\mathfrak{p}$ van L zodat $\mathfrak{a}$ de annihilator is van $(P \bmod \mathfrak{p})$.

Met een *primitieve deler* van een term B_n in een rij gehele getallen $B_1, B_2, B_3, \ldots$ bedoelen we een priemgetal p dat de term B_n deelt, maar geen eerdere termen in de rij.

6. Er is een unieke rij gehele getallen die begint met $B_1 = 1$, $B_2 = 4$, $B_3 = -36$, $B_4 = -448$ en voldoet aan

$$B_{m+n}B_{m-n} = B_{m+1}B_{m-1}B_n^2 - B_{n+1}B_{n-1}B_m^2$$

voor alle gehele getallen $m \geq n \geq 2$.

Gegeven een positief geheel getal n, laat s het aantal priemgetallen p zijn die n delen en rest 1 of 3 hebben bij deling door 8. Voor alle positieve gehele getallen n, op eindig veel na, heeft B_n tenminste $s+1$ primitieve delers, waaronder tenminste s die rest 1 of 3 hebben bij deling door 8.

7. Er bestaat een algoritme met invoer een positief geheel getal k, een niet-normaal vierdegraads CM-lichaam K, en een priemgetal $r \equiv 1 \pmod{2k}$ dat volledig splitst in K, zodat, als het algoritme eindigt, de uitvoer bestaat uit een priemgetal p en een geslacht-2-kromme $C/\mathbf{F}_{p^2}$ met p-rang 1 en CM met $\mathcal{O}_K$, zodat $J(C)(\mathbf{F}_{p^2})$ een ondergroep van orde r heeft met inbeddingsgraad k, en zodat geldt $\log \#J(C)(\mathbf{F}_{p^2}) \approx 16 \log r$. Naast het triviale algoritme bestaat er ook een algoritme met de genoemde eigenschappen dat voor de meeste K een heuristische looptijd polynomiaal in $\log r$ heeft.

8. Dit is de beste noch de slechtste tijd voor supersinguliere abelse variëteiten in de cryptologie.

9. Bij het lezen van een Engelstalige wiskundetekst kan het een groot voordeel opleveren het verschil tussen 'which' en 'that' te kennen. Het kan ook kleine irritaties opleveren.

10. Het weglaten van trema's in email is een slechte gewoonte.

11. Eén van de meest gangbare afstandsbegrippen in het openbaar vervoer, de reistijd, voldoet niet aan de driehoeksongelijkheid.

12. Beschouw het polynoom

$$\begin{aligned} f = \; & 127^4 281^2 X^4 \\ & - 997691447037028736007137864988287640 X^3 \\ & + 216828302684042094592462046363702878416549094730940 0 X^2 \\ & + 120705291850874391830424802937983070574734193436369380000 X \\ & - 606989693442504390905950710479181446796615241114849105110000 \quad \in \mathbf{Z}[X]. \end{aligned}$$

Zij p een priemgetal copriem met de discriminant van f. Het getal p is van de vorm

$$p = \left(w + x\sqrt{2}\right)^2 + 17(2 - \sqrt{2})\left(y + z\sqrt{2}\right)^2$$

voor gehele getallen w, x, y en z precies dan als zowel f als het polynoom $Y^4 + 68Y^2 + 578 \in \mathbf{Z}[Y]$ een nulpunt heeft modulo p.