ALGORITHMEN VOOR DIOPHANTISCHE VERGELIJKINGEN.

SAMENVATTING.

Deze dissertatie gaat over het oplossen van *diophantische vergelijkingen*. Dat zijn vergelijkingen waarbij de oplossingen beperkt zijn tot gehele getallen. In dit boek worden alleen diophantische vergelijkingen bestudeerd die zijn op te lossen met behulp van de methode van Gelfond-Baker. De gebruikte methode kent ruwweg drie stappen.

In de eerste stap vormt men de vergelijking om tot een exponentiële vergelijking of ongelijkheid, d.i. één waarin de onbekenden alleen in de exponenten voorkomen. Als zo'n exponentiële vergelijking drie, en zo'n exponentiële ongelijkheid twee termen bezit, is ze gemakkelijk om te vormen tot een ongelijkheid voor een p-adische respectievelijk reëel/complexe lineaire vorm in logarithmen van algebraische getallen

$$\Lambda = \log \alpha_0 + \sum_{i=1}^{n} x_i \cdot \log \alpha_i \ .$$

Hierin zijn de x_i de onbekenden, die in $\mathbb{Z}$ liggen. Voor deze lineaire vorm Λ geldt nu dat ze extreem dicht bij 0 ligt voor grote waarden van de onbekenden, nl. er zijn constanten c, δ zodat met $X = \max|x_i|$ geldt dat

$$|\Lambda| < c \cdot \exp(-\delta \cdot X) \ .$$

De tweede stap bestaat in het toepassen van één van de diepe resultaten van de Gelfond-Baker theorie, die voor dergelijke lineaire vormen in logarithmen van algebraische getallen ondergrenzen geeft van de vorm

$$|\Lambda| > \exp\left(-(C_1 + C_2 \cdot \log X)\right)$$

voor constanten C_1, C_2. Het vergelijken van ondergrens en bovengrens voor $|\Lambda|$ levert een absolute bovengrens voor X op. Zo is het probleem eindig geworden, maar nog niet triviaal. De gevonden bovengrens voor X is namelijk vrijwel altijd bijzonder groot, in een typisch geval in de orde van grootte van 10^{40} .

De derde stap van de methode beoogt nu alle oplossingen van de diophantische vergelijking onder deze bovengrens te vinden met behulp van een computer. De grootte van de bovengrens maakt het echter noodzakelijk dit op een slimme manier te doen. Vrijwel altijd blijkt dat de werkelijk grootste oplossing ver onder de bovengrens ligt. Daarom is het de moeite waard om naar methoden te zoeken om dergelijke bovengrenzen te reduceren. In dit proefschrift, met name in hoofdstuk 3, worden zulke methoden gegeven voor verschillende typen van lineaire vormen Λ . Algemeen kenmerk van deze methoden is dat de redelijke verwachting bestaat dat ze een bovengrens van grootte-orde X_0 kunnen reduceren tot de grootte-orde $\log X_0$ (bv. van 10^{40} tot 1000).

Deze methoden liggen op het terrein van de diophantische approximatie van lineaire vormen. Ze zijn soms gebaseerd op klassieke ideeën, zoals het kettingbreukalgorithme, soms ook op het recente 'L^3-algorithme' voor het reduceren van bases van roosters. Het bestaan van een extreem grote oplossing van de diophantische vergelijking (in de orde van grootte van $\log X_0$ tot X_0) kan vertaald worden in het bestaan in een bepaald rooster van een roosterpunt met een extreem korte lengte, of extreem dicht bij een gegeven punt buiten het rooster. Het L^3-algorithme is in staat aan te tonen dat zulke extreme roosterpunten niet bestaan, ofwel welke dat zijn.

Als eenmaal een voldoende gereduceerde bovengrens gevonden is, kunnen alle oplossingen eronder gevonden worden met bv. een recht-toe-recht-aan methode. Zo kan de diophantische vergelijking volledig worden opgelost in enkele minuten rekentijd op een mainframe computer.

Deze methode wordt in dit proefschrift op verschillende diophantische problemen losgelaten. We geven een kort overzicht. Laten $p_1, \ldots, p_s$ vaste priemgetallen zijn. Zij S de verzameling van positieve gehele getallen die slechts deze priemgetallen als priemfactoren hebben.

Hoofdstuk 4 geeft een algorithme voor het bepalen van alle elementen van een gegeven binaire recurrente rij (zoals de rij van Fibonacci) die in S liggen. Een toepassing is de gegeneraliseerde Ramanujan-Nagell vergelijking $x^2 + k \in S$ voor een gegeven geheel getal k .

Hoofdstuk 5 bestudeert het probleem van elementen in S die dicht bij elkaar liggen, bv. $0 < x - y < \sqrt{y}$ met $x, y \in S$. In hoofdstuk 6 komt de vergelijking $x + y = z$ met $x, y, z \in S$ aan de orde. Beide problemen leiden direct tot een ongelijkheid voor een lineaire vorm in logarithmen, zodat ze de simpelste voorbeelden zijn van de toepassing van de diophantische approximatiemethoden gebaseerd op het L^3-algorithme. Ze worden volledig opgelost voor $p_1, \ldots, p_6 = 2, 3, 5, 7, 11, 13$. Als bijprodukt wordt de relatie

$$3^2 \cdot 5^6 \cdot 7^3 + 11^2 = 2^{21} \cdot 23$$

gevonden, die interessant is in verband met het de laatste tijd in het middelpunt van de belangstelling van de getaltheoretici staand 'abc-vermoeden'.

In hoofdstuk 7 wordt een methode gegeven om alle elementen x, y met $x \in S$, $\pm y \in S$, zodat $x + y$ een kwadraat is, te bepalen. Dat wordt uitgevoerd voor $p_1, \ldots, p_4 = 2, 3, 5, 7$. Hoofdstuk 8 behandelt een methode om de algemene Thue vergelijking $F(X,Y) = m$ voor een irreducibele binaire vorm F van graad ≥ 3 met variabelen $X, Y \in \mathbb{Z}$, en met $m \in \mathbb{Z}$ vast, volledig op te lossen. Deze methode wordt toegepast op de diophantische vergelijking $y^2 = x^3 - 4 \cdot x + 1$. Tenslotte wordt een eerste aanzet gegeven voor het behandelen van de Thue-Mahler vergelijking $F(X,Y) \in S$, met F als bij de Thue vergelijking.