SOLVING NORM FORM EQUATIONS OVER NUMBER FIELDS

Paraskevas Alvanos
Dimitrios Poulakis

pari

Pell Equation

$$x^2 - dy^2 = 1$$

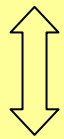
where *d* integer > *1*.

(x_1, y_1): the least positive solution of Pell equation ordered by the value of $x_1 + y_1\sqrt{d}$

Solutions:

$$x_n + y_n\sqrt{d} = \pm(x_1 + y_1\sqrt{d})^n, \quad \mathrm{n} \in \mathbb{Z}$$

Solving the Pell Equation



Determining the unit group

$$\left\langle x_1 + y_1\sqrt{d} \right\rangle \text{ of } \mathbb{Z}[\sqrt{d}]$$

Computing of Pell Equation

- J.Buchmann and H.C.Williams (1988). Deterministic $O(d^{1/4+\varepsilon})$-algorithm.
- R.deHaan, M.J.Jacobson Jr, H.C.Williams (2007). Deterministic $O(d^{1/6+\varepsilon})$-algorithm, under the assumption of the Generalized Riemann Hypothesis.

•C.S. Abel (1994) and U.Vollmer (2000). Subexponential probabilistic algorithms, under the assumption of the Generalized Riemann Hypothesis.

•V. Arvind and P.P. Kurur (2004). Pell's equation is in the complexity class SPP.

•S.Hallgren (2007). Polynomial-time quantum algorithm.

Generalized Pell Equation

$$x^2 - dy^2 = k$$

Solutions: The elements of $\mathbb{Z}[\sqrt{d}]$ with norm equal to k.

Solving: 1. We find a maximal set of pairwise non associate elements of $\mathbb{Z}[\sqrt{\mathrm{d}}]$ with norm k

2. We solve the pell equation $x^2 - dy^2 = 1$

Some recent methods have been given by:

- K. Matthews, 2000
- R. A Mollin, 2001

Applications of Pell Equation

- Construction of pseudorandom number generators
- Elliptic curves suitable for cryptographic applications
- Cryptographic applications of the Pell equation over finite fields or the rings $\mathbb{Z}_N$.

Pell Equation Over Number Fields

$x^2 - dy^2 = 1$

- 1842, Dirchlet, Pell Equation over $\mathbb{Z}[i]$.
- 1943, Niven, Pell Equation oven any quadratic field.
- 2001, Shastri, Pell Equation over any number field for $d = -1$.
- 2006, Schmid, determined the structure of the solutions of Pell Equation over any number field for any algebraic integer, d.

Structure of the solutions of Pell Equation over Number Fields

K: Number field

O_K: The ring of integers of K

$d \in O_K$

$C_K^d = \{(x, y) \in O_K \mid x^2 - dy^2 = 1\}$

For $(x_1,y_1),(x_2,y_2) \in K^2$ we define

$(x_1,y_1)\times(x_2,y_2)= (x_1x_2+dy_1y_2,\ x_2y_1+x_1y_2)$

$(C_K^d,\times)$ abelian group

Schmids Structure Theorem (2006)

***r_1*:** The number of real embeddings of K

***r_2*:** The number of conjugated pairs of complex embeddings of K

***$\rho(a)$*:** The number of real embeddings σ, with $\sigma(a)>0$, for $a \in \mathrm{O_K}$

Theorem:

$$\mathrm{C_K^d} \cong \begin{cases} C_m \times \mathbb{Z}^{\rho(r_1)+r_2} & \text{if } \sqrt{d} \notin K \\ C_m \times \mathbb{Z}^{r_1+r_2-1} & \text{if } \sqrt{d} \in K \end{cases}$$

where C_m cyclic, $m = 4$, if $\sqrt{-d} \in O_K$ and $m = 2$ otherwise.

The Problem

- L: finite extension of K with $[L:K] = \ell$,
- $\omega_1=1, \omega_2,\ldots,\omega_\ell$: K-linearly independent integers of L,
- $k \in O_K$,
- $N_{L/K}(a)$: Relative Norm of a over K. That is the product of the roots of the minimal polynomial of a over K

Find $(x_1,\ldots,x_\ell)$, $x_i \in O_K$ such that

$$N_{L/K}(x_1\omega_1+\cdots+x_\ell\omega_\ell) = k$$

The Pell Equation over Number Fields

For $\ell = 2$ and $\omega_2 = \sqrt{d}$

$$N_{L/K}(x_1 + x_2\sqrt{d}) = k \Rightarrow$$

$$x_1^2 - dx_2^2 = k$$

Solutions of the equation

$$N_{L/K}(x_1\omega_1 + \cdots + x_\ell\omega_\ell) = 1$$

R^* : Unit Group of R (Integral Domain)

$$N : O_K[\omega_2, ..., \omega_\ell]^* \to O_K{}^*$$

$$x_1\omega_1 + \cdots + x_\ell\omega_\ell \to N_{L/K}(x_1\omega_1 + \cdots + x_\ell\omega_\ell)$$

$$(x_1, ..., x_\ell) : solution \Leftrightarrow x_1\omega_1 + \cdots + x_\ell\omega_\ell \in Ker(N)$$

The Kernel of N

$Ker(N) \cong \langle \zeta \rangle \times \langle \varepsilon_1, \ldots, \varepsilon_\mu \rangle$

- $\zeta = \tau_1 \omega_1 + \cdots + \tau_\ell \omega_\ell$
- $\varepsilon_j = x_{j1} \omega_1 + \cdots + x_{j\ell} \omega_\ell$, $j=1,\ldots,\mu$

Fundamental set of solutions:
$(x_{j1}, \ldots, x_{j\ell})$, for $j=1,\ldots,\mu$
Torsion Solution:
$(\tau_1, \ldots, \tau_\ell)$

Theorem of Structure

Let r_1 (respectively s_1) be the number of real embeddings and r_2 (respectively s_2) the number of conjugated pairs of complex embeddings of K (respectively L). Let F be a fundamental set of solutions for the norm form equation

$$N_{L/K}(x_1\omega_1 + \cdots + x_\ell\omega_\ell) = 1$$

Then

$$|F| = s_1 + s_2 - r_1 - r_2$$

Solving the Equation

$$N_{L/K}(x_1\omega_1 + \cdots + x_\ell\omega_\ell) = 1$$

Algorithm 1

Input: K, L, $\{1,\omega_2,\ldots,\omega_\ell\}$

Output: A set of Fundamental Solutions F and a Torsion Solution ζ

1. Compute a basis $\{\varepsilon_1,...,\varepsilon_r\}$ of the group $O_K[\omega_2,...,\omega_\ell]^*$, where $\varepsilon_i = \varepsilon_{i,j}\omega_1 + \cdots + \varepsilon_{i,\ell}\omega_\ell$
2. Compute the set $\{\lambda_1,...,\lambda_r\}$, where $\lambda_i = N(\varepsilon_i)$
3. Compute a basis $z_j = \{z_{j1},...,z_{jr}\}$, $j = 1,...,s$ for the lattice $\Lambda = \left\{(x_1,...,x_r) \in \mathbb{Z}^r / \lambda_1^{x_1} \cdots \lambda_r^{x_r} = 1\right\}$
4. Compute the set $F := \{b_1,...,b_s\}$, $b_j = \varepsilon_1^{z_{j,1}} \cdots \varepsilon_r^{z_{j,r}}$
5. Compute a generator ζ for the torsion subgroup of *Ker(N)*
6. Output the set F and ζ.

$$N : O_K[\omega_2, \ldots, \omega_\ell]^* \rightarrow O_K^*$$

$$\{\zeta\}, \{\varepsilon_1, \ldots, \varepsilon_r\} \longrightarrow \{\eta\}, \{\lambda_1, \ldots, \lambda_r\}$$

KASH or MAGMA

$O(RD^{\varepsilon})$

GAP

$$\left\langle \zeta^z \right\rangle \times \left\langle \varepsilon_1^{z_{1,1}} \cdots \varepsilon_r^{z_{1,r}}, \ldots, \varepsilon_1^{z_{s,1}} \cdots \varepsilon_r^{z_{s,r}} \right\rangle \longleftarrow \{z\}, \{z_{j,1}, \ldots, z_{j,r}\}, j = 1, \ldots, s$$

Solutions of the Equation

$$N_{L/K}(x_1\omega_1 + \cdots + x_\ell\omega_\ell) = k$$

$W=\{w_1,\ldots,w_t\}$ is a maximal set of pairwise non associate elements of $O_K[\omega_2,\ldots,\omega_\ell]$ with $N_{L/K}(w_i)=k$

$(x_1,\ldots,x_\ell)$ solution

$\Updownarrow$

$\exists\, w_i \in W, \eta = \eta_1\omega_1 + \cdots + \eta_\ell\omega_\ell \in O_K[\omega_2,\ldots,\omega_\ell]^*$ such that

$$x_1\omega_1 + \cdots + x_\ell\omega_\ell = \eta w_i$$

Algorithm 2

Input: $K, L, k, \omega_1, \ldots, \omega_\ell$

Output: Solutions of $N(x_1\omega_1 + \cdots + x_\ell\omega_\ell) = k$

1. Determine a maximal set $\{w_1, .., w_t\} \subseteq O_K[\omega_2, \ldots, \omega_\ell]$ of pairwise non associate elements with $N_{L/K}(w_i)=k$. If the set is empty output "*The equation has no solutions*". Else go to step 2
2. Using *Algorithm 1*, compute a set F of fundamental solutions and a torsion solution ζ for the equation $N(x_1\omega_1 + \cdots + x_\ell\omega_\ell) = 1$
3. Output the elements obtained by step 1 and 2

Complexity

For $O_K[\omega_2,\ldots,\omega_\ell]$ maximal order the running time of computing a maximal set of pairwise non associate elements with $N_{L/K}(w_i)=k$ is

$$O\left(\ell^{(r+\ell)}\left|N_{K/\mathbb{Q}}(k)\right|\frac{reg_{L/K}(L)}{\sqrt{\left|d_{L/K}\right|}}\right)$$

Example 1. Let ω root of t^4+3t^2-2t-5. Solve

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(x_0+x_1\omega+x_2\omega^2+x_3\omega^3)=16$$

Solution: $N_{\mathbb{Q}(\omega)/\mathbb{Q}}:\mathbb{Q}[\omega]^* \rightarrow \{-1,1\}$

$$\{-1\},\{\omega+1,-2\omega^2+\omega+2\} \longrightarrow \{1\},\{1,-1\}$$

$$\downarrow$$

$$\langle -1\rangle \times \langle \omega+1,(-2\omega^2+\omega+2)^2\rangle \longleftarrow \{1\},\{(1,0),(0,2)\}$$

We compute a maximal set W of pairwise non associate elements of $\mathbb{Z}[\omega]$ with Norm 16.

$$W=\{2,-\omega^3-2\omega^2+2\omega+3,\ -12\omega^3+7\omega^2+13\omega-3\}$$

Solutions: $(x_0,x_1,x_2,x_3) \in \mathbb{Z}$ such that

$$x_0 + x_1\omega + x_2\omega^2 + x_3\omega^3 = \pm(\omega+1)^m\,(-4\omega^3-19\omega^2+12\omega+24)^n\,w$$

Where $n,m \in \mathbb{Z}$ and $w \in W$

Example 2: Solve over $O_K = \mathbb{Z}[\sqrt{6}]$

$$x^2 - 7y^2 = -17 + 4\sqrt{6}$$

Solution: for $K = \mathbb{Q}(\sqrt{6})$ and $L = K(\sqrt{7})$

$$N_{L/K}(x+y\sqrt{7}) = -17 + 4\sqrt{6}$$

$$N : O_K[\sqrt{7}]^* \rightarrow O_K{}^*$$

$$\{-1\}, \{\sqrt{6}+\sqrt{7}, 5-2\sqrt{6}, 8+3\sqrt{7}\} \rightarrow \{-1\}, \{1, 49-20\sqrt{6}, 1\}$$

$$\langle -1\rangle \times \langle (\sqrt{6}+\sqrt{7})^2, 8+3\sqrt{7}\rangle \leftarrow \{2\} \cup \{(2,0,0),(0,0,1)\}$$

We compute a maximal set W of pairwise non associate algebraic integers of $O_K[\sqrt{7}]$ with Norm -17+4$\sqrt{6}$

$$W = \{1 + 2\sqrt{6} \pm \sqrt{6}\sqrt{7}\}$$

Solutions: $(x,y) \in O_K$ such that

$$x + y\sqrt{7} = \pm(8 + 3\sqrt{7})^n \ (13+2\sqrt{6}\sqrt{7})^m \ \text{w}$$

Where $n,m \in \mathbb{Z}$ and $w \in W$

Example 3. Let a root of t^5-3t^2+1. Solve

$$x^2-(1-a^2)y^2 = 2a^2+a^3-a^4$$

Solution: for $K=\mathbb{Q}(\alpha)$ and $L=K(\sqrt{1-\alpha^2})$

$$N_{L/K}(x+y\sqrt{1-\alpha^2}) = 2\alpha^2+\alpha^3-\alpha^4$$

$$\mathrm{N}: \mathrm{O_K}[\sqrt{1-a^2}]^* \rightarrow \mathrm{O_K}^*$$

The solution are $(x,y) \in O_K$ such that

$$x + y\sqrt{1-a^2} = \pm \prod_{i=1}^{3} (\gamma_i + \delta_i \sqrt{1-a^2})^{z_i} (\pm\kappa + \lambda\sqrt{1-a^2})$$

where $z_1, z_2, z_3 \in \mathbb{Z}$ and

$$\gamma_1 = -29 - 62\alpha + 8\alpha^2 + 10\alpha^3 + 22\alpha^4$$

$$\gamma_2 = 7 - 6\alpha^2 + 2\alpha^3$$

$$\gamma_3 = -3\alpha + \alpha^4$$

$$\kappa = 10 + 18\alpha - 2\alpha^2 - 4\alpha^3 - 6\alpha^4$$

$$\delta_1 = -46 - 60\alpha + 8\alpha^2 + 16\alpha^3 + 22\alpha^4$$

$$\delta_3 = 3\alpha - \alpha^4$$

$$\lambda = -13 + 22\alpha - 3\alpha^2 - 5\alpha^3 - 8\alpha^4$$

Example 4. Let a root of $t^3 - t + 1$ and $K=\mathbb{Q}(a)$. Let b be a root of $t^3 - (1-a+2a^2)t^2 - a$.

$L=K(b)$ and $\omega = -1 + \alpha + (1-\alpha+\alpha^2)b^2$. Then the solutions $(x_1,x_2,x_3) \in \mathbb{Z}[a]$ of the equation

$$N_{L/K}(x_1 + x_2\omega + x_3\omega^2) = a^2 - a - 3$$

are given by

$$x_1 + x_2\omega + x_3\omega^2 = \prod_{i=1}^{4} (\mu_i + \nu_i\omega + \xi_i\omega^2)^{z_i}\,\Omega$$

Where $z_1,z_2,z_3,z_4 \in \mathbb{Z}$,

$$\Omega = (-13\alpha+21)\omega^2 + (-1754a^2 + 2269a - 1280)\omega - 1654\alpha^2 + 2178a - 1223$$

$$\mu_1 = -\alpha^2 + 1, \qquad \mu_2 = -35\alpha^2 - 7\alpha + 40,$$

$$\nu_1 = -\alpha^2 + 1, \qquad \nu_2 = -91\alpha^2 - 59\alpha + 67,$$

$$\xi_1 = 0, \qquad \xi_2 = -83\alpha^2 - 70\alpha + 532,$$

$$\mu_3 = -169163\alpha^2 - 210187\alpha + 577987,$$

$$\nu_3 = -192789\alpha^2 - 635482\alpha + 506567,$$

$$\xi_3 = -254575\alpha^2 - 253327\alpha + 111177,$$

$$\mu_4 = -1429\alpha^2 - 1778\alpha - 875,$$

$$\nu_4 = -1743\alpha^2 - 1865\alpha + 989,$$

$$\xi_4 = -71\alpha^2 - 29\alpha + 120,$$

thank you