Norm Form Equations and Linear Divisibility Sequences

Elisa Bellah · University of Oregon

Abstract

Finding integer solutions to norm form equations is a classic Diophantine problem. Using the units of the associated coefficient ring, we can produce sequences of solutions to these equations. It turns out that such a sequence can be written as a tuple of integer linear recurrence sequences, each with characteristic polynomial equal to the minimal polynomial of our unit. We show that in some cases, these sequences are linear divisibility sequences.

Background and Motivation

Let $K$ be a number field, and let $W = \{w_1, \ldots, w_n\}$ be a $Q$-linear independent subset of $K$.

Definition 1. The norm form associated to $W$ is the rational form $F_W$ defined by

$$F_W(x_1, \ldots, x_n) := N_K(x_1w_1 + \cdots + x_nw_n).$$

We are interested in studying integer solutions to equations

$$F_W(x_1, \ldots, x_n) = c,$$

where $c$ is a fixed nonzero integer.

Modules Associated to Norm Forms

Fact. Up to integral equivalence, every norm form is associated to a unique module $M$ in $K$, as follows:

$$F_W \mapsto \text{Module generated by } W$$

This demonstrates the following important observation.

Key Observation. Finding integer solutions to the norm form equation $F_W(x_1, \ldots, x_n) = c$ is equivalent to finding elements in the associated module $M$ of fixed norm $c$.

Theorem 1. Let $F_W$ be a norm form, and $M$ its associated module. If $M$ is full, then the set of elements in $M$ of fixed norm $c$ is equivalent to a disjoint union of finitely many families of the form

$$\alpha_1O_K^n + \cdots + \alpha_dO_K^n,$$

where $O_K^n$ denotes the units in $O_K$ of positive norm.

Solutions Sequences

By Theorem 1 and Dirichlet’s Unit Theorem, every element in the module $M$ of fixed norm $c$ can be written in the form $x = \sum a_iu_i$, where $u_i$ is a fundamental unit in $O_K^n$.

Theorem 2. The sequences $x_i(k)$ above are linear recurrence sequences, with characteristic polynomial equal to the minimal polynomial of $c$.

A Divisibility Property

Definition 2. A sequence $a(k)$ is called a linear divisibility sequence (LDS) if $a(n) \mid a(m)$ whenever $n \mid m$.

Lemma 1. Let $a(k)$ be an order 2 linear recurrence sequence. If $a(0) = 0$, then $a(k)$ is a LDS.

In our Pell equation example, we saw that $x_i(k)$ was an order 2 linear recurrence sequence with $x_i(0) = 0$. So, by Lemma 1, $x_i(k)$ is a LDS.

Main Question: Does this divisibility property hold for other norm form equations? More precisely, given our module so that the sequence $x_i(k) = (\sqrt{c}x_i^k)$ is a LDS?

Philosophy: Linear divisibility sequences have particularly nice properties. So, if you are interested in learning about a linear recurrence sequence, it is a good idea to first check if your sequence is a LDS.

Real Biquadratic Extensions

It turns out that if $c$ is a real quadratic unit, then there is always a choice of basis so that the sequence $x_i(k)$ is a LDS. A natural next step is to consider norm forms over real biquadratic extensions. Let $K$ be such an extension with quadratic subfields $L_1, L_2$, and $L_3$.

Theorem 3 ([2]). Let $\epsilon_i$ denote the fundamental unit in $O_{L_i}$ for $i = 1, 2, 3$. Then, we can always find a system of fundamental units for $O_{L_i}$ whose elements are one or more of the following forms: $c_1\sqrt{\epsilon_1}, \sqrt{c_2}, \sqrt{c_3}, \sqrt{c_4}\epsilon_1, \sqrt{c_5}\epsilon_1\epsilon_2, \sqrt{c_6}\epsilon_1\epsilon_3, \sqrt{c_7}\epsilon_1\epsilon_2\epsilon_3, \sqrt{c_8}\epsilon_1\epsilon_2\epsilon_3\epsilon_4$.

So, to answer our main question for real biquadratic extensions, we should first investigate the sequences associated to these four possibilities for fundamental units.

Main Result

Let $K$ be a real biquadratic extension, as before.

Theorem (B). Let $M$ be a full module in $K$, and suppose that $\sqrt{z} \in O_K$ for some $z \in O_K$. For any $\beta \in M$, let $M_\beta$ be the submodule generated by $(\beta \sqrt{z}^k \mid k \in Z)$. Then, there exists a choice of basis for $M_\beta$ so that the norm form sequence $x_i(k) = (\sqrt{\gamma}x_i^k)$ is a LDS.

Idea for Proof

We use Theorem 2 to show that $x_i(k)$ satisfies recurrence

$$x_i(k + 4) = 3x_i(k) + 2x_i(k - 1) + x_i(k - 2).$$

Using results in [3] we then show that there exists a choice of basis for $M_\beta$ so that our sequence has initial conditions $x(0) = 0, x(1) = x(2) = 1, x(3) = x(4) = 1$.

This implies that

$$x_i(k) = \begin{cases} u_0, & \text{if } k = 2n \\ u_{n+1} + u_n, & \text{if } k = 2n + 1, \end{cases}$$

where $u_n$ is the Lucas sequence with characteristic roots $\epsilon$ and $\bar{\epsilon}$. We use Lucas sequence identities and elementary methods to show that the desired divisibility property holds in all cases.

Future Work

• Finish the remaining two cases for fundamental units in biquadratic extensions.
• Determine whether results in [2] generalize to real multiquadratic extensions, and study norm forms here.
• Investigate what the characterization of divisibility sequences in [1] might imply in this context.

References