Elemente der Mathematik 81 (2026), 176–178
DOI 10.4171/EM/579

© 2026 Swiss Mathematical Society
Published by EMS Press
This work is licensed under a CC BY 4.0 license

Short note

A note on integers represented by quadratic norm forms

Bayarmagnai Gombodorj

Abstract. In this note, we revisit the classical question of which integers can be represented as norms of algebraic integers in a given Euclidean quadratic field. We present a proof based on basic properties of finite groups.

Euclidean quadratic fields

Let d be a square-free integer not equal to 0 or 1. The ring of integers $\mathcal{O}_K$ of the quadratic field $K = \mathbb{Q}(\sqrt{d})$ consists of all elements of the form $a + \omega b$, where $a, b \in \mathbb{Z}$ and

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

We assume that K is Euclidean; that is, there exists a function $\phi\colon \mathcal{O}_K \setminus \{0\} \to \mathbb{N}$ with the property that, for any $a, b \in \mathcal{O}_K$ with $b \neq 0$, there exist $q, r \in \mathcal{O}_K$ such that

$$a = bq + r \quad \text{with either } r = 0 \text{ or } \phi(r) < \phi(b).$$

It is known that there are only finitely many Euclidean quadratic fields with respect to the norm $\phi = N_{K/\mathbb{Q}}$. These are the fields $K = \mathbb{Q}(\sqrt{d})$ with

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

In fact, there are no further Euclidean quadratic fields with $d < 0$ (see, e.g., Alaca–Williams [1]). On the other hand, for $d > 0$, it remains unknown whether there are infinitely many Euclidean quadratic fields. Note that the field $\mathbb{Q}(\sqrt{69})$ is not Euclidean with respect to the norm map, but is Euclidean (see Clark [2]).

Integers represented by the norm map

The study of integers represented by quadratic forms is a classical and fascinating topic in number theory. One of the most famous examples is Fermat's two squares theorem: every prime p of the form $4n + 1$ can be written as a sum of two squares. A modern presentation of Euler's proof consists of two steps which are called reciprocity step and descent step.

- *Reciprocity step.* If $p \equiv 1 \pmod 4$, then p divides $a^2 + b^2$ for some coprime $a, b \in \mathbb{Z}$.
- *Descent step.* If p divides $n^2 + 1$, then p can be written in the form $a^2 + b^2$.

In this note, we provide a proof of the descent step for the norm $N_{K/\mathbb{Q}}$ over a Euclidean quadratic field K, derived primarily from the basic properties of finite groups.

Theorem 1. *Let $n \geq 2$ be an integer coprime to $N_{K/\mathbb{Q}}(\omega)$. If there exists an integer $r \in \mathbb{Z}$ such that $N_{K/\mathbb{Q}}(r + \omega) \equiv 0 \pmod n$, then n can be written as the absolute value of the norm of some algebraic integer $\alpha \in \mathcal{O}_K$.*

A classical proof, based on Lagrange's theory of reduced forms, can be found in Cox [3]. Note that the reciprocity step follows directly from Gauss's law of quadratic reciprocity.

Proof of Theorem 1. Let G denote the additive group $(\mathcal{O}_K, +)$ and let $\bar{\alpha}$ denote the algebraic conjugate of $\alpha \in \mathcal{O}_K$. For a fixed $\alpha \in G$, we consider two subgroups of G defined by

$$G_\alpha = \{\alpha z \mid z \in \mathcal{O}_K\} \quad \text{and} \quad \alpha\mathbb{Z} = \{n\alpha \mid n \in \mathbb{Z}\}.$$

Claim 1. *Let $\alpha = a + b\omega$ be an algebraic integer in $\mathcal{O}_K$ such that $ab \neq 0$. If a and b are coprime, then the quotient group G/G_α is cyclic of order $|N_{K/\mathbb{Q}}(\alpha)|$.*

Proof. Set $N = |N_{K/\mathbb{Q}}(\alpha)|$ and fix integers u, v such that $au + bv = 1$. Then

$$\alpha(v - u\bar{\omega}) - \omega \in \mathbb{Z},$$

so each coset of G_α in G is of the form $m + G_\alpha$ for some $m \in \mathbb{Z}$. Moreover, since $N \in G_\alpha$, we may assume that $0 \leq m < N$. Thus

$$|G/G_\alpha| = [G : G_\alpha] \leq N. \tag{1}$$

Denote by n_α the order of the element $1 + G_\alpha \in G/G_\alpha$. Then $n_\alpha = \alpha(x + y\bar{\omega})$ for some $x, y \in \mathbb{Z}$. Multiplying by $\bar{\alpha}$, we obtain $n_\alpha a = xN_{K/\mathbb{Q}}(\alpha)$ and $n_\alpha b = yN_{K/\mathbb{Q}}(\alpha)$, and therefore $(xu + yv)N_{K/\mathbb{Q}}(\alpha) = n_\alpha$. By (1), this implies that $n_\alpha = N$, and hence G/G_α is a cyclic group generated by $1 + G_\alpha$. ∎

Set $\gamma = r + \omega$, and let H denote the subgroup $n\mathbb{Z} + \gamma\mathbb{Z}$ of G.

Claim 2. *The quotient group G/H is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$.*

Proof. We have $j\omega + H = -jr + H$ for all $j \in \mathbb{Z}$. Hence each coset of H in G is of the form $m + H$ for some $m \in \mathbb{Z}$. Since $n \in H$, we may assume that $0 \leq m < n$; hence $[G : H] \leq n$.

Set $N = |N_{K/\mathbb{Q}}(\gamma)|$. By Claim 1, we have an isomorphism $G/G_\gamma \cong \mathbb{Z}/N\mathbb{Z}$. Composing the natural projection $G \to G/G_\gamma$ with the homomorphism $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, we obtain a surjective homomorphism

$$\varphi\colon G \to \mathbb{Z}/n\mathbb{Z}.$$

Then $G/\mathrm{Ker}(\varphi) \cong \mathbb{Z}/n\mathbb{Z}$ by the First Isomorphism Theorem. Since $\gamma, n \in \mathrm{Ker}(\varphi)$, we have $H \subseteq \mathrm{Ker}(\varphi)$, and hence $|G/H| \geq n$. Consequently, we have $|G/H| = n$, and thus $\mathrm{Ker}(\varphi) = H$. ∎

We have $\gamma\omega, n\omega \in H$ since $\gamma\omega + N_{K/\mathbb{Q}}(\gamma) \in \gamma\mathbb{Z}$ and $n\omega = \gamma n + n(-r)$. Therefore, if $\delta \in H$, then $\delta\omega \in H$, and hence $G_\delta \subseteq H$. Now choose a nonzero element $\delta \in H$ such that $\phi(\delta)$ is minimal. If $H \neq G_\delta$, let $z_1 \in H \setminus G_\delta$. The division property of ϕ then yields an element $z_2 \in G$ such that $\phi(z_1 - \delta z_2) < \phi(\delta)$. This contradicts the minimality of $\phi(\delta)$ since $z_1 - \delta z_2 \neq 0$ and $z_1 - \delta z_2 \in H$. Thus $H = G_\delta$.

As n and $N_{K/\mathbb{Q}}(\omega)$ are coprime, it follows that r and n are coprime. Hence $1 + \omega c \in H$ for some $c \in \mathbb{Z}$. Writing $\delta = a + b\omega$ with $a, b \in \mathbb{Z}$, we see that a and b are coprime since $1 + \omega c \in G_\delta$. Combining Claims 1 and 2, we conclude that

$$n = |G/G_\delta| = |N_{K/\mathbb{Q}}(\delta)|,$$

completing the proof of Theorem 1. ∎

Remark 1. Every Euclidean number field has class number one (i.e., $\mathcal{O}_K$ is a PID), but the converse statement is false. For example, the fields $\mathbb{Q}(\sqrt{-d})$ with $d = 19, 43, 67$ and 163 have class number one but are not Euclidean (see, e.g., Lemmermeyer [4]). Moreover, in the proof above, the Euclidean function ϕ is used only to deduce that $H = G_\delta$ for some $\delta \in H$. Therefore, the same argument applies to any number field of class number one, since $\gamma\omega, n\omega \in H$ ensures that H is an ideal of $\mathcal{O}_K$.

Acknowledgements. The author would like to thank the anonymous reviewers for carefully reading the note and for helpful comments.

Funding. The research has received funding from the National University of Mongolia under the grant agreement P2023-4562.

References

[1] Ş. Alaca and K. S. Williams, *Introductory algebraic number theory*. Cambridge University Press, Cambridge, 2004 Zbl 1035.11001 MR 2031707

[2] D. A. Clark, A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* **83** (1994), no. 3-4, 327–330 Zbl 0817.11047 MR 1277533

[3] D. A. Cox, *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989 Zbl 0701.11001 MR 1028322

[4] F. Lemmermeyer, The Euclidean algorithm in algebraic number fields. *Exposition. Math.* **13** (1995), no. 5, 385–416 Zbl 0843.11046 MR 1362867

Bayarmagnai Gombodorj
Department of Mathematics
National University of Mongolia
Ikh surguuliin gudamj-1, Baga Toiruu, Sukhbaatar District
14201 Ulaanbaatar, Mongolia
bayarmagnai@num.edu.mn
Author IDs: zbMATH bayarmagnai.gombodorj MR 846321
ORCID 0000-0002-6998-623X

Licensed under the Creative Commons Attribution 4.0 International Licence CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, and redistribution with appropriate credit, a link to the licence, and indication of changes.