ANALYTIC NUMBER THEORY, SPRING 2022
EUCLIDEAN FIELDS

ZEÉV RUDNICK

1. The Euclidean algorithm and its failure

We now know that there are several (in fact, 9) imaginary quadratic fields $K = \mathbb{Q}(\sqrt{D})$ where the ring of integers has unique factorization, since the class number is one, namely those where $D_K = -3, -4, \dots, -163$. Before our study of the correspondence with the class number of binary quadratic forms, one way to show unique factorization was by showing that there was a Euclidean algorithm, for instance as in the case of the Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ ($D = -4$). A natural question is to find other example which are Euclidean. We shall see that for imaginary quadratic fields, we can have unique factorization without a Euclidean algorithm.

We define the concept of a Euclidean algorithm:

Definition. *An integer domain R is Euclidean if there is a function $\psi : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ such that for each pair $\alpha, \beta \in R$, $\beta \neq 0$, there are $q, r \in R$ (quotient and remainder) so that $\alpha = q\beta + r$ and either $r = 0$ (in which case $\beta \mid \alpha$) or $\psi(r) < \psi(\beta)$.*

Thus we have a division algorithm with "small" remainder, where "small" means with respect to the function ψ.

Examples are the integers $\mathbb{Z}$ with $\psi(n) = |n|$; the Gaussian integers $\mathbb{Z}[i]$ with $\psi(\alpha) = N(\alpha) = |\alpha|^2$; or the polynomial ring over a field where $\psi(f) = \deg f$.

Proposition 1.1. *A Euclidean ring is a PID.*

Proof. Let $(0) \neq I \subseteq R$ be an ideal. We want to show that it is principal. Let $\beta_0 \in I$ be an element with ψ minimal, that is $\psi(x) \geq \psi(\beta_0)$ for all $0 \neq x \in I$; it exists because ψ takes values in $\mathbb{Z}_{\geq 0}$. Then we claim $I = (\beta_0)$. Indeed, if $\alpha \in I$, either $\beta_0 \mid \alpha$, in which case we are done, or else $\alpha = q\beta_0 + r$ with $q, r \in R$, $\psi(r) < \psi(\beta_0)$. But since $\alpha, \beta_0 \in I$, we have $r = \alpha - q\beta_0 \in I$, but with $\psi(r) < \psi(\beta_0)$ contradicting our choice of β_0. □

It is not difficult to find all cases that the ring of integers of the quadratic fields $\mathbb{Q}(\sqrt{d})$ is Euclidean w.r.t. the norm $\psi(x) = N_{K/\mathbb{Q}}(x)$:

Theorem 1.2. *For $d = -1, -2, -3, -7, -11$, the fields $\mathbb{Q}(\sqrt{d})$ are Euclidean with respect to the norm.*

Proof. We first show that it suffices to show that for every $x \in K = \mathbb{Q}(\sqrt{d})$, there is some $q \in O_K$ for which $N(x-q) < 1$. Indeed, given nonzero $\beta, \alpha \in O_K$, if we find $q \in O_K$ with $N(\frac{\alpha}{\beta} - q) < 1$ then set $r := \alpha - q\beta \in O_K$; by multiplicativity of the norm we have

$$\frac{N(r)}{N(\beta)} = N(\frac{r}{\beta}) = N\left(\frac{\alpha - q\beta}{\beta}\right) = N\left(\frac{\alpha}{\beta} - q\right) < 1$$

giving $N(r) < N(\beta)$.

Now take $x = u + v\omega_K \in K$, $u, v \in \mathbb{Q}$ and look for integers $m, n \in \mathbb{Z}$ so that $q = m + n\omega_K$ satisfies $N(x-q) < 1$. We treat separately the case $D_K = 4d = 0 \bmod 4$ and $D_K = d = 1 \bmod 4$.

If $D_K = 4d$, then $\omega_K = \sqrt{d}$ and take $|u - m| \le 1/2$, $|v - n| \le 1/2$. Then

$$N(x-q) = (u-m)^2 - d(v-n)^2 \le \frac{1}{4} - \frac{d}{4} = \frac{1-d}{4}$$

so that $N(x-q) < 1$ is guaranteed if $1 - d < 4$, that is $0 > d > -3$. Since $d = 2, 3 \bmod 4$ we are left with $d = -1, -2$ or $D_K = -4, -8$.

If $D_K = d = 1 \bmod 4$, then we proceed differently: First pick an integer n so that $|u - m| \le 1/2$, and then pick an integer m so that

$$|(v-n) + 2u - 2m| \le 1.$$

Then for $q = m + n\omega_K$ we have

$$\begin{aligned} N(x-q) &= (u-m)^2 + (u-m)(v-n) + \frac{1-d}{4}(v-n)^2 \\ &= \frac{[2\,(u-m) + (v-n)]^2 - d(v-n)^2}{4} \\ &\le \frac{1^2 - d(\frac{1}{2})^2}{4} = \frac{4-d}{16} \end{aligned}$$

which is less than 1 if $-12 < d < 0$, that is $D_K = d = -3, -7, -11$. □

Motzkin (1949) showed that the remaining 4 imaginary quadratic fields of class number one, namely those with discriminant -19, -43, -67, -163, are not Euclidean for any ψ.

Theorem 1.3. *If $d < 0$ is squarefree, and $d \neq -1, -2, -3, -7, -11$, then the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ is not Euclidean for any function.*

Proof. A Euclidean field necessarily has class number one. We know (say by computing the class number) that for $-19 < d < 0$, the class number is one only for the five norm-Euclidean examples. So we may assume that $d \leq -19$.

Assume that there is a Euclidean function ψ on O_K. Let $\alpha_0 \in O_K \backslash (O_K^\times \cup \{0\})$ have the minimal value of ψ on non-units:

$$\psi(\alpha_0) = \min\left(\psi(\alpha) : \alpha \in O_K, \alpha \neq 0, \alpha \notin O_K^\times\right).$$

Then the possible remainders r after division by α_0 are either zero or units, since we must have $\psi(r) < \psi(\alpha_0)$ which is the minimal value of ψ on nonunits. In other words, every coset of $O_K/(\alpha_0)$ is represented by 0 or a unit. Since the unit group here is $O_K = \{\pm 1\}$ only has 2 elements (as with any imaginary quadratic field with discriminant other than $-3, -4$ which is excluded), we find that $N(\alpha_0) = \#O_K/(\alpha_0) \leq 3$.

Now we show that if $\alpha \in O_K$ is not zero or a unit then $N(\alpha) \geq 4$: We have $O_K = \mathbb{Z}[\omega_K]$ where $\omega_K = \sqrt{d}$ if $d \neq 1 \bmod 4$, and $\omega_K = (1+\sqrt{d})/2$ if $d = 1 \bmod 4$. Write $\alpha = m + n\omega_K$, where then for $d \neq 1 \bmod 4$ we have

$$N(\alpha) = m^2 - dn^2.$$

If $n = 0$ and $\alpha = m \neq \pm 1$ then $N(\alpha) = m^2 \geq 2^2 = 4$, while for $n \neq 0$ then $N(\alpha) \geq |d|n^2 \geq |d| > 4$ since we assume d is not on the list.

If $d = 1 \bmod 4$ then

$$N(\alpha) = m^2 + mn + \frac{1-d}{4}n^2 = \frac{(2m+n)^2 + |d|n^2}{4}.$$

If $n = 0$ and $\alpha = m \neq \pm 1$ then $N(\alpha) = m^2 \geq 2^2 = 4$, while for $n \neq 0$ then

$$N(\alpha) \geq \frac{|d|n^2}{4} \geq \frac{19n^2}{4} \geq \frac{19}{4} > 4.$$

□

Real quadratic fields are norm-Euclidean for 16 cases

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

and these are the only ones. It is a conjecture of Gauss that there are infinitely many real quadratic fields of class number one. In stark contrast to the imaginary quadratic case, Peter Weinberger showed (1972) that assuming GRH, a real quadratic field has class number one if and only if it is Euclidean (In fact this holds for any number field which is not imaginary quadratic, the condition is that there are infinitely many units). Unconditionally, Narkiewicz showed in 2007 that there are at most two real quadratic fields of class number one which are not Euclidean.