Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam

EUCLID'S ALGORITHM IN LARGE DEDEKIND DOMAINS

H.W. Lenstra, Jr.

Report 86-25

Received October 1986.

EUCLID'S ALGORITHM IN LARGE DEDEKIND DOMAINS.

H.W. Lenstra, Jr.

Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam
The Netherlands

Abstract. It is proved that any Dedekind domain with many more elements than prime ideals is Euclidean.

Key words: Euclidean ring, Dedekind domain.
1980 Mathematics subject classification (1985): 13F07, 13F05.

Let A be a Dedekind domain, and denote by Z the set of its non-zero prime ideals. It is well known that A is a principal ideal domain if Z is finite. An infinite analogue of this result was obtained by Claborn [~~1~~ 2; ~~2~~ 3, chapter III, section 13]. He proved that A is a principal ideal domain if

(1) $\qquad \#A > (\#Z)^{\mathfrak{a}}$,

where $\mathfrak{a}$ is the least infinite cardinal and $\#S$ denotes the cardinality of S.

If Z is finite then A is not only a principal ideal domain but even a *Euclidean* domain [~~4~~ 5, Proposition 5]. The latter statement means that there exists a map ϕ from $A-\{0\}$ to a well-ordered set W such that for all $a, b \in A$ with $b \neq 0$, $a \notin Ab$, there exists $r \in a+Ab$ with $\phi(r) < \phi(b)$. For finite Z one can take for W the set of non-negative integers.

It is a natural question whether Claborn's result can be extended in a similar way, *i.e.* whether A is Euclidean if (1) holds. In the present paper we show that this is indeed the case. For W we take a well-ordered set of order type ω^2, where ω is the least infinite ordinal. The elements of W can be written in a unique way as $\omega a + b$, where a, b are non-negative integers; and $\omega a + b < \omega a' + b'$ if and only if either $a < a'$ or $a = a'$, $b < b'$.

We shall see that the other results that Claborn obtained in [~~1~~ 2] can be extended in an analogous way.

We let K denote the field of fractions of A, and $v_{\mathfrak{p}}$, for $\mathfrak{p} \in Z$, the normalized exponential valuation of K corresponding to $\mathfrak{p}$. The group of units of A is denoted by A^*.

Claborn's first result [~~1~~ 2, Proposition; ~~2~~ 3, Proposition 13.7] states that A is a principal ideal domain if A contains a field k satisfying $\#A = \#k > \#Z$. A sharper result is as follows.

(2) Proposition. *Let A be a Dedekind domain, and suppose that A contains a subset k with the properties*

(3) $\qquad \#k > \#Z$,

(4) $\qquad \lambda - \mu \in A^* \cup \{0\}$ *for all* $\lambda, \mu \in k$.

Then A is Euclidean.

Proof. For $x \in A-\{0\}$, let $\phi(x) = \sum_{\mathfrak{p}\in Z} v_{\mathfrak{p}}(x)$. We prove that A is Euclidean with respect to ϕ.

Let $a, b \in A$, $b \neq 0$, $a \notin Ab$. First suppose that for some $\lambda \in k$ we have $A\cdot(a+\lambda b) = Aa + Ab$. Then

$$v_{\mathfrak{p}}(a+\lambda b)=\min\{v_{\mathfrak{p}}(a),v_{\mathfrak{p}}(b)\}\leqslant v_{\mathfrak{p}}(b)$$

for all $\mathfrak{p}\in Z$, with strict inequality for at least one $\mathfrak{p}$. Hence the element $r=a+\lambda b$ of $a+Ab$ satisfies $\phi(r)<\phi(b)$, as required.

Next suppose that no such λ exists. Then for every $\lambda\in k$ there exists $\mathfrak{p}_\lambda\in Z$ such that $a+\lambda b\in\mathfrak{p}_\lambda\cdot(Aa+Ab)$. The map $k\to Z$ sending λ to $\mathfrak{p}_\lambda$ is not injective, by (3), so there are λ, $\mu\in k$, $\lambda\neq\mu$, with $\mathfrak{p}_\lambda=\mathfrak{p}_\mu$. Then $(\lambda-\mu)b=(a+\lambda b)-(a+\mu b)\in\mathfrak{p}_\lambda\cdot(Aa+Ab)$, so $b\in\mathfrak{p}_\lambda\cdot(Aa+Ab)$, by (4). We conclude that $Aa+Ab=A\cdot(a+\lambda b)+Ab$ is contained in $\mathfrak{p}_\lambda\cdot(Aa+Ab)$, which is a contradiction. This proves (2).

If A is the ring of integers in an algebraic number field then condition (3) can be substantially weakened, see [3, Theorem (1.4)]. ∠ 4

For a subset $Y\subset Z$, we define the subring $A_Y\subset K$ by

$$A_Y=\{x\in K\colon\ v_{\mathfrak{p}}(x)\geqslant 0 \text{ for all } \mathfrak{p}\in Y\}.$$

Notice that $A_Z=A$. Claborn [1, Theorem; 2, Theorem 13.8] proved that every ideal of A_Y is generated by an element of A if the inequality $\#A>(\#Y)^{\mathfrak{a}}$ is satisfied. To formulate our stronger result we need a definition. Let the pair (A,Y) be called *Euclidean* if there exist a well-ordered set W and a map $\phi\colon A-\{0\}\to W$ such that for all a, $b\in A$, $b\neq 0$, $a\notin A_Yb$, there exists $r\in a+Ab$ with $\phi(r)<\phi(b)$. We have $A_Z=A$, and (A,Z) is Euclidean if and only if A is. ∠ 2 ∠ 3

Let (A,Y) be Euclidean and $\mathfrak{b}$ a non-zero A_Y-ideal. Then $\mathfrak{b}$ is generated by $\mathfrak{b}\cap A$, and if $b\in\mathfrak{b}\cap A$ has minimal ϕ-value then it follows easily that $A_Yb=\mathfrak{b}$. Hence, if (A,Y) is a Euclidean pair, then every ideal of A_Y is generated by an element of A. This shows that the following theorem is indeed sharper than Claborn's result.

(5) Theorem. *Let A be a Dedekind domain, and Y a set of non-zero prime ideals of A such that $\#A>(\#Y)^{\mathfrak{a}}$, where $\mathfrak{a}$ denotes the least infinite cardinal. Then (A,Y) is a Euclidean pair.*

The proof uses the following lemma. Let W be the well-ordered set of order type ω^2 defined above.

(6) Lemma. *Let A be Dedekind, $Y\subset Z$ a subset, and suppose that there exists a finite subset $X\subset Y$ with the property that for every $x\in A_X-A_Y$ there exists $q\in A$ such that $(x+q)^{-1}\in A_Y$. Then (A,Y) is a Euclidean pair with respect to the map $\phi\colon A-\{0\}\to W$ defined by*

$$\phi(x)=\omega\cdot\sum_{\mathfrak{p}\in X}v_{\mathfrak{p}}(x)\ +\ \sum_{\mathfrak{p}\in Y-X}v_{\mathfrak{p}}(x).$$

Proof of (6). Let a, $b\in A$, $b\neq 0$, $a\notin A_Y\cdot b$. We have to find $r\in a+Ab$ such that $\phi(r)<\phi(b)$.

First suppose that $v_{\mathfrak{p}}(a)\geqslant v_{\mathfrak{p}}(b)$ for all $\mathfrak{p}\in X$. Then $x=a/b$ belongs to A_X, but not to A_Y, so by the hypothesis of the lemma there exists $q\in A$ such that $(x+q)^{-1}=b/(a+qb)$ belongs to A_Y. Then $b\in A_Y\cdot(a+qb)$, and therefore $A_Y\cdot(a+qb)=A_Ya+A_Yb$. Hence $r=a+qb\in a+Ab$ satisfies

$$v_{\mathfrak{p}}(a+qb)=\min\{v_{\mathfrak{p}}(a),v_{\mathfrak{p}}(b)\}\leqslant v_{\mathfrak{p}}(b)$$

for all $\mathfrak{p}\in Y$, with strict inequality for at least one $\mathfrak{p}$ because $a\notin A_Yb$. It follows that $\phi(r)<\phi(b)$.

Secondly, suppose that $v_{\mathfrak{p}}(a)<v_{\mathfrak{p}}(b)$ for at least one $\mathfrak{p}\in X$. Since X is finite, the approximation theorem[1] for Dedekind domains implies that there exists $r\in A$ with the following properties:

$$v_{\mathfrak{p}}(r-a)\geqslant v_{\mathfrak{p}}(b) \text{ for all } \mathfrak{p}\in Z \text{ with } v_{\mathfrak{p}}(a)<v_{\mathfrak{p}}(b),$$

1 [1, Section 2.4, Proposition 2]

$$v_{\mathfrak{p}}(r)=v_{\mathfrak{p}}(b) \text{ for all } \mathfrak{p}\in X \text{ with } v_{\mathfrak{p}}(a)\geqslant v_{\mathfrak{p}}(b),$$
$$v_{\mathfrak{p}}(r)=v_{\mathfrak{p}}(b) \text{ for all } \mathfrak{p}\in Z-X \text{ with } v_{\mathfrak{p}}(a)\geqslant v_{\mathfrak{p}}(b)>0.$$

Then we have $v_{\mathfrak{p}}(r-a)\geqslant v_{\mathfrak{p}}(b)$ for *all* $\mathfrak{p}\in Z$, so $r\in a+Ab$. Also, $v_{\mathfrak{p}}(r)\leqslant v_{\mathfrak{p}}(b)$ for all $\mathfrak{p}\in X$, with strict inequality if $v_{\mathfrak{p}}(a)<v_{\mathfrak{p}}(b)$, which occurs for at least one $\mathfrak{p}\in X$. Hence $\sum_{\mathfrak{p}\in X} v_{\mathfrak{p}}(r) < \sum_{\mathfrak{p}\in X} v_{\mathfrak{p}}(b)$, and it follows that $\phi(r)<\phi(b)$, as required. This proves (6).

Notice that the lemma implies that (A, Y) is a Euclidean pair if Y is *finite*.

Proof of the theorem. It suffices to show that some for finite subset $X\subset Y$ the condition of the lemma is satisfied. By the remark just made we may assume that Y is infinite. Let $\mathfrak{p}\in Z$, and let $\hat{A}_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of A. Then from

$$(\# Y)^{\alpha}<\# A\leqslant \# \hat{A}_{\mathfrak{p}}=(\# A/\mathfrak{p})^{\alpha}$$

we see that $\# Y<\# A/\mathfrak{p}$. So $A/\mathfrak{p}$ is infinite for every $\mathfrak{p}\in Z$.

Suppose that there does not exist a finite subset $X\subset Y$ satisfying the condition of (6), *i.e.*:

(7) for every finite $X\subset Y$ there exists $x\in A_X-A_Y$ such that $(x+q)^{-1}\notin A_Y$ for all $q\in A$.

We derive a contradiction.

Using (7) we construct a sequence $(x_m)_{m=0}^{\infty}$ of elements of $K-A_Y$ with the following two properties:

(8) $(x_n+q)^{-1}\notin A_Y$ for all $n\geqslant 0$ and all $q\in A$,

(9) if $X_n=\{\mathfrak{p}\in Y\colon v_{\mathfrak{p}}(x_n)<0\}$ then $X_i\cap X_j=\varnothing$ for all $i, j\geqslant 0$, $i\neq j$.

The construction is by induction on m. Let $m\geqslant 0$, and let x_n, for $0\leqslant n<m$, be such that (8), (9) hold when restricted to $i, j, n<m$. Applying (7) to $X=\bigcup_{n<m} X_n$ we find $x_m\in A_X-A_Y$ such that $(x_m+q)^{-1}\notin A_Y$ for all $q\in A$. For $n<m$ we then have $x_m\in A_X\subset A_{X_n}$, so $X_n\cap X_m=\varnothing$. Hence (8) and (9) hold for $i, j, n\leqslant m$. This concludes the induction step and the construction of the sequence $(x_m)_{m=0}^{\infty}$.

If $(a_m)_{m=0}^{\infty}$ is any sequence of elements of A, then plainly also $(y_m)_{m=0}^{\infty}=(x_m+a_m)_{m=0}^{\infty}$ satisfies (8) and (9), with $x_.$ replaced by $y_.$. We claim that for a suitable choice of $(a_m)_{m=0}^{\infty}$ the sequence $(y_m)_{m=0}^{\infty}$ has the following additional property:

(10) there is no $\mathfrak{p}\in Y$ such that there exist i, j, k with

$$v_{\mathfrak{p}}(y_i-y_j)>0,\ v_{\mathfrak{p}}(y_j-y_k)>0,\ i<j<k.$$

The proof is again by induction. Let $m\geqslant 0$, and let $a_n\in A$, for $n<m$, be such that (10) holds when restricted to $k<m$. The only $\mathfrak{p}\in Y$ which can possibly violate (10), with $k=m$, are those for which $v_{\mathfrak{p}}(y_i-y_j)>0$ for certain i, j with $i<j<m$. There are only finitely many such $\mathfrak{p}$, since $y_i=y_j$ would imply that $X_i=X_j$, so $X_i=\varnothing$ by (9), contradicting that $x_i\notin A_Y$. Notice that $v_{\mathfrak{p}}(y_i-y_j)>0$, with $i<j<m$, implies that $\mathfrak{p}\notin X_i$ and $\mathfrak{p}\notin X_j$. If $\mathfrak{p}\in X_m$, then regardless of the choice of a_m we have $v_{\mathfrak{p}}(y_j-y_m)<0$. If $\mathfrak{p}\notin X_m$, then we have $v_{\mathfrak{p}}(y_j-y_m)=0$ provided that

$$a_m\not\equiv y_j-x_m \bmod \mathfrak{p}$$

(in the local ring at $\mathfrak{p}$). Hence, for (10) to be valid with $k=m$, it suffices that a_m avoids a finite set of residue classes modulo each of a finite number of prime ideals of A. Since $A/\mathfrak{p}$ is infinite for all $\mathfrak{p}\in Z$, the approximation theorem [1] guarantees the existence of an element $a_m\in A$ satisfying these conditions. This completes our inductive proof of (10).

From (8), (9) (with $y_.$ for $x_.$) and (10) we derive a contradiction. Fix $q \in A$. Then for each $n \geqslant 0$ there exists $\mathfrak{p}_n \in Y$ with $v_{\mathfrak{p}_n}(y_n + q) > 0$, by (8). If $\mathfrak{p}_i = \mathfrak{p}_j = \mathfrak{p}_k$ for $i < j < k$, then with $\mathfrak{p} = \mathfrak{p}_i$ we obtain a contradiction to (10). Hence each $\mathfrak{p} \in Y$ occurs at most twice as $\mathfrak{p}_n$, and the map f_q: $\{0,1,2,...\} \to Y$ defined by $f_q(n) = \mathfrak{p}_n$ has infinite image.

The number of maps $\{0,1,2,...\} \to Y$ is $(\# Y)^{\mathfrak{a}}$, so from $\# A > (\# Y)^{\mathfrak{a}}$ it follows that there exist $q \neq r$ in A with $f_q = f_r$. For $\mathfrak{p} = f_q(n)$ we then have $v_{\mathfrak{p}}(y_n + q) > 0$, $v_{\mathfrak{p}}(y_n + r) > 0$, and therefore

$$v_{\mathfrak{p}}(q - r) > 0 \text{ for all } \mathfrak{p} \text{ in the image of } f_q.$$

But f_q has infinite image, so it follows that $q - r = 0$, a contradiction.

This proves the theorem.

(11) Corollary. *Let A be a Dedekind domain, and suppose that the set Z of non-zero prime ideals of A satisfies $\# A > (\# Z)^{\mathfrak{a}}$. Then A is Euclidean.*

This follows from (5), with $Y = Z$.

References.

1. N. Bourbaki, Algèbre commutative, Ch. 7, Diviseurs, Hermann, Paris 1965; English translation: Commutative Algebra, ibid., 1972.

2 ~~1~~. L. Claborn, *A generalized approximation theorem for Dedekind domains*, Proc. Amer. Math. Soc. **18** (1967), 378-380.

3 ~~2~~. R.M. Fossum, *The divisor class group of a Krull domain*, Ergeb. Math. Grenzgeb. **74**, Springer-Verlag, Berlin 1973.

4 ~~3~~. H.W. Lenstra, Jr., *Euclidean number fields of large degree*, Invent. Math. **38** (1977), 237-254.

5 ~~4~~. P. Samuel, *About Euclidean rings*, J. Algebra **19** (1971), 282-301.