Euclidean number fields 3

Lenstra, H.W.

Euclidean Number Fields 3

Hendrik W. Lenstra, Jr.*

Artin's Conjecture

In the previous sections, when we spoke of division with remainder $\alpha = \kappa\beta + \rho$ with ρ smaller than β, we did our measuring by means of the norm

$$N(\rho) < N(\beta)$$

In this section we see just what freedom we gain in admitting functions other than the norm

Let T be a commutative ring with 1, $1 \neq 0$, without divisors of zero We will mostly be interested in rings of the type $R[\delta^{-1}]$, see section 2, (14) We call these rings *number rings* If ψ is a map which associates to each non-zero element β of T a non-negative integer $\psi(\beta)$, then T is said to be *euclidean with respect to* ψ, or ψ is said to be a *division algorithm* on T, if for all α and β in T, $\beta \neq 0$, there are κ and ρ in T with

(1) $\alpha = \kappa\beta + \rho$, and $\rho = 0$ or $\psi(\rho) < \psi(\beta)$

If there is such a ψ then we call T *euclidean* If T is euclidean then T has unique factorisation into primes

Our present knowledge suggests that in the case of number rings we are not dealing with a more general concept than our earlier one

(2) every known euclidean number ring T is euclidean with respect to the norm N_T defined in section 2, (14)

But (2) is more probably a sign of our ignorance than it is a reflection of reality there are infinitely many number rings with unique factorisation that are not euclidean with respect to N_T But as we shall see, there is reason to believe that these T, with four exceptions, are euclidean with respect to some other function

This supposition rests on analysis that arises from an idea of Motzkin, see [5], [6] As above, let T be a commutative ring with 1, $1 \neq 0$, and without divisors of zero We try to construct a function ψ on T that is a division algorithm on T For which β in T, $\beta \neq 0$, can we set $\psi(\beta) = 0$? For such β, the alternative in (1) that $\psi(\rho) < \psi(\beta)$ is excluded So we must have $\rho = 0$ and $\alpha = \kappa\beta$ and every α must be divisible by β This is to say that β is a unit If we now fix

$$\psi(\beta) = 0 \text{ if } \beta \text{ is a unit,}$$

then indeed we can satisfy (1) for these β, by taking $\rho = 0$ and $\kappa = \alpha\beta^{-1}$ Next we ask for which β may we take $\psi(\beta) = 1$ For these β we may have $\rho = 0$ or $\psi(\rho) = 0$ in (1), so $\rho = 0$ or ρ is a unit In other words every α in T that is not divisible by β must be *congruent modulo* β to a unit If we set

$$\psi(\beta) = 1 \text{ if every residue class modulo } \beta \text{ contains either 0 or a unit}$$

then we can satisfy (1) for all α, β in T with $\psi(\beta) \leqslant 1$ In general we can use induction on n to define

$$T_{-1} = \{0\}$$

$$T_n = \{\beta \text{ every residue class modulo } \beta \text{ contains an element of } T_{n-1}\}$$

for $n \geqslant 0$, and we can take

(3) $\psi(\beta) = n$ if β belongs to T_n but not to T_{n-1}, $n \geqslant 0$

It is now easy to prove the following proposition

(4) If there is an element of T that does not belong to any T_n then T is not euclidean If conversely each element of T belongs to some T_n then T is euclidean with respect to the function ψ defined by (3) Moreover ψ is then the *smallest* division algorithm on T in the sense that

$$\psi(\beta) \leqslant \chi(\beta)$$

for all β of T distinct from zero and all division algorithms χ on T

If we take T to be the ring of (ordinary rational) integers then the above construction yields

$$\psi(\beta) = 0 \quad \text{for} \quad \beta = \pm 1$$

$$\psi(\beta) = 1 \quad \text{for} \quad \beta = \pm 2, \pm 3$$

---

* Translated by Alf van der Poorten

and generally

(5) $\psi(\beta) = [\log |\beta| / \log 2], \quad \beta \neq 0,$

where $[x]$ denotes the greatest integer $\leqslant x$

If T is the ring of polynomials in one variable over a field then one easily sees that

$$\psi(\beta) = \text{degree } (\beta)$$

for all non-zero β in T

To understand what Motzkin's general procedure looks like in the case at hand, that of number rings, we must first have some information about the units of such rings From *Dirichlet's unit theorem* we see that the example of the ring of integers we gave above is not at all typical in most cases a number ring has infinitely many units If we confine ourselves to number rings with unique factorisation – for only these rings can be euclidean – then there are in fact only ten cases which have a finite number of units if γ is one of the nine numbers

(6) $\frac{1}{2}(1+\sqrt{-3}), \sqrt{-1}, \frac{1}{2}(1+\sqrt{-7}), \sqrt{-2}, \frac{1}{2}(1+\sqrt{-11}),$

(7) $\frac{1}{2}(1+\sqrt{-19}), \frac{1}{2}(1+\sqrt{-43}), \frac{1}{2}(1+\sqrt{-67}),$

$\frac{1}{2}(1+\sqrt{-163})$

then the set of numbers $a + b\gamma$, with a and b integers, is such a ring, and the tenth case is the ring of integers itself Four of these ten rings, the cases (7), are not euclidean The remaining six cases are euclidean and in the cases (6) ψ can be approximated as follows Set

$$c = 3, 2, \frac{7}{4}, \frac{4}{3}, \frac{11}{9}$$

for the respective five values (6) of γ and define

$$\chi(a + b\gamma) = [\log N(a + b\gamma)/\log c]$$

for a and b integers, not both zero, compare (5) Then χ is a division algorithm and the difference between χ and ψ is bounded These results can be found in [7], [6], [3] For an exact description of ψ in the cases $\gamma = \frac{1}{2}(1+\sqrt{-3})$ and $\gamma = \sqrt{-1}$, see [3] and figures 3 and 4

In the rest of this section we take T to be a number ring with infinitely many units and we assume T to have unique factorisation Our aim is to determine the function ψ We already know that $\psi(\beta) = 1$ if and only if β has the following property

(8) each α in T either is divisible by β or is congruent to a unit modulo β

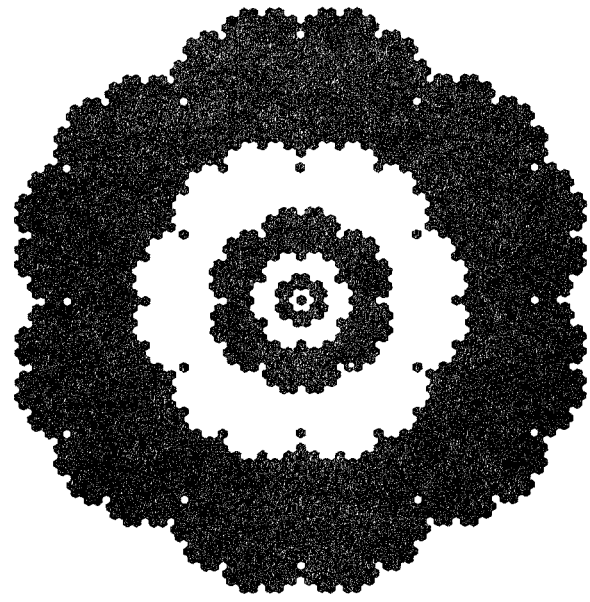

Figure 3. The smallest division algorithm on the ring $\mathbb{Z}[\rho] = \{a + b\rho$ a and b are integers$\}$, where $\rho = (-1 + \sqrt{-3})/2$ is a primitive cube root of unity The ring is a triangular lattice in the complex plane, and the points of the lattice are the centers of a regular hexagonal tiling of the plane The black hexagons in the picture correspond to the elements α of $\mathbb{Z}[\rho]$ for which $\alpha = 0$ or $\psi(\alpha) = 1$, 3 or 5

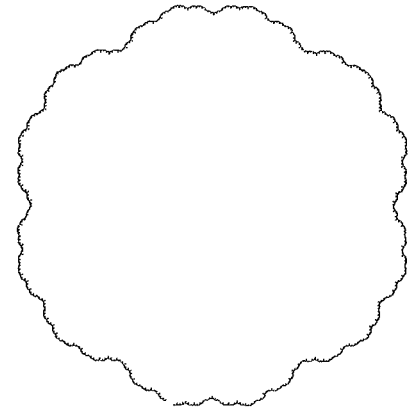

Figure 4. The limit case of figure 3 The centre of the picture is 0, the six dots nearest to 0 are the elements $+1$, $+\rho$, $+\rho^2$ of the ring For α in $\mathbb{Z}[\rho]$, $\alpha \neq 0$, we have $\psi(\alpha) < n$ if and only if $\alpha(1-\rho)^{-n}$ is inside the dodecagonal figure, but not equal to one of the dots The intersection of the closure of the set and the boundary of its convex hull consists of twelve copies of the Cantor discontinuum

In particular, if α is not divisible by β then it has no factors in common with β if $\psi(\beta) - 1$, so β must be a prime, this also follows from (9) If we denote by P the set of primes with the property (8) then we plainly have

$$\psi(\eta) \geqslant 2 \text{ for every prime } \eta \text{ of } T \text{ that does not belong to } P$$

Here we set, for convenience, $\psi(\eta) = \infty$ in the event that η does not belong to any T_n. If we now apply the general inequality

(9) $\psi(\alpha_1\alpha_2) \geqslant \psi(\alpha_1) + \psi(\alpha_2) \quad (\alpha_1 \cdot \alpha_2 \neq 0)$

(cf. [6, prop. 12]) then we find the following result. If α is an arbitrary non-zero element of T with a factorisation

$$\alpha = \epsilon\beta_1\beta_2 \ldots \beta_v\eta_1\eta_2 \ldots \eta_w$$

where ϵ is a unit, $\beta_1, \ldots, \beta_v$ are primes belonging to P and $\eta_1, \ldots, \eta_w$ are primes not belonging to P then

(10) $\psi(\alpha) \geqslant v + 2w.$

It is now true that:

(11) *Let T be a number ring with infinitely many units and with unique factorisation, and assume a number of generalised Riemann-hypotheses. Then T is euclidean and the equality sign in* (10) *holds for all non-zero α in T.*

This result, which extends a theorem of Weinberger [9] and Queen [8], is proved in [4].

The proof of (11) depends on the fact that, under the assumption of the Riemann-hypotheses, which we shall denote by GRH, the collection P is *sufficiently large*. Suppose for example that the following were true:

(12) for each pair of relatively prime elements α and β of T, with $\beta \neq 0$, there is an element of P that is congruent to α modulo β.

Then (11) can be proved as follows. Let χ be the function defined by the right hand side of (10):

$$\chi(\alpha) = v + 2w \quad \text{for } \alpha, v, w \text{ as above.}$$

Clearly it suffices to show that χ is a division algorithm on T. Thus, given α and β in T, with $\beta \neq 0$, we have to find a ρ, with $\rho = 0$ or $\chi(\rho) < \chi(\beta)$, which is congruent to α modulo β.

Without loss of generality we may suppose α and β to be relatively prime: for if not we could divide α and β by their greatest common divisor without changing the problem.

If $\chi(\beta) = 0$ then β is a unit and we can take $\rho = 0$. If we have $\chi(\beta) = 1$ then β belongs to P, and from the definition of P we can find a unit ρ that is congruent to α modulo β. Then indeed

$$\chi(\rho) = 0 < 1 = \chi(\beta).$$

Finally, if $\chi(\beta) \geqslant 2$ then, applying (12), we choose an element ρ of P that is congruent to α modulo β, and for this ρ we have

$$\chi(\rho) = 1 < 2 \leqslant \chi(\beta),$$

as required. It remains only to study (12).

We consider an example. Let T be the set of those rational numbers whose denominator is a power of 2. This is a number ring with unique factorisation. The units of T are exactly the numbers $\pm 2^j$ with j integral, so there are infinitely many of them. It is not difficult to decide that in this case the set P is, up to multiplication by units, the same as the set of odd prime numbers p with the following property:

(13) each integer a, $1 \leqslant a \leqslant p - 1$, is congruent, modulo p, to a number of the shape $\pm 2^j$, with j an integer, $j \geqslant 0$.

Of the fourteen odd primes < 50 only 17, 31, 41 and 43 miss out on having this property. But however much one might guess that (13) is true for more than half of all the primes – to be exact, for 56.0933720. . .% – it has not even been shown that there are infinitely many such primes; let alone that any property such as (12) has been proved to hold.

If we drop the $\pm$-sign in (13) then one can describe (13) as saying that 2 is a *primitive root* modulo p. This calls to mind a conjecture of Artin of 1927 which asserts that for each integer t, $|t| > 1$, the limit

(14)
$$\lim_{x \to \infty} \frac{\text{number of primes} < x \text{ which have } t \text{ as a primitive root}}{\text{number of primes} < x}$$

exists. Moreover the conjecture gives a formula for the value of the limit. One can think of the limit as the *fraction* of primes that have t as a primitive root. Plainly the number of such primes is infinite if this fraction is positive.

Artin's conjecture was proved in 1967 by Hooley under the assumption of a series of generalised Riemann-hypotheses, see [2]. If we are prepared to work subject to similar assumptions then there are three questions to be disposed of in order to prove (12). Firstly, can Artin's conjecture and Hooley's proof be generalised so as to deal with the set P? Secondly, can one, in so doing, take into account the condition that the primes must also be congruent to α modulo β? Thirdly, can it not happen that the formula for the fraction of primes yields the value *zero*? In this case the relevant set could even be empty.

We will not pause for long over the first question. Artin's conjecture does indeed admit a straightforward generalisation that makes a prediction of the fraction of primes that belong to P, and this generalisation can be proved, modulo

GRH, by Hooley's methods For this see [1] Here we do not go into the precise meaning of *fraction* in the case of general number rings T

Concerning the second question if α and β are relatively prime elements of T, with $\beta \neq 0$, then the condition

(15) $\rho \equiv \alpha \bmod \beta$

is indeed satisfied by a positive fraction of all prime elements ρ This is a theorem that goes back to Dirichlet But, for primes ρ, the condition (15) is not independent of the condition

(16) ρ belong to P,

as we see below from an example But it is possible to take (15) into account in a new generalisation of Artin's conjecture, which on closer inspection turns out to be equivalent to the previous version

The third question is still with us is it possible that, under assumption of GRH, we find that asymptotically 0% of all primes satisfy both of (15) and (16)? In the case of the original conjecture the predicted value of the limit (14) is 0 only if t is a square For P this phenomenon does not arise the proportion of primes that belongs to P is positive if the Riemann-hypotheses are true But it is unpleasant to discover that the condition (15) can conflict with (16) It is easy to find such an example for Artin's original conjecture the two requirements

$p \equiv 1 \bmod 8$

2 is a primitive root mod p

cannot be reconciled for prime integers p From $p \equiv 1 \bmod 8$ one can deduce that 2 is a square modulo p and so cannot be a primitive root With somewhat more difficulty one can also construct an example in the situation that interests us here

(17) let T consist of the numbers

$a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$,

a_0, a_1, a_2, a_3 integers,

with $\zeta^5 = 1, \zeta \neq 1$, then P contains no elements that are 1 modulo 4

The proof is quite similar if ρ is prime, $\rho \equiv 1 \bmod 4$, then it follows that every unit of T is a square mod ρ and one can conclude that ρ cannot belong to P

We see from (17) that (12) is not valid in general Luckily, the full force of (12) is not needed to prove (11) In fact, suppose $\chi(\beta) \geqslant 3$ Then, according to the theorem mentioned at (15), we can choose a prime ρ with $\rho \equiv \alpha \bmod \beta$ and then

$$\chi(\rho) \leqslant 2 < 3 \leqslant \chi(\beta)$$

So it would be enough to know (12) for the case $\chi(\beta) = 2$ Sadly, the example above shows that even then (12) need not be true This almost means that (11) is not true – almost, because to reach $\chi(\rho) < \chi(\beta) = 2$ we may also take ρ to be a unit So, to show (11), it is sufficient to prove the following weakened version of (12)

(18) for every pair of relatively prime elements α, β of T, with $\chi(\beta) = 2$, there is a ρ in T with

$\rho \equiv \alpha \bmod \beta$,

so that ρ is an element of P or a unit of T

Moreover, this is as far as we can go the validity of (18), modulo GRH, is not only sufficient but also necessary for (11) It is therefore a matter of good fortune that the objections against (12) do not hold against (18), and that (18) in fact is a consequence of the above mentioned generalisation of Artin's conjecture

We conclude this section with a short discussion of the role played by the Riemann-hypotheses in the proof of (18)

If ρ is a prime of T then the residue classes modulo ρ that do not contain 0 constitute a multiplicative group, say G_ρ Those classes that contain units of T form a subgroup H_ρ of G_ρ Plainly ρ belongs to P if and only if $G_\rho = H_\rho$ So if we set

k_ρ = index $(G_\rho \quad H_\rho)$

then

$P = \{\rho \quad k_\rho = 1\}$

If we now write

$P_m = \{\rho \quad k_\rho$ has no prime factors $\leqslant m\}$,

for $m = 1, 2, 3, \ldots$, then we have

$$P = \bigcap_{m=1}^{\infty} P_m, \quad P_1 \supset P_2 \supset P_3$$

Now let α, β be as in (18) and suppose that α is not congruent to a unit modulo β We are interested in the set

$V = \{\rho \quad \rho \equiv \alpha \bmod \beta$, and ρ belongs to $P\}$

which we can of course write as

(19) $$V = \bigcap_{m=1}^{\infty} V_m, \quad V_1 \supset V_2 \supset V_3$$

where V_m consists of all primes $\rho \equiv \alpha \bmod \beta$ that belong

to P_m. Without any unproved assumptions it can then be shown that for each m some positive fraction, δ_m say, of all primes belongs to V_m, where

$$\delta_1 \geqslant \delta_2 \geqslant \delta_3 \geqslant \ldots,$$

and that

$$(20) \quad \delta = \lim_{m \to \infty} \delta_m > 0.$$

It seems plausible to conclude from (19) and (20) that some positive fraction, namely δ, of all the prime elements belongs to V, and this would imply (18). It is exactly in reaching this conclusion that one uses the Riemann-hypotheses. That this is what one might need can be readily understood: generalised Riemann-hypotheses yield the remainder term in the generalised prime number theorem for algebraic number fields and, by way of the mechanism whereby one analyses V_m, also yield the remainder term in the asymptotic assertion above that some positive fraction δ_m of all the prime elements belong to V_m.

The author is indebted to A. K. Lenstra for preparing the drawings.

References to § 3

1. G. Cooke, P. J Weinberger, On the construction of division chains in algebraic number fields, with applications to SL_2, *Comm. Alg.* 3 (1975), 481–524
2. C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* 225 (1967), 209–220
3. H. W. Lenstra, Jr., *Lectures on euclidean rings,* Bielefeld 1974
4. H. W. Lenstra, Jr., On Artin's conjecture and Euclid's algorithm in global fields, *Inventiones Math.* 42 (1977), 201–224
5. T. Motzkin, The euclidean algorithm, *Bull. Amer Math. Soc.* 55 (1949), 1142–1146
6. P. Samuel, About euclidean rings, *J. Algebra* 19 (1971), 282–301
7. H. M. Stark, A complete determination of the complex quadratic fields of class-number one, *Mich. Math. J.* 14 (1967), 1–27
8. C. Queen, Arithmetic euclidean rings, *Acta Arith.* 26 (1974), 105–113
9. P. J. Weinberger, On euclidean rings of algebraic integers, *Proc. Symp. Pure Math.* 24 (*Analytic Number Theory*), 321–332, Amer. Math. Soc., 1973

H. W. Lenstra, Jr.
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam
Netherlands

A. J. van der Poorten
School of Mathematics and Physics
Macquarie University
North Ryde
NSW 2113 Australia