

UNITS IN ARITHMETIC PROGRESSION IN AN ALGEBRAIC NUMBER FIELD

MORRIS NEWMAN

ABSTRACT. It is shown that a given algebraic number field of degree $n \geq 4$ over the rationals can contain at most n units in arithmetic progression, and that this bound is sharp.

In two recent papers ([1], [2]) pairs of consecutive units in a given algebraic number field K of finite degree over the rationals were studied. It is a consequence of the Dirichlet unit theorem, the Thue-Siegel-Roth theorem, and the recent work of Baker that there can be only finitely many such pairs, and that (at least in theory) they can be effectively determined. The question naturally arises as to the maximum number of consecutive units in K . Rather surprisingly, this question admits of a simple and satisfying answer. In fact, we prove the following result in this note:

THEOREM *Let K be an algebraic number field of degree $n \geq 4$ over the rationals \mathcal{Q} . Then K contains at most n units in arithmetic progression, and this bound is sharp in that for each n there is a field K of degree n containing n units in arithmetic progression.*

PROOF. Suppose that $\alpha, \alpha + \beta, \dots, \alpha + (k-1)\beta$ are all units of K , and assume that $k > n$, so that $k-1 \geq n$. Put $\tau = \beta/\alpha$. Then τ is an integer of K and $\tau + 1, \dots, (k-1)\tau + 1$ are also units of K . Thus

$$(1) \quad N(r\tau + 1) = \pm 1, \quad 1 \leq r \leq k - 1.$$

We show first that the ambiguous value in (1) is always $+1$. This is clear if $r > 2$, since $r\tau + 1 \equiv 1 \pmod{r}$, $N(r\tau + 1) \equiv 1 \pmod{r}$. Only the values $r = 1, 2$ are in doubt therefore.

Let τ_i be the i th elementary symmetric function of the conjugates of τ , $1 \leq i \leq n$, so that τ_i is a rational integer. Then

$$(2) \quad N(r\tau + 1) = 1 + r\tau_1 + r^2\tau_2 + \dots + r^n\tau_n, \quad 1 \leq r \leq k - 1.$$

Received by the editors February 12, 1973 and, in revised form, July 16, 1973.
AMS (MOS) subject classifications (1970). Primary 12A45, 12E05.
Key words and phrases. Algebraic number fields, units.

We now show that $N(2\tau+1)=1$. For the choice $r=4$ in (2) is permissible, since $k-1 \geq n \geq 4$. Since $N(4\tau+1)=1$, this implies that

$$\begin{aligned} 1 + 4\tau_1 + 4^2\tau_2 + \cdots + 4^n\tau_n &= 1, \\ \tau_1 + 4\tau_2 + \cdots + 4^{n-1}\tau_n &= 0, \end{aligned}$$

so that τ_1 is even. Hence $N(2\tau+1) \equiv 1 \pmod{4}$, so that $N(2\tau+1)=1$. Finally, $\tau+1 \equiv 4\tau+1 \pmod{3}$, $N(\tau+1) \equiv N(4\tau+1) \equiv 1 \pmod{3}$, which implies that $N(\tau+1)=1$ as well.

We have shown therefore that

$$N(r\tau + 1) = 1, \quad 1 \leq r \leq k - 1.$$

Thus if $\tau \neq 0$, the polynomial $N(r\tau+1)-1$ is of degree n and has the k roots $r=0, 1, \dots, k-1$. Since $k \geq n+1$, this is a contradiction. The first part of the Theorem is thus proved.

To show the bound sharp, consider the field $K=Q(\theta)$, where

$$\theta(\theta + 1) \cdots (\theta + n - 1) = 1.$$

The polynomial $x(x+1) \cdots (x+n-1)-1$ is irreducible over Q (see [3, Vol. II, p. 136], for example) so that K is of degree n . Clearly, $\theta, \theta+1, \dots, \theta, +n-1$ are n units of K in arithmetic progression. This completes the proof.

As the referee points out, the irreducibility of $x(x+1) \cdots (x+n-1)-1$ over Q also follows from the first part of the Theorem above if $n \geq 4$.

The same Proof shows that there cannot be more than 4 units in arithmetic progression when $n=2$ or 3. An easy computation shows that the only quadratic fields containing 2 units differing by 1 are the fields $Q(\sqrt{-3}), Q(\sqrt{5})$.

The requirement that $n \geq 4$ in the Theorem is necessary. For example, let ζ be a primitive p th root of unity, where p is a prime >3 , and put $K=Q(\zeta+\zeta^{-1})$. Then K is of degree $(p-1)/2$, and contains the four consecutive units

$$\zeta + \frac{1}{\zeta} - 1, \quad \zeta + \frac{1}{\zeta}, \quad \zeta + \frac{1}{\zeta} + 1, \quad \zeta + \frac{1}{\zeta} + 2.$$

Here K is of degree 2 for $p=5$ and 3 for $p=7$. The fact that these are units follows from the fact that $(1-\zeta^k)/(1-\zeta)$ is a unit, provided $(k, p)=1$.

The author is indebted to the referee for his valuable comments, which materially improved both the content and the presentation of the paper.

REFERENCES

1. M. Newman, *Units in cyclotomic number fields*, J. Reine Angew. Math. **250** (1971), 3–11. MR **44** #5296.
2. ———, *Diophantine equations in cyclotomic fields*, J. Reine Angew. Math. (to appear).
3. G. Pólya and G. Szegő, *Aufgaben und Lehrsätze aus der Analysis*, Springer, Berlin, 1925; photographic reproduction, Vols. I, II, Dover, New York, 1945. MR **7**, 418.

MATHEMATICS DIVISION, NATIONAL BUREAU OF STANDARDS, WASHINGTON, D.C.
20234