PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 108, Number 2, February 1990

CONSECUTIVE UNITS

MORRIS NEWMAN

(Communicated by William Adams)

In memory of Emil Grosswald

ABSTRACT. Let p be a prime > 3, and let ζ be a primitive pth root of unity. Let k be the maximum number of consecutive units of the cyclotomic field $\mathbf{Q}(\zeta)$. It is shown that $k \leq \max(4, R, N)$, where R is the maximum number of consecutive residues modulo p, and N the maximum number of consecutive non-residues modulo p. This result implies that, for the primes $p > 3$ under 100, k is exactly 4 for $p = 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 47, 73$ (and possibly for the other primes as well). Another consequence is that $k < 2p^{1/2}$.

INTRODUCTION

Let K be an algebraic number field of degree n over the rationals $\mathbf{Q}$. It is known from the Dirichlet basis theorem for the units, the Thue-Siegel-Roth theorem, and the work of Baker, that there are only finitely many units α of K such that $\alpha + 1$ is also a unit, although a complete description of such units is lacking. It was shown in [1] that there cannot be more than n consecutive units in K, and that this bound is best possible, in the sense that, for every $n \geq 4$ there is a field K of degree n over $\mathbf{Q}$ containing n consecutive units. An easy consequence of this work is a necessary and sufficient condition for K to contain n consecutive units: If $n > 4$, $\alpha, \alpha + 1, \ldots, \alpha + n - 1$ are all units of K if and only if

$$\alpha(\alpha + 1) \cdots (\alpha + n - 1) = \pm 1.$$

In this case $K = \mathbf{Q}(\alpha)$, since the polynomials $x(x + 1) \cdots (x + n - 1) \pm 1$ are irreducible over $\mathbf{Q}$.

This result has a direct generalization which may be proved in just the same way: Suppose that $n > 4$. Then K contains at most n units whose differences are rational. If $a_1, a_2, \ldots, a_n$ are any n distinct rational integers, then there is a field K of degree n over $\mathbf{Q}$ and an element α of K such that $\alpha + a_1, \alpha + a_2, \ldots, \alpha + a_n$ are all units of K. These units must satisfy the equation

$$(\alpha + a_1)(\alpha + a_2) \cdots (\alpha + a_n) = \pm 1.$$

Received by the editors January 23, 1989 and, in revised form, March 22, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R27; Secondary 11R18.

©1990 American Mathematical Society
0002-9939/90 $1.00 + $.25 per page

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

In this case as before, $K = \mathbf{Q}(\alpha)$, since the polynomials $(x+a_1)(x+a_2)\cdots(x+a_n) \pm 1$ are irreducible over $\mathbf{Q}$.

We are concerned in this paper with units of $\mathbf{Q}(\zeta)$, where ζ is a primitive pth root of unity and p is a prime > 3. Our object is to obtain some information on the maximum number k of consecutive units of $\mathbf{Q}(\zeta)$. Since

$$\zeta + \zeta^{-1} - 1, \quad \zeta + \zeta^{-1}, \quad \zeta + \zeta^{-1} + 1, \quad \zeta + \zeta^{-1} + 2$$

are all units of $\mathbf{Q}(\zeta)$, k is at least 4. One of our results is that k is exactly 4 for 12 primes under 100, the largest of which is 73. The precise statements of the results are given in the next section.

We note a few facts that will be used in what follows. The algebraic integer $\lambda = 1 - \zeta$ is a prime of norm p in $\mathbf{Q}(\zeta)$; p ramifies completely in $\mathbf{Q}(\zeta)$, and the ideal generated by p is the $(p-1)$st power of the ideal generated by λ. Any integer α of $\mathbf{Q}(\zeta)$ and all of its conjugates are congruent modulo λ to the same rational integer a. If α is a unit, a may be taken to satisfy $1 \le a \le p-1$. If three units of $\mathbf{Q}(\zeta)$ are consecutive, they must be real. This follows from the fact that the complex conjugate of a unit is a power of ζ times the unit. Consequently we may limit our search for consecutive units to elements of $\mathbf{Q}_p = \mathbf{Q}(\zeta + \zeta^{-1})$, the maximal real subfield of $\mathbf{Q}(\zeta)$, which is of degree $n = (p-1)/2$ over $\mathbf{Q}$.

THE RESULTS

Theorem 1. *Let p be a prime > 3. Let R denote the maximum number of consecutive residues modulo p, and N the maximum number of consecutive non-residues modulo p. Then the maximum number k of consecutive units of $\mathbf{Q}_p$ satisfies*

$$k \le \max(4, R, N).$$

Corollary 1. *For the primes > 3 under 100, k is exactly 4 for the following primes (and possibly for the other primes as well):*

$$5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 47, 73.$$

Corollary 2. *The number k satisfies the inequality*

$$k < 2p^{1/2}.$$

THE PROOFS

Proof of Theorem 1. Let $n = (p-1)/2$, the degree of $\mathbf{Q}_p$ over $\mathbf{Q}$. Assume $k > 4$. Suppose that

$$\alpha, \alpha + 1, \ldots, \alpha + k - 1$$

are k consecutive units of $\mathbf{Q}_p$ and put $\beta = 1/\alpha$. Then β is a unit of $\mathbf{Q}_p$ and

$$\beta + 1, \ldots, (k-1)\beta + 1$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

are also units of $\mathbf{Q}_p$, so that their norms must be ± 1. The ambiguous sign is easily resolved: If $r \geq 3$,

$$N(r\beta + 1) \equiv 1 \mod r,$$

which implies $N(r\beta + 1) = 1$. It is only necessary to show that $\beta + 1, 2\beta + 1$ are also of norm 1. For $\beta + 1$ we have

$$N(\beta + 1) \equiv N(4\beta + 1) \mod 3,$$

which implies that $N(\beta + 1) = 1$, since $N(4\beta + 1) = 1$. For $2\beta + 1$ we argue as follows. Let $\beta_1, \beta_2, \ldots, \beta_n$ be the elementary symmetric functions of the conjugates of β so that

$$N(r\beta + 1) = 1 + \beta_1 r + \beta_2 r^2 + \cdots + \beta_n r^n.$$

First choose $r = 4$. Then, because $N(4\beta + 1) = 1$, we find that β_1 is even (in fact, divisible by 4). Next, choose $r = 2$. Then the fact that β_1 is even implies that $N(2\beta + 1) \equiv 1 \bmod 4$, which in turn implies that $N(2\beta + 1) = 1$. Thus all the norms are 1.

Now consider the norm polynomial $f(x) = N(x\beta + 1)$, where x will be restricted to rational values. Then

$$f(0) = f(1) = \cdots = f(k - 1) = 1,$$

so that

$$N(x\beta + 1) = 1 + x(x - 1)\cdots(x - k + 1)g(x),$$

where $g(x)$ is a polynomial with rational integral coefficients. Multiplying by $N(\alpha)$, we get that

$$N(x + \alpha) = N(\alpha) + N(\alpha)x(x - 1)\cdots(x - k + 1)g(x).$$

Now α and all of its conjugates are congruent modulo $\lambda = 1 - \zeta$ to a rational integer a, where $1 \leq a \leq p - 1$. It follows that if x is an integer

$$(x + a)^n \equiv (a^n + a^n x(x - 1)\cdots(x - k + 1)g(x)) \mod p,$$

which implies that

$$((x + a)/p) = (a/p) \quad \text{for } x = 0, 1, \ldots, k - 1.$$

Here $(/)$ is the Legendre symbol, and the conclusion holds by Euler's criterion, since $n = (p - 1)/2$. Hence k cannot exceed both of the numbers R, N defined in the statement of the theorem. Thus either $k \leq 4$, or $k \leq \max(R, N)$. Thus in all cases, $k \leq \max(4, R, N)$. This concludes the proof of Theorem 1.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Proof of Corollary 1. For the primes $p > 3$ under 100 we find the following table, by a simple machine calculation:

p	R	N	p	R	N	p	R	N
5	1	2	31	4	4	67	6	6
7	2	2	37	4	4	71	6	6
11	3	3	41	3	5	73	4	4
13	2	4	43	5	5	79	6	6
17	2	3	47	4	4	83	7	7
19	4	4	53	3	6	87	2	10
23	4	4	59	5	5	89	4	6
29	4	3	61	5	6	97	4	6

The result now follows directly from Theorem 1.

Proof of Corollary 2. It is classical that both R and N are bounded by $2p^{1/2}$, a result which may be found as an exercise in Vinogradov's book on number theory [2], for example. This is by no means the best bound; however, it is simple and explicit, and suffices for our purposes. Thus the proof of Corollary 2 is also complete.

A FINAL COMMENT

I have not succeeded in finding 5 consecutive units in $\mathbf{Q}_p$. A reasonable conjecture is that there are none. However, the numerical evidence available now is too scant to support any conclusion. I leave this as an open problem.

REFERENCES

1. Morris Newman, *Units in arithmetic progression in an algebraic number field*, Proc. Amer. Math. Soc. **43** (1974), 266–268.
2. I. M. Vinogradov, *Elements of number theory*, Dover, 1954; translated from the fifth Russian edition of 1954.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CALIFORNIA 93106

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use