ACTA ARITHMETICA
XXX (1976)

On the solutions of diophantine equations in units

by

EDWARD H. GROSSMAN (New York, N.Y.)

1. Introduction. From the work of Siegel and others it follows that if $f(x)$ is any integral polynomial different from $\pm x^m$, the equation $f(\eta) = \xi$ has only a finite number of solutions in units η, ξ from a fixed number field K. For $f(x) = x^m - 1$, $m \geqslant 2$ and $K = Q(\zeta_p)$, where p is a prime and $\zeta_p = \exp(2\pi i/p)$, the solutions in units of $f(\eta) = \xi$ have been studied by Mordell [3], Newman [4], [5] and Ennola [1], [2]. In this paper we will generalize their results in two directions. For a class of fields which we call almost real (see § 2) and which includes all abelian extensions of Q we prove:

THEOREM 1. *Let K be an almost real field. If $m > 2$ the equation*

(1) $$\eta^m - 1 = \xi$$

has no solutions in units η, ξ of K, where η is not a root of unity.

For the case of cyclotomic fields $Q(\zeta_p)$ we prove a further refinement of this result. Namely, let $\Phi_m(x)$ denote the mth cyclotomic polynomial. In § 3 we prove:

THEOREM 2. *Let $K_p = Q(\zeta_p)$, $p > 3$. If $m > 2$ and $m \neq 3$, or 6 then the equation*

(2) $$\Phi_m(\eta) = \xi$$

has no solutions in units η, ξ of K_p where η is not a root of unity. For $m = 3$ or 6 the only solutions to (2) *with η a unit, not a root of unity, are provided by*

(2a) $$m = 3, \quad \eta = -(1+\zeta_p^a)^{\pm 1}, \quad 1 \leqslant a \leqslant p-1$$

and

(2b) $$m = 6, \quad \eta = (1+\zeta_p^a)^{\pm 1}, \quad 1 \leqslant a \leqslant p-1.$$

2. Almost real fields. In what follows K will always denote a finite extension of Q. If $K \subset C$ we let $\bar{K} = \{a \in C: \bar{a} \in K\}$, where $\bar{a}$ denotes the complex conjugate of a. The class of fields we will consider is given in the following definition.

DEFINITION. A subfield K of C is called *almost real* if $K = \bar{K}$ and for every isomorphism σ of K in C

(3) $$\sigma(\bar{a}) = \overline{\sigma(a)}$$

for all $a \in K$.

It is clear that every finite abelian extension of Q satisfies this definition. Moreover if K is an arbitrary almost real field its normal closure over Q will also be almost real. The justification for the terminology is provided by the next proposition.

PROPOSITION. *Let K_r = the maximal totally real subfield of K.*

(i) *If K is an almost real field then $[K:K_r] \leqslant 2$.*

(ii) *If K is normal over Q and $[K:K_r] \leqslant 2$ then K is an almost real field.*

Proof. (i) Let $K = Q(\theta)$ and observe that by (3) the polynomial $(x-\theta)(x-\bar{\theta})$ has coefficients in K_r.

(ii) We may assume $K \neq K_r$. With $K = K_r(\theta)$ it suffices to show that (3) holds for θ. Let $p(x) = x^2+bx+c$ be the irreducible polynomial satisfied by θ over K_r. Since b and c are real $p(\bar{\theta}) = 0$ and since $K \neq K_r$, $\theta \neq \bar{\theta}$. If σ is any automorphism of K in C then $\sigma(\theta)$ and $\sigma(\bar{\theta})$ are the distinct roots of $x^2+\sigma(b)x+\sigma(c)$. As $\overline{\sigma(\theta)}$ is also a root and $\sigma(\theta)$ is not real we have $\sigma(\bar{\theta}) = \overline{\sigma(\theta)}$ and so K is almost real.

Proof of Theorem 1. We note first the following inequality valid for all integers $m \geqslant 2$ and all complex numbers z.

(4) $$|z^m-1| \geqslant \max(|z|, 1)^{m-2}\big||z|^2-1\big|.$$

Suppose then that η, ξ satisfy (1), where η is not a root of unity and let $\eta = \eta_1, \ldots, \eta_l$, $l = [K:Q]$, be the complete set of conjugates of η with respect to K. Since η is not a root of unity it follows from (3) that $|\eta_i| \neq 1$ for all i. Denoting by N the norm map from K to Q we have from (4) that

$$1 = |N(\eta^m-1)| = \prod_{1\leqslant i\leqslant l} |\eta_i^m-1| \geqslant \prod_{1\leqslant i\leqslant l} \max(|\eta_i|, 1)^{m-2}\big|N(|\eta|^2-1)\big| > 1$$

since $|\eta|^2-1$ is a non zero algebraic integer in K. This contradiction establishes the theorem.

Remark. In fact it may be shown that if $\xi = \eta^m-1$, η not a root of unity, then $N(\xi) \geqslant \sqrt{2}^{m-2}$.

For $m = 2$ the inequality (4) yields the following corollary.

COROLLARY 1. *If K is an almost real field and*

(5) $$\eta^2-1 = \xi$$

has a solution in units η, ξ of K, where η is not a root of unity, then η is totally real.

Proof. Observe that when $m = 2$, (4) becomes $|z^2-1| \geqslant \big||z|^2-1\big|$ and equality holds if and only if z is real. Hence if $\xi = \eta^2-1$ is a unit we have

$$1 = |N(\xi)| \geqslant \prod_{1\leqslant i\leqslant l} \big||\eta_i|^2-1\big| \geqslant 1$$

and by the remark η_i is real for all conjugates.

Remark. Solutions to (5) for cyclotomic fields may be found in [3].

As a second corollary we give another proof of a result due to Mordell [3], Newman [4], [5] and Ennola [1].

COROLLARY 2. *Let $K_p = Q(\zeta)$ where $\zeta = \exp(2\pi i/p)$, $p > 3$ a prime. Let*

$$\eta_k = \frac{1-\zeta^k}{1-\zeta}, \quad 2 \leqslant k \leqslant p-2.$$

Then η_k is never of the form η^m for any $m > 1$.

Proof. Observe that η_k and $\xi_k = \eta_k-1$ are units. Moreover since $k \not\equiv \pm 1 \bmod p$, $|\eta_k| > 1$ so that η_k is not a root of unity. Noting also that η_k is not real, the result follows from Theorem 1 and Corollary 1.

3. Cyclotomic fields. In this section K_m will denote the field $Q(\zeta_m)$ where $\zeta_m = \exp(2\pi i/m)$. We recall that K_m is an abelian extension of Q of degree $\varphi(m)$ with Galois group given by the substitutions $\zeta_m \to \zeta_m^b$ $(b, m) = 1$. Moreover if $(m, n) = 1$ then $K_mK_n = K_{mn}$ and $K_m \cap K_n = Q$. Finally if $\eta \in K_m$ is a unit then $\bar{\eta} = \pm\zeta_m^k\eta$ and if $m = p$ is a prime we have in fact $\bar{\eta} = \zeta_p^k\eta$.

The proof of Theorem 2 depends on two lemmas.

LEMMA 1. *The equation $\Phi_p(\eta) = \xi$, $p > 3$, has no solutions in units η, ξ of K_p, where η is not a root of unity.*

Proof. If η is (totally) real we have from (4) that for $1 \leqslant i \leqslant p-1$,

$$|\xi_i| = \left|\frac{\eta_i^p-1}{\eta_i-1}\right| \geqslant \max(|\eta_i|, 1)^{p-2}|\eta_i+1|$$

and multiplying these inequalities gives the result in this case. If η is not real then $\bar{\eta} = \zeta_p^k\eta$ where $(k, p) = 1$. If $\Phi_p(\eta)$ is a unit so is its divisor $\eta-\zeta_p^{-k}$.

Since

$$\overline{\eta-\zeta_p^{-k}} = \zeta_p^k\eta-\zeta_p^k = \zeta_p^k(\eta-1)$$

it follows that $\eta-1$ is also a unit. Hence $\eta^p-1 = (\eta-1)\xi$ is a unit, which is impossible by Theorem 1.

LEMMA 2. *If $p > 3$ and $p \nmid m$ then for $m > 2$ the only solutions to* (2) *in units η, ξ of K_p, where η is not a root of unity, are given by* (2a) *for $m = 3$ and* (2b) *for $m = 6$.*

Proof. If $\Phi_m(\eta)$ is a unit we obtain that $\eta - \zeta_m$ is a unit in K_{mp}. Thus $\overline{\eta-\zeta_m} = \varrho(\eta-\zeta_m)$ where $\varrho = \pm\zeta_p^s\zeta_m^t$. Using that $\bar\eta = \zeta_p^a\eta$ we obtain

$$(6)\qquad (\zeta_p^a - \varrho)\eta = \zeta_m^{-1} - \zeta_m\varrho.$$

If $\zeta_p^a = \varrho$ then also $\zeta_m^{-2} = \varrho = \zeta_p^a$ which implies that $\zeta_m^2 = 1$ contradicting the assumption that $m > 2$. Thus (6) gives

$$(7)\qquad \eta = \frac{\zeta_m^{-1} - \zeta_m\varrho}{\zeta_p^a - \varrho} = \frac{\zeta_m^{-1} \pm \zeta_m^{t+1}\zeta_p^s}{\zeta_p^a \pm \zeta_m^t\zeta_p^s}.$$

Since $\eta \in K_p$ it is invariant under the automorphism of K_{mp} which takes $\zeta_p \to \zeta_p$ and $\zeta_m \to \zeta_m^{-1}$. Applying this to (7) gives

$$\frac{\zeta_m^{-1} \pm \zeta_m^{t+1}\zeta_p^s}{\zeta_p^a \pm \zeta_m^t\zeta_p^s} = \frac{\zeta_m \pm \zeta_m^{-(t+1)}\zeta_p^s}{\zeta_p^a \pm \zeta_m^{-t}\zeta_p^s},$$

which after cross multiplying and simplifying becomes

$$(8)\qquad (\zeta_p^a - \zeta_p^{2s})(\zeta_m^{-1} - \zeta_m) = \pm(\zeta_m^{t+1} - \zeta_m^{-t-1})(\zeta_p^{a+s} - \zeta_p^s).$$

If $\zeta_p^a = 1$, the right side of (8) is zero and we obtain since $m > 2$ that $\zeta_p^{2s} = 1$, hence $s \equiv 0 \bmod p$. Thus from (7) $\eta \in K_p \cap K_m = Q$ and since η is a unit, $\eta = \pm 1$ a contradiction. Therefore we may assume $\zeta_p^a \neq 1$, and we show then that none of the factors in (8) are zero. This is clear for $(\zeta_m^{-1} - \zeta_m)$ and $(\zeta_p^{a+s} - \zeta_p^s)$. Assuming that $\zeta_p^a = \zeta_p^{2s}$ we must have $\zeta_m^{2(t+1)} = 1$ or $\zeta_m^t = \pm\zeta_m^{-1}$. Substituting this in (7) gives

$$\eta = \frac{\zeta_m^{-1} \pm \zeta_p^s}{\zeta_p^{2s} \pm \zeta_p^s\zeta_m^{-1}} = \pm\zeta_p^{-s}$$

which contradicts the hypothesis that η is not a root of unity. Hence (8) yields

$$(9)\qquad \frac{\zeta_m^{-1} - \zeta_m}{\zeta_m^{t+1} - \zeta_m^{-t-1}} = \pm\frac{\zeta_p^{a+s} - \zeta_p^s}{\zeta_p^a - \zeta_p^{2s}}.$$

Since $K_m \cap K_p = Q$ both sides of this equation are rational and as we show are equal to ± 1. Let $\varepsilon = \zeta_p^a$. Since $\zeta_p^a \neq 1$, ε is a primitive pth root of unity so that $\zeta_p^{2s} = \varepsilon^b$. Then

$$(10)\qquad \frac{\zeta_p^{a+s} - \zeta_p^s}{\zeta_p^a - \zeta_p^{2s}} = \frac{\zeta_p^s(\varepsilon - 1)}{\varepsilon - \varepsilon^b},$$

which is clearly a unit, hence equal to ± 1. Thus

$$(11)\qquad \frac{\varepsilon^{b-1} - 1}{\varepsilon - 1} = \pm\zeta_p^s\varepsilon^{-1}.$$

Considering (11) modulo $(1-\varepsilon)$ we obtain $b - 1 \equiv \pm 1 \bmod p$. If $b \equiv 0 \bmod p$ we have $\zeta_p^{2s} = 1$. Otherwise $b \equiv 2 \bmod p$ and (11) becomes $\pm 1 = \zeta_p^s\varepsilon^{-1}$. Since -1 is not a pth root of unity we must have $\zeta_p^s = \varepsilon = \zeta_p^a$.

Returning then to (9), in all cases

$$\pm 1 = \frac{\zeta_m^t(\zeta_m^2 - 1)}{(\zeta_m^{2t+2} - 1)}$$

and this gives

$$\zeta_m^2(1 \mp \zeta_m^t) = (1 \mp \zeta_m^{-t}).$$

Hence either $1 \mp \zeta_m^t = 0$ or

$$\zeta_m^2 = \frac{1 \mp \zeta_m^{-t}}{1 \mp \zeta_m^t} = \pm\zeta_m^{-t}.$$

We summarize these results in the following four cases.

(i) $\zeta_p^{2s} = 1$; $\zeta_m^t = \pm 1$.
(ii) $\zeta_p^{2s} = 1$; $\zeta_m^2 = \pm\zeta_m^{-t}$.
(iii) $\zeta_p^s = \zeta_p^a$; $\zeta_m^t = \pm 1$.
(iv) $\zeta_p^s = \zeta_p^a$; $\zeta_m^2 = \pm\zeta_m^{-t}$.

Cases (i) and (iv) give respectively upon substitution in (7),

$$(12)\qquad (\zeta_p^a \pm 1)\eta = \zeta_m^{-1} \pm \zeta_m$$

and

$$(13)\qquad (\zeta_p^a \pm 1)(\eta^{-1}\zeta_p^{-a}) = \zeta_m \pm \zeta_m^{-1}.$$

Hence $\zeta_m \pm \zeta_m^{-1}$ is a rational integer and the plus sign must apply. Then the left sides of (12) and (13) being units require that $\zeta_m + \zeta_m^{-1} = \pm 1$ which is possible only if $m = 3$ or 6. In these two cases, noting that $\Phi_m(\eta)$ is a unit if and only if $\Phi_m(1/\eta)$ and $\Phi_m(\bar\eta)$ are units, and recalling that $\bar\eta = \zeta_p^a\eta$ we must consider only $\Phi_6(1+\zeta_p^a)$ and $\Phi_3\big(-(1+\zeta_p^a)\big)$. Since in fact these are both equal to

$$1 + \zeta_p^a + \zeta_p^{2a} = \frac{1 - \zeta_p^{3a}}{1 - \zeta_p^a}$$

which is a unit, we obtain the listed solutions to (2) for $m = 3$ and 6.

If (ii) holds then we obtain again from (7) that

$$\eta = \frac{\zeta_m^{-1} \pm \zeta_m^{-1}}{\zeta_p^a \pm \zeta_m^{-2}} = \frac{2\zeta_m^{-1}}{\zeta_p^a + \zeta_m^{-2}} \tag{14}$$

since $\eta \neq 0$. Applying again the automorphism $\zeta_p \to \zeta_p$; $\zeta_m \to \zeta_m^{-1}$ (14) yields

$$\frac{\zeta_m^{-1}}{\zeta_p^a + \zeta_m^{-2}} = \frac{\zeta_m}{\zeta_p^a + \zeta_m^2}$$

which upon simplification gives

$$\zeta_p^a(\zeta_m^{-1} - \zeta_m) = (\zeta_m^{-1} - \zeta_m)$$

and so $\zeta_p^a = 1$, a contradiction. Case (iii) is treated in a way similar to (ii) and is omitted. This completes the proof of the lemma.

Remark. The case when η is a real unit, i.e. $\zeta_p^a = 1$ is given implicitly in [5].

Proof of Theorem 2. Letting $m = p^k n$ where $p \nmid n$, we use induction on k. If $k = 0$ the solutions are given in Lemma 2. If $k = 1$ then observe that

$$\Phi_m(\eta) = \prod_{\zeta_p^v \neq 1} \Phi_n(\eta, \zeta_p^v) \tag{15}$$

where $\Phi_n(x, y) = y^{\varphi(n)}\Phi(x/y)$. Thus $\Phi_m(\eta)$ is a unit if and only if $\Phi_n(\eta\zeta_p^{-v})$ is a unit for all $v \not\equiv 0 \bmod p$. If $n > 2$ and $n \neq 3$ or 6 this is impossible. If $n = 1$ or 2 then since $\Phi_{2p}(\eta) = \Phi_p(-\eta)$ the result follows from Lemma 1.

In the remaining cases $n = 3$ or 6, letting $\zeta = \zeta_p$ it suffices to show that there exists no η satisfying for all v, $1 \leqslant v \leqslant p-1$,

$$\eta = \zeta^v(1+\zeta^{s_v})^{e_v} \tag{16}$$

where $e_v = \pm 1$.

Suppose first η satisfies (16) with $e_v \neq e_u$ for some $v \neq u$. Then with $s = s_v$ and $t = s_u$

$$(1+\zeta^s)(1+\zeta^t) = \zeta^{v-u}$$

and considering this equation modulo $(1-\zeta)$ gives a contradiction for $p \neq 3$. Thus we may assume in (16) that $e_v = 1$ for all v.

For $v = 1$ or $p-1$ (16) gives, with $a = s_1$, $b = s_{p-1}$,

$$\eta = \zeta(1+\zeta^a) = \zeta^{-1}(1+\zeta^b). \tag{17}$$

Comparing complex conjugates in (17) gives $b \equiv a+4 \bmod p$ which on substituting in (17) gives $a \equiv -2 \bmod p$ and therefore $\eta = \zeta + \zeta^{-1}$. Now consider (16) for $v = 2$ so that $\eta = \zeta + \zeta^{-1} = \zeta^2(1+\zeta^c)$. Again comparing complex conjugates gives $c \equiv -4 \bmod p$ so that $\zeta + \zeta^{-1} = \zeta^2 + \zeta^{-2}$ from which $\zeta^3 = 1$, a contradiction. Therefore (2) has no solutions for $m = pn$, with $p \nmid n$. For $m = p^k n$, $k \geqslant 2$, let $m = p\tilde{m}$ where $p | \tilde{m}$. Then $\Phi_m(\eta) = \Phi_{\tilde{m}}(\eta^p)$ and the proof is completed by induction.

Remark. It follows easily from (4) and the factorization

$$\Phi_m(\eta) = \prod_{d|m} (\eta^d - 1)^{\mu(m/d)}$$

that if K is any almost real field then for $m > m_0([K:Q])$ equation (2) has no solutions with η not a root of unity. I do not know whether in general a lower bound for m_0 may be found independent of $[K:Q]$.

References

[1] V. Ennola, *Proof of a conjecture of Morris Newman*, J. Reine Angew. Math. 264 (1973), pp. 203–206.

[2] — *A note on a cyclotomic diophantine equation*, Acta Arith. 28 (1975), pp. 157–159.

[3] L. J. Mordell, *On a cyclotomic diophantine equation*, Journ. de Math. 42 (1963), pp. 205–208.

[4] M. Newman, *Units in cyclotomic number fields*, J. Reine Angew. Math. 250 (1971), pp. 3–11.

[5] — *Diophantine equations in cyclotomic fields*, J. Reine Angew. Math. 265 (1974), pp. 84–89.

Received on 6. 8. 1974
and in revised form on 10. 12. 1974 (610)