DIOPHANTINE EQUATIONS IN CYCLOTOMIC FIELDS

Dedicated to Professor L. J. Mordell on his 80th birthday

N. C. ANKENY AND S. CHOWLA

1. In this paper we consider the problem: when is a given rational integer equal to the square of the absolute value of an integer α in a cyclotomic field? As an example let us ask for what g is

$$|\alpha|^2 = p \qquad [\alpha \in R(e^{2\pi i/g})],$$

where p is a given rational prime? It is almost trivial (from the theory of the Gaussian sum or otherwise) that a solution exists with $g = p$; it is less trivial that a solution also exists when $g = p^2+p+1$; but it is not asserted that solutions do not exist for other values of g. While we are unable to give anything like a complete answer to the problem proposed, we can prove something in this direction, namely

THEOREM I. *The equation*

$$|\alpha|^2 = p$$

is impossible for integers α belonging to the cyclotomic field $R(e^{2\pi i/g})$, where g is a prime and

$$g > p^{p^2}.$$

THEOREM II. *Under the conditions of Theorem I, the equation*

$$|\alpha|^2 = p^2$$

has no solutions apart from the obvious ones, namely

$$\alpha = \pm p\theta^w, \ \alpha = \pm p.$$

where w is prime to g, and

$$\theta = e^{2\pi i/g}.$$

Theorem II has an application to the theory of difference sets as developed by Marshall Hall [1] and Marshall Hall and Ryser [2]. To use the notation of the latter paper, we call the set of integers

$$d_1, \ldots, d_k$$

a difference set (mod v) if the congruence

$$d_i - d_j \equiv n \pmod v$$

has the same number λ of solutions for every $n \not\equiv 0 \pmod v$. It is easy to see that

$$\lambda = \frac{k(k-1)}{(v-1)}.$$

Further Hall and Ryser define a "multiplier" of a difference set as follows. If $d_1, \ldots, d_k$ are a difference set (mod v) we say that t is a multiplier of the set if for some s the residues $td_1, \ldots, td_k$ (mod v) are $d_1+s, \ldots, d_k+s$ (mod v), apart from order. They prove the following:

THEOREM. *Let p be a prime divisor of $k-\lambda$ such that $p > \lambda$ and $v \not\equiv 0 \pmod p$. Then p is a multiplier of the difference set $d_1, \ldots, d_k$ (mod v).*

Received 19 December, 1967.

[J. LONDON MATH. SOC., 43 (1968), 67–70]

They raise the interesting question whether the restriction $p > \lambda$ is essential here. This conjecture appears difficult, but in many special cases our Theorem II establishes the existence of multipliers p with $p < \lambda$. Details will form the subject of another paper.

2. In this section we shall prove Theorem II. We denote by θ any root $\neq 1$ of $\theta^g = 1$. Write

$$\alpha = S(\theta) = a_0 + a_1\theta + \ldots + a_{g-1}\theta^{g-1}.$$

Suppose that

$$\alpha\bar{\alpha} = p^2. \tag{1}$$

If we write

$$S_1(\theta) = \sum_{i=0}^{g-1} (a_i + m)\theta^i = \sum_{i=0}^{g-1} b_i\theta^i$$

for an arbitrary integer m, it is clear that

$$S(\theta) = S_1(\theta).$$

We shall choose m so that

$$S^2(1) = p^2. \tag{2}$$

Clearly

$$\sum_{n=1}^{g-1} S_1(\theta^n)S_1(\theta^{-n}) + S_1{}^2(1) = g\sum_{i=0}^{g-1} b_i{}^2,$$

$$(g-1)p^2 + S_1{}^2(1) = g\sum_{i=0}^{g=1} b_i{}^2,$$

$$S_1(1) = \sum_{i=0}^{g-1} b_i \equiv \pm p \pmod{g},$$

$$\sum_{i=0}^{g-1} b_i = \pm p + mg,$$

$$\sum_{i=0}^{g-1} a_i = \pm p,$$

$$S(1) = \pm p.$$

Hence (2) is established.

We have from (1)

$$\{p^2\} = \{S(\theta)\}\{S(\theta^{-1})\}, \tag{3}$$

where the curly bracket denotes an ideal. From (3) and the Hilbert theory [3] it follows since $p \neq g$ that

$$\{S(\theta^p)\} = \{S(\theta)\},$$

$$S(\theta^p) = \varepsilon(\theta)S(\theta), \tag{4}$$

where $\varepsilon(\theta)$ is a unit of the field $R(\theta)$. From (1) and (4)

$$\varepsilon(\theta)\varepsilon(\theta^{-1}) = 1. \tag{5}$$

From (5) it follows (see Landau [4]) that

$$\varepsilon(\theta) = \pm\theta^{w}, \tag{6}$$

$$S(\theta^{p}) = \pm\theta^{w} S(\theta). \tag{7}$$

If possible, let

$$S(\theta^{p}) = -\theta^{w} S(\theta); \tag{8}$$

then

$$2\sum_{i=0}^{g-1} a_i \equiv 0 \pmod{g}, \tag{9}$$

which is false for g is an odd prime, and

$$\sum_{0}^{g-1} a_i = \pm p, \text{ and } g > p^{p^2}$$

by the hypotheses of Theorems I and II.

Hence

$$S(\theta^{p}) = \theta^{w} S(\theta). \tag{10}$$

Put

$$S(\theta) = \theta^{c}\, T(\theta), \tag{11}$$

where c is yet to be determined. Then

$$\frac{S(\theta^{p})}{S(\theta)} = \frac{\theta^{cp}}{\theta^{c}}\,\frac{T(\theta^{p})}{T(\theta)}.$$

Choose c so that

$$(p-1)c \equiv w \pmod{g}.$$

Then

$$T(\theta^{p}) = T(\theta). \tag{12}$$

Write

$$T(\theta) = c_0 + c_1\theta + \ldots + c_{g-1}\theta^{g-1},$$

where by (11), the c's here are a cyclic permutation of the a's in the definition of $S(\theta)$. Define f by

$$f \text{ is the least positive integer such that } p^{f} \equiv 1 \pmod{g}. \tag{13}$$

From (12) and (13) we get

$$T(\theta) = c_0 + c_1(\theta + \theta^{p} + \ldots + \theta^{p^{f-1}}) + c_i(\theta^{i} + \theta^{ip} + \theta^{ip^2} + \ldots) + c_j(\theta^{j} + \theta^{jp} + \theta^{jp^2} + \ldots) + \ldots, \tag{14}$$

where $i \not\equiv p^{a}$, $j \not\equiv p^{b}$, $(j/i) \not\equiv p^{d} \pmod{g}$, etc.

Again, as before, we assume the c's chosen so that $|T^2(\theta)| = T^2(1) = p^2$. Then

$$\sum_{h=0}^{g-1} T(\theta^{h})\, T(\theta^{-h}) + T^2(1) = g\sum_{h=0}^{g-1} c_h^{2},$$

$$(g-1)p^2 + p^2 = g\sum_{h=0}^{g-1} c_h^{2},$$

$$p^2 = \sum_{i=0}^{g-1} c_i^{2}. \tag{15}$$

From (14) and (15),

$$c_0{}^2+f(c_1{}^2+c_i{}^2+c_j{}^2+\ldots)=p^2, \tag{16}$$

where c_i, c_j, etc., were defined below (14). From (13),

$$f \geqslant \frac{\log g}{\log p}. \tag{17}$$

From (16) and (17)

$$\frac{\log g}{\log p} \leqslant p^2 \tag{18}$$

unless $c_t=0$ $(1 \leqslant t \leqslant g-1)$; (18) contradicts our hypothesis. Thus

$$c_t=0 \ (1 \leqslant t \leqslant g-1)$$

and so $c_0 = \pm p$ from (15). So

$$S(\theta) = c_0 \theta^c \, T(\theta) = \pm p \theta^c.$$

This completes the proof of Theorem II. The deduction of Theorem I from Theorem II is left to the reader.

References

1. Marshall Hall, " Cyclic Projective Planes ", *Duke Math. J.*, 14 (1947), 1079–1090.
2. ——— and H. J. Ryser, " Cyclic Incidence Matrices ", *Canad. J. Math.*, 3 (1951), 495–502.
3. D. Hilbert, *Gesammelte Abhandlungen* I, 13–14.
4. E. Landau, *Vorlesungen über Zahlentheorie* III, Satz 910.

Institute for Advanced Study,
Princeton, N.J.

University of Kansas.