J. Natn. Sci. Coun. Sri Lanka 1977 **5**(1) : 33—40

Two Diophantine Equations in Cyclotomic Fields

THARMAMBIKAI PONNUDURAI
Department of Mathematics and Statistics, University of Sri Lanka, Jaffna Campus, Thirunelvely, Sri Lanka.

(*Paper accepted:* 6 *January* 1977)

Abstract : If p, g are distinct odd rational primes, it is shown that the diophantine equations $|\alpha|^2 = p^2$ and $|\alpha|^2 = p$ have no solutions in integers belonging to the cyclotomic field $K = R\,(e^{2\pi i/g})$, if $g > \frac{1}{2}p^{p2/3}$. It is also shown that there are values of p and g, other than those satisfying $g = p$ or $g = p^2 + p + 1$, for which the two equations have non-trivial solutions in integers belonging to K.

1. Introduction

Let p and g be distinct odd rational primes. Ankeny and Chowla[1] have proved that the equations

$$|\,\alpha\,|^2 = p^2 \tag{1}$$

and

$$|\,\alpha\,|^2 = p \tag{2}$$

have no non-trivial solutions in integers α belonging to the cyclotomic field $K = R\,(e^{2\pi i/g})$, if $g > p^{p2}$. In section 2, we show that the condition $g > p^{p^2}$ can be replaced by $g > \frac{1}{2}\,p^{p\frac{2}{3}}$ while in section 3 we obtain values of p and g for which the equations (1) and (2) have non-trivial solutions in integers belonging to K.

2. Condition for non-solvability

Theorem 1. If $g > \frac{1}{2}\,p^{p\frac{2}{3}}$, the equation (1) has no solutions in integers α belonging to the field K apart from the trivial ones, namely, $\alpha = \pm p\theta^r$, $\alpha = \pm p$, where r is prime to g, and $\theta = e^{2\pi i/g}$.

Proof. Write

$$\alpha = T\,(\,\theta\,) = c_0 + c_1\,\theta + c_2\,\theta^2 + \ldots + c_{g-1}\,\theta^{g-1}$$

where c_0, c_1, $c_2,\ldots,c_{g-1}$ are defined.[1]

Then, if α is a solution of equation (1), it can be shown,[1] that

$$T\,(\,\theta\,) = c_0 + c_1\,(\,\theta + \theta^p + \theta^{p2} + \ldots + \theta^{p^{f-1}}) + c_2\,(\,\theta^i + \theta^{ip} + \theta^{ip2} + \ldots + \theta^{ip^{f-1}}$$
$$+ c_j\,(\,\theta^j + \theta^{jp} + \theta^{jp2} + \ldots + \theta^{jp^{f-1}}\,) + \ldots\ldots$$

15799—6

where f is the least positive integer such that

$$p^f \equiv 1 \pmod{g} \tag{3}$$

and $i \equiv p^c$, $j \equiv p^b$, $(j|i) \equiv p^d \pmod{g}$, etc.,

and that

$$c^2_0 + f\,(c_1^2 + c_i^2 + c_j^2 + \ldots\ldots) = p^2 \tag{4}$$

and

$$c_0 + f\,(c_1 + c_i + c_j + \ldots\ldots) = \pm p \tag{5}$$

Consider the following three cases: –

Case (*i*). Suppose that $c_0 \neq 0$ and that only one of $c_1, c_i, c_j, \ldots\ldots$, say c_t, is non-zero.

Then, equations (4) and (5) reduce to

$$c_0^2 + f\,c_t^2 = p^2$$

and

$$c_0 + f\,c_t = \pm p.$$

But, since $c_t \neq 0$ and $f \neq 0$, the above two equations give

$$c_0 = \frac{1-f}{2}\,c_t$$

and so $c_0 = \pm \dfrac{1-f}{2}$ and $c_t = \pm 1$, as $(c_0, c_t) = 1$.

Whence

$$p^2 = \left(\frac{1-f}{2}\right)^2 + f = \left(\frac{1+f}{2}\right)^2$$

and therefore

$$p = \frac{1+f}{2} > \frac{f}{2}. \tag{6}$$

By equation (3), $p^f = 1 + \lambda g$, where λ is an even positive integer.

Hence,

$$f \log p = \log (1 + \lambda g) > \log 2g,$$

and so

$$f > \frac{\log 2g}{\log p}. \tag{7}$$

From equations (6) and (7), we obtain

$$2p > \frac{\log 2g}{\log p},$$

which gives

$$g < \tfrac{1}{2} p^{2p} < \tfrac{1}{2} p^{p\frac{2}{3}}, \quad \text{if } p \geqslant 7.$$

Take the exceptional cases $p = 3$ and $p = 5$.

When $p = 3$, we have from equation (6), $f = 5$, and therefore equation (3) gives

$$3^5 \equiv 1 \pmod{g},$$

which implies that the only possible value of g is

$$g = 11 < \tfrac{1}{2} p^{p\frac{2}{3}}.$$

When $p = 5$, we have from equation (6), $f = 9$ and equation (3) gives

$$5^9 \equiv 1 \pmod{g},$$

which implies that the only possible values of g are $g = 19, 31$ or 829, and for each of these values of g,

$$g < \tfrac{1}{2} p^{p\frac{2}{3}}.$$

Thus, in this case, equation (1) has no non-trivial solutions if

$$g > \tfrac{1}{2} p^{p\frac{2}{3}}.$$

Case (ii). Suppose only two of $c_1, c_i, c_j, \ldots\ldots$ say c_t and c_u, are non-zero.

First, suppose $c_t = \pm 1$ and $c_u = \pm 1$.

Then equations (4) and (5) reduce to

$$c_0^2 + 2f = p^2 \tag{8}$$

and

$$c_0 + f(\pm 1 \pm 1) = \pm p. \tag{9}$$

But, since $c_0 \neq \pm p$ as $f \neq 0$, it follows that c_t and c_u must take the same sign and so equation (9) gives

$$c_0 \pm 2f = \pm p. \tag{10}$$

Since $f \neq 0$, from equations (8) and (10), we get $2(f \pm c_0) = 1$, which is clearly impossible. Hence, our supposition that $c_t = \pm 1$ and $c_u = \pm 1$ is false, and so it easily follows from equation (4) that $p^2 \geqslant 5f$.
Proceeding as in case (i), it can be shown that

$$g < \tfrac{1}{2} p^{p\frac{5}{2}} < \tfrac{1}{2} p^{p\frac{2}{3}}.$$

Thus in this case, equation (1) has no non-trivial solution if

$$g > \tfrac{1}{2} p^{p\frac{2}{3}}.$$

Case (iii). Suppose $n\ (\geqslant 3)$ of $c_1, c_i, c_j, \ldots\ldots$ are non-zero.

Then, from equation (4) we have

$$p \geqslant n f$$

Proceeding as in case (i), it can be shown that

$$g < \tfrac{1}{2} p^{p\frac{2}{n}} \leqslant \tfrac{1}{2} p^{p\frac{2}{3}}, \quad \text{since } n \geqslant 3.$$

Thus, in this case also equation (1) has no non-trivial solutions if

$$g > \tfrac{1}{2} p^{p\frac{2}{3}}.$$

The proof of the theorem is now complete.

The next theorem follows directly from Theorem 1.

Theorem 2. If $g > \frac{1}{2} p^{p\frac{2}{3}}$, the equation (2) is impossible in integers α belonging to the field K.

3. Equations with non-trivial solutions

Theorem 3. If p and g are odd primes such that p is a primitive root of g, then the equation (1) has no non-trivial solutions in integers α belonging to the field K.

Proof. Since p is a primitive root of g, we have $f = g - 1$ and so

$$c_1 = c_2 = c_3 = \ldots\ldots = c_{g-1}.$$

Hence,

$$\begin{aligned} \alpha = T(\theta) &= c_0 + c_1 (\theta + \theta^2 + \theta^3 + \ldots\ldots + \theta^{g-1}) \\ &= c_0 - c_1 \end{aligned}$$

and we obtain a trivial solution.

The theorem now follows.

Corollary. Under the conditions of Theorem 3, the equation (2) is impossible in integers α belonging to the field K.

Theorem 4. Let p and g be odd primes such that $g = 2p + 1$, $p \equiv 1 \pmod 4$ and $2p - 1 = k^2$, where k is a rational integer.

Then

$$\alpha = \frac{k+1}{2} + \theta^2 + \theta^{2p} + \theta^{2p^2} + \ldots\ldots + \theta^{2p^{p-1}}$$

is a solution of the equation (2).

Proof. Since $(2|g) = -1$, as $g = 2p + 1$ and $p \equiv 1 \pmod 4$, 2 is a quadratic non-residue of g and so by Euler's Criterion,

$$2^{\frac{g-1}{2}} \equiv -1 \pmod g.$$

Whence,

$$2^p \equiv -1 \pmod g.$$

Since $g > 3$, it follows that $2^t \not\equiv -1 \pmod g$ for $1 \leqslant t \leqslant p$. But, since $2p \equiv -1 \pmod g$, we have

$$(2p)^p = -1 \pmod g,$$

and so $p^p \equiv 1 \pmod{g}$ and $p^t \not\equiv 1 \pmod{g}$ for $1 \leqslant t < p$.

Also $(p|g) = 1$.

Hence, $2, 2p, 2p^2, \ldots\ldots\ldots\ldots, 2p^{p-1}$ are incongruent quadratic non-residues modulo g. But, all the $\frac{g-1}{2}$ incongruent quadratic non-residues modulo g are given by $-1^2, -2^2, -3^2, \ldots\ldots, -\left(\frac{g-1}{2}\right)^2$ and so $2, 2p, 2p^2, \ldots\ldots, 2p^{p-1}$ are congruent to $-1^2, -2^2, -3^2, \ldots\ldots, -\left(\frac{g-1}{2}\right)^2$ modulo g, in some order.

Hence,

$$\alpha = \frac{k+1}{2} + \theta^2 + \theta^{2p} + \theta^{2p^2} + \ldots\ldots\ldots + \theta^{2p^{p-1}}$$

$$= \frac{k+1}{2} + \theta^{-1^2} + \theta^{-2^2} + \theta^{-3^2} + \ldots\ldots + \theta^{\left(\frac{g-1}{2}\right)^2}$$

and therefore

$$\alpha = \frac{k+1}{2} + \theta^{1^2} + \theta^{2^2} + \theta^{3^2} + \ldots\ldots + \theta^{-\left(\frac{g-1}{2}\right)^2}.$$

Since $1^2, 2^2, 3^2, \ldots\ldots, \left(\frac{g-1}{2}\right)^2$ are the incongruent quadratic residues modulo g, and $\left(\frac{g+1}{2}\right)^2, \left(\frac{g+3}{2}\right)^2, \ldots\ldots, (g-1)^2$ are also $\frac{g-1}{2}$ incongruent quadratic residues modulo g, these must be congruent to $1^2, 2^2, 3^2, \ldots\ldots\left(\frac{g-1}{2}\right)^2$ modulo g, in some order. Hence, the Gaussian sum

$$\phi(1, g) = 1 + \theta^{1^2} + \theta^{2^2} + \theta^{3^2} + \ldots\ldots + \theta^{(g-1)^2}$$

$$= 1 + 2\left(\theta^{1^2} + \theta^{2^2} + \theta^{3^2} + \ldots\ldots + \theta^{\left(\frac{g-1}{2}\right)^2}\right)$$

But, $\phi(1, g) = i\sqrt{g}$, since $g \equiv 3 \pmod{4}$.

Therefore,

$$1 + 2\left(\theta^{1^2} + \theta^{2^2} + \ldots\ldots + \theta^{\left(\frac{g-1}{2}\right)^2}\right) = i\sqrt{g},$$

which gives

$$\theta^{1^2} + \theta^{2^2} + \theta^{3^2} + \ldots\ldots + \theta^{\left(\frac{g-1}{2}\right)^2} = \frac{-1 + i\sqrt{g}}{2}.$$

Hence,

$$\alpha = \frac{k+1}{2} + \frac{-1 + i\sqrt{g}}{2} = \frac{k}{2} + i\,\frac{\sqrt{g}}{2}$$

and

$$\bar{\alpha} = \frac{k}{2} - i\,\frac{\sqrt{g}}{2}$$

therefore

$$|\alpha|^2 = \frac{k^2 + g}{4} = p.$$

The theorem now follows.

Theorem 5. If p and g are odd primes such that $g = 4p - 1$ and the order of p modulo g is $2p - 1$, then

$$\alpha = 1 + \theta^2 + \theta^{2p} + \theta^{2p^2} + \ldots\ldots + \theta^{2p^{(2p-2)}}$$

is a solution of the equation (2).

Proof. Since the order of p modulo g is $2p - 1$, it follows that $2, 2p, 2p^2, \ldots\ldots\ldots\ldots, 2p^{2p-2}$ are incongruent modulo g.

Since $g = 4p - 1$, we have $(2|g) = -1$ and $(p|g) = 1$.

Thus, $(2p^r|g) = -1$, for any integer r, such that $0 \leqslant r \leqslant 2p - 2$.

Hence, $2, 2p, 2p^2 \ldots\ldots, 2p^{2p-2}$ are incongruent quadratic non-residues modulo g.

As in the proof of Theorem 4, it can be shown that these must be congruent to $-1^2, -2^2, -3^2, \ldots\ldots, -\left(\frac{g-1}{2}\right)^2$ modulo g, in some order, and so,

$$\begin{aligned}\alpha &= 1 + \theta^2 + \theta^{2p} + \theta^{2p^2} + \ldots\ldots + \theta^{2p^{2p-2}} \\ &= 1 + \theta^{-1^2} + \theta^{-2^2} + \theta^{-3^2} + \ldots\ldots + \theta^{-\left(\frac{g-1}{2}\right)^2}.\end{aligned}$$

Therefore,

$$\bar{\alpha} = 1 + \theta^{1^2} + \theta^{2^2} + \theta^{3^2} + \ldots\ldots + \theta^{\left(\frac{g-1}{2}\right)^2}.$$

Now the Gaussian sum,

$$\begin{aligned}\phi(1, g) &= 1 + \theta^{1^2} + \theta^{2^2} + \theta^{3^2} + \ldots\ldots + \theta^{(g-1)^2} \\ &= 1 + 2\,(\theta^{1^2} + \theta^{2^2} + \theta^{3^2} + \ldots\ldots + \theta^{\left(\frac{g-1}{2}\right)^2}). \\ &= i\sqrt{g}, \text{ since } g \equiv 3 \pmod 4).\end{aligned}$$

Hence,

$$\theta^{1^2} + \theta^{2^2} + \theta^{3^2} + \ldots\ldots + \theta^{\left(\frac{g-1}{2}\right)^2} = \frac{-1 + i\sqrt{g}}{2}$$

and therefore

$$\bar{\alpha} = \frac{1 + i\sqrt{g}}{2} \text{ and } \alpha = \frac{1 - i\sqrt{g}}{2}$$

Whence,

$$|\alpha|^2 = \frac{1+g}{4} = p.$$

The next two theorems can be easily verified using the Gaussian sum.

Theorem 6. If p and g are odd primes such that $4p = a^2 + b^2 g$, where a and b are coprime odd integers, then the equation (2) has a non-trivial solution in K, given by:

$$\alpha = \frac{a-b}{2} + b\,(1 + \theta^{1^2} + \theta^{2^2} + \ldots\ldots + \theta^{\left(\frac{g-1}{2}\right)^2})$$

Theorem 7. If p and g are odd primes such that $p = a^2 + b^2 g$, $g \equiv 3 \pmod 4$, where a, b are coprimes rational integers of opposite parity, then the equation (2) has a non-trivial solution in the field K given by

$$\alpha = a + b\,(1 + \theta^{1^2} + \theta^{2^2} + \theta^{3^2} + \ldots\ldots + \theta^{(g-1)^2}.$$

References

1. ANKENY, N. C. & CHOWLA, S. (1968) *Diophantine Equations in Cyclotomic Fields*, J. Lond. math. Soc., **43** : 67—70.