J. Math. Univ. Tokushima
Vol. 48 (2014), 35–40

Diophantine Equations and Hilbert's Theorem 90

By

Shin-ichi KATAYAMA

Department of Mathematical Sciences,
Faculty of Integrated Arts and Sciences
The University of Tokushima,
Minamijosanjima-cho 1-1, Tokushima 770-8502, JAPAN
e-mail address : katayama@ias.tokushima-u.ac.jp
(Received September 30, 2014)

Abstract

In 1970, Olga Taussky has given a proof of the parameterization of primitive Pythagorean triples as a special case of Hilbert's Theorem 90 in [6]. Later this proof has been rediscovered by Noam Elkies in [1] and Takashi Ono in [5], independently. Here we shall notice the existence of a family of diophantine equations whose rational solutions can be parameterized by using Hilbert's Theorem 90.

2010 Mathematics Subject Classification. Primary 11R34; Secondary 11D25

1 Introduction

In 1970, O. Taussky discovered a new proof of the parameterization of primitive Pythagorean triples as a special case of Hilbert's Theorem 90 in her paper [6]. This proof has been rediscovered by several authors (see for example [1] and [5]). In this short note, we shall show that there exists a family of diophantine equations(including the case of Pythagorean triples) whose rational solutions can be parameterized by using Hilbert's Theorem 90. Since this fact is very simple, it may be already known to the specialists. But we could not find any literature which write down this fact. Thus it should be of some interest and worth to show this fact explicitly in this note. In the first place, we shall recall the statement of Hilbert's Theorem 90. Let K/F be a finite Galois extension of fields with Galois group $G = Gal(K/F)$. If K/F is a cyclic extension of degree $n = [K : F]$ and G is generated by an element σ, then the 90th theorem(Satz 90) in D. Hilbert's Zahlbericht [2] states that:

Hibert's Theorem 90

If α is an element of K of relative norm 1, *i.e.*, $N_{K/F}(\alpha) = \prod_{i=1}^{n} \alpha^{\sigma^i} = 1$. *Then there exists β in K such that*

$$\alpha = \beta/\beta^{\sigma}.$$

We note that this theorem is equivalent to states that $H^{-1}(G, K^{\times}) = \{1\}$, where $K^{\times}$ is the multiplicative group of the field K. From the fact that the cohomological period of any cyclic group is 2, it is also equivalent to the fact $H^{1}(G, K^{\times}) = \{1\}$ when K/F is cyclic. The following cohomological version of Hilbert's Theorem 90 was given by E. Noether:

Generalized Hilbert's Theorem 90

For any finite(or infinite) Galois extension of K/F with the Galois group $G = Gal(K/F)$, the first cohomology group of $K^{\times}$ is trivial, i.e.,

$$H^{1}(G, K^{\times}) = \{1\}.$$

In the following, we shall give a brief sketch of the parameterization of primitive Pythagorean triples given in [1], [5] and [6] for the convenience to the readers. Let K/F be the quadratic extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$, i.e., $K = \mathbb{Q}(\sqrt{-1})$ and $F = \mathbb{Q}$. Then the Galois group $Gal(K/F) = \langle\sigma\rangle$ is a cyclic group of order 2. For any element $\alpha = x + y\sqrt{-1}$ $(x, y \in \mathbb{Q})$, σ acts

$$\sigma : \alpha = x + y\sqrt{-1} \mapsto \alpha^{\sigma} = x - y\sqrt{-1}.$$

If $N_{K/F}(\alpha) = x^2 + y^2 = 1$, then the corresponding rational points (x, y) are on the unit circle $x^2 + y^2 = 1$. From Hilbert's Theorem 90, α can be parameterized by $\beta = m + n\sqrt{-1}$ (with coprime integers m and n) such that

$$\alpha = \frac{\beta}{\beta^{\sigma}} = \frac{m + n\sqrt{-1}}{m - n\sqrt{-1}} = \frac{m^2 - n^2}{m^2 + n^2} + \frac{2mn}{m^2 + n^2}\sqrt{-1},$$

which may be viewed as a rational parameterization of all the rational points (x, y) on the unit circle $x^2 + y^2 = 1$. Since any primitive Pythagorean triples, i.e., triples (a, b, c) of positive integers satisfying $a^2 + b^2 = c^2$ with a, b, c are coprime, correspond to the positive rational points $(x, y) = (a/c, b/c)$ on the unit circle $x^2 + y^2 = 1$, it has been shown the following parameterization:

$$(x, y) = (a/c, b/c) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right).$$

2 Main Theorem

In this section, we shall slightly generalize the above proof of the parameterization of primitive Pythagorean triples to give the rational solutions of certain family of diophantine equations. Let $K/\mathbb{Q}$ be a cyclic extension of degree n. σ denotes the generator of $Gal(K/\mathbb{Q})$. O_K denotes the maximal order of K and $\{\omega_1, \omega_2, \dots, \omega_n\}$ denotes an integral basis of O_K. Then any $\alpha \in K$ can be uniquely expressed as $\alpha = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$, where $x_1, x_2, \dots, x_n \in \mathbb{Q}$. If $N_{K/\mathbb{Q}}(\alpha) = 1$, then Hilbert's Theorem 90 states that there exists $\beta = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$ with $a_1, a_2, \dots, a_n \in \mathbb{Z}$ such that $\alpha = \beta/\beta^\sigma$. Thus Hibert's Theorem may be viewed as follows.

Proposition. *Let $K/\mathbb{Q}$ be a cyclic extension of degree n with the Galois group $Gal(K/\mathbb{Q}) = \langle\sigma\rangle$. For any $\alpha \in K$ with $N_{K/\mathbb{Q}}(\alpha) = 1$, there exists an integer $\beta \in O_K$ of the form $\beta = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$ with $a_1, a_2, \dots, a_n \in \mathbb{Z}$ such that*

$$\alpha = \frac{\beta}{\beta^\sigma} = \frac{a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n}{a_1\omega_1^\sigma + a_2\omega_2^\sigma + \cdots + a_n\omega_n^\sigma}.$$

Denote $N_{K/\mathbb{Q}}(x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n)$ by $f(x_1, x_2, \dots, x_n)$. Then one knows that $f(x_1, x_2, \dots, x_n) \in \mathbb{Z}[x_1, x_2, \dots, x_n]$. We also denote $\dfrac{a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n}{a_1\omega_1^\sigma + a_2\omega_2^\sigma + \cdots + a_n\omega_n^\sigma}$ by $g_1(a_1, a_2, \dots, a_n)\omega_1 + g_2(a_1, a_2, \dots, a_n)\omega_2 + \cdots + g_n(a_1, a_2, \dots, a_n)\omega_n$, where $g_i(a_1, a_2, \dots, a_n) \in \mathbb{Q}(a_1, a_2, \dots, a_n)$ $(1 \le i \le n)$. Consider the rational solutions of the following diophantine equation.

$$f(x_1, x_2, \dots, x_n) = 1. \tag{1}$$

Then the above proposition implies the following theorem.

Theorem. *Any rational solution $(x_1, x_2, \dots, x_n)$ of (1) is given by*

$$x_i = g_i(a_1, a_2, \dots, a_n) \ (1 \le i \le n),$$

where $a_1, a_2, \dots, a_n$ are coprime integers.

Let p be an odd prime and $\zeta = \zeta_{p^k}$ be the primitive p^kth root of unity or $p = 2, k = 2$ and $\zeta = \zeta_4$. Then $K = \mathbb{Q}(\zeta)$ is a cyclic cyclotomic extension of degree $n = \varphi(p^k) = p^{k-1}(p-1)$ and $O_K = \mathbb{Z}[\zeta]$. Taking the power integral basis $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ of O_K, we can apply the above theorem. We note that the special case $\zeta = \zeta_4$ is nothing but the parameterization of primitive Pythagorean triples given in the introduction.

Now we shall consider the following special case of the above theorem. Let g be a primitive root mod p^k and e be a fixed divisor of n. Put $f = n/e$ and define

$$\eta_i = \sum_{j=0}^{f-1} \zeta^{e(i,j)} \ (1 \le i \le e),$$

where $e(i, j) = g^{ej+i-1}$.
Let us denote the Gaussian period η_1 by η. Then $K = \mathbb{Q}(\eta)$ is a cyclic extension over

$\mathbb{Q}$ of degree e. Take the normal integral basis $\{\eta_1, \eta_2, \ldots, \eta_e\}$ of O_K.
Put $N_{K/\mathbb{Q}}(x_1\eta_1 + \cdots + x_e\eta_e) = f(x_1, \ldots, x_e)$ and put

$$\frac{x_1\eta_1 + x_2\eta_2 + \cdots + x_{e-1}\eta_{e-1} + x_e\eta_e}{x_1\eta_2 + x_2\eta_3 + \cdots + x_{e-1}\eta_e + x_e\eta_1} = \sum_{i=1}^{e} g_i(a_1, \ldots, a_e)\eta_i,$$

where each $g_i(x_1, \ldots, x_e)$ is a rational function. Then we have the following special case of the above theorem.

Corollary. *With the above notations, every rational solution* $(x_1, x_2, \ldots, x_e)$ *of the diophantine equation* $f(x_1, \ldots, x_e) = 1$ *is given by*

$$x_i = g_i(a_1, a_2, \ldots, a_e) \ (1 \leq i \leq e),$$

with coprime integers $a_1, a_2, \ldots, a_e$.

Example 1. In [1], N. Elkies noticed that the above theorem holds for any quadratic equation of norm type. Moreover he suggested that one can give the well known parameterization of two types of triangles with integer sides and angles $2\pi/3$(or $\pi/3$). The sides (a, b, c) of triangles of these types satisfy $a^2+ab+b^2 = c^2$(or $a^2-ab+b^2 = c^2$). Let K be $\mathbb{Q}(\sqrt{-3})$ and $F = \mathbb{Q}$. Then the Galois group $Gal(K/F) = \langle\sigma\rangle$ is generated by the following σ. For any element $\alpha = x + y(1 + \sqrt{-3})/2$ $(x, y \in \mathbb{Q})$, σ acts

$$\sigma : \alpha = x + y(1 + \sqrt{-3})/2 \mapsto \alpha^\sigma = x + y(1 - \sqrt{-3})/2.$$

If $N_{K/F}(\alpha) = x^2 + xy + y^2 = 1$, then the corresponding rational points (x, y) are on the ellipse $x^2 + xy + y^2 = 1$. From Hilbert's Theorem 90, α can be parameterized by $\beta = m + n(1 + \sqrt{-3})/2$ (with coprime integers m and n) such that

$$\alpha = \frac{\beta}{\beta^\sigma} = \frac{m^2 - n^2}{m^2 + mn + n^2} + \frac{2mn + n^2}{m^2 + mn + n^2}\left(\frac{1 + \sqrt{-3}}{2}\right),$$

which may be viewed as a rational parameterization of all the rational points (x, y) on the ellipse $x^2 + xy + y^2 = 1$. Since the triple (a, b, c) of positive integers satisfying $a^2 + ab + b^2 = c^2$, corresponds to the positive rational point $(x, y) = (a/c, b/c)$ on the ellipse $x^2 + xy + y^2 = 1$, it has been shown the following parameterization:

$$(x, y) = (a/c, b/c) = \left(\frac{m^2 - n^2}{m^2 + mn + n^2}, \frac{2mn + n^2}{m^2 + mn + n^2}\right),$$

where m and n are coprime integers.
Similarly, triangles with integer sides (a, b, c) with an angle $\pi/3$ correspond to triples (a, b, c) of positive integers satisfying $a^2 - ab + b^2 = c^2$. They also correspond to the positive rational points $(x, y) = (a/c, b/c)$ on the ellipse $x^2 - xy + y^2 = 1$. Similarly one obtains the following parameterization:

$$(x, y) = (a/c, b/c) = \left(\frac{m^2 - n^2}{m^2 - mn + n^2}, \frac{2mn - n^2}{m^2 - mn + n^2}\right).$$

Example 2. We shall calculate the special case $\zeta = \zeta_7$ and $g = 5, e = 3$, that is, the Gaussian periods $\eta = \eta_1 = \zeta + \zeta^{-1}, \eta_2 = \zeta^2 + \zeta^{-2}, \eta_3 = \zeta^3 + \zeta^{-3}$ explicitly.

We denote $K = \mathbb{Q}(\eta)$. Then $K/\mathbb{Q}$ ia a cyclic cubic extension with the Galois group $G = Gal(K/\mathbb{Q})$. Then $\sigma : \zeta \mapsto \zeta^2$ is a generator of G. For any $\alpha = x\eta_1 + y\eta_2 + z\eta_3 \in K$ with $x, y, z \in \mathbb{Q}$, one can verify that $N_{K/\mathbb{Q}}(\alpha) = x^3 + y^3 + z^3 + 3(x^2y + y^2z + z^2x) - 4(xy^2 + yz^2 + zx^2) - xyz$. Assume $N_{K/\mathbb{Q}}(\alpha) = 1$, Then there exists $\ell, m, n \in \mathbb{Z}$ such that

$$\alpha = x\eta_1 + y\eta_2 + z\eta_3 = \frac{\ell\eta_1 + m\eta_2 + n\eta_3}{\ell\eta_2 + m\eta_3 + n\eta_1}.$$

Calculating the right hand side, one obtains that

$$\frac{\ell\eta_1 + m\eta_2 + n\eta_3}{\ell\eta_2 + m\eta_3 + n\eta_1} = \frac{a_1\eta_1 + a_2\eta_2 + a_3\eta_3}{\ell^3 + m^3 + n^3 + 3(\ell^2m + m^2n + n^2\ell) - 4(\ell m^2 + mn^2 + n\ell^2) - \ell mn},$$

where

$$\begin{aligned}
a_1 &= \ell^3 + 2m^3 + n^3 + (\ell^2m - m^2n - 2n^2\ell) - (5\ell m^2 + 2mn^2 + 2n\ell^2) + 8\ell mn,\\
a_2 &= \ell^3 + m^3 + 2n^3 + (-2\ell^2m + m^2n - n^2\ell) - (2\ell m^2 + 5mn^2 + 2n\ell^2) + 8\ell mn,\\
a_3 &= 2\ell^3 + m^3 + n^3 + (-\ell^2m - 2m^2n + n^2\ell) - (2\ell m^2 + 2mn^2 + 5n\ell^2) + 8\ell mn.
\end{aligned}$$

Thus we have obtained that any rational solution of the following diophantine equation

$$x^3 + y^3 + z^3 + 3(x^2y + y^2z + z^2x) - 4(xy^2 + yz^2 + zx^2) - xyz = 1. \qquad (2)$$

is given by

$$\begin{aligned}
x &= \frac{\ell^3 + 2m^3 + n^3 + (\ell^2m - m^2n - 2n^2\ell) - (5\ell m^2 + 2mn^2 + 2n\ell^2) + 8\ell mn}{\ell^3 + m^3 + n^3 + 3(\ell^2m + m^2n + n^2\ell) - 4(\ell m^2 + mn^2 + n\ell^2) - \ell mn},\\
y &= \frac{\ell^3 + m^3 + 2n^3 + (-2\ell^2m + m^2n - n^2\ell) - (2\ell m^2 + 5mn^2 + 2n\ell^2) + 8\ell mn}{\ell^3 + m^3 + n^3 + 3(\ell^2m + m^2n + n^2\ell) - 4(\ell m^2 + mn^2 + n\ell^2) - \ell mn},\\
z &= \frac{2\ell^3 + m^3 + n^3 + (-\ell^2m - 2m^2n + n^2\ell) - (2\ell m^2 + 2mn^2 + 5n\ell^2) + 8\ell mn}{\ell^3 + m^3 + n^3 + 3(\ell^2m + m^2n + n^2\ell) - 4(\ell m^2 + mn^2 + n\ell^2) - \ell mn},
\end{aligned}$$

where ℓ, m, n are relatively coprime integers.
One can easily translate the above parameterization to the following homogeneous diophantine equation

$$a^3 + b^3 + c^3 + 3(a^2b + b^2c + c^2a) - 4(ab^2 + bc^2 + ca^2) - abc = d^3. \qquad (3)$$

Then the integers a, b, c, d are proportional to

$$\begin{aligned}
&\ell^3 + 2m^3 + n^3 + (\ell^2m - m^2n - 2n^2\ell) - (5\ell m^2 + 2mn^2 + 2n\ell^2) + 8\ell mn,\\
&\ell^3 + m^3 + 2n^3 + (-2\ell^2m + m^2n - n^2\ell) - (2\ell m^2 + 5mn^2 + 2n\ell^2) + 8\ell mn,\\
&2\ell^3 + m^3 + n^3 + (-\ell^2m - 2m^2n + n^2\ell) - (2\ell m^2 + 2mn^2 + 5n\ell^2) + 8\ell mn,\\
&\ell^3 + m^3 + n^3 + 3(\ell^2m + m^2n + n^2\ell) - 4(\ell m^2 + mn^2 + n\ell^2) - \ell mn,
\end{aligned}$$

for some integers ℓ, m, n. Here we note that the essential cases $d \neq 0$ are obtained by putting $(x, y, z) = (a/d, b/d, c/d)$ in (2) and the exceptional case $(a, b, c, d) = (0, 0, 0, 0)$ is obtained by putting $\ell = m = n = 0$.

References

[1] N. D. Elkies, Pythagorean triples and Hilbert's Theorem 90, http://www.math.harvard.edu/ elkies/Misc/hilbert.pdf.

[2] D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung, Berlin, 1897.

[3] S. Katayama, Modified Farey trees and Pythagorean triples, J. Math. The Univ., Tokushima, **47** (2013), 1–13.

[4] J. Neukirch, Algebraic Number Theory, Springer-Verlag, Berlin, 1999.

[5] T. Ono, Variations on the Theme of Euler:Quadratic Forms, Elliptic Curves and Hopf Maps, Plenum Press, 1994.

[6] O. Taussky, Sums of squares, Amer. Math. Monthly, **77** (1970), 805–830.

[7] L. C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, New York, 1982.