Hilbert's theorem 90, Dirichlet's unit theorem and Diophantine equations

B. Sury

Stat-Math Unit
Indian Statistical Institute
8th Mile Mysore Road
Bangalore - 560 059
India.
sury@isibang.ac.in

§ Introduction

In a first course on Galois theory, students are introduced to the so-called Hilbert's theorem 90 for cyclic extensions. The first course on algebraic number theory introduces the Dirichlet unit theorem. Our purpose here is to analyse certain concrete special cases, and to notice that, the proofs are totally elementary, and yield novel applications such as parametrisations of solutions of certain Diophantine equations. This includes a proof (new, as far as the author knows) of the well-known classical parametrization of Pythagorean triples.

§ Hilbert's theorem 90

Consider any quadratic extension field of $\mathbb{Q}$. It is given as $\mathbb{Q}(\sqrt{d})$ where d is a square-free (positive or negative) integer.

Theorem 1.
Let $x + y\sqrt{d}$ be an element of norm 1 over $\mathbb{Q}$. Then, $x + y\sqrt{d} = \frac{u+v\sqrt{d}}{u-v\sqrt{d}}$ for some relatively prime $u, v \in \mathbb{Z}$.
Proof.

Let $x, y \in \mathbb{Q}$ satisfy $x^2 - dy^2 = 1$. Now, as $\{1, \sqrt{d}\}$ is a basis of $\mathbb{Q}(\sqrt{d})$, we simply solve for $\alpha \in \mathbb{Q}$ satisfying

$$x + y\sqrt{d} = \frac{\alpha + \sqrt{d}}{\alpha - \sqrt{d}}.$$

In fact, when $(x, y) \neq (1, 0)$ (the case $(1, 0)$ is taken care of by $\alpha = 1$), $\alpha = \frac{1+x}{y}$. One can then clear denominators to obtain u, v as claimed.

§ Dirichlet's unit theorem

Let d be a square-free integer and we consider $K = \mathbb{Q}(\sqrt{d})$ as before. It is well-known and easy to see that the ring of algebraic integers in $K = \mathbb{Q}(\sqrt{d})$ is given either as $\mathcal{O} = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}$ or as $\mathcal{O} = \{x + y\frac{1+\sqrt{d}}{2} : x, y \in \mathbb{Z}\}$ accordingly as to whether $d \equiv 2, 3 \bmod 4$ or $d \equiv 1 \bmod 4$.

Theorem 2.
The group $\mathcal{O}^*$ of units is either the finite cyclic group $\mu(K)$ of roots of unity in K or the direct product of $\mu(K)$ with $\mathbb{Z}$ according as to whether $d < 0$ or $d > 1$.

Before we proceed further, we first prove one of the statements. This is the assertion that when $d > 1$, there are indeed solutions of $x^2 - dy^2 = 1$ other than $(x, y) = (\pm 1, 0)$. This is well-known and is an easy consequence of the continued fraction expansion of $\sqrt{d}$ as we observe now. The (standard) notation $[a_0; a_1, a_2, a_3, \cdots\cdots]$ below for the simple continued fraction stands for the sum

$$a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\cdots$$

Lemma.
If $d > 1$ is a square-free integer, then $u^2 - dv^2 = 1$ can always be solved in positive integers.

Proof.
For any simple continued fraction, the successive convergents $\frac{p_n}{q_n}$ satisfy

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^n$$

as seen by induction. Now, it is a simple exercise to show that the simple continued fraction for $\sqrt{d}$ recurs eventually and has the form

$$[a_1\,;\, b_1, b_2, \cdots, b_n, 2a_1, b_1, b_2, \cdots, b_n, 2a_1, \cdots]. \tag{1}$$

If p/q is a penultimate convergent of a recurring period, then it is easy to check that $p^2 - dq^2 = \pm 1$. In fact, if the period is even, this is always 1. If the period is odd, then the penultimate convergents of the first, second, third period etc. alternately satisfy the equations

$$x^2 - dy^2 = -1, \qquad x^2 - dy^2 = 1.$$

This proves the lemma.

For example,

$$\sqrt{13} = [3\,;\, 1, 1, 1, 1, 6, \cdots].$$

The period is 5 which is odd. The penultimate convergent to the first period is

$$3 + \frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{1} = \frac{18}{5}.$$

Therefore, $(18, 5)$ is a solution of $u^2 - 13v^2 = -1$.
The penultimate convergent to the second period is computed to be $649/180$. Therefore, $(649, 180)$ is a solution of $u^2 - 13v^2 = 1$.

Proof of theorem 2.
First of all, it is clear that all roots of unity in K are units in $\mathcal{O}$. Thus, $\mu(K)$ is precisely the subgroup of all elements of finite order in $\mathcal{O}^*$.
Now, any unit has norm ± 1. Thus, in case $d \equiv 2, 3 \bmod 4$, the units are the complex numbers $x + y\sqrt{d}$ with $x, y \in \mathbb{Z}$ satisfying $x^2 - dy^2 = \pm 1$. In case $d \equiv 1 \bmod 4$, the units are the complex numbers $x + y\frac{1+\sqrt{d}}{2}$ with $x, y \in \mathbb{Z}$ satisfying $(x + \frac{y}{2})^2 - d\frac{y^2}{4} = \pm 1$. Therefore, it is evident that when $d < 0$, there are only finitely many units; thus $\mathcal{O}^* = \mu(K)$.
If $d > 0$, it is clear that $\mu(K) = \{\pm 1\}$. We shall show that when $d > 1$, there is a unit u of infinite order such that every unit is of the form $\pm u^n$ for some

$n \in \mathbb{Z}$.
Let us look at the case of $d \equiv 2, 3 \bmod 4$ first. Suppose $x, y \in \mathbb{Z}$ with $y \neq 0$ such that $x^2 - dy^2 = \pm 1$. By changing the signs, we may assume $x + y\sqrt{d} > 0$ and, by considering its reciprocal $x - y\sqrt{d}$ if necessary, we may assume that $x + y\sqrt{d} > 1$. Suppose $x + y\sqrt{d} > 1$ be the smallest unit bigger than 1. If $u + v\sqrt{d}$ is any unit $\neq \pm 1$, then exactly one of the four units $\pm u \pm v\sqrt{d}$ is > 1. Take $u + v\sqrt{d}$ to be such a unit. If n is the largest natural number such that $(x + y\sqrt{d})^n \leq u + v\sqrt{d}$, we look at

$$\frac{u + v\sqrt{d}}{(x + y\sqrt{d})^n} = \pm(u + v\sqrt{d})(x - y\sqrt{d})^n$$

which is evidently a unit ≥ 1. If it were > 1, then it would be at least $x + y\sqrt{d}$ and this would imply $(x + y\sqrt{d})^{n+1} \leq u + v\sqrt{d}$, a manifest contradiction of the choice of n. Thus, we must have $(x + y\sqrt{d})^n = u + v\sqrt{d}$. This gives us the theorem when $d > 1$ is $\equiv 2$ or $3 \bmod 4$ on using the fact that there is a unit $\neq \pm 1$; that is, a unit of infinite order.
For the case $d > 1, d \equiv 1 \bmod 4$ the argument goes through very similarly with $\frac{1+\sqrt{d}}{2}$ in place of $\sqrt{d}$. Thus, the theorem is proved.

§ Pythagorean triples

In this section, we apply the theorem of the first section to show how all solutions of Diophantine equations of the form $x^2 - dy^2 = 1$ are parametrized for any particular square-free $d < 0$. In particular, we can obtain (for $d = -1$) the classical characterisation of all Pythagorean triplets; that is, all the solutions in positive integers, of the equation $x^2 + y^2 = z^2$.

Theorem 3.
Let $d < 0$ be square-free. Then, the nonzero solutions of the Diophantine equation $x^2 - dy^2 = z^2$ in integers x, y, z satisfy

$$\frac{x}{u^2 - dv^2} = \frac{y}{2uv} = \frac{z}{u^2 + dv^2}$$

for some nonzero $u, v \in \mathbb{Z}$.
In particular, for any Pythagorean triple (a, b, c), *one has*

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$$

for some $u, v \in \mathbb{Z}$.

Further refinement of the statement for $d \neq -1$ is possible but is more complicated as it involves finding the possible common factors of numbers of the form $u^2 - dv^2$ and of the form $u^2 + dv^2$ etc.

Proof of theorem 3.
Any nonzero solution (x, y, z) gives an element $\frac{x}{z} + \frac{y}{z}\sqrt{d}$ of $\mathbb{Q}(\sqrt{d})$ with norm 1 over $\mathbb{Q}$. We know by theorem 1 that there exist relatively prime integers u, v such that

$$\frac{x}{z} + \frac{y}{z}\sqrt{d} = \frac{u + v\sqrt{d}}{u - v\sqrt{d}}.$$

Thus,

$$\frac{x}{z} + \frac{y}{z}\sqrt{d} = \frac{(u + v\sqrt{d})^2}{u^2 - dv^2}.$$

This gives the parametrisation claimed.
In the particular case $d = -1$ we can refine it as follows. For positive integers a, b, c with $a^2 + b^2 = c^2$, we have $1 = (\frac{a}{c})^2 + (\frac{b}{c})^2$, we have

$$a(u^2 + v^2) = c(u^2 - v^2) \ , \ b(u^2 + v^2) = 2uvc.$$

Then, when a, b, c are relatively prime, we obtain (!) either

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$$

or

$$(a, b, c) = (\frac{u^2 - v^2}{2}, uv, \frac{u^2 + v^2}{2}).$$

Actually, the two expressions are really the same (by taking $(u+v)/2$ and $(u-v)/2$ instead of u, v); they correspond to the cases for primitive Pythagorean triples with b even and a even respectively.