# HISTORY OF MATHEMATICS
# MATHEMATICAL TOPIC VI
# DIOPHANTINE EQUATIONS

PAUL L. BAILEY

## 1. Pythagorean Triples

A *Pythagorean triple* $(a, b, c)$ consists of three integers $a, b, c \in \mathbb{Z}$ with $a, b \geq 1$ such that $a^2 + b^2 = c^2$.

The Babylonians produced tablets containing tables of Pythagorean triples. It is conjectured that they may have known of the formula to generate such triples: let $u$ and $v$ be any positive integers, and set

**(a)** $a = u^2 - v^2$;
**(b)** $b = 2uv$;
**(c)** $c = u^2 + v^2$.

Then

$$\begin{aligned} a^2 + b^2 &= (u^2 - v^2)^2 + (2uv)^2 \\ &= u^4 - 2u^2v^2 + v^4 + 4u^2v^2 \\ &= u^4 + 2u^2v^2 + v^4 \\ &= (u^2 + v^2)^2 \\ &= c^2. \end{aligned}$$

Thus we have:

**Proposition 1.** *Let $u, v \in \mathbb{Z}$ and set $a = u^2 - v^2$, $b = 2uv$, and $c = u^2 + v^2$. Then $(a, b, c)$ is a Pythagorean triple.*

The equivalent of this scheme for generating Pythagorean triples can be found in Euclid's *Elements*, Book X, Lemma following Proposition 28. We ask if the converse is true; that is, does this method generate *all* Pythagorean triples?

*Date*: October 27, 2006.

## 2. Diophantine Equations

A *Diophantine equation* is an equation of the form

$$F(x_1, \ldots, x_n) = 0,$$

where $F(x_1, \ldots, x_n)$ is a polynomial in $n$ variables with integer coefficients. A *solution* to a Diophantine equation is a point $(a_1, \ldots, a_n) \in \mathbb{C}^n$, where $a_i \in \mathbb{Z}$ and $F(a_1, \ldots, a_n) = 0$.

This is the modern definition. However, Diophantus looked for rational solutions to polynomial equations with integer (or rational) coefficients. We note that a rational solution to a polynomial equation produces an integer solution to a modified polynomial equation, obtained by clearing the denominators; that is, multiply the expression $F(a_1, \ldots, a_n) = 0$ by the least common multiple of the highest powers of the denominators of $a_1, \ldots, a_n$ to appear in the expression.

**Example 1.** Pythagorean triples are integer solutions to the polynomial equation $x^2 + y^2 = z^2$. Suppose $(a, b, c)$ is such a solution, with $a, b, c \in \mathbb{Z}$. Then $(\frac{a}{c}, \frac{b}{c})$ is a rational solution to the equation $x^2 + y^2 = 1$. Thus the problem of finding integer solutions to $x^2 + y^2 = z^2$ is equivalent to the problem of finding rational solutions to $x^2 + y^2 = 1$.

**Example 2.** Fermat's last theorem essentially states that there are no nontrivial integer solutions to the equation $x^n + y^n = z^n$ for $n \geq 3$. Again, this is equivalent to the nonexistence of nontrivial rational solutions to $x^n + y^n = 1$ for $n \geq 3$.

**Example 3.** Fix $m, n \in \mathbb{Z}$, and let $d = \gcd(m, n)$. The Euclidean algorithm produces unique solutions to the Diophantine equation $mx + ny = d$.

An *plane algebraic curve* is the subset of $\mathbb{C}^2$ which is the set of points $(a, b) \in \mathbb{C}^2$ such that $F(a, b) = 0$ for some polynomial $F(x, y)$ with coefficients in $\mathbb{C}$. We say that the curve is *defined over* $\mathbb{Q}$ if these coefficients are in $\mathbb{Q}$. The *degree* of the curve is the degree of the polynomial $F$. A *rational point* on the curve is a point on the curve with rational coordinates.

Diophantus studied plane algebraic curves, and looked for rational solutions to such polynomial equations, which is to say, he attempted to find rational points on the associated algebraic curve. Keep in mind that the notation used by Diophantus was very dissimilar to that used today.

**Example 4.** We see that $(a, b, c)$ is a Pythagorean triple if and only if $(\frac{a}{c}, \frac{b}{c})$ is a rational point on the curve $x^2 + y^2 = 1$.

**Example 5.** Fermat's Last Theorem amounts to the claim that $(1, 0)$ and $(0, 1)$ are the only rational points on the curve $x^n + y^n = 1$.

## 3. Generation of Pythagorean Triples

One technique used by Diophantus to find rational points on a curve was to find an apparent solution $P$ and intersect the curve with lines through $P$ which have rational slope. That this works for conic sections is exemplified by the following propositions.

**Proposition 2.** *Let $f(x) = ax^2 + bx + c$, where $a, b, c \in \mathbb{Q}$. If $x_1, x_2$ satisfy $f(x) = 0$, and $x_1 \in \mathbb{Q}$, then $x_2 \in \mathbb{Q}$.*

*Proof.* Suppose $x_2 \neq x_1$. Set $d = \sqrt{b^2 - 4ac}$. Then

$$x_1 = \frac{-b + ud}{2a} \quad \text{and } x_2 = \frac{-b - ud}{2a},$$

where $u = 1$ or $u = -1$. Therefore $d = u(2ax_1 + b) \in \mathbb{Q}$. Therefore $x_2 \in \mathbb{Q}$. □

**Proposition 3.** *Let $P = (-1, 0)$ and $Q = (a, b)$ with $a^2 + b^2 = 1$ and $a > -1$. Then $P$ and $Q$ are distinct points on the unit circle $x^2 + y^2 = 1$, and $Q$ is a rational point if and only if the slope of line through $P$ and $Q$ is rational.*

*Proof.* Let $m$ be the slope of the line through $P$ and $Q$; then

$$m = \frac{b}{a + 1},$$

and the equation of the line through $P$ and $Q$ is $y = m(x + 1)$.

If $Q$ is rational, this means that $a, b \in \mathbb{Q}$, so $m = \frac{b}{a+1} \in \mathbb{Q}$.

On the other hand, suppose that the slope is rational. The $x$-coordinate of the intersection of the curve and the line satisfies

$$x^2 + (m(x + 1))^2 = 1.$$

This is a quadratic equation whose solutions, for our given $m$, are $x = -1$ and $x = a$; therefore, $a$ is rational by Proposition 2. □

The problem of finding Pythagoreans triples is equivalent to the problem of finding rational points on the curve $x^2 + y^2 = 1$. Diophantus realized that all such points could be obtained by running a line with rational slope through the point $P = (-1, 0)$ and taking the point of intersection with the unit circle. We compute these points as follows.

Let $m \in \mathbb{Q}$; the line with slope $m$ through $P$ is $y = m(x+1)$. Let $Q$ be the other point of intersection of this line with the unit circle. Substituting $m(x + 1)$ for $y$ in the equation of the unit circle gives $x^2 + (m(x + 1))^2 = 1$, or

$$(m^2 + 1)x^2 + 2m^2x + (m^2 - 1) = 0.$$

This quadratic equation has solutions

$$x = \frac{-2m^2 \pm \sqrt{4m^4 - 4(m^4 - 1)}}{2(m^2 + 1)} = \frac{-m^2 \pm 1}{m^2 + 1},$$

so the solution that produces $P$ is $x = -1$, and the solution that produces $Q$ is

$$\boxed{x = \frac{1 - m^2}{1 + m^2}.}$$

Substitute this into the line to get

$$\boxed{y = \frac{2m}{1+m^2}.}$$

We have shown:

**Proposition 4.** *Let* $\mathbb{U} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ *and let* $P = (-1, 0)$. *The function*

$$\phi : \mathbb{Q} \to \mathbb{U} \quad \text{given by } \phi(m) = \Big(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\Big)$$

*produces a bijective correspondence between the rational numbers and the rational points (other than* $P$*) on the unit circle.*

Now plug these values for $x$ and $y$ into the equation of the circle and get

$$\Big(\frac{1-m^2}{1+m^2}\Big)^2 + \Big(\frac{2m}{1+m^2}\Big)^2 = 1,$$

therefore

$$(1-m^2)^2 + 4m^2 = (1+m^2)^2.$$

Let $m \in \mathbb{Q}$ be positive; then there exist positive $u, v \in \mathbb{Z}$ such that $m = \frac{v}{u}$. Then, substituting this into the above formula and clearing the denominators by multiplying by $u^4$, we obtain

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2.$$

This shows:

**Theorem 1** (Diophantus' Theorem)**.** *Let* $(a, b, c)$ *be a Pythagorean triple. Then there exist* $u, v \in \mathbb{Z}$ *such that* $a = u^2 - v^2$, $b = 2uv$, *and (consequently)* $c = u^2 + v^2$.

## 4. Cubic Equations

Diophantus also applied this technique to cubic equations in two variables, using the fact that the generic degree three polynomial in one variable has three solutions, and if two of them are rational, then so is the third.

Given a degree three curve defined over $\mathbb{Q}$ by the equation $F(x, y) = 0$, the intersection of the curve with a line $y = mx + b$ gives an equation $F(x, mx + b) = 0$. If two rational solutions are known, then the third solution must also be rational.

Suppose we find one rational point $P = (a, b)$ on the curve. If we select a nearby point on the curve and let it approach $P$, the secant line between the points approaches the tangent line $y = mx + b$. Then $m$ is rational, and if this tangent line intersects the curve in another point, the other point will also be rational. This is because $a$ is a double root of $F(x, mx + b) = 0$.

As an aside, we note that this technique re-emerged in the early $19^{\text{th}}$ century in the following context. In attempting to compute the arclength along an ellipse, Niels Henrik Abel discovered certain integrals, known as *elliptic integrals*, with the property that the natural domain of the inverse of the antiderivative was a torus as opposed to the Riemann sphere (this is the traditional name for the complex plane together with a point at $\infty$). This developed into the study of *elliptic curves*, which are curves defined by an equation of the form $y^2 = f(x)$, where $f(x)$ is a cubic polynomial.

In 1835, Carl Gustav Jacob Jacobi created a type of addition of the points on an elliptic curve, called the *chord-tangent law*, which can be defined in terms of taking

lines through points and intersecting them with the curve. Under this addition, the sum of rational points is also rational, so the set of rational points form an algebraic system known as an *abelian group*.

**Example 6.** Find three rational points on the curve $y^2 = x^3 - 3x^2 + 3x + 1$.

*Solution.* We see that $(0, 1)$ and $(0, -1)$ are solutions. Let $P = (0, 1)$; we would like to find the line tangent to the curve through the point $P$. Using implicit differentiation (which was not available to Diophantus), we compute that

$$2y\frac{dy}{dx} = 3x^2 - 6x + 3,$$

so

$$\frac{dy}{dx} = \frac{3(x^2 - 2x + 1)}{2y}.$$

Set

$$m = \frac{dy}{dx}\,|_P = \frac{3}{2}.$$

If $P = (x_0, y_0) = (0, 1)$, the tangent line is

$$y = m(x - x_0) + y_0 = \frac{3}{2}x + 1.$$

Substitute this into the equation of the curve to get

$$\left(\frac{3}{2}x + 1\right)^2 = x^3 - 3x^2 + 3x + 1.$$

Solving for $x$ gives $x = \frac{21}{4}$. Applying this to the line produces $y = \frac{71}{8}$. This is rational; thus $(\frac{21}{4}, \frac{71}{8})$ is a rational point on the curve. □

**Exercise 1.** The equation $y^2 = x^3 - ax + b$ defines an *elliptic curve*.

- **(a)** Use calculus to find all points on the curve with horizontal or vertical tangents.
- **(b)** Let $a = 12$ and $b = 25$. Take a horizontal tangent and intersect it with this curve to find another rational point.
- **(c)** Let $a = 2$ and $b = 0$. Find three rational points on this curve.

Department of Mathematics and CSci, Southern Arkansas University
*E-mail address*: plbailey@saumag.edu