Pythagorean Triples, Complex Numbers, Abelian Groups and Prime Numbers

Amnon Yekutieli

Department of Mathematics
Ben Gurion University
e-mail: amyekut@math.bgu.ac.il

Notes available at
http://www.math.bgu.ac.il/~amyekut/lectures

written 7 June 2015
A *Pythagorean triple* is a triple \((a, b, c)\) of positive integers, satisfying

\[(1.1) \quad a^2 + b^2 = c^2.\]

The reason for the name is, of course, because these are the sides of a right angled triangle:
We say that the triples \((a, b, c)\) and \((a', b', c')\) are equivalent if the corresponding triangles are similar.

This means that there is a positive number \(r\), such that

\[
(a', b', c') = (ra, rb, rc)
\]

or

\[
(a', b', c') = (rb, ra, rc).
\]

Clearly \(r\) is rational.

We say that the triple \((a, b, c)\) is reduced if the greatest common divisor of these numbers is 1. The triple is called ordered if \(a \leq b\).

It is easy to see that any triple \((a, b, c)\) is equivalent to exactly one reduced ordered triple \((a', b', c')\).

**Exercise 1.2.** Let \((a, b, c)\) be a reduced ordered triple. Then \(c\) is odd, and \(a < b\).
Here is an interesting question:

**Question 1.3.** Are there infinitely many reduced ordered Pythagorean triples?

The answer is yes. This was already known to the ancient Greeks. There is a formula attributed to Euclid for presenting all Pythagorean triples, and it proves that there infinitely many reduced ordered triples.

This formula is somewhat clumsy, and I will not display it. It can be found on the web, e.g. here:

http://en.wikipedia.org/wiki/Pythagorean_triple
http://mathworld.wolfram.com/PythagoreanTriple.html

Later we will see a nice geometric argument, essentially based on the Euclid formula, to show there infinitely many reduced ordered triples.
For a given integer $c > 1$, let us denote by $PT(c)$ the set of all reduced ordered Pythagorean triples with hypotenuse $c$.

A more interesting question is this:

**Question 1.4.** What is the size of the set $PT(c)$?

The answer to this was found in the 19th century. We will see it at the end of the lecture.

An even more interesting question is this:

**Question 1.5.** Given $c$, is there an effective way to find the reduced ordered Pythagorean triples with hypotenuse $c$?

An effective method (possibly new!) will be presented at the end of the talk.
It was observed a long time ago that Pythagorean triples can be encoded as *complex numbers on the unit circle*. Starting from a reduced ordered Pythagorean triple \((a, b, c)\), we pass to the complex number

\[ z := a + b \cdot i, \]

that has absolute value \(c\).

Consider the complex number

(2.1) \[ \zeta = s + r \cdot i := \frac{z}{|z|} = \frac{a}{c} + \frac{b}{c} \cdot i. \]
The number $\zeta$ has rational coordinates, it is on the unit circle, in the second octant, and is different from $i$.

We can recover the number $z$, and thus the reduced ordered Pythagorean triple $(a, b, c)$, by clearing the denominators from the pair of rational numbers $(r, s) = \left(\frac{a}{b}, \frac{a}{c}\right)$. 
Actually, there are 8 different numbers on the unit circle that encode the same Pythagorean triple:

(2.2) \[ \pm \zeta, \pm i \cdot \zeta, \pm \bar{\zeta}, \pm i \cdot \bar{\zeta}. \]
Given a complex number $\zeta$ with rational coordinates on the unit circle, other than the four special points $\pm 1, \pm i$, let us denote by $\text{pt}(\zeta)$ the unique reduced ordered Pythagorean triple $(a, b, c)$ that $\zeta$ encodes.

In this fashion we obtain a function $\text{pt}$ from the set of complex numbers on the unit circle with rational coordinates (not including the four special points), to the set of reduced ordered Pythagorean triples.

This function is surjective, and it is 8 to 1.

Therefore, to show that there are infinitely many reduced ordered Pythagorean triples, it suffices to prove:

**Proposition 2.4.** There are infinitely many complex numbers on the unit circle with rational coordinates.
Here is a geometric proof of the proposition.

Let us denote the unit circle by $S^1$.

The stereographic projection with focus at $i$ is the bijective function

$$f : S^1 - \{i\} \rightarrow \mathbb{R},$$

that sends the complex number $\zeta$ to the unique real number $f(\zeta)$ that lies on the straight line connecting $i$ and $\zeta$. 
Exercise 2.5. Show that $\zeta$ has rational coordinates iff the number $f(\zeta)$ is rational.

(Hint: use similar triangles.)

Since there are infinitely many rational numbers, we are done.
Previously we used the notation $S^1$ for the unit circle.

I will now switch to another notation, that comes from algebraic geometry, and is better suited for our purposes.

From now on we shall write

$$G(\mathbb{R}) := S^1 = \{ \zeta \in \mathbb{C} \mid |\zeta| = 1 \}.$$

The set $G(\mathbb{R})$ is a group under complex multiplication, because

$$|\zeta_1 \cdot \zeta_2| = |\zeta_1| \cdot |\zeta_2| \quad \text{and} \quad |\zeta^{-1}| = |\zeta|^{-1}.$$
Let $G(\mathbb{Q})$ be the subset of $G(\mathbb{R})$ consisting of points with rational coordinates; namely

(3.1) $G(\mathbb{Q}) = \{ \zeta = s + r \cdot i \mid s, r \in \mathbb{Q}, s^2 + r^2 = 1 \}$.

Exercise 3.2. Prove that $G(\mathbb{Q})$ is a subgroup of $G(\mathbb{R})$.

Recall that to answer Question 1, namely to show there are infinitely many reduced ordered Pythagorean triples, it suffices to prove that the abelian group $G(\mathbb{Q})$ is infinite.
We first locate all the elements of finite order in the group $G(\mathbb{Q})$. These are the roots of 1, namely the elements $\zeta$ satisfying $\zeta^n = 1$ for some positive integer $n$.

Algebraic number theory tells us that there are just four of them:

\[(3.3) \quad 1, i, -1, -i.\]

Thus, if we take any element $\zeta \in G(\mathbb{Q})$ other than those four numbers, the cyclic subgroup that it generates

$$\{\zeta^n \mid n \in \mathbb{Z}\} \subset G(\mathbb{Q})$$

will be infinite!
Let us consider the familiar reduced ordered Pythagorean triple \((3, 4, 5)\).

The corresponding number in \(G(\mathbb{Q})\) is

\[
\zeta := \frac{3}{5} + \frac{4}{5} \cdot i,
\]

and it is not one of the four special numbers in (3.3). So this element has infinite order in the group \(G(\mathbb{Q})\).

Here are the first positive powers of \(\zeta\), and the corresponding triples.

<table>
<thead>
<tr>
<th>(n)</th>
<th>(\zeta^n)</th>
<th>(\text{pt}(\zeta^n) = (a_n, b_n, c_n))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(\frac{3}{5} + \frac{4}{5} \cdot i)</td>
<td>((3, 4, 5))</td>
</tr>
<tr>
<td>2</td>
<td>(-\frac{7}{25} + \frac{24}{25} \cdot i)</td>
<td>((7, 24, 25))</td>
</tr>
<tr>
<td>3</td>
<td>(-\frac{117}{125} + \frac{44}{125} \cdot i)</td>
<td>((44, 117, 125))</td>
</tr>
<tr>
<td>4</td>
<td>(-\frac{527}{625} - \frac{336}{625} \cdot i)</td>
<td>((336, 527, 625))</td>
</tr>
</tbody>
</table>
Exercise 3.4. Find a reduced Pythagorean triple with hypotenuse $c = 3125$.

(Later we will see that there is only one!)

Remark: the algebraic number theory used above, and all that is needed to complete the proofs in this lecture, can be found in the book

“Algebra”, by M. Artin, Prentice-Hall.
4. The Ring of Gauss Integers

Consider the ring of *Gauss integers*

\[ A := \mathbb{Z}[i] = \{ m + n \cdot i \mid m, n \in \mathbb{Z} \}. \]

Let us denote its field of fractions by

\[ K := \mathbb{Q}[i] = \{ s + r \cdot i \mid s, r \in \mathbb{Q} \}. \]

The reason we want to look at \( K \) is this: equation (3.1) shows that

\[ (4.1) \quad G(\mathbb{Q}) = \{ \zeta \in K \mid |\zeta| = 1 \}. \]

It is known that the ring \( A \) is a unique factorization domain.

There are countably many primes in \( A \). Let us enumerate them as

\[ q_1, q_2, q_3, \ldots. \]
The group $A^\times$ of invertible elements of $A$ turns out to be the group of roots of unity

\begin{equation}
T := \{ \pm 1, \pm i \}.
\end{equation}

Unique factorization tells us that any element $a \in K^\times$ can be written uniquely a product

\begin{equation}
a = u \cdot \prod_{i=1}^{\infty} q_i^{n_i},
\end{equation}

with $u \in T$, $n_i \in \mathbb{Z}$, and all but finitely many $n_i$ are 0 (so the product is actually finite).

We see that as an abelian group,

\begin{equation}
K^\times = T \times F,
\end{equation}

where $F$ is the free abelian group with basis $\{ q_i \}_{i=1,2,\ldots}$. 
It is known that the primes of the ring $A = \mathbb{Z}[i]$ are of three kinds.

The first kind is the prime

$$q := 1 + i.$$

It is the only prime divisor of 2 in $A$, with multiplicity 2:

$$q^2 = (1 + i)^2 = 1 + i^2 + 2 \cdot i = i \cdot 2.$$

Next let $p$ be a prime in $\mathbb{Z}$ satisfying

$$p \equiv 3 \mod 4.$$

For example $p = 3$ or $p = 7$.

Then $p$ is also prime in $A$. This is the second kind of primes.
Finally, let $p$ be a prime of $\mathbb{Z}$ satisfying

$$(4.5) \quad p \equiv 1 \mod 4.$$

For example $p = 5$ or $p = 13$.

Then there are two primes $q$ and $\bar{q}$ in $\mathcal{A}$, conjugate to each other but not equivalent (i.e. $\bar{q} \notin T \cdot q$), such that

$$(4.6) \quad p = u \cdot q \cdot \bar{q}$$

for some $u \in T$.

The numbers $q, \bar{q}$ are the third kind of primes of $\mathcal{A}$.

These will be the interesting primes for us.
It is not hard to find the decomposition (4.6). The number $p$ is a sum of two squares in $\mathbb{Z}$:

$$p = m^2 + n^2.$$ 

We then take

$$q := m + n \cdot i \quad \text{and} \quad \bar{q} := m - n \cdot i.$$ 

Consider the number

(4.7) \hspace{1cm} \zeta := q/\bar{q} \in K.$$ 

It has absolute value 1, and hence, by (4.1), it belongs to the group $G(\mathbb{Q})$. 

Amnon Yekutieli (BGU) 
Pythagorean Triples
5. The Group Structure of the Rational Circle

There are countably many primes of $\mathbb{Z}$ that are 1 mod 4.

Let us enumerate them in ascending order:

$$p'_1 := 5, \quad p'_2 := 13, \quad p'_3 := 17, \ldots$$

Each such prime $p'_j$ of $\mathbb{Z}$ has a prime decomposition in the ring $A = \mathbb{Z}[i] :

$$p'_j = u_j \cdot q'_j \cdot \overline{q'_j}.$$  

We use it to define the element

$$\zeta'_j := q'_j / \overline{q'_j} \in G(\mathbb{Q}).$$

Thus we get a sequence of elements $\{\zeta'_j\}_{j=1,2,\ldots}$ in the group $G(\mathbb{Q})$.  

Here is our main result.

**Theorem 5.2.**

*Any element* $\zeta \in G(\mathbb{Q})$ *is uniquely a product*

$$
\zeta = u \cdot \prod_{j=1}^{\infty} \zeta_j^{n_j},
$$

*with* $u \in T$, $n_j \in \mathbb{Z}$, *and all but finitely many of the* $n_j$ *are 0.*

*In other words, the abelian group* $G(\mathbb{Q})$ *is a product*

$$
G(\mathbb{Q}) = T \times F',
$$

*where* $F'$ *is the free abelian group with basis* $\{\zeta'_j\}_{j=1,2,\ldots}$. 
Sketch of Proof.

Consider the prime decomposition of $\zeta$ as an element of $K^\times$, as in (4.3).

For each prime $q_i$ of $A$ we calculate its absolute value $|q_i| \in \mathbb{R}$.

The equality

$$1 = \prod_{i=1}^{\infty} |q_i|^{n_i}$$

implies that the primes $q_i$ that do not come in pairs must have multiplicity $n_i = 0$.

The primes that do come in pairs, namely the primes of the third kind, must have opposite multiplicities. Thus they appears as powers of the corresponding number $\zeta$. \hfill \Box
6. Back to Pythagorean Triples

Recall that for a number $\zeta \in G(\mathbb{Q}) - T$, we write $\text{pt}(\zeta)$ for the corresponding reduced ordered Pythagorean triple.

Here is our explicit presentation of all reduced ordered Pythagorean triples.
Theorem 6.1. Let $c$ be an integer greater than 1, with prime decomposition

$$c = p_1^{n_1} \cdots p_k^{n_k}$$

in $\mathbb{Z}$. Here $p_1 < \cdots < p_k$ are positive primes; $n_1, \ldots, n_k$ are positive integers; and $k$ is a positive integer.

1. If $p_j \equiv 1 \mod 4$ for every index $j$, then the function

$$\{\pm 1\}^{k-1} \rightarrow \text{PT}(c),$$

$$(\epsilon_2, \ldots, \epsilon_k) \mapsto \text{pt}(\zeta_1^{n_1} \cdot \zeta_2^{\epsilon_2} \cdot n_2 \cdots \zeta_k^{\epsilon_k} \cdot n_k)$$

is bijective. Here $\zeta_j$ is the number defined in formula (4.7) for the prime $p_j$.

2. Otherwise, the set $\text{PT}(c)$ is empty.

(Hint: use Theorem 5.2, and the symmetries in Figure 2.3.)

Here is an immediate consequence of Theorem 6.1.

Corollary 6.3. Let $c$ be an integer $> 1$, with prime decomposition as in Theorem 6.1.

1. If $p_j \equiv 1 \mod 4$ for every index $j$, then the number of reduced ordered Pythagorean triples with hypotenuse $c$ is $2^{k-1}$.

2. Otherwise, there are no reduced ordered Pythagorean triples with hypotenuse $c$.

As I said before, this fact is not new; see discussion at http://mathworld.wolfram.com/PythagoreanTriple.html.

But our proof is possibly new.
Theorem 6.1 is constructive. It lets us solve the next exercise easily.

**Exercise 6.4.**

1. Find the two reduced ordered Pythagorean triples with hypotenuse 85.
2. Find the only reduced ordered Pythagorean triple with hypotenuse 289.

~ END ~