Pythagorean triples and rational geometry

Peter Selinger, Simons Institute / Dalhousie University

Berkeley Math Circle, September 13, 2016

1 Pythagorean triples

Definition. A triple (a, b, c) of integers is called a *Pythagorean triple* if

$$a^2 + b^2 = c^2.$$

Examples. $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$, $(7, 24, 25)$, $(20, 21, 29)$, $(12, 35, 37)$.

Properties. If (a, b, c) is a Pythagorean triple, then so is (na, nb, nc), for any $n \in \mathbb{Z}$. Conversely, if d is a common divisor of a, b, c, then $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ is a Pythagorean triple. We say that such triples are *equivalent*. A Pythagorean triple is *primitive* if a, b, c have no non-trivial common divisor.

Problems

1. Prove: if (a, b, c) is a primitive Pythagorean triple, then exactly one of a, b is even, and c is odd.
2. Find all Pythagorean triples (a, b, c) where $c = b+1$ (Pythagoras's formula).
3. Find all Pythagorean triples (a, b, c) where $c = b + 2$ (Plato's formula).
4. Prove: if n, m are positive integers that are relatively prime, and if nm is a square, then both n and m are squares.

5. Prove: if (a, b, c) is a primitive Pythagorean triple, where $c > 0$ and a is even (and therefore b is odd), the following integers are squares:

$$c + a, \qquad c - a, \qquad \frac{c+b}{2}, \qquad \frac{c-b}{2}.$$

6. Use these facts to derive Euclid's formula for enumerating all primitive Pythagorean triples.

2 Rational geometry

Definition. A point (x, y) is a *rational point* if x and y are rational numbers. A straight line that passes through two rational points is called a *rational line*. A polynomial (or a polynomial equation) is called rational if all its coefficients are rational.

Properties. The slope of a rational line is a rational number (or infinite, if the line is vertical). Conversely, if a line has rational slope and passes through one rational point, then it is a rational line.

Problems

1. Prove: if one of the solutions of a rational quadratic equation is a rational number, then so is the other solution.
2. More generally, consider a rational equation of degree n. Prove: if $n - 1$ of the solutions are rational, then so is the nth solution.
3. Consider a rational line intersecting the unit circle in two points. Prove: if one of the intersection points is rational, then so is the other.
4. Use these facts to derive a formula for finding all the rational points on the unit circle.
5. Use this to derive Euclid's formula for enumerating Pythagorean triples.
6. Derive a formula for finding all rational points in the unit sphere.

7. A *Pythagorean quadruple* is a 4-tuple of integers (a, b, c, d) such that

$$a^2 + b^2 + c^2 = d^2.$$

The first few non-trivial Pythagorean quadruples are $(1, 2, 2, 3)$, $(1, 4, 8, 9)$, $(4, 4, 7, 9)$, $(2, 6, 9, 11)$, $(6, 6, 7, 11)$, $(1, 12, 12, 17)$, $(8, 9, 12, 17)$. Use the solution of the previous problem to derive a formula for enumerating all Pythagorean quadruples up to equivalence.

8. Can you generalize your formula for Pythagorean n-tuples, for all n?

3 Solving equations in finite fields

Definition. A *field* is a number system with zero, one, addition, negation, multiplication, and inverses of non-zero elements, satisfying the usual laws of arithmetic:

$$\begin{array}{ll}
(a+b)+c = a+(b+c) & (ab)c = a(bc) \\
a+b = b+a & ab = ba \\
0+a = a & 1a = a \\
a+(-a) = 0 & aa^{-1} = 1 \\
 & (a+b)c = ac+bc.
\end{array}$$

Examples. The set $\mathbb{R}$ of real numbers. The set $\mathbb{Q}$ of rational numbers. The set $\mathbb{Z}_p$ of integers modulo p, where p is a prime.

Many things that "work" in the rational numbers also work in other fields. Instead of rational geometry, we can consider "geometry" modulo p.

Problems

1. Find all solutions of $x^2 + y^2 = 1$ in $\mathbb{Z}_7$.

2. Find a formula to enumerate all solutions of $x^2 + y^2 = 1$ in $\mathbb{Z}_p$, when p is a prime. Hint: you already know such a formula for the rational numbers.

3. Fact: For an odd prime p, the equation $a^2 = -1$ has a solution in $\mathbb{Z}_p$ if and only if $p \equiv 1 \pmod 4$. Using this, prove that for an odd prime p, the equation $x^2 + y^2 = 1$ has exactly $p - 1$ solutions when $p \equiv 1 \pmod 4$, and exactly $p + 1$ solutions when $p \equiv 3 \pmod 4$.

4 Elliptic curves

Definition. An elliptic curve is a curve with an equation of the form

$$y^2 = x^3 + ax + b.$$

Problems

1. Show that no straight line can intersect the elliptic curve in more than 3 points.

2. Three points (x_1, y_1), (x_2, y_2), and (x_3, y_3) on the elliptic curve are *collinear* if they line on a straight line. Show that if (x_1, y_1) and (x_2, y_2) are rational points, then so is (x_3, y_3).

3. Find a formula for (x_3, y_3) in terms of (x_1, y_1) and (x_2, y_2).