Lesson 2 – The Unit Circle: A Rich Example for Gaining Perspective

Recall the definition of an affine variety, presented last lesson:

Definition Let k be a field, and let $f_1, f_2, \dots, f_d \in k[x_1, x_2, \dots, x_n]$,. Then the **affine variety**, denoted by $\mathbf{V}(f_1, f_2, \dots, f_d)$, is defined by:

$$\mathbf{V}(f_1, f_2, \dots, f_d) = \{(a_1, a_2, \dots, a_n) \in k^n : f_i(a_1, a_2, \dots, a_n) = 0 \text{ for all } 1 \leq i \leq n\}.$$

We will start our study of algebraic varieties with the simplest type: plane algebraic curves. These are zero sets of polynomials *f*(*x*, *y*) in two variables with coefficients in some field. The simplest algebraic curves are lines, that is, zero sets of linear polynomials *ax* + *by* + *c*. Slightly more complicated are curves described by quadratic polynomials: conics. We will discuss the simplest of these: the unit circle.

I. Pythagorean Triples

Let us consider one of the oldest[1] Diophantine problems: finding all Pythagorean triples, that is, all triples (a, b, c) of integers such that $a^2 + b^2 = c^2$. The simplest and best known solution is the triple (3, 4, 5). We will discuss various methods for tackling this problem: a geometric, an analytic, and an algebraic method.

The Geometric Method: Parameterization. The geometric solution turns the problem of finding integral solutions of $a^2 + b^2 = c^2$ into the equivalent one of finding rational points on the unit circle: $\mathcal{C}$: $x^2 + y^2 = 1$. This is easy: any Pythagorean triple (a, b, c) corresponds to a rational point $x = \frac{a}{c}$, $y = \frac{b}{c}$ on the unit circle $\mathcal{C}$ and vice versa.

Exercise 1 Find all rational points on the unit circle $\mathcal{C}$ using the "sweeping line" method. That is, starting with an obvious solution, say P = (-1, 0)[2], intersect the line through P having rational slope t with the circle. There will be two intersection points, P and one other point, P_t. Find the coordinates of P_t.

[1] It is not so clear just how old this problem is: already the Babylonians compiled tables of Pythagorean triples, the Pythagoreans found formulas for generating infinitely many such triples, but not even Diophantus asked for *all* solutions to $x^2 + y^2 = z^2$.

[2] Any rational point on $\mathcal{C}$ would do.

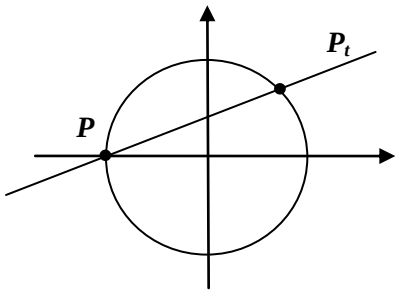

Figure 1: Parameterizing the Unit Circle

Exercise 2 - True or False:

a) If *t* is rational, then P_t is a rational point (meaning that the coordinates of P_t are rational.)

b) If $Q = (x, y) \neq P$ is a rational point on $\mathcal{C}$, then $Q = P_t$ for some rational number *t*.

c) The point *P* = (-1, 0) corresponds to a point P_t for some rational value of *t.*

.

The "sweeping lines" method used geometry to produce the representation: $x = \frac{1-t^2}{1+t^2}$, $y = \frac{2t}{1+t^2}$ of points on the unit circle. This representation is an example of what is known as a *rational parametric representation* of the variety, in this case the variety: $\mathbf{V}(x^2 + y^2 - 1)$.

Definition. If $V = \mathbf{V}(f_1, f_1, \dots, f_s) \subseteq k^n$ is a variety, then a **rational parametric representation** for V is a set of rational functions $r_1, r_2, \dots, r_n \in k(t_1, t_2, \dots, t_m)$ such that the points given by

$$\begin{aligned} x_1 &= r_1(t_1, t_2, \dots, t_m) \\ x_2 &= r_2(t_1, t_2, \dots, t_m) \\ &\vdots \\ x_n &= r_n(t_1, t_2, \dots, t_m) \end{aligned}$$

lie in V.

Note that, over the field of rational numbers, dividing through by $1 + t^2$ is not a problem since $1 + t^2 \neq 0$. Over an arbitrary field *k*, however, one has to be careful. In particular, there is a problem when the field *k* contains a primitive fourth root of unity.

Exercise 3 Consider the finite field $k = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for odd primes p. Does the rational parameterization $x = \frac{1-t^2}{1+t^2}$, $y = \frac{2t}{1+t^2}$ still yield points on the unit circle over $\mathbb{F}_p$?

The Algebraic Method: Unique Factorization. Consider the equation $a^2 + b^2 = c^2$, and assume (a, b, c) is a solution in coprime natural numbers (such solutions are called primitive). It is easy to see that *c* must be odd and that one of *a* or *b* is even. Assume that *b* is even and write $b^2 = c^2 - a^2 = (c - a)(c + a)$. Since $\gcd(c - a, c + a) = 2$ (it divides 2*c* and 2*a*, hence 2; now observe that *a* and *c* are both odd, hence their sum and difference are even), we conclude using unique factorization that $c + a = 2r^2$ and $c - a = 2s^2$, and $b = 2rs$; this shows $c = r^2 + s^2$, $a = r^2 - s^2$, and we have found: the primitive Pythagorean triples (*a*, *b*, *c*) with *b* even are

$$a = r^2 - s^2, \qquad b = 2rs, \qquad c = r^2 + s^2 \qquad (2)$$

where *r* and *s* are coprime integers.

Exercise 4 How do the computations above yield a rational parameterization of the unit circle?

It is of course easy to verify without using unique factorization that (2) are solutions of the equation $X^2 + Y^2 = Z^2$. Showing that this set of solutions is complete, however, requires unique factorization, at least if we want to use the algebraic method.

The Analytic Method: Trigonometry

As is well known, every real point (x, y) on the unit circle can be written as $x = \cos\alpha$, $y = \sin\alpha$ for some real number $\alpha \in [0,2\pi)$.

Exercise 5 Use the well-known identities

$$\cos^2\alpha - \sin^2\alpha = \cos 2\alpha \text{ and } \cos^2\alpha + \sin^2\alpha = 1$$

to produce the rational parameterization of the unit circle: $x = \frac{1-t^2}{1+t^2}, y = \frac{2t}{1+t^2}$.

The Galois Theoretic Method

This method is a lame excuse to discuss some Galois Theory. Let F be a field, and $m \in F$ a nonsquare; then $K = F(\sqrt{m}) = \{a + b\sqrt{m}: a, b \in F\}$ forms a field with respect to the natural addition and multiplication. We say that K/F is a quadratic extension.

The set of all ring homomorphisms $K \to K$ leaving the elements of the base field F fixed forms a group called the **Galois group of K/F**, which is denoted by Gal(K/F). It has two elements, the identify map and the conjugation map $\sigma: a + b\sqrt{m} \mapsto a - b\sqrt{m}$. Note that the set of elements in K fixed by σ is just F.

For general Galois extensions K/F we have the norm map $N: K \mapsto F$ defined by $N(\alpha) = \prod_{\sigma\in \mathrm{Gal}(K/F)} \sigma(\alpha)$.

Exercise 6 What is the norm map, $N: K \mapsto F$, for a quadratic extension $K = F(\sqrt{m}) = \{a + b\sqrt{m}: a, b \in F\}$?

For cyclic extensions (field extensions whose Galois group is cyclic, i.e., generated by one element σ) we have Hilbert's Theorem 90:

Hilbert's Theorem 90 If $\alpha \in K^{\times}$ has norm 1, then α can be written in the form $\alpha = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in K$.

Exercise 7 For quadratic extensions, there is a simple proof of Hilbert's Theorem 90:
a) If $\alpha = -1$, find β such that $\alpha = \frac{\beta}{\sigma(\beta)}$.

b) Now find β such that $\alpha = \frac{\beta}{\sigma(\beta)}$ when $\alpha \neq -1$.

Exercise 8 Now apply Hilbert's Theorem 90 to find all Pythagorean triples (*x*, *y*, *z*).

Remark. The methods are not equivalent. The analytic method requires trigonometric functions and thus, at least at present, only works for subfields of $\mathbb{C}$. The algebraic version works for (fields that are quotients of) unique factorization domains, and the geometric version over general fields. Moreover, the analytic and geometric methods can be applied only to curves of genus 0; the algebraic method gives at least some information as long as one has a factorization to work with.

What the moral of the story? For solving certain problems in arithmetic, there usually are a variety of possible methods you can choose from. Of course, in order to have a choice you have to be familiar with these methods. In this course we will be focusing on methods involving an interplay between algebra and geometry.

Next Lesson: Determine the rational points on the hyperbola $x^2 - 3y^2 = 1$ with as many methods as possible.

I will ask volunteers to present their solutions, and hopefully we will see a variety of approaches!