Points on $x^2 + y^2 = 1$ over $\mathbb{Z}_p$?

John D Mangual

If we want to find points in a circle, we can have $x = \cos\theta$ and $y = \sin\theta$ and the sum of squares is 1:

$$x^2 + y^2 = (\cos\theta)^2 + (\sin\theta)^2 = 1$$

Next we make a choice between nice angles and nice values. In the beginning we get both:

$$\sin\frac{\pi}{6} = \frac{1}{2}, \quad \sin\frac{\pi}{4} = \frac{\sqrt{2}}{2}, \quad \sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$$

There are even some more interesting values, such as the regular octagon[1]:

$$\cos\frac{\pi}{8} = \tfrac{1}{2}\sqrt{2+\sqrt{2}}, \qquad \cos\frac{\pi}{32} = \sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}$$

So there are all sorts of fascinating numbers to be discovered here.

Kronecker-Weber theorem absorbs all these kinds of problems into a single Galois-theoretic result (kinda-sort of):

> Every finite abelian extension F in $\mathbb{Q}$ is $F \subseteq \mathbb{Q}(e^{2\pi i/n})$ for some root of unity $|e^{2\pi i/n}| = 1$

When I was a student I was trained to plug in numbers ("evaluate") in order to feel-out all the steps of the proof. Some of these objects may be uncomputable, take infinite resources to compute.

Whatever.

All these results of cosines and radicals fall under the purview of the Kronecker-Weber theorem and (**Abelian**) **class field theory**. Another approach is to solve these equations over various objects:

- if we solve $x^2+y^2 = 1$ over $\mathbb{Q}$ these solutions are indexed by Pythagorean triples. $5^2+12^2 = 13^2$ so that $\theta = \tan^{-1}(\frac{5}{12})$ sorts of a peculiar angle but at least $\cos\theta = \frac{5}{13}$ and $\sin\theta = \frac{12}{13} \in \mathbb{Q}$.
- In p-adic numbers we can have circles of negative radius: $2^2 + 3^2 = -1 \pmod 7$ and if we have a solution in $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ we can have a solution in the 7-adic numbers,

  $$\mathbb{Z}_7 = \varprojlim \mathbb{Z}/7^k\mathbb{Z}$$

  There is no more concept of angle, but at least $x = \cos\theta, y = \sin\theta \in \mathbb{Q}_7$.

[1] https://en.wikipedia.org/wiki/Trigonometric_constants_expressed_in_real_radicals

Maybe, in the context of another problem, we can rotate by one of these crazy$p$-adic numbers. I can already think of two:

$$x^2 + y^2 + z^2 = 1, \quad x^2 + y^2 + z^2 + w^2 = 1$$

The 4-squares problem is a bit more well-behaved than the 3-squares problem. Yet in the 3-squares, there exists coordinates:

- $x = \cos\theta \sin\phi$
- $y = \cos\theta \cos\phi$
- $z = \sin\theta$

There is a clear rotation action on this space no matter which ring or field we use:

$$\big\{ x^2 + y^2 + z^2 = 1 \big\} \in (\mathbb{Q}_7)^3$$

as long as $\cos\theta, \cos\phi, \sin\theta, \sin\phi \in \mathbb{Q}_7$ we are fine (and we have to check both sine and cosine).

I could totally imagine some exotic arrangement of circles and triangles to get angles like these. Class Field Theory is a rather powerful tool for what is essentially basic fun. And the number theory textbooks leave out all the interesting parts.

References

(1) Nancy Childress **Class Field Theory** (Universitext). Spinger, 2009.