Scratchwork: Pythagorean Triples over $\mathbb{Z}[i]$

The equation $x^2 + y^2 = 1$ defines what we might call a **variety**. Here it's just a circle. Our decision to use Cartesian coordinates, algebra and equations, to describe Euclidean geometry, leads to all sorts of complications. Attempts to finalize what we might call a variety leads to all sorts of difficult **commutative algebra** and ultimately **schemes**.

Taking for granted a minute that circles are a meaningful concept and that we should use algebra and geometry, we observe the variety $X = \{x^2 + y^2 - 1 = 0\}$ has a rational paramterization.

$$t \in \mathbb{Q} \longrightarrow (x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right) \in \mathbb{Q}^2$$

And we can think of fractions as pairs of integers $\frac{m}{n} \in \mathbb{Q}$ or as pairs of integers up to proportion[1] $[m : n] \in P\mathbb{Z}^2$. Therefore we can solve an equation over integers: $a^2 + b^2 = c^2$ over $\mathbb{Z}$:

$$(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2) \in \mathbb{Z}^3$$

The machinery of algebra tells us that all we required is that $K = \mathbb{Q}$ is a field. Therefore we could also try to solve the Pythagoras equation over $\mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{2}]$ and solve it in the same way.

What happens if we write the thing down we could write $a = a_1 + ia_2$ etc. and find:

$$(a_1 + ia_2)^2 + (b_1 + ib_2)^2 = (c_1 + ic_2)^2$$

and we learned we could seprate the real and imaginary components and find two equations:

$$\begin{aligned} (a_1^2 - a_2^2) + (b_1^2 - b_2^2) &= (c_1^2 - c_2^2) \\ 2a_1a_2 + 2b_1b_2 &= 2c_1c_2 \end{aligned}$$

which is the intersection of two conic sections. And here because of the structure of $\mathbb{Z}[i]$ we can expect a spectactular reduction. Is that all?

Let's find a few solutions. The algebra is meaningful if we can find a few number solutions. Let $m = i$ and $n = 1 + i$. Then:

$$\begin{array}{rcccl} m^2 - n^2 & = & (i)^2 - (1 + i)^2 & = & -1 - 2i \\ 2mn & = & i \times (1 + i) & = & -1 + i \\ m^2 + n^2 & = & (i)^2 + (1 + i)^2 & = & -1 + 2i \end{array}$$

Then, using the same algebra identity we used over $\mathbb{Z}$ we obtain another Pythagoras formula:

$$(1 + 2i)^2 + (1 - i)^2 = (1 - 2i)^2$$

What kind of shape is this? Is it a right triangle? What is a "complexified" right triangle?

[1] Yet another word we can scrutinize. What are we calling "proportionate"?

Also we can encode $i = \sqrt{-1}$ as a 2×2 matrix:

$$\sqrt{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Does our Pythagoras equation look any better as relation on 2×2 matrices?

$$\begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}^2 + \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}^2$$

Exact matrix identities like this should be pretty rare. Pythagoras theorem is a machine that consistently produces equations like this. The square-root operator has no guarantee of falling in the integer 2×2 matrices: $\sqrt{A} \stackrel{?}{\in} \mathsf{GL}_2(\mathbb{Z})$.

Are there other 2×2 matrices such that $A^2 = 1$? I can find an invertible matrix $B \in \mathsf{GL}_2(\mathbb{Z})$ and we always obtain:

$$(BAB^{-1})(BAB^{-1}) = (BA)(B^{-1}B)(A^{-1}B^{-1}) = (BA)I_{2\times 2}(BA)^{-1} = I_{2\times 2}$$

If these matrices were perfectly associative, if the transformations we were considering perfectly mapped two variables into two other variables, if A^{-1} is exactly the inverse of A, then our formula always works. Let's try:

$$B = \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix} \in \mathsf{GL}_2(\mathbb{Z}) \text{ and } B^{-1} = \begin{bmatrix} 3 & -4 \\ -2 & 3 \end{bmatrix} \in \mathsf{GL}_2(\mathbb{Z})$$

Then we can multiply the matrices:

$$BAB^{-1} = \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix} \times \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 3 & -4 \\ -2 & 3 \end{bmatrix} = \cdots = \begin{bmatrix} 17 & -24 \\ 12 & -17 \end{bmatrix} \in \mathsf{GL}_2(\mathbb{Z})$$

In the process of computing a square root, for 2×2 matrices, we obtain approximate square roots of integers over $\mathbb{Z}$:

$$1 = 17 \times 17 - 12 \times 24 = \left(17^2 - 2 \times 12^2\right)$$

and these were the types of considerations that I'm hoping can motivate theory of modular forms and dynamical systems to other people.

Using numPy we can multiply 2×2 matrices as a dot product operation:

```
Python 2.7.12 (default, Dec  4 2017, 14:50:18)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import numpy as np

>>> B = np.array([[3,4],[2,3]])
>>> A = np.array([[0,-1],[1,0]])
>>> C = np.dot(B,A)

>>> D = np.dot(C, np.linalg.inv(B))
>>> D
array([[ 18., -25.],
       [ 13., -18.]])
>>> D.astype(int)
array([[ 17, -24],
       [ 12, -17]])
>>> np.dot(D,D)
array([[ -1.00000000e+00,  -2.84217094e-14],
       [ -1.06581410e-14,  -1.00000000e+00]])
```

Using Sympy we can obtain the same answer, staying within the realm of integers.

```
Python 2.7.12 (default, Dec  4 2017, 14:50:18)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from sympy import *
>>> B = Matrix([[3,4],[2,3]])
>>> A = Matrix([[0,-1],[1,0]])
>>> B*A*B**(-1)
Matrix([
[18, -25],
[13, -18]])
```

Our computers can never really behave like $\mathbb{R}$ or $\mathbb{Z}$ but for the moment 10^{-14} scale errors do not qualitatively change our answers.

We do not even scratch the surface. We notes that computing $\sqrt{2}$ motivates finding a circle on the modular surface $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ or even $\Gamma_0(4)\backslash\mathbb{H}$. And then we can study Maaß. forms or theta functions.

Sum of Three Squares

One way to ask for trouble is to ask for details about the proof of the sum of three squares formula. We know from Legendre (or Lagrange) that:

$$n = a^2 + b^2 + c^2 \text{ with } a, b, c \in \mathbb{Z} \leftrightarrow n \neq 4^k(8\ell + 7) \in \mathbb{Z}$$

by 1987 Iwaniec and Duke had shown - through rather severe means - that as $n \to \infty$, these solutions become equidistributed on the sphere. For any $V \subseteq S^2$:

$$\lim_{n\to\infty} \frac{\frac{1}{\sqrt{n}}\big\{(a,b,c) : a^2 + b^2 + c^2 = n\big\} \cap V}{n} = \mu(V)$$

I have many many doubts about the proof. Their argument is certainly correct, and I can verify the result overall with a calculator. So what's the problem? There are many intermediate steps that I must take on faith in order to declare this result to be proven. Who needs mathematical proof anyway? I can always check the result with a calculator.

Number Theory is great at teasing out philosophical points like these.[2] When I make a telephone call, did I use the Nyquist bound?[3] Or any Fourier Analysis at all? Did the electrician handling the wires . How does my phone recontruct my telephone call from invisible signals, literally from thin air? Let $x : \mathbb{R} \to \mathbb{C}$:

$$\begin{aligned} \hat{x}(t) &:= \int_{\mathbb{R}} x(t)\, e^{2\pi i\, ft}\, dt \\ x(t) &= \sum_{T\in\mathbb{Z}} T \cdot \hat{x}(nT)\, e^{-2\pi i\, nfT} \end{aligned}$$

We don't ask any of these questions and we don't have to if we want to make that phone call. As soon as we want to fix the wires, or create our own wireless nework, or design our own WiFi protocol, we almost need to make these considerations.

This formula is *known* why do we need to prove it again?
We can find it on a calculator why do we need to prove it?
Someone else did the work already, why do I need to do it over??
Why is my word not good enough?

Maybe, when I try to study these equations - which I thought I was suppsed to be doing anyway - I have calld bullshit on everybody. These statements are always true, but very hard to prove. They contain an infinite amount of information. Are these statements isolated phenomenon? Can I make them into someone useful?

Back to earth. We have a highly *non-trivial* statement about the equidistribution of the set of points on the sphere. There are even modern theorems that tell us that *patterns* should exist in such random point-sets. We are told that:

$$\theta(z; u) = \sum_{m\in\mathbb{Z}^3} u(m)\, e(z|m|^2)$$

is a holomorphic $\Gamma_0(4)$ cusp form of degree $k = \ell + \frac{3}{2}$ where m is a Spherical Harmonic of degree ℓ.

[2] Mathematics is the Queen of the Sciences, and Number Theory is the Queen of Mathematics.
[3] `https://en.wikipedia.org/wiki/Nyquist%E2%80%93Shannon_sampling_theorem`

One day I attempted to write down such a cusp form. What is a cusp form anyway? Automorhic forms specialists love their jargon and when you ask to many questions, they merely call you incompetent and move on.

$$\theta(z; u = x_1^2 - x_2^2) = \sum_{m \in \mathbb{Z}^3} \left(m_1^2 - m_2^2\right) e(z|m|^2)$$

In fact it is zero. It is zero because we have that $m_1 \leftrightarrow m_2$ then $\theta(z;u) = -\theta(z;u)$. Somewhat more methodically we have that $(m_1, m_2, m_3) \mapsto (\pm m_1, \pm m_2, \pm m_3)$ is an action of $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$ on $\mathbb{Z}^3$ and this induces a group action on the space of modular forms.

These is also equidistribution of rational points on the sphere acted on by $\mathsf{SO}_3(\mathbb{Q})$ and we could quantify that, or even S-arithemtic points in $\mathsf{SO}_3\left(\mathbb{Z}[\frac{1}{5}]\right)$ as argued by Benoist and Oh around 2012. Here we say that $X = \{x^2 + y^2 + z^2 = 1\}$ is variety or something like that. Finally we recoganize that: $\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \subseteq \mathsf{SO}_3(\mathbb{Z})$. The rotation group of integers is rather small, only 24 elements.

Humans make mistakes and we have bigger, more exotic number systems to describe.

$$u = \frac{3}{16}\sqrt{\frac{1}{\pi}}\frac{1}{r^4}\left(35z^4 - 30\,z^2\,r^2 + 3\,r^4\right)$$

then here is another modular form. It doesn't look very elegant and the $\Gamma_0(4)$ invariance is less than obvious.

$$\theta(z;u) = \frac{3}{16}\sqrt{\frac{1}{\pi}} \sum_{m \in \mathbb{Z}^3} \frac{35\,m_3^4 - 30\,m_3^2\left(m_1^2 + m_2^2 + m_3^2\right) + 3\left(m_1^2 + m_2^2 + m_3^2\right)^2}{\left(m_1^2 + m_2^2 + m_3^2\right)^2} e(z\,|m|^2)$$

The cusp forms have to with the limit $\theta(x + 0i; u) = 0$ for $x + 0i \in \mathbb{Q} \subseteq \mathbb{H}$. The cusps of $\Gamma_0(4)$ are not exactly $\mathbb{Q}$. They are fractions $\frac{p}{q} \in \mathbb{Q}$ with either $4|p$ or $4|q$. So these are the "singular" fractions $\pmod 4$, right? Since these are $\frac{0}{4}$ or $\frac{4}{0}$ in the Farey Fractions.

It was very difficult to find a $\theta(z;u)$ that wasn't zero. I don't even know the normalization constant for: $u(x,y,z) = xy(7z^2 - r^2)$. Do we know what is $\int u(z)^2\,dS$, here? Lots of these exmples are zero, but if we take square of the examples listed on wikipedia to ensure positivity. So he barely says anything about what's going on within $L^2(S^2)$ except that it's graded by degree. And then he uses a bound from another place.

So these proofs have been exceedingly polite.

$\mathbf{\Gamma_0(4)}$

To the best of my reading one of the punchlines is that we don't know fractions nearly as well as we thought. Here's the definition of a congruence subgroup.

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}$$

What about $\mathsf{SL}_2(\mathbb{Z}[i])$? Here's another congruence subgroup:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod N \right\}$$

These objects look almost self-explanatory since we could take any solution to $ad - bc = 1$ and move forward.

Let's take two prime numbers $p = 31$ and $q = 43$. Bezout's theorem says we can find $a, b \in \mathbb{Z}$ such that:

$$\begin{vmatrix} p & a \\ q & b \end{vmatrix} = p \times b - a \times q = 1$$

The **Euclidean algorithm** which is well studied over $\mathbb{Z}$ gives us (in a rather ugly layout):

$$\begin{aligned} 43 &= 31 \times 1 + 12 \\ 31 &= 12 \times 2 + 7 \\ 12 &= 7 \times 1 + 5 \\ 7 &= 5 \times 1 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

Fortunately for us, this algorithm terminates. In real life, $31, 43 \in \mathbb{Z}$ would not be perfect integers. Desptite having the entire Euclidean algorithm in front of me, I'm still tempted to use Guess and Check[4]

$$\frac{31}{43} = [0; 1, 2, 1, 1, 2, 1]$$

The reconstruction is not instant to me.

$$\begin{aligned} \big(43 \times 1\big) - \big(31 \times 1\big) &= 12 \\ \big(31 \times 3\big) - \big(43 \times 2\big) = 31 - \Big(\big(43 \times 1\big) - \big(31 \times 1\big)\Big) \times 2 &= 7 \\ \big(43 \times 3\big) - \big(31 \times 4\big) = \Big(\big(43 \times 1\big) - \big(31 \times 1\big)\Big) - \Big(\big(31 \times 3\big) - \big(43 \times 2\big)\Big) \times 1 &= 5 \\ \big(31 \times 7\big) - \big(43 \times 5\big) = \Big(\big(31 \times 3\big) - \big(43 \times 2\big)\Big) - \Big(\big(43 \times 3\big) - \big(31 \times 4\big)\Big) \times 1 &= 2 \\ \big(31 \times 11\big) - \big(43 \times 8\big) = \Big(\big(31 \times 3\big) - \big(43 \times 2\big)\Big) - \Big(\big(43 \times 3\big) - \big(31 \times 4\big)\Big) \times 2 &= 1 \end{aligned}$$

Should we check this with a calculator? I did and it's correct. Now I have said that my Python computer, using it's own method, the above computation is correct.. What happens when we encode a taylor series, and we're using infinitely many elementary school operations, so many that we lose track? While computers are helpful, Number Theory starts to turn into ways to play tricks on the computer. While they don't know modular forms or algebraic number theory, they canon case of n-digit multiplication or addition with carries, is just another algorithm to a Theoretical Computer Scientist.

What would happen if we didn't have the Euclidean algorithm memorized? [5]

Our final result, a solution to $ad - bc = 1$ is extremely informative. This identity carries several bits of information.

$$\begin{vmatrix} 31 & 11 \\ 43 & 8 \end{vmatrix} = \big(31 \times 11\big) - \big(43 \times 8\big) = 1$$

However, we may have left the realm of $\Gamma(2)$ or $\Gamma_0(4)$. At least $\Gamma(2)$ has an easy reading in terms of fractions. $\frac{31}{68}$ is a reduce fraction. Can we find:

$$31 \times b - 68 \times (2 \times a) = 1 \quad \text{with} \quad a \in \mathbb{Z}$$

Does some kind of Euclidean algorithm still hold? In a fairly advanced textbook, theorem mechanically states that $[\Gamma(2) : \mathrm{SL}_2(\mathbb{Z})] = 2^3 \times (1 - \frac{1}{2^2}) = 6$. This will fall out of **First isomorphism theorem** which we should state and use. Apparently, I don't know how to fix Euclid's algorithm in this case, or my isomorphism theorems anymore.

[4] What algorithm does "guess-and-check" correspond to here? Is it Breadth-First Search, Greedy Algorithm, Knapsack Problem? I wish I knew my computer science jargon better.

[5] Knowing an algorithm is something like having a computer on hand. Searching for a pair of socks, crossing the street, drinking a beer. These are all computations.

It's hard to see the generalization with the basic example. It's too familiar. $\mathfrak{p}_1 = 9 + 4i$ and $\mathfrak{p}_2 = 9 + 16i$ are primes. With computer I found that these are the only primes $\mathfrak{p} \in 1 + 8\mathbb{Z}[i]$ with $N(\mathfrak{p}) = \mathfrak{p}\overline{\mathfrak{p}} < 1000$, there are only three!

- $9 + 16i$
- $17 + 8i$
- $25 + 16i$ (how is it that $\mathfrak{q} = 5^2 + 4^2 \times i \in \mathbb{Z}$ is a prime?)

and Dirichlet's Unit Theorem - I am guessing holds for all number fields, and so there are infinitely many Gaussian prime numbers in the list. And here is the command for that:

```
for(a=1,sqrtint(10000),for(b=1,sqrtint(10000),p=64*(a^2+b^2)+16*a+1;
if(isprime(p)&&p<10000,print([8*a+1+8*b*I,p]),)))
```

As a programmer I question the PARI/GP code used here, but at least we get started. This could probably have been coded with only `Python` and `numpy`. There are about 30 such primes with norms less than 10^5. Norm is such an overused word here, they are not even Euclidean.

We could have pairs of relatively prime numbers in $\mathbb{Z}[i]$ and there's even a Euclidean algorithm, still. So there is such a thing as $\mathsf{SL}_2(\mathbb{Z}[i])$. And it could even have a congruence group such as $\mathsf{SL}_2(\mathbb{Z}[i])(9 + 4i)$ and this could have it's own special continued fraction problem. If we have two fractions, we could try something:

$$\frac{\mathfrak{p}}{\mathfrak{q}_1 \times \mathfrak{q}_2} = \frac{(9 + 16i)}{(9 + 4i) \times (2 + i)} \in \mathbb{Q}(i)$$

How can we create such an object?

$$\Gamma\big(9 + 4i\big) = \mathsf{SL}_2\big(\mathbb{Z}[i]\big)(9 + 4i) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{9 + 4i} \right\}$$

The ending diophantine equation should look identical to the $\mathbb{Z}$ case (maybe I'm writing, Number Theorists have such elaborate protocols, I don't even care):

$$(9 + 16i) \times b - (9 + 4i)^2 \times (2 + i) \times a = 1$$

What's new is the steps we're allowed to use in the Eucludean algorithm have changed somewhat.

$$a = (9 + 4i) \times q \times b + r$$

It seems rather unlikely we could obtain a smaller number this way. What about the fraction $\frac{9}{16}$ and we'd like to see that:

$$16 = 9 \times 2 - 2 \text{ however } \begin{vmatrix} 16 & 9 \\ 7 & 4 \end{vmatrix} = 16 \times (2 \times 2) - 9 \times 7 = 1$$

and the matrix we have obtained is in $\Gamma(2)$ and it's even in $\Gamma(4)$ but I can't find it as a factorization of "generating elements" that stay within the group.

$$\begin{bmatrix} 16 & 9 \\ 7 & 4 \end{bmatrix} \to \begin{bmatrix} 16 - 9 & 9 \\ 7 - 4 & 4 \end{bmatrix} = \begin{bmatrix} 7 & 9 \\ 3 & 4 \end{bmatrix} \notin \Gamma(2), \Gamma(4)$$

Row operations, *themselves* encode elements of $\mathsf{SL}_2(\mathbb{Z})$ so a single row operation is not enough to stay within a congruence group like $\Gamma(2)$ or $\Gamma(4)$. The question become can we ever find a path to the identity matrix, while remaining in this group? And what row operations do they represent?