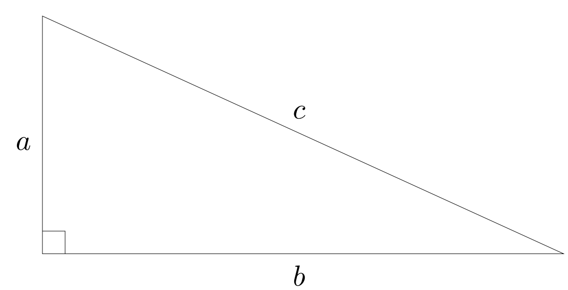
Number Theory Homework.

1. Pythagorean triples and rational points on quadratics and cubics.

1.1. **Pythagorean triples.** Recall the Pythagorean theorem which is that in a right triangle with legs of length a and b and hypotenuse of length c then

$$a^2 + b^2 = c^2. \tag{1}$$



It is interesting to find examples of right triangles where all the sides have integer lengths.

Definition 1. A ***Pythagorean triples*** is an triple of positive integers (a, b, c) with $a^2 + b^2 = c^2$. $\square$

Probably the best known Pythagorean triple is $(3, 4, 5)$. Here are some other examples:

$$(5, 12, 13), \quad (7, 24, 25), \quad (8, 15, 17), \quad (65, 72, 97), \quad (203, 394, 445)$$

Our current goal is to find all such triples.

We first divide equation (1) by c^2 to get

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right) = 1.$$

Then the numbers

$$x = \frac{a}{c} \qquad y = \frac{b}{c}$$

are rational numbers. Thus (x, y) is a ***rational points*** on the circle $x^2+y^2 = 1$. We will start our search for all Pythagorean triples by finding all rational points on $x^2 + y^2 = 1$.

We start with any rational point on the circle. Psychologically the most natural is $(x, y) = (1, 0)$. We now look at lines through this point with rational slope and show that such line intersect the circle in one other points and this point has rational coordinates. A vector with slope m is

$$\begin{bmatrix} 1 \\ m \end{bmatrix}.$$

Thus the vector point equation of a line through $(1,0)$ with slope m is

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} 1 \\ m \end{bmatrix}$$

or in parametric form

$$\begin{aligned} x &= 1 + t \\ y &= mt. \end{aligned}$$

Using these equations in $x^2 + y^2 = 1$ gives

$$(1+t)^2 + (mt)^2 = 1.$$

The values of t that make this equation true correspond to the points on the line through $(1,0)$ with slope m that are on the circle $x^2 + y^2 = 1$. This equation for t simplifies to

$$t\big((m^2+1)t + 2\big) = 0.$$

which has solutions

$$t = 0, \qquad t = \frac{-2}{m^2+1}.$$

That $t = 0$ is a solution does not surprise us, as $t = 0$ corresponds to the point $(1,0)$ with we know to be on the circle $x^2 + y^2 = 1$. Using $t = -2/(m^2+1)$ in our formulas for x and y gives

$$x = 1 + t = \frac{m^2-1}{m^2+1}, \qquad y = mt = \frac{-2m}{m^2+1}.$$

If m is a rational number, then it is not hard to see these are both rational and therefore (x,y) is a rational point on $x^2 + y^2 = 1$. The converse also holds.

Proposition 2. *Let m be any rational number, then the point (x,y) with*

$$x = \frac{m^2-1}{m^2+1}, \qquad y = \frac{-2m}{m^2+1} \tag{2}$$

is a rational point on $x^2 + y^2 = 1$. Conversely if (x,y) is a rational point on $x^2 + y^2 = 1$ then either $(x,y) = (1,0)$, or there is some rational rational number m such that x are y are given by the above formulas.

Problem 1. Prove this. *Hint:* All that remains to be one is to show that if $(x,y) \neq (1,0)$ is a rational point on the circle, then there is a rational number m such that x and y are given by the desired formulas. Recall that the geometric meaning of m is the slope of the line through $(1,0)$ and (x,y). This slope (see Figure 1) is

$$m = \frac{y}{x-1}.$$

Now show that using this value of m in (2) gives x and y. This is not quite as easy as one would like, as we have to use that $x^2+y^2=1$ to simplify. To start

$$\begin{aligned} m^2+1 &= \left(\frac{y}{x-1}\right)^2+1 \\ &= \frac{y^2+(x-1)^2}{(x-1)^2} \\ &= \frac{y^2+x^2-2x+1}{(x-1)^2} \\ &= \frac{1-2x+1}{(x-1)^2} && \text{(as } y^2+x^2=1\text{)} \\ &= \frac{2(1-x)}{(x-1)^2} \\ &= \frac{2}{1-x}. \end{aligned}$$

Do a similar calculation to show

$$m^2-1=\frac{2x}{1-x}.$$

Using these it should not be hard to verify that

$$\frac{m^2-1}{m^2+1}=x, \qquad \text{and} \qquad \frac{-2m}{m^2+1}=y$$

hold. Use this to finish the proof. □

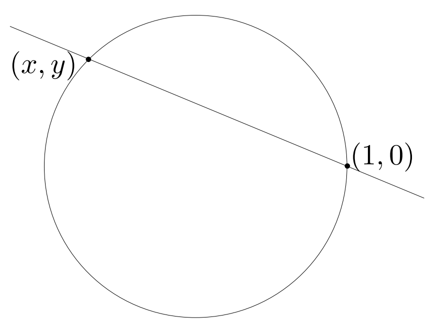


FIGURE 1. If $(x,y)\neq(1,0)$ is a rational point on $x^2+y^2=1$ then line through $(1,0)$ and (x,y) has slope $m=\dfrac{y}{x-1}$, which is a rational number.

Example 3. We we use the same cirlce of ideas to find all the rational points on the curve, C, defined by

$$x^2-5xy+2y^2=-1.$$

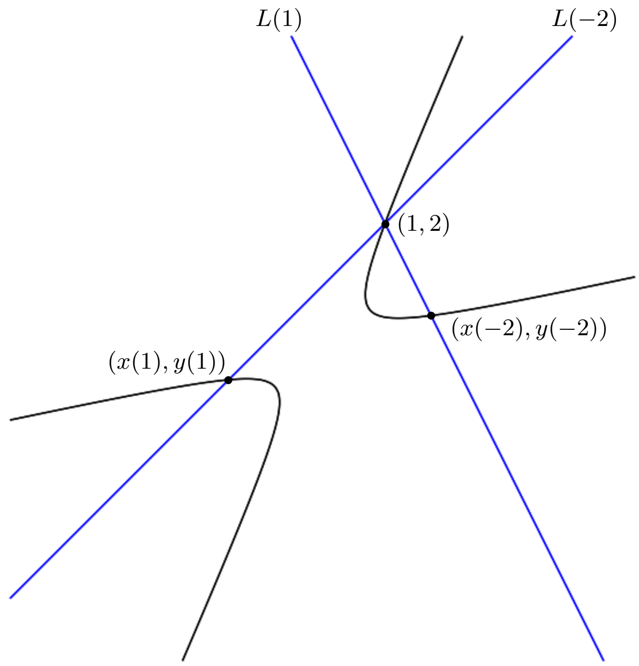


Figure 2. The hyperbola, C, defined by $x^2-5xy+2y^2=-1$, the lines $L(1)$ and $L(-2)$ through the rational point $(1,2)$ of C with slopes 1 and -2. The the points $(x(1),y(1))$ and $(x(-2),y(-2))$ where these lines intersect C are also shown. These points are also rational points on C.

This curve is a hyperbola, see figure 2. We tart by finding one rational point. In this we note $(x,y)=(1,2)$ is on the curve. The parametric form of a line through $(1,2)$ with slope m is

$$x = 1+t, \qquad y = 2+mt.$$

Plug these into $x^2-5xy+2y^2+1=0$ and group by powers of t.

$$\begin{aligned} x^2-5xy+2y^2+1 &= (1+t)^2 - 5(1+t)(2+mt) + 2(2+mt)^2 + 1 \\ &= (2m^2-5m+1)t^2 + (3m-8)t \\ &= t\left[(2m^2-5m+1)t + (3m-8)\right] \\ &= 0. \end{aligned}$$

Solving for t gives $t=0$ (corresponding to the point $(1,2)$) and

$$t = \frac{-3m+8}{2m^2-5m+1}$$

Plugging this back into $x=1+t$ and $y=2+mt$ gives

$$x = x(m) = 1 + \frac{-3m+8}{2m^2-5m+1} = \frac{2m^2-8m+9}{2m^2-5m+1}$$

$$y = y(m) = 2 + mt = 2 + m\frac{-3m+8}{2m^2-5m+1} = \frac{m^2-2m+2}{2m^2-5m+1}$$

One solution will be $t = 0$ (why?). Use the other solution in $x = 1 + t$ and $y = 2 + mt$ to get rational points on C. This is all of them, but you do not have to prove that. □

1.2. **Rational points on quadratic curves.**

Problem 2. Using this same circle of ideas to find all the rational points on the curve, C, defined by

$$x^2 - 5xy + 2y^2 = -1.$$

Hint: Start by finding one rational point. In this case check that $(x, y) = (1, 2)$ is on the curve. The parametric form of a line through $(1, 2)$ with slope m is

$$x = 1 + t, \qquad y = 2 + mt.$$

Plug these into $x^2 - 5xy + 2y^2 = -1$ and solve for t in terms of m. One solution will be $t = 0$ (why?). Use the other solution in $x = 1 + t$ and $y = 2 + mt$ to get rational points on C. This is all of them, but you do not have to prove that. □

More generally we can look for all the rational points on a curve, C, defined by

$$f(x, y) = 0$$

where $f(x, y)$ is a quadratic polynomial

$$f(x, y) = c_{20}x^2 + c_{11}xy + c_{02}y^2 + c_{10}x + c_{01}y + c_{00}$$

and all the coefficients, c_{ij} are integers[1] We assume there is at least one rational point, (x_0, y_0), on C, that is a rational point with $f(x_0, y_0) = 0$. Motivated by what we did to find the rational points on the unit circle we let

$$x = x_0 + t, \qquad \text{and} \qquad y = y_0 + tm$$

[1] It is enough to assume the coefficients are rational numbers. For by multiplying the equation $f(x, y) = 0$ by the least common denominator of the coefficients we get an equation defining C with integer coefficients.

and substitute this into $f(x,y) = 0$ and group by powers of t and use $f(x_0, y_0) = 0$

$$\begin{aligned}
f(x,y) &= c_{20}(x_0+t)^2 + c_{11}(x_0+t)(y_0+mt) + c_{02}(y_0+mt)^2 \\
&\qquad + c_{10}(x_0+t) + c_{01}(y_0+mt) + c_{00} \\
&= (c_{02}m^2 + c_{11}m + c_{20})t^2 \\
&\qquad + (2c_{20}x_0 + c_{11}(mx_0+y_0) + 2c_{02}my_0 + c_{10} + c_{01}m)t \\
&\qquad\qquad + f(x_0,y_0) \\
&= t\big[(c_{02}m^2 + c_{11}m + c_{20})t \\
&\qquad + 2c_{20}x_0 + c_{11}(mx_0+y_0) + 2c_{02}my_0 + c_{10} + c_{01}m\big] \\
&= 0
\end{aligned}$$

Solving for t gives $t = 0$ (corresponding to the points (x_0, y_0)) and

$$t = \frac{-\left[2c_{20}x_0 + c_{11}(mx_0+y_0) + 2c_{02}my_0 + c_{10} + c_{01}m\right]}{c_{02}m^2 + c_{11}m + c_{20}}$$

which is rational whenever m is rational. Using this value of t back in our formulas $x = x_0 + t$ and $y = y_0 + mt$ gives (after some unpleasant algebra)

$$\begin{aligned}
x = x(m) &= \frac{c_{02}x_0m^2 - (2c_{02}y_0 + c_{01})m - (c_{20}x_0 + c_{11}y_0 + c_{10})}{c_{02}m^2 + c_{11}m + c_{20}} \\
y = y(m) &= \frac{-(c_{11}x_0 + c_{02}y_0 + c_{01})m^2 - (2c_{20}x_0 + c_{10})m + c_{20}y_0}{c_{02}m^2 + c_{11}m + c_{20}}
\end{aligned}$$

2. Some problems related to Pythagorean truples

Problem 3. If a, b, and c are positive integers with $a^2 + b^2 = c^2$ show that $\gcd(a,b,c) = 1$ if and only if $\gcd(a,b) = 1$. □

Definition 4. A ***fundamental Pythagorean triple*** is triple with of positive integers a, b, c with $a^2 + b^2 = c^2$ and $\gcd(a,b,c) = 1$. □

Problem 4. Let a, b, and c be a Pythagorean triple. Show that there is a primitive Pythagorean α, β, and γ and a positive integer k such that $a = k\alpha$, $b = k\beta$, and $c = k\gamma$. *Hint:* $k = \gcd(a,b,c)$.

Problem 5. If a, b, and c are a fundamental Pythagorean triple then show that exactly two of a, b, and c are odd and that c is always odd. □

We have seen that for positive integers p and q with $q < p$ that

$$\begin{aligned}
a &= 2pq \\
b &= p^2 - q^2 \\
c &= p^2 + q^2
\end{aligned}$$

is a Pythagorean triple.

Problem 6. With this notation show that a, b, and c is a fundamental Pythagorean triple if and only if $\gcd(p,q) = 1$. □

Problem 7. Put the last several problems together to give a method to

(a) Make a list of all fundamental Pythagorean triples.
(b) Make a list of all Pythagorean triples. $\square$

In looking in books for problems I came across the following two problems that I had not seem before and which look like fun.

Problem 8. Show that in any Pythagorean triple a, b, and c that at least one of the numbers a, b, or c is divisible by 5. $\square$

Problem 9. Find all fundamental Pythagorean triangles where the area is twice the the perimeter. $\square$