SOLUTIONS
Math 345
Homework 2
9/13/2017

Exercise 6. Recall, we get every Pythagorean triple (a, b, c) with b even from the formula

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$$

by substituting in different integers for u and v. For example, $(u, v) = (2, 1)$ gives the smallest triple $(3, 4, 5)$.

(a) If u and v have a common factor, explain why (a, b, c) will not be a primitive Pythagorean triple.

Answer. If $u = dn$ and $v = dm$,

$$\begin{aligned} a &= u^2 - v^2 = (dn)^2 - (dm)^2 = d^2(n^2 - m^2); \\ b &= 2uv = 2(dn)(dm) = d^2(2nm); \\ c &= u^2 + v^2 = (dn)^2 + (dm)^2 = d^2(n^2 + m^2). \end{aligned}$$

So a, b, and b are all be divisible by d^2, so the triple will not be primitive. □

(b) Find an example of integers $u > v > 0$ that do not have a common factor, yet the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is not primitive.

Answer. Take $(u, v) = (3, 1)$, so that $(a, b, c) = (8, 6, 10)$, which is not primitive. □

(c) Make a table of the Pythagorean triples that arise when you substitute in all values of u and v with $1 \leq v < u \leq 10$.

Answer.

u	v	a	b	c
2	1	3	4	5
3	1	8	6	10
3	2	5	12	13
4	1	15	8	17
4	2	12	16	20
4	3	7	24	25
5	1	24	10	26
5	2	21	20	29
5	3	16	30	34
5	4	9	40	41
6	1	35	12	37
6	2	32	24	40
6	3	27	36	45
6	4	20	48	52
6	5	11	60	61
7	1	48	14	50
7	2	45	28	53
7	3	40	42	58
7	4	33	56	65
7	5	24	70	74
7	6	13	84	85

u	v	a	b	c
8	1	63	16	65
8	2	60	32	68
8	3	55	48	73
8	4	48	64	80
8	5	39	80	89
8	6	28	96	100
8	7	15	112	113
9	1	80	18	82
9	2	77	36	85
9	3	72	54	90
9	4	65	72	97
9	5	56	90	106
9	6	45	108	117
9	7	32	126	130
9	8	17	144	145
10	1	99	20	101
10	2	96	40	104
10	3	91	60	109
10	4	84	80	116
10	5	75	100	125
10	6	64	120	136
10	7	51	140	149
10	8	36	160	164
10	9	19	180	181

□

(d) Using your table from (c), find some simple conditions on u and v that ensure that the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is primitive.

Answer. It looks like (a, b, c) will be primitive if and only if $u > v$ and u and v have no common factor and one of u or v is even. □

(e) Prove that your conditions in (d) really work.

Answer. If both u and v are both odd or both even, then all three of a, b, and c are even (and therefore divisible by 2), so the triple is not primitive. And we already saw that if u and v have a common factor, then the triple is not primitive. And if we're only looking for positive values of a, then we must have $u > v$. This proves one direction.

To prove the other direction, suppose that the triple is not primitive, so there is a number $d \geq 2$ that divides all three terms. Then d divides

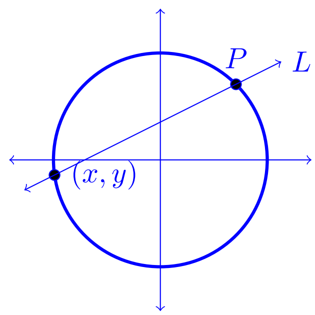
$$(u^2 - v^2) + (u^2 + v^2) = 2u^2 \quad \text{and} \quad (u^2 - v^2) - (u^2 + v^2) = 2v^2,$$

so either $d = 2$ or else d divides both u and v. In the latter case we are done, since u and v have a common factor. On the other hand, if $d = 2$ and u and v have no common factor, then at least one of them is odd. So the fact that 2 divides $u^2 - v^2$ tells us that they are both odd. □

Exercise 7. Rational points on other curves.

(a) Use the lines through the point $(1, 1)$ to describe all the points on the circle $x^2 + y^2 = 2$ whose coordinates are rational numbers. Be sure to draw pictures.

Answer. Take the line L with slope m through $P = (1, 1)$, where m is a rational number:



$L : y = m(x - 1) + 1$

Then let (x, y) be the other point where L intersects the circle. Solving for x we have

$$2 = x^2 + y^2 = x^2 + (m(x-1)+1)^2 = x^2 + m^2(x^2 - 2x + 1) + 2m(x-1) + 1,$$

so that

$$0 = (1 + m^2)x^2 + (-2m(m-1))x + (m^2 - 2m - 1).$$

Then, letting $A = 1 + m^2$, $B = -2m(m-1)$, and $C = m^2 - 2m - 1$, we have

$$\begin{aligned} B^2 - 4AC &= (-2m(m-1))^2 - 4(1+m^2)(m^2 - 2m - 1) \\ &= 4m^2(m^2 - 2m + 1) - 4(m^2 - 2m - 1) - 4m^2(m^2 - 2m - 1) \\ &= 4m^2 + 8m + 4 \\ &= 4(m+1)^2. \end{aligned}$$

So

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A} = \frac{2m(m-1) \pm 2(m+1)}{2(1+m^2)} = 1 \text{ or } \frac{m^2 - 2m - 1}{1 + m^2}.$$

The solution $x = 1$ is the expected point P; the other gives

$$y = m\left(\frac{m^2 - 2m - 1}{1 + m^2} - 1\right) + 1 = \frac{-m^2 - 2m + 1}{1 + m^2}.$$

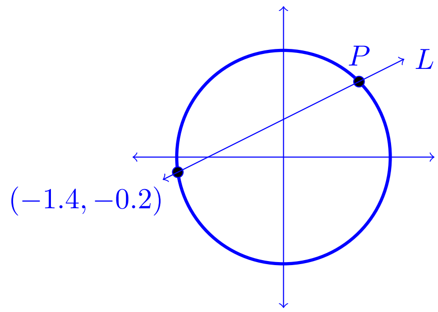
So since m is a rational number, so are x and y.

□

(b) Provide 2 illustrative examples of the results you acquired in part (a).

Answer. For example, if $m = 1/2$, then

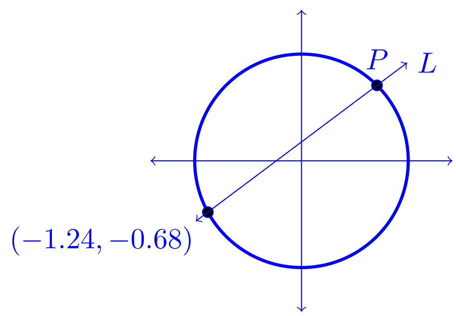
$$x = \frac{(1/2)^2 - 2(1/2) - 1}{1 + (1/2)^2} = -1.4 \quad \text{and} \quad y = \frac{-(1/2)^2 - 2(1/2) + 1}{1 + (1/2)^2} = -0.2:$$



$$L: y = \frac{1}{2}(x-1)+1$$

And if $m = 3/4$, then

$$x = \frac{(3/4)^2 - 2(3/4) - 1}{1 + (3/4)^2} = -1.24 \quad \text{and} \quad y = \frac{-(3/4)^2 - 2(3/4) + 1}{1 + (3/4)^2} = -0.68 :$$



$$L: y = \frac{3}{4}(x-1)+1$$

□

(c) What goes wrong if you try to apply the same procedure to find all the points on the circle $x^2 + y^2 = 3$ with rational coordinates?

Answer. There are no rational points on $x^2 + y^2 = 3$
Proof: Suppose $x = a/b$, $y = c/d$ with $a, b, c, d \in \mathbb{Z}$ with no common divisors between a and b or c and d. Then

$$3 = \frac{a^2}{b^2} + \frac{c^2}{d^2} = \frac{(ad)^2 + (bc)^2}{(bd)^2}.$$

So $(ad)^2 + (bc)^2$ is a multiple of 3. But we saw on HW 1 that this means that both ad and bc are multiples of 3. Since $x = a/b$ and $y = c/d$ were in lowest terms, that means that either a and c are multiples of 3 but not b or d, or vice versa. Either way, 3 will divide $(ad)^2 + (bc)^2$ exactly as many times as c^2d^2 will, which is a contradiction.

□