1. Fill out the (short) course survey here. You do not need to submit anything about this with the assignment.

   `http://goo.gl/forms/0MnAuJx4gl`

2. *Fermat's Last Theorem* states that for any natural number $n \geq 3$, the equation $a^n + b^n = c^n$ has no solutions for natural numbers a, b, c. Prove that if Fermat's last theorem is true for the special case $n = 4$, and also whenever n is equal to an odd prime number, then Fermat's last theorem is true for all $n \geq 3$.

3. (a) Follow the method of chapter 3 to describe all the *rational* solutions to the equation $x^2 + y^2 = 2$. Note that you will need to choose a different "center of projection" than was used for the equation $x^2 + y^2 = 1$.

   (b) Using your answer to part (a), find an *integer* solution to the equation $a^2 + b^2 = 2c^2$, such that $a \neq b$.

Note. For the following two problems, please compute the answer *by hand*, showing all of your steps.

4. Using the Euclidean algorithm, compute each of the following.

   (a) $\gcd(180, 364)$ (b) $\gcd(1001, 1456)$

5. Use the Euclidean algorithm to find an *integer* solution to the following equation

$$181x + 293y = 1$$

6. (a) Suppose that you have a large supply of 5 dollar coins and a large supply of 6 dollar coins. What is the largest number of dollars that you can *not* make out of some combination of these coins? You do not need to prove your answer, but briefly describe how you have decided upon it.

   (b) Suppose instead that you have 5 dollar and 7 dollar coins. What is the largest amount that you cannot make?

   (c) Suppose instead that you have 5 dollar coins and 8 dollar coins. What is the largest amount that you cannot make?

   (d) Conjecture a formula for the largest amount that you cannot make out of 5 dollar coins and k dollar coins, where k is any integer greater than 1 that is not divisible by 5. You do not need to prove that your formula is correct (but you are encouraged to attempt to do so!).

P. Set 2 Solutions

Math 42
Spring 2015

(1) //Online survey: nothing to submit.

(2) Let $n \geq 3$ be any integer. Consider two cases separately:

A – n is divisible by an odd prime

B – n is not divisible by any odd primes.

In case A, write $n = p \cdot m$, where p is an odd prime and $m \in \mathbb{N}$. Then the equation $a^n + b^n = c^n$ can be rewritten

$$(a^m)^p + (b^m)^p = (c^m)^p.$$

We have assumed, since p is an odd prime, that there are no $x, y, z \in \mathbb{N}$ such that $x^p + y^p = z^p$. Since any solution to $a^n + b^n = c^n$ would give such a solution, namely $x = a^m$, $y = b^m$, $z = c^m$, it follows that $a^n + b^n = c^n$ can have no solutions in $\mathbb{N}$, as desired.

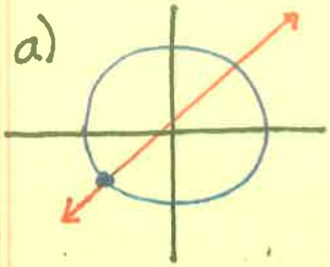
Now, consider case B. Since n has no odd prime factors, its only prime factor can be 2. So $n = 2^e$ for some $e \in \mathbb{N}$. Since $n \geq 3$, e must be at least 2. Therefore 4 divides n, since $n = 4 \cdot 2^{e-2}$ and $e \geq 2$ (so 2^{e-2} is an integer). So $a^n + b^n = c^n$ can be rewritten

$$(a^{2^{e-2}})^4 + (b^{2^{e-2}})^4 = (c^{2^{e-2}})^4$$

Now, since we are assuming that $x^4 + y^4 = z^4$ has no solutions in $\mathbb{N}$, it follows that $a^n + b^n = c^n$ has no solutions in $\mathbb{N}$.

Therefore in both cases A and B, $a^n + b^n = c^n$ has no solutions in $\mathbb{N}$.

③ a)



Let $C=(-1,-1)$ be the "center of projection." (any point (x,y) w/ $x^2+y^2=2$ and $x,y\in\mathbb{Q}$ will work). Let L_m be the line of slope m through C.

L_m has equation $(y+1)=m(x+1)$, or $y=mx+(m-1)$. We can find where L_m meets the circle $x^2+y^2=2$ as follows:

$$y = mx+(m-1)$$
$$x^2+y^2=2$$
$$\Rightarrow x^2+\left[mx+(m-1)\right]^2=2$$
$$x^2+m^2x^2+2m(m-1)x+(m-1)^2=2$$

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

since we know for sure that $x=-1$ is one solution, we can factor:

$$(x+1)\left[(m^2+1)x+(m^2-2m-1)\right]$$

$$\Rightarrow x=-1 \quad \text{or} \quad x=\frac{1+2m-m^2}{1+m^2}$$

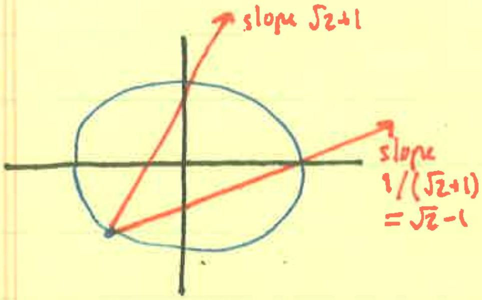
Taking the second solution only, we get

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

So we obtain this description: $\boxed{(x,y)=\left(\frac{1+2m-m^2}{1+m^2},\ \frac{-1+2m+m^2}{1+m^2}\right)}$ for m any <u>rational</u> number. This gives rational pts whenever m is rational. Conversely, if (x,y) is a rational point, then the slope $m=\frac{y+1}{x+1}$ will be rational. so this recipe is guaranteed to produce <u>all</u> rational points.

Comment: Technically, this recipe misses one point: $(-1,1)$. Here, the line from C is vertical, so the slope isn't defined. However, note that if you "plug in ∞" (take a limit as $m \to \infty$) you get this "missing point."

b) Any rational slope m between $\sqrt{2}-1$ and $\sqrt{2}+1$ (not inclusive, since these aren't rational!) will give a positive pair (x,y); as long as $m \neq 1$ & we will have $x \neq y$. Any such x,y will give a,b,c by clearing denominators. For example:



- $m = 1/2$ gives $(x,y) = \left(\dfrac{1+1-1/4}{1+1/4}, \dfrac{-1+1+1/4}{1+1/4}\right) = \left(\dfrac{7}{5}, \dfrac{1}{5}\right)$

  and $\left(\frac{7}{5}\right)^2 + \left(\frac{1}{5}\right)^2 = 2 \Rightarrow \underline{7^2 + 1^2 = 2 \cdot 5^2}$

- $m = 2/3$ gives $(x,y) = \left(\dfrac{1+4/3-4/9}{1+4/9}, \dfrac{-1+4/3+4/9}{1+4/9}\right) = \left(\dfrac{17}{13}, \dfrac{7}{13}\right)$

  and $\left(\frac{17}{13}\right)^2 + \left(\frac{7}{13}\right)^2 = 2 \Rightarrow \underline{17^2 + 7^2 = 2 \cdot 13^2}$

And many other solutions are possible.

4 a) $\gcd(180, 364)$

$= \gcd(180, 4)$ since $4 = 364 - 2 \cdot 180$

$= \gcd(0, 4)$ since $0 = 180 - 4 \cdot 45$.

$= \boxed{4}$.

b) gcd(1001, 1456)

$= \gcd(1001, 455)$ · since $456 = 1456 - 1001$

$= \gcd(91, 455)$ since $91 = 1001 - 2\cdot 455$

$= \gcd(91, 0)$ since $0 = 455 - 5\cdot 91$

$= \boxed{91}$.

(5) Using the "coins & virtual coins" notation I used in class:

$293 \quad 181$

$181 \quad \boxed{112} = 293 - 181$

$\boxed{112} \quad \boxed{69} = \boxed{181} - \boxed{112} = 181 - (293 - 181)$

$= 2\cdot 181 - 293$

$\boxed{69} \quad \boxed{43} = \boxed{112} - \boxed{69} = (293 - 181) - (2\cdot 181 - 293)$

$= 2\cdot 293 - 3\cdot 181$

$\boxed{43} \quad \boxed{26} = \boxed{69} - \boxed{43} = (2\cdot 181 - 293) - (2\cdot 293 - 3\cdot 181)$

$= -3\cdot 293 + 5\cdot 181$

$\boxed{26} \quad \boxed{17} = \boxed{43} - \boxed{26} = (2\cdot 293 - 3\cdot 181) - (-3\cdot 293 + 5\cdot 181)$

$= 5\cdot 293 - 8\cdot 181$

$\boxed{17} \quad \boxed{9} = \boxed{26} - \boxed{17} = (-3\cdot 293 + 5\cdot 181) - (5\cdot 293 - 8\cdot 181)$

$= -8\cdot 293 + 13\cdot 181$

$\boxed{17}$ $\boxed{9}$

$\boxed{9}$ $\boxed{8} = \boxed{17} - \boxed{9} = (5\cdot 293 - 8\cdot 181) - (-8\cdot 293 + 13\cdot 181)$

$= 13\cdot 293 - 21\cdot 181$

$\boxed{8}$ $\boxed{1} = \boxed{9} - \boxed{8} = (-8\cdot 293 + 13\cdot 181) - (13\cdot 293 - 21\cdot 181)$

$= -21\cdot 293 + 34\cdot 181$

$\boxed{1}$ $\boxed{0} = \boxed{8} - 8\boxed{1}$.

So one solution is $\boxed{\begin{array}{l} x = 34 \quad y = -21 \\ 34\cdot 181 - 21\cdot 293 = 1 \end{array}}$

Comment: all other solutions have the form $x = 34 + 293k$, $y = -21 - 181k$.

6 a) Here is a table of some values you can obtain:

0	5	10	15	20	25	...
6	11	16	21	26	31	...
12	17	22	27	32	37	...
18	23	28	33	38	43	...
24	29	34	39	44	49	...
⋮	⋮	⋮	⋮	⋮	⋮	

NOTE One useful fact: once you've found 5 numbers in a row (e.g. 20, 21, 22, 23, 24), you can be sure that all subsequent numbers are present (by adding 5 repeatedly).

Everything above 20 is present. Indeed either

- going one down & one left, or
- going four up & five right

will add one to a number. One of these two moves is always possible beyond the number 20. The last missing number is $\boxed{19}$.

b) Similarly:

0	5	10	15	20	25	...
7	12	17	22	27	32	...
14	19	24	29	34	39	...
21	26	31	36	41	46	...
28	33	38	43	48	53	...
35	40	45	50	55	60	...
⋮	⋮	⋮	⋮	⋮	⋮	

Everything 24 & higher can be reached by, at each step, either:

- moving two up & three right, or
- moving three down & four left.

So from any place that is either below the second row or to the right of the fourth column, some "motion" can be used to add 1.

The largest missing number is $\boxed{23}$.

c)

0	5	10	15	20	25	30	..
8	13	18	23	28	33	38	..
16	21	26	31	36	41	46	..
24	29	34	39	44	49	54	..
32	37	42	47	52	57	62	..
40	45	50	55	60	65	70	..
⋮	⋮	⋮	⋮	⋮	⋮	⋮	

5 numbers in a row are here, starting at 28.

Using similar methods, you may find that all numbers beyond 28 are present, but $\boxed{27}$ is missing.

d) Parts (a)-(c) suggest the following pattern:

largest missing number (using 5 and k)

$$= \boxed{4k-5}.$$

This conjecture turns out to be true. We will give a proof later in the course.