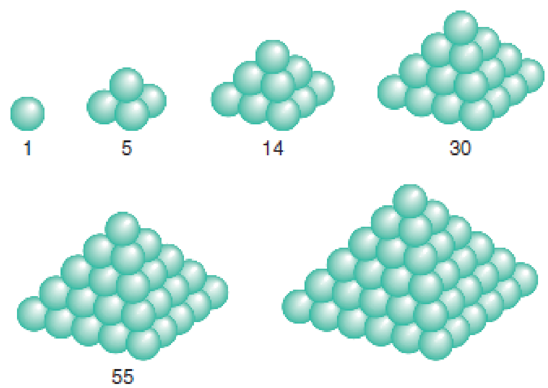
CCS Discrete Math I	Professor: Padraic Bartlett

Homework 18: More Elliptic Curves

Due Friday at 11:30am, Finals Week	*UCSB 2014*

Solve **three** of the following **six** problems. Also, this set is **extra-credit!** This set can be submitted by email if you can't turn it in to my office. Have fun!

1. Consider the following problem: you have a large collection of tangerines. You, being really bored, want to stack them in a pyramid! Specifically, suppose you are stacking them in a square pyramid: that is, your first layer has one tangerine, your second layer has four tangerines, your third layer has nine tangerines, and so on/so forth.



If you have a square number of tangerines that is strictly greater than 1, is it possible that you can stack all of them in a single pyramid? Or is this impossible for any square? (That is; you cannot stack 9 tangerines in such a pyramid, because our pyramid sizes go 1,5,14,30... Our question is the following: is there some n such that n^2 is a "pyramidal" number?)

2. In class, we said that a curve like $y^2 = x^3$ is not an elliptic curve, because its derivative at $(0, 0)$ was undefined.

   A thing you might hope would work: what happens if you just delete the point $(0, 0)$? To make this a concrete problem, take the collection of all points (x, y) with $y^2 = x^3$ and $(x, y) \neq (0, 0)$ in $\mathbb{Z}/7\mathbb{Z}$.

   (a) Plot all of the points that are on this curve and not equal to (0,0).

   (b) Add in the point at infinity, and try to make a group table. Do you get a group, and/or is our operation + well-defined on these points? Or when you go to add points together, do you sometimes get (0,0)?

3. Consider the elliptic curve $y^2 = x^3 + 7$. Prove that it has no integer solutions. (Hint: look at things mod 4 or 8!)

4. Like the above: consider the elliptic curve $y^2 = x^3 - 6$. Prove that it has no integer solutions.

5. Show that the only integral point on the elliptic curve $y^2 = x^3 - 1$ is $(1, 0)$. (Hint: work in $\mathbb{Z}[i]$, and write $x^3 = y^2 + 1 = (y - i)(y + i)$. Show that $y + i, y - i$ are relatively prime, and work from there!)

6. In class, we saw that sometimes an elliptic curve over a finite field could have no points other than $\mathcal{O}$! For example, consider $y^2 = x^3 + 2x + 2$ over $\mathbb{Z}/3\mathbb{Z}$. We know that the only squares are $0^2 = 0, 1^2 = 1, 2^2 \equiv 1 \mod 3$. Therefore,

   - at $x = 0$ the equation $0^3 + 2 \cdot 0 + 2 = 2 = y^2$ has no solutions,
   - at $x = 1$ the equation $1^3 + 2 \cdot 1 + 2 = 5 \equiv 2 = y^2$ has no solutions, and
   - at $x = 2$ the equation $2^3 + 2 \cdot 2 + 2 = 14 \equiv 2 = y^2$ has no solutions.

   So our curve has no points other than $\mathcal{O}$!

   Find the largest value of p for which this can happen.