

Math 392: Homework 5 (due F February 22)

Part I: reading. Read section 9.3. In this section you'll find the proof due to Gauss that there are no integer solutions to the equation $x^3 + y^3 = z^3$. This is the $n = 3$ case of "Fermat's last theorem". I thought about trying to go over this $n = 3$ proof in class but decided it was too long and technical, so don't expect to find it easy to follow in the book either! But see how all the things like EDs, PIDs and UFDs are being used in the proof in essential ways.

Part II: problems. I've decided to set a different sort of homework. What I'd like from you is a complete, comprehensive, and beautifully written solution to the following problems.

1. Describe how to calculate all integer solutions to the Diophantine equation $2x^2 - y^2 = 1$ and prove that you have them all.
2. Describe how to calculate all integer solutions to the Diophantine equation $x^2 + y^2 = z^2$ (better known as "Pythagorean triples") and prove that you have them all.

I would expect that if done properly each answer would take at least one full page of nicely written text!

HINTS FOR PROBLEM 1

I'm going to explain how to calculate all integer solutions to the equation $x^2 - 2y^2 = 1$... The answer to problem 1 should be very similar but not quite the same. Remember I still want you to write out all the details, even if you are just copying, because I really want you to own every line!

The answer: Start from $(x, y) = (1, 0)$ and then iterate the transformation $(x, y) \mapsto (3x + 4y, 2x + 3y)$. You get a sequence

$$(1, 0) \mapsto (3, 2) \mapsto (17, 12) \mapsto \dots$$

which gives *every* solution (x, y) to the equation $x^2 - 2y^2 = 1$ with $x, y \geq 0$.

The proof: There are actually several ways to prove this. The one I started to show you in class uses the ring $\mathbb{Z}[\sqrt{2}]$ and the following lemma:

Lemma. Let R be a subring of \mathbb{R} . Suppose there is a unit $u \in R^\times$ with $u > 1$ such that there is no other unit in R between 1 and u . Then

$$R^\times = \{\pm u^n \mid n \in \mathbb{Z}\}.$$

Proof. Let v be a unit in R . We want to show $v = \pm u^n$ for some $n \in \mathbb{Z}$. Replacing v by $-v$ if necessary, we may assume $v > 0$. Replacing v by $1/v$ if necessary, we may assume $v \geq 1$. If $v = 1$ we are done already, so suppose $v > 1$. Then actually $v \geq u$. Now let n be the positive integer such that $u^n \leq v < u^{n+1}$. Then $1 \leq vu^{-n} < u$. Since vu^{-n} is a unit we see it must equal 1. Hence $v = u^n$.

Next we show the ring $R = \mathbb{Z}[\sqrt{2}]$ satisfies the hypothesis of this lemma with $u = 1 + \sqrt{2}$. We'll use the fact that $x + y\sqrt{2}$ is a unit in R if and only if $x^2 - 2y^2 = \pm 1$ (you might want to recall why this is true!). Suppose that $x + y\sqrt{2}$ is a unit with

$$(1) \quad 1 < x + y\sqrt{2} < 1 + \sqrt{2}.$$

Inverting gives

$$(1 + \sqrt{2})^{-1} < (x + y\sqrt{2})^{-1} < 1.$$

If $x^2 - 2y^2 = 1$ then $(x + y\sqrt{2})^{-1} = x - y\sqrt{2}$ and this shows that

$$\sqrt{2} - 1 < x - y\sqrt{2} < 1.$$

Multiplying this inequality through by -1 and then adding to the inequality (1) above gives that

$$0 < 2y\sqrt{2} < 2.$$

There's clearly no such integer y . On the other hand, if $x^2 - 2y^2 = -1$ then $(x + y\sqrt{2})^{-1} = y\sqrt{2} - x$ and we get that

$$\sqrt{2} - 1 < y\sqrt{2} - x < 1.$$

From this and the inequality (1) you get

$$0 < 2x < 2$$

which again cannot happen for an integer x .

Therefore we've found all the units in the ring $\mathbb{Z}[\sqrt{2}]$: they are

$$\{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}.$$

Also $x + y\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$ if and only if $x^2 - 2y^2 = \pm 1$. So all you have to do to finish is work out which of the units have $x^2 - 2y^2 = 1$. You find you only want the even powers $\pm(1 + \sqrt{2})^{2n}$. You can forget the signs too as you only want the ones with $x, y \geq 0$.

Conclusion: the solution is all x, y appearing as coefficients of $x + y\sqrt{2} = (1 + \sqrt{2})^{2n} = (3 + 2\sqrt{2})^n$ for $n \geq 0$. Now observe

$$(x + y\sqrt{2})(3 + 2\sqrt{2}) = (3x + 4y) + (2x + 3y)\sqrt{2}$$

which is the recurrence in the answer given at the beginning.

HINTS FOR PROBLEM 2

This is the problem of finding *all* Pythagorean triples (x, y, z) , i.e. right angled triangles with integer sides. The solution to this was known to the Greeks! You probably know some already: $(3, 4, 5)$, $(6, 8, 10)$, $(5, 12, 13)$, \dots . But $(6, 8, 10)$ isn't really a new Pythagorean triple, its similar to the $(3, 4, 5)$ triangle. This is the first reduction:

Step 1: Reduce to the case that $GCD(x, y) = GCD(x, z) = GCD(y, z) = 1$.

Step 2: This means that two of x, y, z have to be odd and the third has to be even. In fact z must be odd. Show this by reducing modulo 4...

Step 3: So now (switching x and y if necessary) we're down to the situation that x and z are odd and y is even. Write

$$\frac{y^2}{4} = \frac{z-x}{2} \frac{z+x}{2}.$$

Suppose p is a prime that divides $\frac{z-x}{2}$. Explain why it doesn't divide $\frac{z+x}{2}$, and vice versa. The left hand side is a perfect square. Hence so is the right hand side. Thinking about the fundamental theorem of arithmetic, deduce that

$$\frac{z+x}{2} = u^2, \frac{z-x}{2} = v^2$$

for some integers u, v not both odd with $1 \leq v < u$ and $GCD(u, v) = 1$.

Step 4: Conclude that

$$(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2)$$

for integers u, v not both odd with $1 \leq v < u$ and $GCD(u, v) = 1$. Show conversely that any such pair of integers gives rise to a Pythagorean triple via this formula.

For example:

$$u = 2, v = 1: (x, y, z) = (3, 4, 5).$$

$$u = 4, v = 1: (x, y, z) = (15, 8, 17).$$

$$u = 3, v = 2: (x, y, z) = (5, 12, 13).$$

$$u = 5, v = 2: (x, y, z) = (21, 20, 29).$$

$$u = 4, v = 3: (x, y, z) = (7, 24, 25).$$

...