

NUMBER THEORY TRACK, LECTURE 1

DAVID SAVITT

1. INTRODUCTION

Suppose I write out the equation $x^2 + y^2 = 1$, and I ask you to find its solutions. Your reply to me should be, “What *kind* of solutions am I looking for?” For example, if I want you to find pairs x, y which are real numbers (which symbolically I would write: $x, y \in \mathbb{R}$) then you know that the collection of solutions is precisely the circle of radius 1 centered at the origin in the plane. On the other hand, if I want you to find pairs x, y which are complex numbers (symbolically: $x, y \in \mathbb{C}$) then it’s a little more complicated: for any x other than ± 1 there are exactly two y ’s which solve the equation, whereas for $x = \pm 1$ there’s only one, $y = 0$. Thus, if you imagine two planes, one above another, which touch at exactly two points, that’s what the complex solutions look like.

So far, there’s a very geometric flavour to what we’ve done. But what if you try to find solutions which are *integers* ($x, y \in \mathbb{Z}$, for Zahlen, the German word for number) or are *rationals* ($x, y \in \mathbb{Q}$, and I don’t remember why \mathbb{Q} is the letter used - maybe for quotient)? Well, the former is quite easy: you can verify in an instant that the only solutions are $(\pm 1, 0)$ and $(0, \pm 1)$. The latter, however, isn’t at all transparent. With a little thought, you’d realize that the familiar equation $3^2 + 4^2 = 5^2$ tells you that $(\pm \frac{3}{5}, \pm \frac{4}{5})$ and $(\pm \frac{4}{5}, \pm \frac{3}{5})$ all work, and it’s pretty clear that you can do the same thing for $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$, and so on. But it’s certainly not obvious how to go about making a complete list of all the solutions! These, now, are problems of number theory, and the techniques of number theory were invented to try to find good ways of handling them.

Let’s change tacks a little bit. We’ve seen that $x^2 + y^2 = 1$ has exactly four solutions with x and y integers. Suppose we move in a perpendicular direction, and ask: given an integer n , how can we tell (without actually trying all the possibilities) if there are any integers solutions to $x^2 + y^2 = n$; that is, whether or not n is equal to a sum of two perfect squares? Well, to begin with, certainly n had better be non-negative. This is not an observation to laugh at (in fact it’s quite important) but it’s nowhere close to solving the problem. With no ideas jumping out at us, a sensible thing to do is to try a few cases – it’s certainly very easy to decide whether a particular small number is the sum of two squares, because there are only a few possibilities to try. To make matters clearer, let’s also stick to *odd* n , because (as it turns out) the pattern is murkier if you include even numbers. Forging ahead, we see that $1 = 1^2 + 0^2$, that 3 doesn’t work, that $5 = 2^2 + 1^2$, that 7 doesn’t work, that $9 = 3^2 + 0^2$, that 11 doesn’t work, that $13 = 3^2 + 2^2$, that 15 doesn’t work, and that $17 = 4^2 + 1^2$. Great! There seems to be a plausible pattern here – that it alternates, so an odd number is a sum of two squares when it’s 1 more than a multiple of 4, and not when it’s 3 more.

We’ve got a conjecture now, so let’s try to prove it. Since the issue is the remainder when n is divided by 4, it’s sensible to look at what you get when x any y are divided by 2. Obviously, x and y couldn’t both be even or both be odd, since then n would be even. One is even and one is odd, then, and without loss of generality let’s suppose that $x = 2x'$ is even and $y = 2y' + 1$ is odd. Expanding the hypothesis $x^2 + y^2 = n$, we find

$$(2x')^2 + (2y' + 1)^2 = 4((x')^2 + (y')^2 + y') + 1 = n.$$

Indeed, as we had hoped, if n odd is going to be the sum of two squares, then n had better be 1 more than a multiple of 4. Without even doing the computation, we now know that 19 and 23 can’t be the sum of two squares. But it looks like it might be harder to prove which things actually can be written as the sum of two squares... and in fact, testing the case $n = 21$, we find that 21 *isn’t* the sum of two squares, so our beautiful pattern has broken down.

Can we see what went wrong at 21? Well, 21 is the product of 3 and by 7, neither of which were the sum of two squares, so maybe that has something to do with it. Let’s start out with a hypothetical x and y so that $x^2 + y^2 = n$, with n divisible by 3 (say $n = 3k$) and see what happens. Dividing x by 3 gives a remainder of $a = 0, 1$, or 2, and

similarly dividing y by 3 gives a remainder of b . Writing $x = 3x' + a$ and $y = 3y' + b$, we get

$$3((x')^2 + 2x'a + (y')^2 + 2y'b) + a^2 + b^2 = 3k,$$

so visibly $a^2 + b^2$ has to be divisible by 3. Yet there are only nine possibilities for the pair a, b , and it's easy to check that $a = b = 0$ is the only one which yields $a^2 + b^2$ divisible by 3. Thus

$$n = x^2 + y^2 = (3x')^2 + (3y')^2 = 9((x')^2 + (y')^2)$$

and so n has to be divisible by 9 as well. So that's what's gone wrong: if n is divisible by 3 and is a sum of two squares, then n must also be divisible by 9. And 21 is divisible by 3 and not by 9. (Exercise: verify also that if n is divisible by 7 and is a sum of two squares, then n must also be divisible by $7^2 = 49$!)

Perhaps by now you're wondering what the point of all this is. Of course, part of the point is that we're finding out interesting things about which integers can be written as the sum of two squares. But a secondary point is that these last couple of arguments have been a little cumbersome, and it'd be fantastic to have a better way of executing these techniques (e.g. studying a problem by studying the possibilities for what the remainders could be, when you divide by various things) which work more smoothly and slickly. Miraculously, it'll turn out that a little bit of notation will save us so much work that it will allow us new insight into number theory problems.

2. DIVISIBILITY

Let's start out with a seemingly innocuous definition:

Definition 1. An integer b is divisible by a nonzero integer a if there exists an integer x so that $b = ax$. In this case, we write $a|b$, whereas if a does not divide b we write $a \nmid b$.

If $a|b$ and $0 < a < b$, we say that a is a proper, or nontrivial, divisor of b , whereas if $a = 1$ or $a = b$, we say that a is a trivial divisor of b . Instead of proving a number of basic properties of divisibility here, we'll prove only one example, relegating a few more to Problem Set 1. (See Problem Set 1, #1.) We'll show:

Proposition 2.1. *If $a|b$ and $b|a$, then $a = \pm b$.*

Proof. Since $a|b$, we can find x so that $b = ax$, and similarly we can find y so that $a = by$. Multiplying these equations together gives $ab = abxy$. Implicit in our hypothesis that $a|b$ is the hypothesis that $a \neq 0$, and similarly $b \neq 0$. So we may divide through by ab and conclude that $xy = 1$. Thus x and y are each ± 1 , and the result follows. \square

Alright. So our definition of divisibility covers the case when one number divides exactly into another, but of course that isn't always the case – there's often a remainder left over. The fundamental result regarding this is:

Theorem 2.2. (The Division Algorithm) *Given integers a, b with $a > 0$, there exist unique integers q and r so that $b = qa + r$ and $0 \leq r < a$. Also, $b|a$ if and only if $r = 0$.*

Proof. To prove the theorem, let's first prove that such q and r exist, and after that we'll show that they're unique. Now, consider the infinite sequence of numbers

$$\dots b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, \dots$$

Since $a > 0$, as the sequence goes off to the right the numbers increase towards $+\infty$, and as the sequence goes off to the left the numbers decrease towards $-\infty$. This means that we can pick out the left-most non-negative term in the sequence, and call this r . So $r \geq 0$, and also $r - a < 0$ since the term to the left of r is negative, so indeed r is in the desired range. Every term in our sequence, and particular r , is of the form $b - qa$, so indeed we've got $b = qa + r$ with r in the right range.

If $b = q'a + r'$ as well, suppose without loss of generality that $r' \leq r$. Then $0 = (q - q')a + (r - r')$, so $a|r - r'$. If $r - r' > 0$, then #1(d) from Problem Set 1 would imply that $r - r' \geq a$, which it most certainly isn't. So $r = r'$, which implies quickly that $q = q'$, and uniqueness follows. \square

3. GREATEST COMMON DIVISORS

Let's do an example of division, say, $b = 4891$ and $a = 1105$. We get

$$4891 = 4 \cdot 1105 + 561.$$

Continuing on, using 1105 and 561 instead, we successively get:

$$1105 = 1 \cdot 561 + 544$$

$$561 = 1 \cdot 544 + 17$$

$$544 = 32 \cdot 17 + 0.$$

Now a remarkable thing happens. Because of the last equation, 17 divides 544; then, because of the next-to-last, it divides 561 as well; and, cascading upwards, we find that 17 must divide both 4891 and 1105. Conversely, if d divides both 4891 and 1105, we could work down this list of equations to conclude that d would have to divide 17 as well. Thus 17 is the the largest number that divides both 4891 and 1105, their so-called greatest common divisor:

Definition 2. The greatest common divisor (GCD) of a and b is the largest positive integer which divides both a and b . We write (a, b) to denote the GCD of a and b , and if $(a, b) = 1$ we say that a and b are relatively prime.

So, I've already demonstrated to you that you can compute the GCD of two numbers by repeated use of the division algorithm. To set it down on paper in the general case, we have

$$\begin{aligned} b &= q_0 a + r_0 \\ a &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned}$$

and then $r_k = (a, b)$. The proof of this is exactly the same as the demonstration in the example above, except for one detail: we have to give an argument as to why this process of successive division eventually terminates. But that's no problem, because by definition $0 \leq r_{i+1} < r_i$, so eventually the sequence of remainders must reach zero.

It should be clear from the above algorithm that if d divides both a and b , then d divides (a, b) as well.

To finish up, we need one more fact about GCDs – seemingly straightforward, this is an absolutely fundamental fact which comes up all over the place. Possibly this is the most important idea in this entire Number Theory course.

Theorem 3.1. *The GCD of a and b is equal to the smallest positive integer which can be written as $ax + by$, for x any y integers.*

I'll give two proofs of this fact. The first, which I'll only sketch, is useful for actually constructing such x and y :

Proof 1. Use the algorithm above to determine the GCD, and then unwind the equations that you get. We know that

$$r_i = r_{i-2} - q_i r_{i-1},$$

while $r_1 = a - q_1 r_0$ and $r_0 = b - q_0$. So starting from $r_k = r_{k-2} - q_k r_{k-1}$, substitute in our equation for r_{k-1} in terms of r_{k-2} and r_{k-3} . Then substitute for r_{k-2} , and so on all the way back up the list of divisions, and when we're done we'll have written r_k in the form $ax + by$, where x and y will be very complicated expressions in terms of the q 's. Letting l denote the smallest positive integer of the form $ax + by$, this tells us that $(a, b) = r_k \geq l$.

On the other hand, (a, b) certainly divides a and it certainly divides b , so it certainly divides $ax + by$ for any x any y . In particular (a, b) divides l , so $(a, b) \leq l$, and combined with the previous inequality we conclude that indeed $(a, b) = l$. \square

The second proof, while non-constructive, is a good argument to know, because it's an argument with more general applications than the first one:

Proof 2. Again let l denote the smallest positive integer of the form $ax + by$, and again observe that $(a, b)|l$. Next, I claim that $l|a$. By the division algorithm, $a = lq + r$ with $0 \leq r < l$. So

$$r = a - lq = a - q(ax + by) = a(1 - qx) - bqy$$

for some x, y . So r is expressible as $a \cdot (\text{something}) + b \cdot (\text{something})$, and since r is nonnegative and smaller than l , it must equal 0 by the definition of l . Similarly $l|b$, so l is a common divisor of a and b . Therefore, l divides (a, b) , and we conclude once more that $l = (a, b)$. \square

Corollary 3.2. *If d is a common divisor of a and b (i.e. $d|a$ and $d|b$) then d divides (a, b) .*

Proof. Write $(a, b) = ax + by$ for integers x and y . Since d divides a , it divides ax ; similarly, d divides by . Hence d divides their sum, which is (a, b) . \square