# MATH 115, SUMMER 2012
# LECTURE 1
# MONDAY, JUNE 18TH

JAMES MCIVOR

## 1. Introduction

Number theory is the study of integers. Mostly we care about positive integers, but it's usually convenient to work with the negative integers too. Some of the main problems of number theory are incredibly old, but have eluded many of the best mathematicians for centuries. Often these problems sound simple enough that they can be explained to a child, yet their solutions involve incredibly advanced techniques drawn from all areas of mathematics. To give you a feeling for the subject, here are some typical questions a number theorist might ask:

1. How many prime numbers are there?
2. Find all positive integer solutions $x, y, z$ to the equation $x^2 + y^2 = z^2$ (Pythagorean triples).
3. Find all positive integer solutions $x, y, z$ to the equation $x^n + y^n = z^n$, where $n$ is greater than 2 (Fermat's Last Theorem).
4. Can every even integer be written as the sum of two primes? (Goldbach Conjecture)
5. Can every positive integer be written as the sum of two squares? (Fermat)
6. Are there infinitely many pairs of primes spaced two units apart? (Twin Prime Conjecture)

The first is easy, the second only slightly less easy. The third is very hard - it took 358 years to solve. The fourth is still unsolved, despite being first asked in 1742. For a little while, you could get a million dollars if you solved it, but I think the offer is no longer available. We'll be able to solve the fifth by early next week. We won't get a million dollars for it, though. The sixth is also still unknown. I'm not sure how much money you'd get if you solved it, but I'd give you an A+ in the class.

## 2. Divisibility and Division Algorithm

As mentioned above, the integers have two primary operations - addition and subtraction. Much of the subtlety in studying number theory concerns the interaction of these two operations. However, in this section we focus on only the multiplicative aspect. In many ways this is a more complicated operation. Under addition, we can obtain every integer by adding and subtracting a bunch of copies of 1. We say that the integer 1 *generates* $\mathbb{Z}$ as an additive group.

By contrast, there is no one number with which we can build up all others by multiplying many copies. Actually, what we need in order to build all the numbers by multiplication are the primes (and -1, to get the negative integers). Even then we cannot get zero. So you see that multiplication in integers is a more complicated matter than addition. To study it, we introduce the notion of divisibility, which is a relationship between two integers.

**Definition 1.** If $a$ and $b$ are two integers, with $a \neq 0$, then $a$ **divides** $b$ if there is another integer $k$ such that $b = ka$. We write this as $a|b$, and also say $a$ **is a factor, or divisor, of** $b$, or $b$ **is divisible by** $a$. If $a$ does not divide $b$, we write $a \not| b$.

**Example 2.1.** 3 and -4 both divide -12, but 5 does not. 0 doesn't divide anything, by our definition, not even zero, even though $0 = k0$ for any $k$. On the other hand, every integer *except zero* divides zero, since we can always take $k = 0$.

**Basic properties of divisibility:**

(1) If $a|b$ then $a|bc$ for any $c$.
(2) "If a divides b and b divides c, then a divides c" - we can express this by saying that the divisibility relation is *transitive.*
(3) If a divides both b and c, then a divides any $\mathbb{Z}$-linear combination of b and c, i.e., $a|bx + cy$ for any integers $x$ and $y$.
(4) If a divides b and b also divides a, then a and b are equal up to plus or minus, i.e, $a = \pm b$.
(5) For *positive* integers a.b, if $a|b$, then $a \leq b$.

As you know from your early years, we may attempt to divide b by a, even when a is not a divisor of b, but then we will get a remainder, which is less than b. The fact that this always works is the next theorem - it's a key tool for the rest of this course.

**Theorem 1** (Division Algorithm)**.** *For any integers a and b, with a positive, there exists a unique* quotient $q$ *and* remainder $r$*, where* $0 \leq r < a$ *such that*

$$b = aq + r.$$

*Moreover, this* $r$ *is zero if and only if* $a|b$.

You already know how to produce q and r - long division. What you may want to prove is that $0 \leq r < a$, and the uniqueness. The idea is that $r$ is the smallest non-negative member of the infinite sequence

$$b + ka,$$

where $k$ runs through all integers. Then $r \geq 0$ by our choice, and it's smaller than $a$ since the numbers are spaced a units apart. Uniqueness is proved by supposing there are two pairs $q_1, r_1$ and $q_2, r_2$ that make the equality true, then using the inequalities of $r_1, r_2$ to conclude that $r_1 = r_2$, and hence $q_1 = q_2$, too. This is a common trick - the inequalities on $r$ are perhaps the most useful part of the theorem.

## 3. Ideals and the gcd

– NOTE: this section contains material not covered in the book –

**Definition 2.** If $a|b$ and $a|c$, then $a$ is a **common divisor** of $b$ and $c$. If $b$ and $c$ are not both zero, the **greatest common divisor (gcd)** of $b$ and $c$ is the largest of these, denoted by $(b, c)$.

The reson for the requirement that $b$ and $c$ not both be zero is that if they're both zero, then every nonzero integer is a divisor of both of them, so there is no greatest.

Here's an alternate point of view on the gcd, not covered in your book, involving the notion of ideals. You may have seen this in an abstract algebra course - it's a very important concept that you will run into in the future anyway, so I'll discuss it here for a moment.

**Definition 3.** An **ideal** in $\mathbb{Z}$ is a nonempty subset $I$ with the following two properties:

(1) If $a, b \in I$, then $a + b \in I$ (closed under addition)
(2) If $a \in \mathbb{Z}$ and $i \in I$, then $ai \in I$ (closed under "scalar multiplication")

The properties are similar to those of a subspace of a vector space. Note that the second condition is stronger than "closure under multiplication" - here we take an element $i$ in our ideal, and we are allowed to multiply it by not just something else in $I$, but *anything* in $\mathbb{Z}$, and the result still lands in $I$. I remember being confused about this when I first saw ideals. Note also that an ideal must always contain zero (just like subspaces) - this gives an easy way to see that some things *aren't* ideals, if they don't contain zero.

**Examples 3.1.** (1) The set of all integers $\mathbb{Z}$ is itself an ideal.
(2) The subset $\{0\}$ is an ideal, which we denote by $(0)$.
(3) Every other ideal contains infinitely many elements. Reason: if $I$ is an ideal and $a$ is a nonzero element in $I$, then we can keep adding $a$ to itself and stay in $I$, by property 1. This gives infinitely many elements.
(4) If $a$ is any integer, then the set $\{ka \,|\, k \in \mathbb{Z}\}$ of multiples of $a$ is an ideal, denoted by $(a)$. Note examples 1 and 2 are just special cases of this, when $a = 1$ or 0, respectively. An ideal of this form is called **principal**, and $a$ is called a **generator** for the ideal.
(5) If $a$ and $b$ are two integers, the set of all $\mathbb{Z}$-linear combinations $\{ax + by \,|\, x, y \in \mathbb{Z}\}$ is an ideal.
(6) There are ideals in other settings, too: the set of all (real, complex, whatever) polynomials $p(x)$ such that $p(1) = 0$ forms an ideal in the set (ring) of all polynomials.

Our main theorem here is that actually *every* ideal in $\mathbb{Z}$ is principal! This is something very special about the integers - it's not always true for ideals in other situations.

**Theorem 2.** *Every ideal in $\mathbb{Z}$ is principal, i.e., for any ideal $I \subseteq \mathbb{Z}$, there is an integer $a$, unique up to $\pm$, such that $I = (a)$.*

*Proof.* Out of all the elements in $I$, pick the smallest positive one[1] and call it $a$. We'll show that $a$ is a "generator", namely $I = (a)$. This means we have to show that everything in $I$ is a multiple of this $a$, or in other words, that $a$ is a divisor of everything in $I$. So pick any $b \in I$. To show $a$ is a divisor, we can just show that the remainder when you divide $b$ by $a$ is 0. Applying the division algorithm to $a$ and $b$ gives some $q$ and $r$ such that

$$b = qa + r, \text{ or } r = b - qa$$

[1] If there is no positive element, then there is no negative element either, so $I = (0)$, which is principal.

with $0 \leq r < a$. But $a$ is in $I$, so $-qa$ is also in $I$, and since $b$ is also in $I$, $b - qa$ is in $I$. Thus by the properties of ideals we've found that the remainder $r$ is in $I$. But then $r$ can't be positive, since it's smaller than $a$, and we chose $a$ to be the smallest positive thing in $I$. So that means that $r$ must be zero, which means $b = qa$, so $a|b$. This shows that every element $b$ in $I$ is a multiple of $a$, so $I = (a)$.

□

Notice that this proof used the inequalities $0 \leq r < a$ - this is the key fact when you're applying the division algorithm!