MAT 302: LECTURE SUMMARY

Recall the following theorem, which we proved last lecture:

Theorem 1. *$H \leq \mathbb{Z}$ if and only if $H = n\mathbb{Z}$ for some $n \in \mathbb{N}$.*

We first deduced the following nonobvious consequence:

Corollary 2. *For any $a, b \in \mathbb{N}\backslash\{0\}$, we have $a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$.*

Here $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \ : \ x, y \in \mathbb{Z}\}$, and (a, b) denotes the greatest common divisor of a and b. For example, $(28, 49) = 7$.

Proof of Corollary. We proceed in stages:

Step 1: $a\mathbb{Z} + b\mathbb{Z} \leq \mathbb{Z}$. (This is an exercise!)

Step 2: $a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$ for some $n \in \mathbb{N}$. (This immediately follows from Theorem 1.)

Step 3: n is a common factor of a and b.

> Observe that $a \in n\mathbb{Z}$, since $a \in a\mathbb{Z} + b\mathbb{Z}$. It follows that $n \mid a$. Similarly, $n \mid b$. (Recall the notation $d \mid N$ means that N is a multiple of d.)

Step 4: $n = (a, b)$

> First, observe that $n \in a\mathbb{Z} + b\mathbb{Z}$, since $n \in n\mathbb{Z}$. It follows that $n = ax + by$ for some integers x and y. Therefore, if d is a common factor of a and b, d must also be a factor of n; in particular, $d \leq n$. Thus, n is the largest common factor of a and b.

□

Calculating $(28, 49)$ was relatively easy, since we know the factorizations of both numbers. But what if we don't know the factorizations, for example, if the numbers are large?

As a first example, we looked at $(198, 199)$. Intuitively, it's clear that these are relatively prime (i.e. have GCD equal to 1); they're too close together to have common factor. We can make this intuition rigorous as follows. Let d be a common factor of 198 and 199, i.e. $d \mid 198$ and $d \mid 199$. Then d must divide $199 - 198$ (why?). But this implies that d must be 1. Note that at no point did we factor 198 or 199.

Date: February 3rd, 2011.

We next applied the same method to $(154, 164)$. Suppose d is a common factor. Then d must divide the difference, i.e. $d \mid 10$. This means d must be 1, 2, 5, or 10. Which of these can it be? It's clear that d could be 1 or 2, and that it cannot be 5 or 10; it follows that $(154, 164) = 2$. Once again, we did not need the factorization of either 154 or 164; instead, we only needed to know the factorization of their difference.

But what if the difference between the two numbers isn't so small? For example, what's $(203, 416)$? Suppose d is a common factor of 203 and 416. Then d must divide their difference, 213. So now we know that $d \mid 203$, $d \mid 213$, and $d \mid 416$. This implies that $d \mid 213 - 203 = 10$, so once again d must be 1, 2, 5, or 10. This time, 1 is the only possible common factor of 203 and 416, so we conclude that 203 and 416 are relatively prime.

One final example: $(282, 947)$. As before, suppose d is a common factor. Then $d \mid 947 - 282 = 665$ as well. We deduce that $d \mid 665 - 282 = 383$, and therefore, that $d \mid 383 - 282 = 101$. From all of this, it follows that $d \mid 282 - 101 = 181$, whence $d \mid 181 - 101 = 80$. Now, 80 is pretty easy to factor, but it has a *lot* of factors, so it's annoying to check. So rather than stopping here, we make one more iteration: since $d \mid 101$ and $d \mid 80$, we must have $d \mid 101 - 80 = 21$. This leaves few possibilities for d: it must be 1, 3, 7, or 21. It is easy to check that 947 isn't divisible by 3, and that 282 isn't divisible by 7; it follows that d can only be 1, so $(282, 947) = 1$. Note that in this example, we first subtracted 282 three times from 947; of course, if $d \mid 947$ and $d \mid 282$, then $d \mid 947 - 3 \times 282$, so we could have subtracted all three 282's right away. Similarly, we subtracted 101 twice from 282; we could have saved some time by subtracting 2×101. The idea is: at each stage, take the two smallest numbers of the ones you've deduced to be multiples of d, and subtract the smaller from the larger *as many times as possible*. For example, we couldn't subtract 282 a fourth time from 947, since that would lead to a negative result. This type of approach in which we repeat a process as many times as possible, it called a *greedy algorithm*.

In each of these examples, we saw that one can determine the GCD of two large numbers by first reducing the problem to factoring a very small number, and then checking directly whether the two original (large) numbers are divisible by the factors of the small one. The moral is this: it's very hard to factor large numbers, but given any large number N and a potential factor d, it's easy to *check* whether or not $d \mid N$. This idea will play a crucial role in our future discussions.

In class, I referred to this process as the Euclidean algorithm. However, we never really decided when to stop – we simply stopped when the output was small enough that we could easily factor it. It is traditional to include in the Euclidean algorithm an instruction on when to stop: start with the original inputs a and b (say $a > b$), subtract b as many times as possible from a to get c, subtract c as many times as possible from b to get d, etc. At each stage of this procedure the output is smaller than all the previous outputs, so eventually you will reach 0. It turns out that the final positive output of this algorithm is (a, b). The key to proving this is the following observation:

Lemma 3. *Suppose x and y are positive integers, and $x > y$. Then $(x, y) = (x, x - y)$.*

Thus in our description of the algorithm above, we have $(a, b) = (b, c) = (c, d) = \cdots$ This guarantees that the last positive output of the algorithm will be (a, b). (Why?)

Proof of Lemma. As usual, we do this in two steps.

Step 1: $(x, y) \leq (x, x - y)$

> Suppose d is a common factor of x and y. Then $d \mid x - y$, so that d is a common factor of x and $x - y$. In particular, $d \leq (x, x - y)$. Since this is true for any common divisor of x and y, we conclude that $(x, y) \leq (x, x - y)$.

Step 2: $(x, x - y) \leq (x, y)$

> Suppose d is a common factor of x and $x - y$. Then $d \mid x - (x - y)$, whence d is a common factor of x and y. Thus, $d \leq (x, y)$. It follows that $(x, x - y) \leq (x, y)$.

□

We finished the lecture with a discussion of two fundamental examples of groups: the integers modulo n under addition, and under multiplication.

Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$.[*] We make $\mathbb{Z}_n$ into a group by endowing it with binary operation $\oplus$: $a \oplus b = a + b \pmod{n}$, where $+$ is standard addition on $\mathbb{Z}$. Equivalently, one can define the operation by

$$a \oplus b = \begin{cases} a + b & \text{if } a + b < n \\ a + b - n & \text{otherwise.} \end{cases}$$

We must verify that $\mathbb{Z}_n$ is a group under this operation. Closure and identity are straightforward. Inverses are also pretty easy: the inverse of $a \in \mathbb{Z}_n$ is $n - a$. (Note that $-a$ is not the inverse of a, since $-a \notin \mathbb{Z}_n$.) This leaves only associativity, which (unlike our previous examples) is *not* automatic, since $\oplus$ is quite a different operation from ordinary addition. To prove this, one must show that $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ for any $a, b, c \in \mathbb{Z}_n$. Can you do this?

We next turned to multiplication $\pmod{n}$. A natural first attempt is to take $\mathbb{Z}_n$ and endow it with $\otimes$, defined $a \otimes b = ab \pmod{n}$. This would certainly be closed, can be shown to be associative, and has identity element 1. Trouble is, $\mathbb{Z}_n$ contains elements which are not invertible with respect to $\otimes$, for example, the element 0. We fix this by simply removing all the non-invertible elements! Namely, let $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \ : \ a \text{ is invertible under } \otimes\}$. Clearly, every element of $\mathbb{Z}_n^\times$ is invertible – but are the other group axioms satisfied? Let's check:

- Closure: Suppose $a, b \in \mathbb{Z}_n^\times$. Then a has an inverse $a^{-1} \in \mathbb{Z}_n^\times$ and b has inverse $b^{-1} \in \mathbb{Z}_n^\times$, i.e. $a \otimes a^{-1} = 1 = a^{-1} \otimes a$ and $b \otimes b^{-1} = 1 = b^{-1} \otimes b$. We wish to show that $a \otimes b \in \mathbb{Z}_n^\times$, which is the same as showing it's invertible. In fact, we can explicitly write down the inverse: $b^{-1} \otimes a^{-1}$. This is straightforward to verify, but note the crucial role played by associativity.
- Associativity: Think about this one; we'll discuss it next lecture.
- Identity: The element 1 is the identity.
- Inverses: By definition.

[*] This group is more commonly called $\mathbb{Z}/n\mathbb{Z}$, but we will use $\mathbb{Z}_n$ for notational convenience.

So $\mathbb{Z}_n^\times$ is indeed a group under $\otimes$. The following theorem gives a more concrete way of thinking about the elements of this group.

Theorem 4. $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \ : \ (a, n) = 1\}$

Proof. As usual, we do this in two steps.

Step 1: $\mathbb{Z}_n^\times \subseteq \{a \in \mathbb{Z}_n \ : \ (a, n) = 1\}$

Pick any $a \in \mathbb{Z}_n^\times$, and let $d = (a, n)$. There exists an $a^{-1} \in \mathbb{Z}_n^\times$ such that $a \otimes a^{-1} = 1$, whence $a \times a^{-1} \equiv 1 \pmod n$. In other words, $a \times a^{-1} = 1 + kn$ for some integer k. Since $d \mid a$ and $d \mid n$, we deduce that $d \mid a \times a^{-1} - kn$, which implies that $d = 1$.

Step 2: $\{a \in \mathbb{Z}_n \ : \ (a, n) = 1\} \subseteq \mathbb{Z}_n^\times$

Suppose $a \in \mathbb{Z}_n$ and $(a, n) = 1$. By Corollary 2, we can find integers x and y such that $ax + ny = 1$. It follows that $ax \equiv 1 \pmod n$. We're almost done, but note that x might not belong to $\mathbb{Z}_n$. Accordingly, set $a^{-1} = x \pmod n$. This is easily seen to be the inverse of a; in particular, a is invertible.

□

We finished lecture with the following remarkable result, which we will prove next time:

Theorem 5 (Fermat's Little Theorem). *Let p be a prime. Then for any $a \in \mathbb{Z}_p^\times$, we have $a^{p-1} = 1$.*