LECTURE 13: SUMMARY

Recall that we've been been exploring arithmetic on the set

$$\mathbb{Z}_d := \{0, 1, 2, \ldots, d-1\}.$$

We have notions of addition and multiplication on this set. Subtraction is just addition in disguise, so we have that too. Division, however, poses a problem. Certainly, you can't divide by 0 (for the same reasons as in $\mathbb{Z}$), but sometimes there are other elements you can't divide by, either. To illustrate this, consider the multiplication table for $\mathbb{Z}_8$:

$\times$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

It's clear that no multiple of 4 is ever equal to 3; in other words, $3 \div 4$ has no answer. This might not seem so problematic, since 3 isn't divisible by 4 in $\mathbb{Z}$, either. More troubling is that $4 \div 2$ has two possible answers: 2 and 6. In this lecture, we discuss one approach to resolving this: removing all elements which are noninvertible. This will let us do division, but at a cost, as we shall see.

Last time, we saw that $n\mathbb{Z}_d = \mathbb{Z}_d$ iff n is invertible in $\mathbb{Z}_d$. To avoid writing the word "invertible" over and over, we define

$$\mathbb{Z}_d^\times := \{n \in \mathbb{Z}_d : n \text{ is invertible in } \mathbb{Z}_d\}.$$

From our work last time, we see that

$$\mathbb{Z}_d^\times = \{n \leq d-1 : (n, d) = 1\}.$$

Thus, for example, $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$. To gain some intuition, we explored this simple case by looking at the multiplication table for $\mathbb{Z}_8^\times$:

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Date: February 26th, 2013.

One fact which jumps out is that $\mathbb{Z}_8^\times$ is *closed* under multiplication, i.e. for any $a, b \in \mathbb{Z}_8^\times$, the product $ab \in \mathbb{Z}_8^\times$ as well. We quickly prove this in general:

Proposition 1. *$\mathbb{Z}_d^\times$ is closed under multiplication (i.e. if $a, b \in \mathbb{Z}_d^\times$, then $ab \in \mathbb{Z}_d^\times$).*

Remark. *We know that $\mathbb{Z}_d$ is closed under multiplication, so the product of two invertible elements lives in $\mathbb{Z}_d$. What's not obvious is whether this product is itself invertible! Hence, the proposition.*

Proof. Recall that for $x \in \mathbb{Z}_d$ to be invertible means that it has an inverse in $\mathbb{Z}_d$; in other words, we do *not* require the inverse to be in $\mathbb{Z}_d^\times$.

Suppose $a, b \in \mathbb{Z}_d^\times$; then they have inverses $a^{-1}, b^{-1} \in \mathbb{Z}_d$, respectively. It's easy to verify that $a^{-1}b^{-1}$ is an inverse of ab, thus proving that ab is invertible. □

So, $\mathbb{Z}_d^\times$ has a natural notion of multiplication. The *raison d'être* of $\mathbb{Z}_d^\times$ is that it also has division. For example, going back to the multiplication table for $\mathbb{Z}_8^\times$, we see that $3 \div 5 = 7$ (in other words, $5x = 3$ in $\mathbb{Z}_8^\times$ holds for $x = 7$ and nothing else). To get more intuition, we found $2/5$ in $\mathbb{Z}_9^\times$. There were three strategies people took to do this:

Strategy 1. Write out the multiplication table for $\mathbb{Z}_9^\times$, and search the 5th row for the entry 2. It turns out 2 is in the 4th column of the 5th row; in other words, $4 \times 5 = 2$, or equivalently, $2/5 = 4$.

Strategy 2. Starting with 2, add 9 to it as many times as necessary until we get to an integer multiple of 5. In this case, we have $2 + 9 + 9 = 20$. Thus, $2/5 = 20/5 = 4$.

Strategy 3. Find 5^{-1}; this is easily seen to be 2. It follows that $2/5 = 2 \times 5^{-1} = 4$.

Armed with this intuition, we next proved that division is a well-defined operation in $\mathbb{Z}_d^\times$.

Proposition 2. *Given $a, b \in \mathbb{Z}_d^\times$, there exists a unique $x \in \mathbb{Z}_d^\times$ such that $bx = a$. In other words, $a \div b$ exists, and is uniquely defined.*

Proof. First we prove that inverses are well-defined. More precisely, suppose $b \in \mathbb{Z}_d^\times$. By definition, b has an inverse $b^{-1} \in \mathbb{Z}_d$, and it's easy to see that $b^{-1} \in \mathbb{Z}_d^\times$: the inverse of b^{-1} is b itself. To show that the inverse is well-defined, it remains to show that it's unique. We gave a slick proof of this: if x and y are both inverses of b, then

$$x = xby = y.$$

Thus, for any $b \in \mathbb{Z}_d^\times$, it makes sense to talk about *the* inverse b^{-1}.

So, what is $a \div b$? In other words, is it true that there exists a unique $x \in \mathbb{Z}_d^\times$ such that $bx = a$? It's clear that a solution to this equation exists, namely, $x = ab^{-1}$. Moreover, if $y \in \mathbb{Z}_d^\times$ satisfies $by = a$, then we have $y = b^{-1}by = b^{-1}a$, which proves uniqueness. □

Thus, by passing from $\mathbb{Z}_d$ to $\mathbb{Z}_d^\times$, we have added division to our arithmetic. In the process, however, we have lost something: $\mathbb{Z}_d^\times$ is no longer closed under addition! To sum up, if we work in $\mathbb{Z}_d$, we can add and multiply, but not divide; if we work in $\mathbb{Z}_d^\times$ we can multiply and divide, but not add. As we shall see in the near future, there is a middle ground – a set in which both addition and division work, and which (therefore) has a very rich arithmetic structure. These are called finite fields, and play an important role in many areas of mathematics.

We finished lecture by returning to $\mathbb{Z}_8^\times$ and making another observation about its multiplication table. The 3 row of the table reads $3, 1, 7, 5$; these are simply $3 \times 1, 3 \times 3, 3 \times 5$, and 3×7. We therefore have

$$\begin{aligned} 1 \times 3 \times 5 \times 7 &= 3 \times 1 \times 7 \times 5 \\ &= (3 \times 1) \times (3 \times 3) \times (3 \times 5) \times (3 \times 7) \\ &= 3^4 \times (1 \times 3 \times 5 \times 7) \end{aligned}$$

Dividing both sides by $1 \times 3 \times 5 \times 7$, we deduce that $3^4 = 1$. Of course, this is sort of silly; directly from the multiplication table we see that $3^2 = 1$, so of *course* we must have $3^4 = 1$ in $\mathbb{Z}_8^\times$. But the idea above generalizes quite nicely. Given a set A, denote the number of elements in A by $|A|$.

Theorem 3 (Euler's theorem)**.** *For all $a \in \mathbb{Z}_d^\times$, we have $a^{|\mathbb{Z}_d^\times|} = 1$.*

Proof. We follow the same procedure as for $\mathbb{Z}_8^\times$ above. Pick $a \in \mathbb{Z}_d^\times$, and observe that $a\mathbb{Z}_d^\times = \mathbb{Z}_d^\times$. (Why?) It follows that multiplying all of the elements of $\mathbb{Z}_d^\times$ together gives the same answer as multiplying all the elements of $a\mathbb{Z}_d^\times$ together. Note that if $k \in a\mathbb{Z}_d^\times$, then $k = am$ for some $m \in \mathbb{Z}_d^\times$. We deduce that

$$\begin{aligned} \prod_{n \in \mathbb{Z}_d^\times} n = \prod_{k \in a\mathbb{Z}_d^\times} k &= \prod_{m \in \mathbb{Z}_d^\times} am \\ &= \left(\prod_{m \in \mathbb{Z}_d^\times} a \right) \left(\prod_{m \in \mathbb{Z}_d^\times} m \right) \\ &= a^{|\mathbb{Z}_d^\times|} \left(\prod_{m \in \mathbb{Z}_d^\times} m \right). \end{aligned}$$

Dividing both sides by $\left(\prod_{n \in \mathbb{Z}_d^\times} n \right)$ yields the theorem. □

For convenience, we introduce the following notation:

$$\varphi(d) := |\mathbb{Z}_d^\times|.$$

Thus, Euler's theorem reads: $a^{\varphi(d)} = 1$ for all $a \in \mathbb{Z}_d^\times$. Can we write $\varphi(d)$ in a more explicit way? For example, is there a fast way to calculate $\varphi(1000000)$? It's not immediately clear. However, we did observe one case in which it's easy: if p is prime, then $\varphi(p) = p - 1$. Applying this in Euler's theorem above, we deduce the following result:

Theorem 4 (Fermat's Little Theorem)**.** *Let p be a prime. For all $a \in \mathbb{Z}_p^\times$, we have $a^{p-1} = 1$.*