LECTURE 12: SUMMARY

Today we continued discussing our conjectures from last lecture, but introduced some notation which made the task much easier. First, we defined

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

A fairly easy argument showed that every $a \in \mathbb{Z}$ is congruent to a *unique* element of $\mathbb{Z}_d$ modulo d. We can now do arithmetic on $\mathbb{Z}_d$: given $a, b \in \mathbb{Z}_d$, we can add them to get some other element of $\mathbb{Z}_d$ – namely, the unique element of $\mathbb{Z}_d$ which is congruent to $a + b \pmod{d}$ – and similarly, we can multiply a and b to get an element of $\mathbb{Z}_d$. We will write $a + b$ and ab for this addition and multiplication, but don't be fooled: these are *not* the same operations as in $\mathbb{Z}$. For example, in $\mathbb{Z}_8$ we have $5 + 6 = 3$ and $5 \times 3 = 7$. I will try, as much as possible, to make it clear from the context which universe we're doing arithmetic in: in $\mathbb{Z}$ or in $\mathbb{Z}_d$.

We next re-examined our conjectures from last lecture. To make this discussion easier, we recalled one of the multiplication tables from last time: the 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

(We continued our tradition from last time of not writing down the 0th row and column.) The 'good' rows (the Sudoku-like rows, without repeated entries) are 1, 3, 5, and 7; the 'bad' ones (with repeats) are 2, 4, and 6. Another way to distinguish good rows from bad rows is to look at the set consisting of all the entries appearing in the row. For example, the set of entries appearing in the 3rd row is $\{3, 6, 1, 4, 7, 2, 5\}$, while the set of elements appearing in the 4th row is $\{4, 0\}$. Of course, it's sort of silly to write $\{3, 6, 1, 4, 7, 2, 5\}$ rather than $\{1, 2, 3, 4, 5, 6, 7\}$, since sets don't distinguish the order in which elements are written. But there is one advantage of writing the set in the first form: it reminds us of what the third row actually *is*, namely

$$\{3 \times 1, 3 \times 2, 3 \times 3, \ldots, 3 \times 7\}.$$

Recall that we're missing the 0th column. If we were to write in this missing entry, the 3rd row would read

$$\{3 \times 0, 3 \times 1, 3 \times 2, \ldots, 3 \times 7\}.$$

A natural notation for this set is $3\mathbb{Z}_8$. More generally, define

$$n\mathbb{Z}_d := \{na : a \in \mathbb{Z}_d\},$$

Date: February 14th, 2013.

where the multiplication na is the multiplication of $\mathbb{Z}_d$, not of $\mathbb{Z}$. This allows us to reformulate our first conjecture from last lecture in purely mathematical terms: a 'good' row is simply one in which $n\mathbb{Z}_d = \mathbb{Z}_d$. Thus, our conjecture reads:

Conjecture 1. *$n\mathbb{Z}_d = \mathbb{Z}_d$ if and only if $(n, d) = 1$.*

Before proving this conjecture, we recall our second conjecture from last lecture, which asserted that a row is bad iff one of the entries is a zero. In other words, all the bad rows have 0 as a common entry, and none of the good rows have a 0. Is there another entry which works in reverse? In other words, is there some element of $\mathbb{Z}_d$ which appears in all the good rows, and in none of the bad rows? Some experimentation quickly led us to the following:

Conjecture 2. *$n\mathbb{Z}_d = \mathbb{Z}_d$ if and only if $1 \in n\mathbb{Z}_d$.*

Both of these conjectures will be easy to prove once we introduce a new concept: that of invertibility. We say $n \in \mathbb{Z}_d$ is *invertible* iff there exists $k \in \mathbb{Z}_d$ such that $kn = 1$. (As usual, this is multiplication in $\mathbb{Z}_d$, not in $\mathbb{Z}$.) In this case, k is called the *inverse* of n. In $\mathbb{Z}_8$, for example, from the multiplication table we see that the invertible elements are 1, 3, 5, and 7 (with inverses 1, 3, 5, and 7, respectively); 0, 2, 4, and 6 don't have inverses in $\mathbb{Z}_8$. A bit of thought shows that 0 is not invertible in $\mathbb{Z}_d$ for any $d \geq 2$.

In proving our conjectures, the following lemma will be useful.

Lemma 3. *n is invertible in $\mathbb{Z}_d$ iff $(n, d) = 1$.*

Proof. We know that $(n, d) = 1$ iff $\exists x, y \in \mathbb{Z}$ such that $nx + dy = 1$. But this is the case iff $\exists k \in \mathbb{Z}_d$ such that $nk = 1$ in $\mathbb{Z}_d$. □

We can now prove our conjectures with relative ease.

Proof of Conjecture 1. By the lemma, it suffices to show that $n\mathbb{Z}_d = \mathbb{Z}_d$ iff n is invertible in $\mathbb{Z}_d$.

($\Longrightarrow$) If $n\mathbb{Z}_d = \mathbb{Z}_d$, then $1 \in n\mathbb{Z}_d$, whence n is invertible in $\mathbb{Z}_d$.

($\Longleftarrow$) If n is invertible in $\mathbb{Z}_d$, then there exists $n^{-1} \in \mathbb{Z}_d$ such that $n^{-1}n = 1$. Since $n^{-1}\mathbb{Z}_d \subseteq \mathbb{Z}_d$, we deduce that

$$\mathbb{Z}_d = n\, n^{-1}\mathbb{Z}_d \subseteq n\mathbb{Z}_d.$$

On the other hand, the inclusion $n\mathbb{Z}_d \subseteq \mathbb{Z}_d$ is trivial. We conclude that $n\mathbb{Z}_d = \mathbb{Z}_d$ as claimed. □

Conjecture 2 follows easily from this.