MAT 302: LECTURE SUMMARY

Recall that RSA works only because we don't know how to efficiently solve congruences of the form

$$x^a \equiv b \pmod{N}$$

for x (which in turn is due to our inability to efficiently calculate $\varphi(N)$ for large N). There are plenty of other types of congruences we currently don't know how to efficiently solve, for example those of the form

(*) $$a^x \equiv b \pmod{N}.$$

It turns out that this, too, can be leveraged to make public key ciphers. The most famous of these, which we will discuss next lecture, are the Diffie-Hellman key exchange, and Elgamal.

We started by building up some intuition for congruences of the form (*).

Example (1). *Find all x such that $2^x \equiv 3 \pmod{5}$.*

> *List the powers of 2:* $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8 \equiv 3 \pmod{5}, \ldots$ *We get the following sequence:* $1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, \ldots$ *(Why does it repeat forever?) Therefore,* $x \equiv 3 \pmod{4}$.

Example (2). *Find all x such that $2^x \equiv 3 \pmod{7}$.*

> *As above, we generate a sequence by starting with 1 and multiplying by* $2 \pmod{7}$ *repeatedly:* $1, 2, 4, 1, 2, 4, 1, \ldots$ *Therefore we see that* 2^x *will* never *be* $3 \pmod{7}$.

There's a fundamental difference between the two examples: 2 'generates' all of $\mathbb{Z}_5^\times$, but not all of $\mathbb{Z}_7^\times$. What does generate $\mathbb{Z}_7^\times$?

$$\begin{aligned}
&1 \text{ generates the set } \{1\} \neq \mathbb{Z}_7^\times \\
&2 \text{ generates the set } \{1, 2, 4\} \neq \mathbb{Z}_7^\times \\
&3 \text{ generates the set } \{1, 3, 2, 6, 4\} = \mathbb{Z}_7^\times \\
&4 \text{ generates the set } \{1, 4, 2\} \neq \mathbb{Z}_7^\times \\
&5 \text{ generates the set } \{1, 5, 4, 6, 2, 3\} = \mathbb{Z}_7^\times \\
&6 \text{ generates the set } \{1, 6\} \neq \mathbb{Z}_7^\times
\end{aligned}$$

So 3 and 5 generate $\mathbb{Z}_7^\times$, but nothing else does. Before developing this idea, we gave a formal definition the term *generate*:

Definition. *Given a group G and any $g \in G$. The set generated by g, denoted $\langle g \rangle$, is defined to be*

$$\langle g \rangle = \{g^n\}_{n \in \mathbb{Z}}$$

Date: March 22nd, 2011.

Thus for example in $\mathbb{Z}_5^\times$ we have $\langle 2\rangle = \mathbb{Z}_5^\times$, while in $\mathbb{Z}_7^\times$ we have $\langle 2\rangle = \langle 4\rangle = \{1, 2, 4\}$. Although $\langle g\rangle$ is defined to be a set, it's not hard to see that it's actually a group:

Proposition 1. $\langle g\rangle \leq G$

Make sure you can prove this! Next, we reviewed a classical theorem from group theory:

Theorem 2 (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then $|H| \,\Big|\, |G|$.*

Here I am using the notation $|S|$, the *order* of S, to denote the number of elements of S.

We didn't go over the proof in detail, but the idea is simple: tile G by many copies of H. More precisely, we can write $G = H \cup aH \cup bH \cup \ldots$, where $a, b, \ldots$ are elements of G and gH is just H translated by g (i.e. multiply every element of H by g). It isn't too hard to cover all of G by a collection of non-overlapping translations of H; since each translation of H has order $|H|$, this shows that $|G|$ is a multiple of $|H|$.

We can see this theorem in action in $\mathbb{Z}_7^\times$:

$$|\langle 1\rangle| = 1 \qquad |\langle 2\rangle| = 3 \qquad |\langle 3\rangle| = 6 \qquad |\langle 4\rangle| = 3 \qquad |\langle 5\rangle| = 6 \qquad |\langle 6\rangle| = 2$$

all of which divide $6 = |\mathbb{Z}_7^\times|$.

Rather than writing $|\langle a\rangle|$, it is common to write $|a|$, which is called the *order* of a. In other words, the order of a is the order of the group generated by a. Thus the order of 2 (mod 7) is 3, while the order of 3 (mod 7) is 6. Observe that if G is a finite group and $|g| = |G|$ for some element $g \in G$, then $G = \langle g\rangle$; in other words, g generates the entire group G. In this case, G is said to be *cyclic*, and g is called a *primitive root* of G. For example, $\mathbb{Z}_5^\times$ is cyclic, and 2 is a primitive root; $\mathbb{Z}_7^\times$ is cyclic, and 3 is a primitive root. It is important to note that a cyclic group may have many elements which are *not* primitive roots – so long as at least one of the elements generates the whole group, it is cyclic.

Is $\mathbb{Z}_n^\times$ always cyclic? No: $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ is not, since $3^2 = 5^2 = 7^2 = 1$ in this group. It turns out that $\mathbb{Z}_n^\times$ is cyclic iff $n = 2, 4, p^k$, or $2p^k$, where p is an odd prime. Next lecture we will prove that $\mathbb{Z}_p^\times$ is cyclic for any prime p, a result due to Gauss. We will also discuss some of the problems we don't know how to solve about primitive roots, and how these can be used to create new ciphers.