MAT 302: LECTURE SUMMARY

We began by completing our discussion of the linear congruential generator. Recall that the purpose of the linear congruential generator is to replace a true random number generator. Once we generate a sequence of seemingly random numbers $\{s_i\}$, we shift the first letter of the plaintext by s_1, the second by s_2, etc. If the sequence is 'random enough', Oscar won't be able to decrypt the message, even if he knows a piece of the message.

Trouble is, the linear congruential generator is *not* random enough. Recall that it is generated from a seed value s_0 by iterating a linear function $f(x) = Ax + B \pmod m$, i.e. $s_{i+1} = f(s_i)$ for each i. Here, s_0, A, and B are secret, while m is public. Note that Oscar cannot see the sequence s_i itself; rather, he sees the ciphertext, i.e. the plaintext shifted sequentially by the s_i. Suppose he somehow knows a little bit of the plaintext, for example the header; say he figures out s_{n-1}, s_n, and s_{n+1}. This gives him the system of equations

$$s_n \equiv As_{n-1} + B \pmod m$$
$$s_{n+1} \equiv As_n + B \pmod m$$

It follows that $(s_{n+1} - s_n) \equiv A(s_n - s_{n-1}) \pmod m$, so if $s_n - s_{n-1}$ is invertible $\pmod m$ then he can determine A and B, and therefore the rest of the message.

Before further discussing systems of equations $\pmod m$, we review some group theory. What is a group? Somewhat imprecisely, it is a set with a binary operation such that

- we can (unambiguously) combine as many elements as we like using the binary operation; and
- we can get from any element to any other using only the binary operation.

Before making this more precise, we give some examples and non-examples:

(1) $(\mathbb{Z}, +)$ is a group: if I write $3 + 5 + 7$ you know exactly what that means, and given two elements it's easy to get from one to the other, e.g. to get from 3 to 5 just add 2, and to get from 5 to 3 just add -2.
(2) $(\mathbb{Z}, \times)$ isn't a group: $3 \times 5 \times 7$ is unambiguous, but you can't get from 3 to 5.
(3) $(\mathbb{Q}, \times)$ isn't a group either: now you can get from 3 to 5 (by multiplying by 5/3), but you can't get from 0 to 5.
(4) $(\mathbb{Q}^\times, \times)$ is a group, where $\mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$. This is because multiplication is an unambiguous way of combining multiple elements, and to get from any nonzero α to β one can simply multiply by β/α.
(5) $(\mathbb{Q}^\times, \div)$ isn't a group: one can still move freely between any two elements (e.g. to get from 3 to 5, simply divide by 3/5), but one cannot unambiguously combine more than two elements. For example, $4 \div 2 \div 2$ might equal 1 or 4.

Date: January 27th, 2011.

(6) $\Big(A(S), \circ\Big)$ is a group, where S is an arbitrary set, $A(S)$ is the set of all bijections from S to itself, and $\circ$ is composition: $(f \circ g)(x) = f\big(g(x)\big)$. One can certainly unambiguously compose multiple bijections (why is this?). It is less clear that one can get from any $f(x)$ to any $g(x)$. How does one do it? Easy: first undo f, but applying f^{-1}; then apply g! In other words, apply the function $g \circ f^{-1}$ to f.

The situation in the last example is indicative of a general approach to testing whether a given set G is a group under a binary operation @: find an element which is easy to get to, and from which it is easy to get to any other element. For example, in $(\mathbb{Z}, +)$ it is very easy to get from any $n \in \mathbb{Z}$ to 0; just add $-n$. It is also easy to get from 0 to m, but adding m. This means that getting from n to m is an easy task, if one goes by way of 0. Similarly, in $(\mathbb{Q}^\times, \times)$ it is easy to get to 1, and then easy to get from 1 to any other element. In $\Big(A(S), \circ\Big)$ the special element is the identity function $\mathbb{1} : S \to S$, which maps any element x to itself. Given any function $f \in A(S)$, it's easy to get from f to $\mathbb{1}$: just undo whatever f does. And to get from $\mathbb{1}$ to $g \in A(S)$, simply apply g!

So, in all the examples we've seen, there is a special element which is easy to get to, and from which one can easily get to any other element. Keep this in mind as you read the following formal definition of a group:

Definition of a group. *Let G be a set, and suppose @ is a binary operation (i.e. @ is a function mapping $G \times G$ to G). Then G is said to be a **group** under the binary operation @ if:*

(1) *Associativity: $(a@b)@c = a@(b@c)$ for any $a, b, c \in G$*
(2) *Identity: there exists an element $e \in G$, called the identity of G, such that $e@x = x@e = x$ for every $x \in G$*
(3) *Inverses: for every $g \in G$ there exists an element $g^{-1} \in G$, called the inverse of g, such that $g@g^{-1} = g^{-1}@g = e$.*

If @ is a binary operation on G, we will say the G is *closed* under @.

Let's connect the formal definition to the informal notion discussed previously. Associativity essentially says that the symbol $a@b@c$ is unambiguously defined. From this it follows that $a_1@a_2@\cdots@a_n$ is unambiguous for any number of elements $a_i \in G$. The second property says that it's easy to get from the identity to any other element. The third property says that it is easy to get from any element to the identity. Combined, these two agree with the earlier idea that one can get from any element to any other. You will explore this further in your problem set this week.