MAT 302: LECTURE SUMMARY

In this lecture we will prove the following fundamental theorem:

Theorem 1 (Gauss, 1801)**.** *$\mathbb{Z}_p^\times$ is cyclic for every prime p.*

Here are a few other ways this theorem can be expressed:

(1) There exists an $a \in \mathbb{Z}_p^\times$ which is a primitive root.
(2) $\mathbb{Z}_p^\times = \langle a \rangle$ for some $a \in \mathbb{Z}_p^\times$.
(3) There exists $a \in \mathbb{Z}_p^\times$ such that $|a| = p - 1$.
(4) There exists $a \in \mathbb{Z}_p^\times$ such that $1, a, a^2, \ldots, a^{p-2}$ are all distinct $\pmod p$.

It will follow from the proof given below (which comes straight out of Gauss' masterwork *Disquisitiones Arithmeticae*) that $\mathbb{Z}_p^\times$ has $\varphi(p-1)$ primitive roots. He also proved that the sum of all the primitive roots is $\equiv \mu(p-1) \pmod p$, and that their product is $\equiv 1 \pmod p$. Beyond these global results, primitive roots are still pretty poorly understood. For example, after some experimentation one sees that 2 and 3 are often primitive roots of $\mathbb{Z}_p^\times$. Is 2 a primitive root for infinitely many p? This question is open. (This is a special case of one of Artin's conjectures.) In a similar vein, one might suspect that $\mathbb{Z}_p^\times$ has a small primitive root; it is widely believed that it has one which is smaller than a small power of $\log p$. However, all that is currently known is that there is a primitive root of size $O(p^{1/4+\epsilon})$, a decades-old result due to Burgess.

Suppose g is a primitive root of $\mathbb{Z}_p^\times$. Then for any $a \in \mathbb{Z}_p^\times$,

$$(*) \qquad g^x \equiv a \pmod p$$

has a solution x. Moreover, this solution is unique modulo $p-1$. (Can you prove this?) Thus, we will refer to 'the' solution to (*). This solution is called the *discrete logarithm* of a with respect to g, written $\log_g a$. For example, in $\mathbb{Z}_5^\times$ we have $\log_3 4 = 2$, whereas in $\mathbb{Z}_7^\times$, $\log_3 4 = 4$.

More generally, given any cyclic group $G = \langle g \rangle$, the discrete log of $a \in G$ with respect to g is the smallest non-negative integer x such that $g^x = a$. How can go about evaluating $\log_g a$ in practice? Certainly we could find it by trial-and-error: simply raise g to higher and higher powers until we get a. This is a highly inefficient procedure which could potentially take as long as $O(|G|)$. This inspired the Diffie-Hellman Key Exchange, which we now describe.

1. Diffie-Hellman Key Exchange

Alice and Bob publicly agree on a large integer N, and on a $g < N$. Alice secretly picks an integer a, computes $g^a \pmod N$, and sends the result to Bob. Bob secretly picks an integer b, computes $g^b \pmod N$, and sends the result to Alice. Alice raises Bob's message to the a, obtaining

Date: March 24th, 2011.

$g^{ab} \pmod N$; Bob raises Alice's message to the b, also obtaining $g^{ab} \pmod N$. They now have a mutual key $g^{ab} \pmod N$, which they can use to securely communicate via a symmetric cipher.

Why is this secure? Well, suppose Oscar is listening in. He knows $g, N, g^a \pmod N$, and $g^b \pmod N$. He doesn't know a and b. His goal is to determine $g^{ab} \pmod N$. How could he do this? This is called the Diffie-Hellman problem. So far, the only known solution to the Diffie-Hellman problem is to determine a or b, after which it is a simple matter to find $g^{ab} \pmod N$. Note that since Oscar knows g, N, and $g^a \pmod N$, he needs only to find the discrete logarithm of a. Thus, we have two problems: the Diffie-Hellman problem, and the Discrete Logarithm problem. We don't know how to efficiently solve DLP, and we don't know how to solve DH without DLP. This is what makes Diffie-Hellman Key Exchange (presumably) secure.

So far, we haven't made any requirements on g and N. Is DHKE secure for any large N? Suppose N is enormous, but $|g|$ is small, say, $|g| = 6$ in $\mathbb{Z}_N^\times$. Then whatever Alice's secret choice of a is, $g^a \equiv g^k \pmod N$ for some $k \in \{0, 1, 2, 3, 4, 5\}$, and by trial-and-error Oscar easily identifies what this value of k is. But then

$$(g^b)^k \equiv (g^k)^b \equiv (g^a)^b \equiv g^{ab} \pmod N$$

so Oscar can use his knowledge of $g^b \pmod N$ to determine the secret shared key $g^{ab} \pmod N$. This example shows that for DHKE to be secure, it is not enough for N to be large; it is crucial that the order of $g \pmod N$ be enormous. Of course, this also forces N itself to be huge, since the order of g is smaller than N.

How can Alice and Bob choose appropriate N and g to guarantee that $|g|$ is large? One nice idea is the following. Let p be a huge prime such that $2p + 1$ is also prime, and set $N = 2p + 1$. Then $|\mathbb{Z}_N^\times| = 2p$. Pick any $g \in \mathbb{Z}_N^\times$. By Lagrange's theorem, we must have

$$|g| \;\Big|\; 2p.$$

This implies that $|g| = 1, 2, p$, or $2p$. It is easy to check whether or not g has order 1 or 2. If it doesn't, then it *automatically* has order $\geq p$, which is enormous! For this reason, such primes $N = 2p + 1$ are called *safe primes*. The prime p also has a special name: it is called a *Sophie Germain prime*, after the 19th-century mathematician who proved an important case of Fermat's Last Theorem for all exponents which are divisible by such primes.

This leaves only the issue of finding large safe primes. Heuristically, by the Prime Number Theorem, the probability that $n \leq x$ is prime is roughly $\frac{1}{\log x}$. Therefore, the probability that both n and $2n + 1$ (of size x) are prime, should be roughly $\asymp \frac{1}{(\log x)^2}$. Thus, we expect that

$$\#\{p \leq x \;:\; 2p + 1 \text{ is prime}\} \asymp \frac{x}{\log^2 x}$$

This means that safe primes should be in plentiful supply, and in practice, they are. Theoretically, however, our knowledge of safe primes falls far short of the above prediction; it is not even known whether infinitely many safe primes exist!

One drawback to Diffie-Hellman is that although Alice and Bob ultimately have the same secret shared key, they have no control over this key. This was resolved by Taher Elgamal in the 1980's as follows: once Alice evaluates $g^{ab} \pmod N$ according to the DHKE, she chooses whichever key K

she likes, computes $g^{ab}K \pmod N$, and sends this to Bob. Since Bob knows $g^{ab} \pmod N$, it is a simple matter for him to determine K from this – he needs only to find the inverse of $g^{ab} \pmod N$ (easily accomplished using the Euclidean algorithm) and multiply Alice's message by this inverse. This method is now called Elgamal.

Note that Elgamal could also be used as a cipher in its own right, if we think of K as a message rather than as a key. However, in practice, symmetric ciphers are much faster than DHKE, so it is best to share a key using Elgamal (or DHKE or RSA) and then switch to a symmetric cipher such as AES.

2. Proof of Theorem 1

We concluded the lecture by proving Gauss' theorem that $\mathbb{Z}_p^\times$ is cyclic for any prime p. The proof comes out of studying solutions to the congruence $x^d \equiv 1 \pmod p$.

Proof of Theorem 1. Let $G = \mathbb{Z}_p^\times$, and set

$$G_d = \{x \in G \ : \ x^d \equiv 1 \pmod p\}.$$

In assignment 5, you will prove that $G_d \leq G$. The following result will play a crucial role in the sequel:

Lemma 2. $|G_d| \leq d$.

Colloquially, this lemma says that the equation $x^d = 1$ has at most d solutions in G. This might not be so surprising; it's true in $\mathbb{C}$, for example. Moreover, it's true in any *field*. However, the lemma is *not* true for the general group G. For example, $\mathbb{Z}_8^\times$ has 4 solutions to $x^2 = 1$.

The lemma is a special case of Theorem 4, which we will prove below. Taking the lemma on faith for now, we carry on with the proof of Theorem 1. Let

$$\psi(d) = \#\{x \in G \ : \ |x| = d\}.$$

To prove the theorem, it suffices to show that $\psi(p-1) \geq 1$. To accomplish this, we will study the size of $\psi(d)$ for all d. We start by examining what happens for those d which appear as the order of some element in G.

What can we say if $\psi(d) \geq 1$?

> If $\psi(d) \geq 1$, there must exist $g \in G$ such that $|g| = d$. In particular, $g \in G_d$. Since G_d is a group, $\langle g \rangle \subseteq G_d$. It follows that $|g| \leq |G_d|$, i.e. $d \leq |G_d|$. Combining this with our lemma we see that $|G_d| = d$, whence
>
> $$G_d = \langle g \rangle.$$
>
> Thus, $G_d = \{1, g, g^2, g^3, \ldots, g^{d-1}\}$. How many of these have order d? The following result implies the answer:
>
> **Proposition 3.** *Suppose $|g| = d$. Then $|g^k| = d$ if and only if $(k, d) = 1$.*

You will prove this (actually, a stronger statement than this) in assignment 5. It follows that the number of elements of G_d which have order d is precisely $\varphi(d)$, i.e.

$$\#\{x \in G_d \ : \ |x| = d\} = \varphi(d).$$

Since $\{x \in G_d \ : \ |x| = d\} = \{x \in G \ : \ |x| = d\}$ (why is this?), we have shown that

$$\psi(d) = \varphi(d).$$

So, we have proved that <u>if</u> $\psi(d) \geq 1$, <u>then</u> $\psi(d) = \varphi(d)$. Actually, there's another consequence which will be useful to us: if $\psi(d) \geq 1$, then $d \mid p-1$ by Lagrange's theorem.

Now, every element of G has *some* order. It follows that

$$\sum_d \psi(d) = |G| = p - 1.$$

Since $\psi(d) = 0$ unless $d \mid p-1$, we deduce that

$$\sum_{d|p-1} \psi(d) = p - 1.$$

In assignment 5, you will prove a similar result for $\varphi(d)$:

$$\sum_{d|p-1} \varphi(d) = p - 1.$$

In particular, we have

(♣) $$\sum_{d|p-1} \Big(\varphi(d) - \psi(d)\Big) = 0.$$

What can we say about $\varphi(d) - \psi(d)$? Quite a bit, actually:

$$\varphi(d) - \psi(d) = \begin{cases} 0 & \text{if } \psi(d) \geq 1 \\ \varphi(d) & \text{otherwise.} \end{cases}$$

Combining this with (♣), we see that we must have $\varphi(d) - \psi(d) = 0$ for all $d \mid p-1$. Therefore, $\psi(p-1) = \varphi(p-1)$, which concludes the proof. □

What we actually proved above is that for every $d \mid p-1$, $\psi(d) = \varphi(d)$. This is curious, because $\varphi(d)$ is independent of which group we're working with, while $\psi(d)$ is (on the surface, at least) intimately tied to the ambient group! For example, this shows that there are 2 elements of order 3 in $\mathbb{Z}_7^\times$, $\mathbb{Z}_{13}^\times$, and $\mathbb{Z}_{19}^\times$, three groups which are quite different in other respects.

Actually, we haven't quite finished the proof of Theorem 1 yet, since we didn't go back and take care of that Lemma. We do this now. In fact, we will prove rather more:

Theorem 4. *Suppose $f(x)$ is a monic polynomial with integer coefficients, and that $\deg f \geq 1$. Then*

$$\#\{x \in \mathbb{Z}_p \ : \ f(x) \equiv 0 \pmod p\} \leq \deg f$$

Recall that f has degree n (written $\deg f = n$) if the highest power of x appearing in $f(x)$ is x^n. f is *monic* if the coefficient of the highest-degree term is 1. Thus a monic polynomial of degree n looks like $f(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_{n-1}x + c_n$.

It will be convenient to define $\mathbb{Z}[x]$ to be the collection of *all* polynomials with integer coefficients.

Proof. Let $\mathfrak{Z}_p(f) = \{x \in \mathbb{Z}_p \ : \ f(x) \equiv 0 \pmod p\}$. We need to show that

$$|\mathfrak{Z}_p(f)| \leq \deg f$$

for every monic polynomial $f \in \mathbb{Z}[x]$ with $\deg f \geq 1$. We do this by induction:

$\deg f = 1$:
In this case, we must have $f(x) = x - a$ for some integer a. The only solution of the congruence $f(x) \equiv 0 \pmod p$ is $x \equiv a \pmod p$. Thus, the theorem is true in this case.

$\deg f = n$:
This is where we induct. Suppose that

$$|\mathfrak{Z}_p(g)| \leq n - 1$$

for all monic polynomials $g \in \mathbb{Z}[x]$ with $\deg g = n - 1$, i.e. that we have already proved the theorem for polynomials with degree $n - 1$. We will deduce the theorem for f in three steps.

STEP 1: for any $a \in \mathbb{Z}$, we can write

$$\frac{f(x)}{x - a} = q(x) + \frac{r}{x - a}$$

where r is an integer and $q \in \mathbb{Z}[x]$ is monic of degree $n - 1$. (This should be a familiar fact from high school, and is also a great exercise in induction – induct by degree.)

STEP 2: If $\alpha \in \mathfrak{Z}_p(f)$, then from Step 1 we can find a monic $g \in \mathbb{Z}[x]$ with $\deg g = n - 1$ such that

$$f(x) = (x - \alpha)g(x) + r$$

for some $r \in \mathbb{Z}$. Taking $x = \alpha$ we deduce that $r \equiv 0 \pmod p$. Thus, for every $x \in \mathbb{Z}$,

$$f(x) \equiv (x - \alpha)g(x) \pmod p.$$

STEP 3: Suppose that α and β both belong to $\mathfrak{Z}_p(f)$, and $\beta \not\equiv \alpha \pmod p$. From Step 2,

$$f(\beta) \equiv (\beta - \alpha)g(\beta) \pmod p$$

but also since $\beta \in \mathfrak{Z}_p(f)$ we see that $f(\beta) \equiv 0 \pmod p$. Thus,

$$(\beta - \alpha)g(\beta) \equiv 0 \pmod p.$$

Since we are assuming that $\beta \not\equiv \alpha \pmod p$, we conclude that

$$\beta \in \mathfrak{Z}_p(g).$$

Thus we have shown that for any $\alpha \in \mathfrak{Z}_p(f)$, there exists a monic $g \in \mathbb{Z}[x]$ of degree $n - 1$ such that

$$\mathfrak{Z}_p(f) \backslash \{\alpha\} \subseteq \mathfrak{Z}_p(g).$$

In particular, by our inductive hypothesis we see that

$$|\mathfrak{Z}_p(f)| - 1 \leq |\mathfrak{Z}_p(g)| \leq \deg g = n - 1$$

whence

$$|\mathfrak{Z}_p(f)| \leq n$$

and the theorem is proved. □