# CS 346 Class Notes

Mark Lindberg

Mar 23, 2016

**This Time:**

Chapter 8.1. Preliminaries and basic group theory.

Proposition 8.2. If $a, b \in \mathbb{N}$, $\exists X, Y \in \mathbb{Z}$ s.t. $X \cdot a + Y \cdot b = \gcd(a, b)$, and $\gcd(a, b)$ is the least positive integer that can be written in this way.

Proof: Let $I = \{x \in \mathbb{Z} | \exists X^*, Y^* \in \mathbb{Z}\ x = aX^* + bY^*\}$. Note that $a, b \in I$. Let $d$ denote the minimum positive integer in $I$. Let $X'$, $Y'$ be integers such that $d = aX' + bY'$. Note: $\forall c \in I$, $d \mid c$. (And therefore, $d|a$ and $d|b$.) Note that there are $X'', Y'' \in \mathbb{Z}$ such that $c = aX'' + bY''$. Then we can write $c = qd + r$, where $0 \leq r < d$, and $q, r \in \mathbb{Z}$. Therefore, $r = aX'' + bY'' - q(aX' + bY') = a(X'' - qX') + b(Y'' - qY')$. Therefore, $r \in I$. We noted that $d$ was the minimum positive integer in $I$, and since $0 \leq r < d$, this means that $r = 0$, and therefore, $c = qd$, and $d \mid c$.

Also $\neg\exists d' > d$ such that $d' \mid a$ and $d' \mid b$. Suppose that there was such a $d' > d$ such that $d'|a$ and $d'|b$. But then, $d' \mid a \cdot X'$ and $d' \mid b \cdot Y'$. Then $d' \mid (aX' + bY')$, but $aX' + bY' = d$, and this contradicts the fact that $d' > d$. Therefore, $d = \gcd(a, b)$.

Extended Euclidean Algorithm! A polynomial time algorithm to compute the $\gcd(a, b)$ as above.

Proposition 8.74. $b, N \in \mathbb{N}$, $b \geq 1$, $N > 1$. $b$ is "invertible" modulo $N$ iff $\gcd(b, N) = 1$.

Invertible: $\exists c$ such that $bc \equiv 1 \pmod N$.

($\Leftarrow$): Assume $\exists c$. Then $bc = 1 + \gamma N$, for some integer $\gamma$. Then $bc - \gamma N = 1$, so by proposition 8.2, $\gcd(b, N) = 1$.

($\Rightarrow$): Assume $\gcd(b, N) = 1$. Then $\exists X, Y$ such that $bX + NY = 1$ by proposition 8.2. Then $bX = 1 - NY$, and so $bX \equiv 1 \pmod N$. Therefore, $X$ is a multiplicative inverse of $b$ modulo $N$.

Groups: A set of elements $G$ and a binary operator $\circ : G \times G \to G$ such that

1. Identity: $\exists e \in G$ such that $\forall e \in G$, $x \circ g = g \circ e = g$. This element must be unique.
2. Inverse: $\forall g \in G$, $\exists h \in G$ such that $g \circ h = e$.
3. Associative: $(g \circ g') \circ g'' = g \circ (g' \circ g'')$.

The order of a finite group $G$, written $|G|$, is the number of elements in $G$.

In an abelian group, we have commutativity.

There are a bunch of examples. I kinda spaced out because I've taken a few group theory math classes.

Theorem 8.14. If $G$ is a finite abelian group, and $g \in G$, then $g^{|G|} = 1$.

Corollary 8.15. $g^x = g^{(x \mod m)}$, where $m = |G|$.

Corollary 8.17. Define $f_i : G \to G$ as $f_i(g) = g^i$.

Let $e$ be such that $\gcd(e, m) =' $.

Led $d$ be $e^{-1} \mod m$, so that $de \equiv 1 \pmod{m}$.

Then $f_e$, $f_d$ are permutations and $f_d$ is the inverse permutation of $f_e$.

$\mathbb{Z}_N$ is $\mathbb{Z}_N^+$, the set of all $\{0, 1, \ldots, N-1\}$ with addition.

$\mathbb{Z}_N^*$ is $\{i | 1 \leq i < N \land \gcd(i, N) = 1\}$. All the invertible numbers mod $N$. Then $\mathbb{Z}_1 5^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.