NOTES ON GROUPS AND CONGRUENCES

MATH 3320, LARRY ROLEN

To study elliptic curve cryptography, and to prove some of the key facts needed for RSA, we require some algebra.

Definition 1. A **group** $(G, *)$ is a non-empty set G together with an operation $G \times G \to G$ such that

(1) (Closure): $a * b \in G \quad \forall a, b \in G$.
(2) (Associativity): $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$.
(3) (Identity element): There is an $e \in G$ such that $a * e = e * a = a \quad \forall a \in G$.
(4) (Inverses): For all $a \in G$, there exists a $b \in G$ such that $a * b = b * a = e$.

Remarks. (1) By induction, one can always reorder parentheses in any length expression of elements of the group.
(2) Inverses are always unique, and so the inverse of a is typically denoted by a^{-1}.
(3) Often, we refer to just the set G as the group, and the operation $*$ is often known by context.

Examples. (1) The real numbers $\mathbb{R}$ are a group under addition $+$. The identity is 0, and the inverse of x is $-x$. This is also an *abelian group*, meaning that the operation is commutative:

$$a + b = b + a \quad \forall a, b \in \mathbb{R}.$$

(2) Vector spaces are abelian groups of vectors with *additional* structure of a field of scalars which act nicely on them by scalar multiplication.
(3) The sets $\mathbb{Z}$ or integers and $\mathbb{Q}$ of rational numbers (fractions of whole numbers) are groups under $+$. They are **subgroups** of $\mathbb{R}$. The set $\mathbb{N}$ of natural numbers $1, 2, \ldots$ is not a group under $+$, since it doesn't contain the identity element 0 and isn't closed under taking inverses (negation).
(4) The set of real numbers is not a group under multiplication because you can't invert 0. However, the set $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ of non-zero reals is a group under multiplication. The inverse of x is $1/x$, and the identity is 1.
(5) The set of $n \times n$ invertible real matrices is a group under multiplication with identity matrix I_n. It is not abelian, as $AB \neq BA$ in general for matrices under multiplication.
(6) Our final key example will be congruences classes modulo n. To set this us, we first recall that $a \equiv b \pmod{n}$ means that $n|(a - b)$. These **partition** $\mathbb{Z}$. The reason for this is that they give an **equivalence relation** on $\mathbb{Z}$, and those always give rise to partitions of sets (splitting the set into a disjoint union of subsets). We will define the equivalence relation by example in this case. Being an equivalence relation means that there are three properties which are a little like how the equals sign works:
   (a) Reflexive: $a \equiv a \pmod{n}$ (why: $n|0$ for all n).
   (b) Symmetric: $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$ (why: $n|(a - b) \implies n|(b - a)$ by multiplying by -1).

(c) Transitive: $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$ (why: if $n|(a-b), (b-c)$, then $n|(a-b+b-c) \implies n|(a-c)$.

An **equivalence class** *represented* by a is

$$a + n\mathbb{Z} = \{\dots, a-2n, a-n, a, a+n, a+2n \dots\} = \{b \in \mathbb{Z} | a \equiv b \pmod{n}\}.$$

This is a *coset* of the *subgroup* $n\mathbb{Z} \subseteq$ of multiples of n. Because this relates to congruences, we call this equivalence class a **congruence class**, and we will denote it by

$$a + n\mathbb{Z} = [a].$$

The point is that one can do arithmetic on congruence classes themselves. That is, we can add and multiply classes by doing so on *representatives.* We define

$$[a] + [b] = [a+b], \qquad [a][b] = [ab].$$

This is *well-defined* as if

$$a \equiv c \pmod{n}, \quad b \equiv d \pmod{n},$$

say $a - b = pn$, $b - d = qn$, then

$$a + b - (c+d) = (p+q)n \equiv 0 \pmod{n} \implies a + b \equiv c + d \pmod{n},$$

and

$$a = c + pn,\ b = d + qn \implies ab = (c+pn)(d+qn) = cd + n(pd + cq + pqn) \implies ab \equiv cd \pmod{n}.$$

Thus, the set of congruence classes modulo n is a group under addition. This gives us the following:

Definition 2. The group $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n = \mathbb{Z}_n$, pronounced "Z mod n Z" or "Z mod n" or "Z n" (all notations are common) is the set of congruence classes modulo n under the operation of addition. The identity is $[0]$, and the inverse of $[a]$ is $[-a]$.

One possible choice of representatives for the classes, which is the most common one, is as follows. By dividing a by n with remainder, we get

$$a = nq + r$$

so $a \equiv r \pmod{n}$, and $0 \leq r < n$. Thus, the remainder is in $\{0, 1, \dots, n-1\}$, and every integer is equivalent to exactly one number in this set. Thus, we have the partition

$$\mathbb{Z} = [0] \coprod [1] \coprod \dots \coprod [n-1],$$

and

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}.$$

Another good choice of representatives is to pick ones with smallest possible absolute values. For example, if $n = 11$, we have

$$\mathbb{Z}_{11} = \{[-5], [-4], [-3], [-2], [-1], [0], [1], [2], [3], [4], [5]\}.$$

What about multiplication? Just as $\mathbb{R}$ isn't a group under multiplication, because 0 doesn't have a multiplicative inverse, not all elements have a multiplicative inverse mod n. For example, if $n = 6$, then $[2]$ has no inverse, as that would mean that $[2][x] = 1$, or in terms of congruences,

$$2x \equiv 1 \pmod{6}.$$

This is clearly impossible as $x \in \mathbb{Z}$ and so it would mean that 1 is an even number. However, just like with $\mathbb{R}$, we can throw out the elements without inverses to obtain a group.

Definition 3. We denote by $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}_n^*$ the set of **invertible congruence classes modulo** n, that is, the set of $[a]$ such that $[a][b] = [1]$ for some congruence class $[b]$. This is a **group** under multiplication.

We can characterize the elements in this group without too much difficulty.

Lemma 0.1. *We have*

$$a \in \mathbb{Z}_n^* \iff (a, n) = 1.$$

Proof. If a is invertible, then $ax \equiv 1 \pmod{n}$ for some $x \in Z$, and so

$$n|(ax - 1) \implies ax - 1 = ny \implies ax + ny = 1$$

for some $y \in \mathbb{Z}$. Either from our "Bezout Identity" Theorem from before, or just by noting that any common divisor of a, n clearly divides the right hand side 1, we see that $(a, n) = 1$.

Conversely, if $(a, n) = 1$, by using the steps in the extended Euclidean algorithm, one can find integers x, y such that $ax + ny = 1$, which directly gives $ax \equiv 1 \pmod{n}$. □

Remark. This proof also shows how to **compute** the inverse using the Euclidean algorithm.

The size of $\mathbb{Z}_n^*$ is an important quantity, called **Euler's totient function**:

$$\varphi(n) := |\mathbb{Z}_n^*|.$$

To compute $\mathbb{Z}_n^*$, we can strike out all elements in $\{1, \ldots, n-1\}$ which are **not** coprime to n.

Example. To find $\mathbb{Z}_{10}^*$, we remove the elements which are even or a multiple of 5, giving

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\} \implies \varphi(10) = 4.$$

Remark. Note that here, we denoted [1] simply by the number 1; we use congruence classes frequently so its inconvenient to always write the brackets. The identification of the class with its representative has to be read off by context.

If p is a prime, it is very easy to determine $\mathbb{Z}_p^*$; the only element which doesn't survive is 0 itself, so we have

$$\mathbb{Z}_p^* = \{1, \ldots, p-1\},$$

and $\varphi(p) = p - 1$.

One of the most striking, and useful, facts about products modulo p is given by

Theorem 0.2 (Fermat's Little Theorem)**.** *If p is prime and $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

This is a special case of the more general:

Theorem 0.3 (Euler's Totient Theorem)**.** *If $n \geq 2$ and $(a, n) = 1$, then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

To explain what this is saying, we consider the following:

Definition 4. The order of $a \in \mathbb{Z}_n^*$, denoted $\mathrm{ord}(a)$, is the smallest positive integer t such that

$$a^t \equiv 1 \pmod{n}.$$

In particular, Euler's Totient Theorem implies that the order of **all** elements $a \in \mathbb{Z}_n*$ is at most $\varphi(n)$. We will see below that in fact the order must **divide** $\varphi(n)$.

To prove these, we develop a little more algebra.

Definition 5. A **subgroup** $H \subseteq G$ is a subset of G which is a group **under the same operation**. We denote this by $H \leq G$.

Just like with subspaces, subgroups must contain the identity element and be closed under the group operation and inverses. From now on, instead of writing $a * b$, we will write the operation simply as ab, just like we do with multiplying real numbers.

Definition 6. Let $H \leq G$. The (left) cosets of H are the sets

$$aH := \{ah | h \in H\}.$$

Example.
(1) The set of integer multiples of n, $n\mathbb{Z}$, is a subgroup of $\mathbb{Z}$. Its cosets are precisely the congruences classes modulo n.
(2) A subspace of a vector space is in particular a subgroup, and we saw the cosets of linear codes in that case.

We now want to generalize the observation we saw for congruence classes: the cosets of a subgroup **always** partition G. To see this, we will check the same conditions of an equivalence relation; it is a good idea to write each one in the example of congruences modulo n to see how it relates to what we did above. Note that this is also very similar to the fact that cosets partitioned K^n in the linear codes section.

Specifically, we make an equivalence relation on G by saying aRb (a is "related" to b) if $a \in bH \equiv b^{-1}a \in H$. We check the three conditions in order:

(1) **Reflexive:** aRa as $a^{-1}a = e \in H$.
(2) **Symmetric:** If aRb, then $b^{-1}a \in H$. Now in general, we have the **socks and shoes property** (you have to take off socks and shoes in opposite order as you put them on): $(ab)^{-1} = b^{-1}a^{-1}$ as $b^{-1}a^{-1}ab = b^{-1}b = e = aa^{-1} = abb^{-1}a^{-1}$. Thus, if $b^{-1}a \in H$ and H is closed under inverses, $a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$, and so bRa.
(3) **Transitive:** If aRb and bRc, then $b^{-1}a, c^{-1}b \in H$ and so

$$c^{-1}a = (c^{-1}b)(b^{-1}a) \in H \implies aRc.$$

Thus, G is a **disjoint union** of the cosets of H.

Definition 7. If G is a finite group, the number of cosets of H is called the **index** of H in G, and is denoted by $[G\colon H]$.

Example. If $a \in Z_n^*$, the **cyclic subgroup** generated by a, $\langle a \rangle$, is the subgroup of powers of a:

$$\langle a \rangle = \{1, a, a^2, \ldots, a^{\mathrm{ord}-1}\}.$$

Thus,

$$|\langle a \rangle| = \mathrm{ord}(a).$$

Example. We have that

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}, \quad \varphi(15) = 8.$$

We further have

$$\langle 2 \rangle = \{1, 2, 4, 8\}$$

as $2^4 = 16 \equiv 1 \pmod{15}$. Thus, $\text{ord}(2) = 4$.

The cosets of $\langle 2 \rangle$ are

$$1 \cdot \langle 2 \rangle = \langle 2 \rangle,$$
$$7 \cdot \langle 2 \rangle = \{7, 14, 13, 11\} = \mathbb{Z}_{15}^* \setminus \langle 2 \rangle.$$

Just as in the linear codes section, if there are two cosets, they are the subgroup itself and its complements, and you can find all the cosets by repeatedly taking cosets represented by elements not seen yet. Thus, we have the disjoint union

$$\mathbb{Z}_{15}^* = \langle 2 \rangle \coprod 7\langle 2 \rangle,$$

and

$$[\mathbb{Z}_{15}^* \colon \langle 2 \rangle] = 2.$$

Note that this is

$$\frac{|\mathbb{Z}_{15}^*|}{|\langle 2 \rangle|} = \frac{8}{4} = 2.$$

This is analogous to the fact that for cosets in the linear code section, we had

$$\text{number of cosets} = \frac{2^n}{2^k} = \frac{|K^n|}{|C|},$$

the quotient of the size of the "big space" K^n and the subgroup C.

It turns out this last observation holds in general, and has an almost identical proof as we saw in the linear codes section:

Theorem 0.4 (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then we have*

$$|G| = [G \colon H] \cdot |H|.$$

In particular, we have the divisibility:

$$|H| \;\Big|\; |G|.$$

Proof. Just as we did in the coding theory part, we first show that all cosets have the same size, in particular, the same size as the trivial one. Specifically, we show that there is a *bijection* (one-to-one correspondence) from H to an arbitrary coset aH. We define this function $f \colon H \to aH$ by $f(h) = ah$. This is surjective/onto by the definition of aH. It is injective/one-to-one as if $f(h_1) = f(h_2)$, then $ah_1 = ah_2$. Multiplying both sides on the left by a^{-1} shows $h_1 = h_2$. Thus, the function f is a bijection, and $|H| = |aH|$.

Now the cosets, all of size $|H|$, partition G. That is, G is a disjoint union of these sets, of which there are $[G \colon H]$ of them. This proves the claim. □

Corollary 0.5. *In a finite group, the order of any element divides $|G|$.*

Proof. The order of an element is the order of the cyclic subgroup it generates. □

Corollary 0.6. *In $\mathbb{Z}_n^*$, the order of a always divides $\varphi(n)$.*

Proof. This is the special case $G = \mathbb{Z}_n^*$ of the last corollary. □

Corollary 0.7. *Euler's Theorem, and hence Fermat's Little Theorem, is true.*

Proof. If $\mathrm{ord}(a)|\varphi(n)$, then we have

$$a^{\varphi(n)} = a^{\mathrm{ord}(a)\cdot t} \equiv 1^t \equiv 1 \pmod{n}$$

for some t. □

Example. Computing big powers of thing modulo n is easy thanks to Euler's Theorem. For instance, let's compute $128^{129} \pmod{17}$. First, rules of congruences give us that we can reduce the base mod 17. As $128 \equiv 9 \pmod{17}$, we have

$$128^{129} \pmod{17} \equiv 9^{129} \pmod{17}.$$

Now we divide 129 by $\varphi(17) = 16$ with remainder:

$$129 = 16 \cdot 8 + 1.$$

Fermat's Little Theorem then gives

$$9^{129} \equiv 9^{16\cdot 8} \cdot 9^1 \equiv 1 \cdot 9 \equiv 9 \pmod{17}.$$

Thus, $128^{129} \equiv 9 \pmod{17}$.

We have a special case of orders:

Definition 8. If $\mathrm{ord}(a) = \varphi(n)$, then $\langle a \rangle = \mathbb{Z}_n^*$ and we call a a **generator** of $\mathbb{Z}_n^*$, or a **primitive root modulo n.**

Not all groups $\mathbb{Z}_n^*$ have a generator. However, if n is a prime, then there is (the real "reason" for this is that $\mathbb{Z}_p$ is a field for a prime p).

To effectively use Euler's Theorem, we'd like to compute $\varphi(n)$. To do so, we can use the following two facts:

Fact 8. *We have that $\varphi(n)$ is* **multiplicative***, that is, if $(a, b) = 1$, then*

$$\varphi(ab) = \varphi(a)\varphi(b).$$

The reason for this is an explicit version of the **Chinese Remainder Theorem**.

Fact 9. *If $n = p^a$ is a power of a prime, then*

$$\varphi(p^a) = p^{a-1}(p-1) = p^a - p^{a-1}.$$

This is easy to check: when forming $\mathbb{Z}_{p^a}^*$, you only have to strike out the multiples of p among $\{0, 1, \ldots, p^{a-1}$, of which there are p^{a-1} of them.

Corollary 0.10. *If we have a factorization $n = p_1^{a_1} \cdots p_k^{a_k}$ of n into powers of distinct primes, then*

$$\varphi(n) = \prod_{i=1}^{k} p^{a_i - 1}(p-1).$$

Example. We compute

$$\varphi(20) = \varphi(2^2 \cdot 5) = \varphi(2^2) \cdot \varphi(5) = 2 \cdot 4 = 8.$$

In particular, as $(11, 20) = 1$, we have

$$11^8 \equiv 1 \pmod{20},$$

and the order of 11 modulo 20 is a divisor of 8 (its 2 since $11^2 = 121 \equiv 1 \pmod{20}$).