FINITE MATHEMATICS

Igor Rivin, St Andrews, Fall 2015

WHAT IS THIS ABOUT?

- We will be learning about some basic basic techniques, which include:
- Residue arithmetic
- Elements of finite groups
- Elements of finite rings and fields. One of the goals is proving Wedderburn's theorem, which states that every finite division ring is a field.
- Elements of number theory (Extended Euclidean algorithm, Chinese Remainder Theorem, etc)
- Elements of cyclotomic polynomials.
- The very basics of finite vector spaces, as well as affine and projective spaces.

WHAT IS THIS ABOUT, CONTINUED

- The style of the course is leisurely and discourcive – we will take interesting diversions where we find them, The main point of the course is learning how (some) mathematicians think, and how we discover mathematics. While much of the mathematics we are covering is quite classical, all (or most) of it is new to us.
- Our main criterion is not some putative utility, but aesthetics and elegance. One of the wonderful things about mathematics, is that beautiful things wind up being more useful!
- What this means is that we often don't know where we are going, until we get there, and these notes will be trailing behind the actual course a lot of the time.

RESIDUES

- Consider an integer *n*. The set $n\mathbb{Z}$ is the set of multiples of *n*, so $n\mathbb{Z} = \{n, 2n, 3n, \dots\}$. We define an equivalence relation on the integers $\mathbb{Z}$, by saying that $a \equiv b \ (mod\ n)$, whenever $a - b \ \in n\mathbb{Z}$. We denote the set of equivalence classes of this relation by $\mathbb{Z}/n\mathbb{Z}$.
- Given two equivalence classes, we can add and multiply them (by taking integer representatives, adding or multiplying those, and taking the equivalence class of the sum or product, respectively).
- It is not hard to see that the classes of 0 and 1 are the additive and multiplicative identities, respectively, in $\mathbb{Z}/n\mathbb{Z}$.

RESIDUES

- We thus see that $\mathbb{Z}/n\mathbb{Z}$ is a *commutative ring with 1.* (look up the definition!)
- Recall that such a ring is called an *integral domain* if no non-zero element a is a divisor of zero. In other words, given a, there is a b, such that $a\,b = 0$, if and only if $a=0$.
- Observation: $\mathbb{Z}/n\mathbb{Z}$ is *not* an integral domain *unless* n is **prime.** Why? If n is not prime, then there are $1<k$, $1<n$, such that $n = k\,l$. Clearly the residue classes of k and l are 0-divisors.
- Similarly, we see that $\mathbb{Z}/p\mathbb{Z}$, for p prime *is* an integral domain (if k is not a multiple of p, and l is not a multiple of p, we can't have $k\,l$ a multiple of p by the **fundamental theorem of arithmetic.**

FUNDAMENTAL THEOREM OF ARITHMETIC

- Any positive integer n can be written as $n = p_1^a p_2^b \ldots p_k^c$, where the p_i are prime, and this representation is *unique* up to the order of the factors.
- Proof: existence is easy by induction: either n is prime, in which case there is nothing to do, or $n = k\,l$, in which case represent k and l by induction. The harder part is uniqueness, which we leave as a challenging problem (we will need the method we develop in the next little while.

RESIDUE RINGS MODULO A PRIME

- For a prime *p,* we can show that $\mathbb{Z}/p\mathbb{Z}$ is not just an integral domain, but a *field.* This means that for any nonzero *a,* there exists a *b,* such that $a\ b\ \equiv 1\ (mod\ p)$.
- **PROOF 1:** Consider the map $M(a)$: $\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$, given by *M(a)(b) = a b.* Since we know that $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, this map is 1-1, but a 1-1 map of finite sets of the same cardinality is a bijection, so there is a *b,* such that *M(a)(b) = 1 = ab.*
- The above proof has the virtue of extreme simplicity, but the downside of being non-constructive (we know that the inverse exists, but don't really know how to find one).
- **PROOF 2:** This uses the fundamental properties of the Euclidean Algorithm (see the sequel) to show the following fundamental result:

CHARACTERIZATION OF THE GREATEST COMMON DIVISOR

- Suppose m, n are integers. Then, the greatest common divisor of m, n is the *smallest positive value* of a linear combination with integer coefficients $a\ m + b\ n$.
- The proof uses the Euclidean Algorithm, which is the following (essentially optimal)
- We want to find the greatest common divisor of n *and* m.
- Divide with remainder to write $n = q\ m + r$.
- Note that the greatest common divisor of n and m is the same as the greatest common divisor of m and r, but note also that $r < min(n, m)$.
- Which means that the algorithm terminates.

EUCLIDEAN ALGORITHM

- What is more, the remainder *r* is an integer linear combination of *m* and *n.* The next remainder will be a linear combination of *m* and *r*, and so of *m* and *n.* So will the last remainder (which is the gcd). That shows that the value of the smallest linear positive linear combination of *m* and *n* is no bigger than the gcd of *m* and *n.* But obviously, the gcd has to divide any linear combination, so we are done…

APPLICATIONS

- $\mathbb{Z}/p\mathbb{Z}$ is a field. Indeed, any *n* not divisible by a prime *p* is relatively prime to it, so there exist *a, b* such that *a n + b p = 1.* Taking equivalence classes modulo *p* of both sides, get $an \equiv 1 \ (mod\ p)$
- Chinese remainder theorem: given moduli $n_1, n_2, \ldots n_k$, pairwise relatively prime, and remainders $r_1, r_2, \ldots r_k$, there exists an integer *x,* such that $x \equiv r_i \pmod{n_i}$, for every *i.*
- Proof of CRT by induction on *k:* first, do it for *k=2.* Look for *x* in the form
- $x = a\, n_1 + b\, n_2$. We see that $an_1 \equiv r_2 \ (mod\ n_2)$, and $bn_2 \equiv r_1 \ (mod\ n_1)$, so we see that $a \equiv r_2 n_1^{-1} (mod\ n_2)$, and $b \equiv r_1 n_2^{-1} (mod\ n_1)$.

PROOF OF FUNDAMENTAL THEOREM OR ARITHMETIC

- Uses *Euclid's Lemma:* if p (a prime) divides ab then it divides a or it divides b.
- **PROOF:** if p does not divide a, then it is relatively prime to a. So, there exist some $k, l,$ such that $k\ p + l\ a = 1$. Multiply both sides of this equation by b, to get
- $\boldsymbol{kpb + lab = b}$. We see that p divides both summands on the left hand side (the first obviously, and the second by hypothesis). This means that it divides the right hand side.

FIELDS

CHARACTERISTIC OF A FIELD

- The *characteristic* of a field *F* is the smallest integer *c* such that *c x = 0,* for any element *x* of *F.* If there is no such positive integer, the characteristic is said to be equal to *0.*
- Observation: the characteristic, if not equal to *0,* has to be *prime.* If not, *c = a b*, so $0 = c \times 1 = (a \times 1) \times (b \times 1)$, which contradicts the existence of 0-divisors in a field.
- Another observation: any field *F* of characteristic *p* contains a copy of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Indeed, the elements *0, 1, …, p-1* are such a copy. This copy is called **the prime field** of *F.*

VECTOR SPACES

- A vector space V over a field F is an abelian group (which we will denote additively) with an action by F, satisfying:
- $0x = 0$, for all x in V.
- $1x = x$, for all x in V.
- $c(d\,x) = (cd)x$, for all x in V, and c, d in F.
- $(c + d)x = c\,x + d\,x$, for all x in V, c, d in F.
- $c(x + y) = c\,x + c\,y$, for all c in F, and x, y in F.

VECTOR SPACES

- A set of elements $S=\{v_1, v_2 \dots, v_k\}$ has a span, which is the set of all linear combinations of elements in S. This is denoted by $\langle S \rangle$. A set S is called spanning, if $\langle S \rangle = V$.
- A set of elements S is called *independent,* if $f_1 v_1 + f_2 v_2 + \cdots f_k v_k = 0$ impliest that all of the f_i are zero.
- A set of elements S is called a basis, if it is both spanning and independent.
- Every finite vector space V has a basis (keep adding elements) B, and the cardinality $|V| = |F|^{|B|}$

VECTOR SPACES AND FINITE FIELDS

- Note that every finite field is a vector space over its prime field, so we see that
- **The cardinality of every finite field is p^k, for some prime p.**
- **Interesting fact: up to isomorphism, there is *exactly one* field of given cardinality.**

A LITTLE ABOUT GROUPS

- A subgroup H of a group G is a subset of G which is also a group (with the same operation).
- A left *coset* of H in G is the set of elements of the form $x\,h$, for some (fixed) x in G, and h in H.
- An easy observation is that two cosets of H are either the same, or they are disjoint.
- Another easy observation is that any two cosets of H are of the same cardinality.
- It now follows that left cosets partition G into subsets, the cardinality of each of which is the same (and thus, the same as the cardinality of H).

LAGRANGE THEOREM

- We have proved that (for a finite *G*), $|G| = k\ |H|$, for some integer *k*. This ratio of the orders of of *G* and *H* is called the *index* of *H* in *G*. (this is called Lagrange's Theorem).
- Now, let $x \in G$. We denote the smallest subgroup of *G* containing *x* by $\langle x \rangle$. It is easy to see that $\langle x \rangle$ is the set of all integer powers of *x*, including $x^0 = 1$. The *order* of *x* is the smallest $k > 0$, such that $x^k = 1$. For an infinite *G* such *k* might not exist (in which case we say that *x* is of infinite order), but the pigeonhole principle tells us that it always does exist for a finite *G*. This *k* is easily seen to be the order of $\langle x \rangle$, and is called the *order* of *x* (and written as $|x|$. By Lagrange's theorem, this divides $|G|$.

FERMAT'S LITTLE THEOREM

- Let us apply the preceding discussion to the multiplicative group of $\mathbb{F}_p$. The order of the multiplicative group is $p-1$, from which we see that:
- $a^p \equiv a(mod\ p)$, for any *a.* This is known as *Fermat's Little Theorem,* to distinguish it from *Fermat's last Theorem,* proved (confusingly) by Andrew Wiles some three hundred years after Pierre de Fermat shuffled off this mortal coil.
- Now, let *n* be a not necessarily prime number. The order of the group of units of $\mathbb{Z}/n\mathbb{Z}$ is denoted by $\boldsymbol{\varphi}(n)$. Otherwise, $\boldsymbol{\varphi}(n)$ is the number of positive integers not exceeding *n* and relatively prime to *n.*
- Applying the preceding reasoning to the group of units of $\mathbb{Z}/n\mathbb{Z}$, we get *Euler's extension of Fermat's little theorem:*
- $a^{\boldsymbol{\varphi}(n)} \equiv 1\ (mod\ n)$, for any *a* relatively prime to *n.*

MORE ON $\phi(n)$

- It is clear that, given k, the smallest multiple of k divisible by n is the least common multiple of k and n. It follows that the order of k in $\mathbb{Z}/n\mathbb{Z}$ equals $n/(k, n)$. It follows that the number of elements of a given order $x|n$, equals $\varphi(x)$. Since every element has some order, we obtain the fundamental identity
- $\sum_{d|n} \varphi(d) = n$.
- This identity can also be proved by noting, first, that $\varphi(n)$ is a multiplicative function: that is, if k is relatively prime to l, then $\varphi(k\ l) = \varphi(k)\varphi(l)$,
- Then noting that if a function f is multiplicative, so is the function F, where
- $F(n) = \sum_{d|n} f(d)$,
- And finally checking the identity for prime n.

MULTIPLICATIVE GROUP OF A FINITE FIELD

- We will show that the multiplicative of a finite field is *always cyclic.* This means that if the order of the multiplicative group *G* is *n,* then, there exists an element *g* in *G,* such that *every h* in *G* has the form g^k, for some integer *k.*
- The proof is by contradiction. First, let *g* be an element of biggest order in *G*. Since *G* is finite, such a *g* exists. Let the order of *g* be *o(g).* We first show that the order *o(h)* of *every* element *h* in *G* divides *o(g).* Indeed, if *o(h)* does not divide *o(g)*, then the order of *gh* is the least common multiple of the orders of *g* and *h,* and thus exceeds the order of *g.*
- Now, if N is the largest order of an element $g \in G$, we see that

MULTIPLICATIVE GROUP OF A FINITE FIELD

- $1-h^N=0$, for *every* element h of G. Since we are in a field, it follow that the number of elements of G is at most N. But this means that the order of the group equals the order of some element, so the group is cyclic.
- Some remarks: first, the converse of our statement is also true: the multiplicative group of a field F is cyclic if and only if F is finite,
- Further, this shows that for every divisor d of the order of the multiplicative group of the finite field F, there is exactly one subgroup of order d.

CYCLOTOMIC POLYNOMIALS

- The roots of the polynomial x^n-1=0 are known as the *nth roots of unity.* They can be written explicitly as $e^{2\pi ki/n} = \cos 2\pi k/n + i \sin 2\pi k/n$, with *k=0, …, n-1.* A root is known as a *primitive nth root,* if it is not also an *mth* root, for some $\mathrm{m} < n$. It is not hard to see that $e^{2\pi ki/n}$ is a primitive *nth* root of unity if and only if *k* is relatively prime to *n.*
- This motivates the following definition: the *nth* cyclotomic polynomial $\Phi_n(\mathrm{x})$ is defined to be the product of *(x-r),* where *r* run over all primitive *nth* roots of unity.

CYCLOTOMIC POLYNOMIALS

- Important observation is that $\Phi_n(x)$ has integer coefficients (it is not *a priori* obvious that the coefficients are even real). The proof uses the identity
- $x^n - 1 = \prod_{d|n} \Phi_d(x)$
- And mathematical (complete) induction.