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 $b \equiv r_1 n_2^{-1} (mod\ n_1)$.

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.**