Honors Algebra II, Courant Institute, Spring 2021

http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2021/HonorsAlgebraII.html

Check the class forum for corrections and hints

Assignment 1, due February 9 (before class starts).

Corrections

- January 29: Exercise 1, the multiplication formula is corrected. The old one was garbled.
- February 1: Exercise 2, clarified the relation between n and 12.
- February 1: Exercise 3, clarified the notation, particularly $\phi(n)$.
- February 1: Exercise 4, reworded to make it clear that the hypothesis involves all $x \in \mathbb{F}_p$.
- February 1: Exercise 6, typo fixed $\mathbb{F}[x] \longrightarrow \mathbb{F}(x)$ in one place.
- February 1: Unassigned Exercise 1, typo fixed: $\mathbb{F}_p \longrightarrow \mathbb{F}_p^*$.
- February 8: Exercise 6, corrected.

Instructions

- Do not hand in a rough draft. Copy or type answers neatly and clearly. Points may be deducted for writing that is sloppy, has excessive cross-outs, or is hard to read.
- State facts precisely in clear language or notation. Put assertions in logical order. State clearly what the hypotheses and conclusions. Put the steps of an argument in logical order, including definitions. Points may be deducted for an incorrectly stated argument even if you seen to understand it. Clear mathematical exposition is an important goal for the class.
- Learn the Greek letters used in math. Learn their mathematical names and write them clearly.

Review of $\mathbb{F}_p$. There is no recitation on Friday January 29 as I had thought and planned. Instead of going to recitation, please spend those 75 minutes on the following "review" of $\mathbb{F}_p \cong \mathbb{Z}/(p)$. You need be aware of these facts to do some exercises in this assignment. Everything here is in the textbook (or any other appropriate abstract algebra book), but maybe not collected in one place.

If p is a prime number, then the quotient ring $\mathbb{Z}/(p)$ is a field. If $x \in \mathbb{Z}$ and $x \neq 0 \mod p$, then there is $y \in \mathbb{Z}$ with $xy = 1 \mod p$. Every non-zero element of the quotient ring has a multiplicative inverse, which makes the quotient ring a field. This field, which has p elements, is denoted $\mathbb{F}_p$. The multiplicative group $\mathbb{F}_p^*$ consists of the $p-1$ non-zero elements of $\mathbb{F}_p$ with multiplication as the group operation. The *structure theorem* for $\mathbb{F}_p^*$ is the *little Fermat theorem*. This

states that $\mathbb{F}_p^*$ is cyclic (definition and proof outline below). A cyclic group has a generator (not unique) g so that as a set, $\mathbb{F}_p^*$ is $\left\{g, g^2, \cdots, g^{p-1} = 1\right\}$. This is a way of saying that the powers of g fill out $\mathbb{F}_*^p$. For any $x \in \mathbb{F}_p^*$ there is a power k so that $g^k = x$. As a consequence, any $x \in \mathbb{F}_p^*$ satisfies $x^{p-1} = 1$, because

$$x^{p-1} = \left(g^k\right)^{p-1} = \left(g^{p-1}\right)^k = 1^k = 1 \; .$$

You can multiply this by x to get the equivalent statement $x^p = x$ if $x \neq 0$ in $\mathbb{F}_p$.

Pierre de Fermat died in 1665, centuries before abstract algebra and finite fields. He stated his theorem in terms of powers of numbers mod p. For any p there generator g so that if x is not a multiple of p then $x \equiv g^k \mod p$. This generator has the property that $g^{p-1} \equiv 1 \mod p$. Therefore (as above) $x^p \equiv x \mod p$. This applies to any $x \in \mathbb{Z}$ as long as x is not a multiple of p. Note the difference in notation. For $x \in \mathbb{F}_p$ we write $x^p = x$, which is true in the finite field. For $x \in \mathbb{Z}$, we write $x \equiv x^p \mod p$, because the two integers x and x^p are not the same integer.

Fermat's little theorem has an interesting modern application. Large primes are the basis of the RSA public key cryptography system which is used in all internet credit card transactions. You can find a large prime by choosing a large integer at random and testing whether it's prime. If you take a random number with d digits (say, $d = 100$), the probability that it is prime is $O(d^{-1})$, by the *prime number theorem*. This is not so small. To find a 100 digit prime, you have to test on the order of 100 numbers. The *Miller Rabin* test is a way to test whether an integer n is prime. The algorithm is a "randomized algorithm" that does a sequence of independent tests using different randomly chosen numbers $x \in \mathbb{Z}$, with $1 < x < n$. If n is not prime, there is a 75% chance (at least) that x will be a *witness*. If you try 50 times, and n is not prime, there the chance that none of the x values you chose were witnesses is less than $2^{-100} \approx 10^{-30}$. This is not impossible in the mathematical sense, but it is impossible in the practical sense. A surprising feature of this is that you can tell that n is not prime without finding a factor of n.

The test starts with a "little Fermat" test. You check whether $x^n = x \mod n$. If not, then x is a witness to the fact that n is not prime. The full Miller Rabin test does some more checks with the same x using the structure that $\mathbb{F}_n$ would have if n were prime. If these tests fail, then x is a witness. The test does not produce a factor of n. The class web page has a link to Rabin's original paper with this amazing algorithm and theorem.

The RSA public key cryptography system is based on the fact that if you know $K = pq$ with p and q prime, then it is impractical to learn p or q. If p and q have d digits and K has $2d$ digits, the best known factoring algorithm requires $O(e^{Cd})$ work to find p and q. If "Bob" wants to receive a secure message from "Alice" (these names are used to describe any encryption/decryption scheme), Bob generates p and q by generating d digit numbers at random and using the Miller Rabin test to find primes. The Bob tells Alice K, keeping p and q secure. Anyone who "hears" Bob's message to Alice can learn K, but they can't learn p

or q. Alice uses K to encrypt her message. But nobody can decrypt the message without knowing p and q. Anyone can "hear" the message from Alice to Bob, but only Bob can decrypt it.

I don't know how Fermat proved the little theorem, but today it may be seen as a consequence of the structure theorem for finite abelian groups. You may not "remember" (have seen) all of the proofs. These facts are just stated here for your information. You are invited to write out the easy proofs, but please do not hand them in. They are not part of the assignment.

1. The cyclic group C_n with n is the quotient of the additive group $\mathbb{Z}$ by the subgroup (all subgroups of abelian groups are normal) $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

2. For $x \in C_n$ we use the notation $kx = x + \cdots + x$ (k times). We use multiplicative notation, but multiplication is not part of the group C_n. For any k the number $m = \#\{x \in C_n \mid kx = 0\}$ (the number of elements with ...) is given by $m = \gcd(k, n)$. For example, in C_{10} there are five elements with $15x = 0$, namely $x = 0, 2, 4, 6, 8$.

3. In particular, if $k|n$ (k divides n), then $k = \#\{x \in C_n \mid kx = 0\}$. For example, $x = 0, 2, 4, 6, 8$ are the elements of C_{10} with $5x = 0$.

4. If $\gcd(n, m) = 1$ (they are relatively prime), then $C_n \times C_m \cong C_{nm}$ (the product group on the left is isomorphic to the cyclic group on the right).

5. If $\gcd(m, n) > 1$ (not relatively prime), then $C_n \times C_m$ is not isomorphic to C_{nm}. In fact, if $k|n$ and $k|m$, then $\#\{x \in C_n \times C_m \mid kx = 0\} = k^2$. These are $x = (y, z) \in C_n \times C_m$ with $my = 0$ in C_n and $mz = 0$ in C_m.

6. (*Structure theorem for finite abelian groups*) If G is a finite abelian group, then G is isomorphic to a finite product of cyclic groups: $G \cong C_{n_1} \times \cdots \times C_{n_r}$. [This is proved in the Modules chapter in the textbook. The proof is not hard, but we probably won't get to it this semester.]

7. If the number of factors is $r \geq 2$, we may assume that no pair of sizes n_j and n_i are relatively prime, because of part (4). In particular, if $r > 1$, there is a $k > 1$ with $k|n_1$ and $k|n_2$.

8. If $\mathbb{F}_p^*$ is not cyclic, then it has a cycle decomposition, by part (6), with $r > 1$. Then there is a k as in part (7). Part (5) then implies that there are at least $k^2 > k$ elements $x \in \mathbb{F}_p^*$ with $x^k = 1$. This is the main step in the proof of the little Fermat structure theorem. It may be confusing because the group operation here is multiplication in $\mathbb{F}_p^*$, but we wrote the operation "additively" in the beginning.

9. Since $\mathbb{F}_p$ is a field, the polynomial $f(x) = x^k - 1$ can have at most k roots. This is possible only if $r = 1$ (one cyclic factor) in the step (6) structure theorem of the abelian group $\mathbb{F}_p^*$. This is the only step that uses the fact that p is prime. Exercise 3 below demonstrates that there can be more then one factor, and more than k roots of $x^k = 1$, if n is not prime.

Assigned Exercises, to hand in

1. Let p be a rational prime and $\mathbb{F}_p = \mathbb{Z}/(p)$ the finite field with p elements. Suppose d is not a square, which means $d \in \mathbb{F}_p$ with $d \neq x^2$ for any $x \in \mathbb{F}_p$. Let R be the set of p^2 elements of the form $x + \delta y$ with the addition and multiplication rules

$$\begin{aligned}(x + \delta y) + (u + \delta v) &= (x + u) + \delta(y + v) \\ (x + \delta y) \cdot (u + \delta v) &= (xu + dyv) + \delta(xv + yu)\ .\end{aligned}$$

   This is a formal way of saying $\delta = \sqrt{d}$, which is not in $\mathbb{F}_p$ because d is not a square.

   (a) Show that the non-zero squares in $\mathbb{F}_p$ are all the elements of the form $x = g^{2k}$, where g is a generator of $\mathbb{F}_p^*$. Use this to make a list of the squares in $\mathbb{F}_{17}$.

   (b) Show that R a ring. Identify the additive and multiplicative identity.

   (c) Show that R is a field. Show that for any $\xi = x + \delta y \in R$ with $\xi \neq 0$ there is a unique $\eta = u + \delta v \in R$ with $\xi\eta = 1$. Construct a 2×2 matrix $M(\xi)$ with entries in $\mathbb{F}_p$ so that $\xi\eta = 1$ is equivalent to

$$M \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

   Show that $M(\xi)$ is invertible for $\xi \neq 0$ by showing that $\det(M(\xi)) \neq 0$. How is the hypothesis that d is not a square come in?

2. Write $f(x) = x^{12} - 1$ as a product of monic polynomials irreducible over $\mathbb{Q}$. Explain how the degrees of the factors $f = g_1 \cdot \cdots \cdot g_k$ are related to the numbers $\phi(j)$ where $j|n$. The distinct complex roots of f have the form $\omega_j = e^{2\pi ij/n}$ for $j = 0, \ldots, n-1$. For each factor g_i, identify the set R_i with $\omega_j \in R_i$ if ω_j is a root of g_i. Show explicitly that $g_i(x) = \prod_{j \in R_i}(x - \omega_j)$. *Note.* This problem is about $n = 12$, but a lot of the structure may be understood with general n. Decide for yourself when you want to go from general n to $n = 12$.

3. Find an n so that $G = [\mathbb{Z}/(n)]^*$ is not cyclic. This G is the multiplicative group of residue classes relatively prime to n. It has $|G| = \phi(n)$, and $\phi(n) < n - 1$ if n is not prime.

$$\text{notation: } |G| = \text{the number of elements in } G\ .$$

   Unassigned Exercise 3 has more about the Euler ϕ function. Find the group $C_{j_1} \times C_{j_2} \times \cdots$ (at least two non-trivial factors) that G is isomorphic to. [This is related to Exercise 2.3 of Chapter 12.]

4. If $f(x) \in \mathbb{Z}[x]$ and $g(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)$ for all $x \in \mathbb{Z}$, then $f = g$ as polynomials (all coefficients equal). Now consider $f, g \in \mathbb{F}_p[x]$. Show that if $f(x) = g(x)$ for all $x \in \mathbb{F}_p$, *and* if $\deg(f) < p$, $\deg(g) < p$, then $f = g$ as polynomials. Give an example to show it need not be true if $\deg(f) \geq p$.

5. Consider the four variable polynomial $f(x, y, z, w) = xw - yz$ (the determinant). Show that f is irreducible in $\mathbb{C}[x, y, z, w]$.

6. Prove the following theorem. Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x]$ a polynomial. If there is a rational function $r \in \mathbb{F}(x)$ with $r(x)^2 = f(x)$, as elements of $\mathbb{F}(x)$, then there is a polynomial $g \in \mathbb{F}[x]$ and an $a \in \mathbb{F}$ with $ag^2 = f$. *Hint.* $\mathbb{F}[x]$ is a domain where there is unique prime factorization up to units. What are the units in $\mathbb{F}[x]$?

Unassigned Exercises, for practice, not to hand in From the Chapter 12 exercises: 2.1, 2.2, 2.3, 4.1 Also

1. Find generators for $\mathbb{F}_p^*$ for $p = 2, 3, 5, \cdots$. You will see that it isn't easy and there doesn't seem to be a pattern to them.

2. Check that $2^p \equiv 2 \bmod p$ for $p = 3, 5, 7, \cdots$. For example, $2^5 = 32$ and $32 = 30 + 2 \equiv 2 \bmod 5$. Check that this is not true for non-primes. For example, $2^6 = 64 \equiv 4 \bmod 6$. It is possible that $x^n \equiv x \bmod n$ even when n is not prime. Can you find an example?

3. To illustrate the formula, where $m = n$ is a term in the sum but $m = 1$ is not.
$$n = \sum_{m|n} \phi(m) \ .$$
   (a) (related to Exercise 2 above) Make a list (non-zeros mod 30) of the non-zero integers $\{1, 2, \cdots, 29\}$, non-zeros mod 30. Underline the ones relatively prime to 30 and count them.
   (b) Make a list of the integers $\{1, 2, \cdots, 14\}$, underline the ones relatively prime to 15. For each k in this list, find $2k$ in your list from part (a). It should not be underlined, but underline it.
   (c) Do the same for $m = 10$, underline the ones relatively prime to 10 and for each such k, find $3k$ in the list from part (a). The pattern from parts (b) and (c) is that 2 is the complementary factor to 15 $(2 \cdot 15 = 30)$ and 3 is the complementary factor to 10.
   (d) Continue with factors $m = 6$, (complementary factor $= 5$), with $m = 5$ (complementary factor $= 2 \cdot 3 = 6$), $m = 3$ and $m = 2$. When you're done, every number in the part (a) list should be underlined exactly once.

4. Show that the polynomial $f(x) = x^3 + 2x^2 + 3x + 5$ is irreducible in $\mathbb{Z}[x]$. *Hint.* Look mod 2 and see that $x = 0$ and $x = 1$ are not roots. If f factors in $\mathbb{Z}$ then f factors in $\mathbb{F}_2$ (why)? You also can check that f mod 2 is on the list of irreducible polynomials in $\mathbb{F}_2[x]$ on page 373.