Math 4030 Homework

Adam Boocher

Fall 2016

Welcome to Math 4030! You are encouraged to work on homework in groups of 2 -3 people. Make sure you clearly write your names on the top of your submitted work, and make sure you take turns writing up the problems from week to week. Occasionally, there might be pop-quizzes on homework days that test some of the easier homework questions, so that I can make sure everyone is on the same page with the material.

Working on homework in a group serves two purposes - first it means you have people to talk through problems with. Secondly (and more importantly) it means that you get a chance to experience many different parts of the learning process. At times you'll feel stuck; at others you'll be the only one in the group who knows how to solve the problem and your task will be to explain and teach to others; at others you might remain stuck despite your group's efforts to help. This is all normal and part of the learning process. As future teachers, experiencing this first-hand is important, and I encourage you to reflect on these things throughout the course.

1 Natural Numbers - Due August 31

1.1 Topics to Know

1. Most important: Natural numbers, well-ordered axiom, principle of induction, how to prove things by induction, how to define things by induction, correct statement of division with remainder, definition of prime numbers, fundamental theorem of arithmetic, there are infinitely many primes, factoring numbers, Euclid's algorithm for finding gcd.
2. Important: Have a good gut feeling why addition multiplication are commutative, associative. Be able to think through what's going on with the distributive law.
3. Don't worry too much about the delicate proofs in the notes involving the properties of multiplication, addition, etc.

1.2 Exercises

1. Find the error in the following "Fake" definition of subtraction of two natural numbers. We fix a natural number m and will define $f(n) = m - n$ inductively, where $f : \mathbb{N} \to \mathbb{N}$.
   - $f(1) = m - 1$ is the number before m.
   - $f(n+1) = m - (n+1)$ is the number before $f(n)$.
2. Consider the following "proof" that there are infinitely many primes. Is it a valid proof? Why or why not?

   Proof Suppose that there are finitely many primes $\{2, 3, 5, \ldots, p\}$ where p is the biggest. Then consider the number
   $$N = (2 \cdot 3 \cdot 5 \cdots p) + 1$$
   that is one more than the product of all the primes. Clearly it is not divisible by any of the primes in our list (it leaves a remainder of 1) so thus N must be prime, which is a contradiction, since N is bigger than p. $\square$
3. Define the factorial function $f(n) = n!$ by induction. Make sure you specify the domain and codomain for this function and check that your definition will define $n!$ for every n in your range.
4. Prove by induction that the sum of the first n even numbers is $n(n+1)$.
5. Find and count all the prime numbers between
   - 1 and 100
   - 101 and 200
   - 201 and 300
   - 301 and 400
6. Factor each of the following numbers as a product of primes
   - 9699690
   - 82861
   - 10001
7. Find the gcd of 159477 and 241133 using Euclid's algorithm.
8. Let X_n be the set $\{1, 2, \ldots, n\}$. Write down X_4 and all of its subsets. (Don't forget the empty set!) Prove by induction that there are in general 2^n subsets of X_n. Hint: exactly half of the subsets of X_{n+1} contain $n+1$.
9. (The postage stamp problem) In the Kingdom of Daventry, the post office sells postage in denominations of 3 and 7. Thus it's easy to pay exactly 10, or 6 or 14. However it's impossible to pay 1 or 4 or 8.
   - Write down exactly which denominations can be gotten exactly in Daventry.
   - Prove that this list is correct using induction (a paragraph will be good here)

   Play around with some other pairs of numbers (m, n) and see what patterns you get. You might start with 4 and 6 and then 11 and 15. You should see that these cases are different - why?

1.3 Some food for thought

(food for thought doesn't need to be turned in)

10. We didn't define 0 to be a natural number. Does this matter?

11. What if we were equally frivolous and decided to define

$$\mathbb{N} = \{1, 2, 4, 5, 6, 7, ...\}$$

leaving out the number three, but with the same "usual" rules of addition? Would this be an "ok" definition? Why or why not?

2 The Integers and Rationals - Due September 7

2.1 Topics to Know

1. Most important: The integers, subtraction, definition of additive inverse, additive identity. Experience proving abstract statements. Further practice with the Euclidean algorithm - doing it backwards,
2. Important: Have a good mathematical grounding on why multiplication and addition are related. Why is a negative times a negative a positive?

2.2 Exercises

1. In Aaron's notes Exercise 2.1 (worked on in class)
2. In Aaron's notes Exercise 2.2
3. In Aaron's notes Exercise 2.3
4. In Aaron's notes Exercise 2.6
5. In Aaron's notes Exercise 2.7 (It's easier than it looks!)
6. Use the Euclidean algorithm to show that the gcd of 54 and 201 is 3.
7. The last line of your work above should be

   $$9 = 6(1) + 3.$$

   This means that you can write $3 = 9 - 6(1)$. In other words, you have written 3 in terms of 9 and 6.... **Keep working backwards and write** 3 **as a combination of 201 and 54.**

   This leads to the

   General Fact If $c = gcd(a, b)$ then it is possible to write $c = ax + by$ for some integers x and y. (You may use this in the course, but don't need to prove it)
8. Explain (i.e. prove) why the equation $12x + 15y = 4$ has no solutions in $\mathbb{Z}$. I.e. there are no integers x, y that solve this equation. (Hint: Think about divisibility)
9. Let $a, b, d \in \mathbb{Z}$ be nonzero integers. Can you give a necessary and sufficient conditions for the equation $ax + by = d$ to have a solution.
10. On the other hand, determine when the equation $ax + by = d$ has solutions $(x, y) \in \mathbb{Q}$. (a, b, d could be zero)

2.3 Some food for thought

One component of classroom participation is that I'd like each student in the course to give a short presentation at some point during the course. This can really be on any topic you like - and I'll suggest some in the food for thought portions of the homework. This week we have some really fun problems that are pretty open-ended. The presentations will not be graded for a grade - just for participation. The goal is to get practice presenting cool math to the class!

1. Take a look at Exercise 2.8 in Aaron's notes. Try to think of a good algorithm - if you're stuck, come talk to me, or try to decipher the hieroglyphics (literally!) on Wikipedia.
2. This week we did a warmup about Euclid's proof of the infinitude of primes. But primes come in lots of different types. For instance,
   - All primes are odd except for 2.
   - All odd numbers are either 1 more than a multiple of 4, or they are 1 less than a multiple of 4.
   - Consult a list of a bunch of prime numbers and sort them into these two categories.
   - Do you think it's true that there are infinitely many primes that are in each type?
   - Try to prove that there are infinitely many primes of the form $4k-1$ by mimicking Euclid's proof.
   - What goes wrong if you try this method with $4k + 1$.
   - Come talk to me about this proof and we can work on a short presentation.

3 Rationals and Modular Arithmetic - Due Sept 14th

3.1 Topics to Know

1. Important: Know what a rational number is, what equivalence classes are, and why our rules for addition and multiplication are well-defined. Be able to prove that some numbers are irrational.

3.2 Exercises

1. A Pythagorean triple is a set (x, y, z) of integers such that

$$x^2 + y^2 = z^2.$$

Using the technique I showed in class let's find a formula for Pythagorean triples. Let $y = \left(-\frac{a}{b}\right) x + 1$ and find the x and y coordinates of the intersection of the line with with the unit circle. This will give you rational solutions to $x^2 + y^2 = 1$. Now clear denominators to get integers x, y, z such that $x^2 + y^2 = z^2$. Your answer should say what x, y, z are in terms of the slope a/b.

2. We've worked a lot with clock arithmetic, and we're going to make things a bit more formal. Let n be a natural number. We say that two integers x and y are "**equivalent modulo** n" if $x - y$ is divisible by n.

   (a) Write down a few pairs of numbers that are equivalent modulo 6

   Let $[x]$ denote the equivalence class of all integers equivalent to x modulo 6. Is $[1] = [7]$?

   (b) Is $[1] = [7]$?

   (c) Is $[1] = [2]$?

   (d) How many equivalence classes are there modulo 6? If the answer is finite (hint: it is), write down the list of all equivalence classes.

   In general, we define

$$\mathbb{Z}/n\mathbb{Z} = \{\text{the set of equivalence classes } [x] \text{ modulo } n\}.$$

3. **This problem is all modulo 7.** That means we are working in $\mathbb{Z}/7\mathbb{Z}$. We can use our normal arithmetic operations on this set of numbers. For instance, we have $[4] \cdot [3] = [12] = [5]$, so we could say that $[4][3] = [5]$. Notice that $\mathbb{Z}/n\mathbb{Z}$ has an additive identity $[0]$ it also has a multiplicative identity $[1]$.

   (a) Get some practice with this by computing the following in $\mathbb{Z}/7\mathbb{Z}$:

$$[4] + [5], \quad [3][3], \quad [3][3][3], \quad [2][7], \quad [5][5].$$

   (b) Convince yourself that $[2]^3 = [1]$, and this means that $[2]^6 = ([2]^3)^2 = [1]^2 = [1]$. This is sooo important - just write down "I am convinced."

   (c) I'm not joking - this fact is really important: Do you see that $[2][5] = [3]$? And therefore if you want to compute $([2][5])[8]$ this is the same as $([3])[8]$? There'd be NO reason to compute $[2 \cdot 5 \cdot 8] = [80]$ and then reduce! The point is that you can reduce your numbers part way through the computation! Write down "I get it. If ever I have big numbers in my computation, I should reduce them modulo 7 before I multiply more."

   (d) Compute $[5][4][2][3][4][4]$ in your head using what you just learned. (Remember - reduce at each step!)

   (e) Use the fact that $[2]^3 = [1]$ to compute $[2]^{1000}$.

   (f) Compute all the powers of $[3]$ modulo 7. You should see a pattern.

   (g) What is $[3]^{50}$?

   (h) Find a number $0 < r < 7$ such that $3^{50} - r$ is divisible by 7. (Hint: How is this related to the previous question.

4. How about a proof! Let $x \in \mathbb{Z}$. We will work modulo 4. Show that modulo 4, x^2 is either equivalent to 0 or 1. (Hint: Don't be scared by the word proof! How many equivalence classes are there for x? Why not just text them all and see what $[x]^2$ is?)

5. Prove that if $x \in \mathbb{Z}$ then x^2 is equivalent to either $0, 1$ or 4 modulo 5.

6. How many elements are there in $\mathbb{Z}/6\mathbb{Z}$? Write them down. Which elements have a multiplicative inverse? Which have an additive inverse?

7. How many elements are there in $\mathbb{Z}/11\mathbb{Z}$? Write them down. Which elements have a multiplicative inverse? Which have an additive inverse?

8. Let's end with a warning! Modulo n it is NOT always true that we can cancel using multiplication. Find a number n and number a, b, c such that

$$[a][c] = [b][c] \text{ mod } n$$

   but $[a] \neq [b]$. (Hint: You can do it with $n = 6$)

9. Is the following a valid argument? (Yes or No)

   We will work in $\mathbb{Z}/n\mathbb{Z}$, so all equations are to be interpreted modulo n. Suppose that

$$[a][c] = [b][c].$$

   Now suppose that $[c]$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$. Then we can multiply both sides of this equation by the multiplicative inverse to get that $[a] = [b]$.

Some Thoughts This assignment looks long, but that's mostly because I've put lots of computational exercises to make sure you know how the operations work. My hope is that this gives you experience working with this new number system. Main goals for this assignment are:

- Begin to get familiar with how equivalence classes represent a bunch of different numbers. For instance, modulo 6, we have $[3] = [21] = [27]$ etc.
- Get practice with arithmetic with these numbers.
- Understand that, say, mod 5 there are only 5 equivalence classes - so if we want to know what $[x^5]$ is mod 5, we can just work out $[x]^5$ for each equivalence class.
- Think about how this is similar to saying something like "Oh we can assume that the fraction is in lowest terms" (we're just choosing a particular representative)
- Finally - this is probably challenging and new - please feel free to email me or come by my office hours - Monday after class or Tuesday 11am-12pm. Or email me to set up an appointment!

4 Decimal Expansions and Real Numbers

Reminder There is an exam on September 21st. It will cover up to and including the material on this homework assignment, which is due the day of the exam. If you would like to turn the homework in on Monday, that is also ok - I can try to grade the homework on Monday night in order to offer feedback during office hours on Tuesday.

4.1 Exercises

1. 3-1 Aaron's Notes
2. 3-2 Aaron's Notes
3. 3-3 Aaron's Notes
4. 3-4 Aaron's Notes
5. 3-5 Aaron's Notes
6. One problem that you will be teaching a lot of in mathematics is "How to solve equations". Occasionally we are able to solve explicitly for x. For instance, with things like $8x-7=15$. Or $x^2=8$. Or $x^2-1=0$ However, sometimes it is a bit harder, like $e^x=3x$. In this case (and most real life cases) we can only hope to answer the following:

   - Does the equation even have a solution?
   - If it does - can we approximate it?

   First, explain why solving any equation $f(x)=g(x)$ for x is the same as solving some for x in some equation $h(x)=0$. (What is $h(x)$?)

7. Let's take $e^x=3x$ as an example. How could you explain to a high school student that this has some solution? If you wanted to approximate a solution, how could you find one? Does $e^x=x$ have a solution? Why or why not?

5 Exam 1 Info

The exam will have 6 questions and I will write it so that time will not be an issue. The questions below are meant to help you prepare for the exam. No calculators will be allowed.

5.1 Numbers 1 - 2

The exam will start with some basic computational problems. Here are some example problems:

- Use the euclidean algorithm to compute $\gcd(84, 117)$. (Ans: 3)
- Use your work from this problem to go "backwards" to write 3 as a combination of 84 and 117. In other words, find a solution to the equation $84x + 117y = 3$.
- Or I might ask you to solve $30 = 84x + 117y$. Think about how this is related to the previous problem.
- I'll definitely ask you about how to write down repeating decimals for rational numbers
- Know how to do continued fraction expansions for rational numbers.

5.2 Number 3

An induction problem. For example - can you prove that $1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$. Or can you prove an inequality like we did on the worksheet? Or it might be a more abstract problem, like the one with the subsets of $\{1, \ldots, n\}$. A great selection of 5 practice problems with solutions (each) can be found here: `http://www.math.tamu.edu/~joel.zinn/433sum11/additional-material/induction-practice.pdf`

5.3 Number 4

This will be a short answer question with some questions about proofs, definitions. I might ask something like "what's wrong with this proof by induction" or "why is this not a well-defined function." or "here is the definition of additive inverse: the additive inverse of s in an abelian group is the element t such that $s + t = 0$. Tell me why this definition implicitly implies that there is a unique additive identity."

5.4 Number 5

This problem will be devoted to modular arithmetic, divisibility and properties of the integers. There might be a true false question or two. Maybe something like: If n is divisible by a and also by b then n is divisible by ab.

I really like modular arithmetic and noticing patterns! Maybe I'll ask you to compute $[7]^{10}$ modulo 11. Or maybe I'll ask you which elements in $\mathbb{Z}/11\mathbb{Z}$ have multiplicative inverses. or which ones have additive inverses?

5.5 Number 6

This will be a grab bag. I might ask you to interpret things in terms of their definitions. Maybe things like:

- If $\gcd(a, b) = 6$ then explain why a must be even.
- If $[n] = [6]$ in $\mathbb{Z}/15\mathbb{Z}$ then explain why $n - 6$ must be divisible by 3.
- Explain further why this means that n must be divisible by 3.
- Write a paragraph about what is easy / hard / confusing about real numbers. Are they more subtle than you thought before? (No incorrect answers here)

5.6 Extra Credit

There will be math extra credit - I'm pretty picky with extra credit. Points will only be given for significant progress and well written solutions.

**Ask me about my favorite "extra credit on an exam" story, from my friend Emma.

6 The Complex Numbers - Due October 5

Solve the following from Aaron's notes

1. 4-1
2. 4-2
3. 4-4
4. 4-5
5. 4-6 (drawing pictures will be very helpful here)
6. 4-7
7. Consider the two matrices

$$A = \begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix}, \quad B = \begin{pmatrix} \cos b & -\sin b \\ \sin b & \cos b \end{pmatrix}.$$

   The first rotates the plane by an angle a and the second rotates the plane by an angle b.

   a) First, let's talk about the product BA. This is the matrix that would correspond to "first multiplying by A and then multiplying by B". Forget about the formulas - for a moment, think about what the matrices mean geometrically (i.e. rotations). What would the effect be if we did BA - would it be a rotation? If so, by what angle?

   b) Using your answer for part a), explain why the matrix for BA must be

$$C = \begin{pmatrix} \cos(a+b) & -\sin(a+b) \\ \sin(a+b) & \cos(a+b) \end{pmatrix}.$$

   c) Now actually do the computation. Multiply BA out as matrices and compare the 4 entries with those of C above. You've just proven the sum formulas for sine and cosine!

8. Finally, let's stay flexible with what we've already learned:

   Write down an expression like $1 + 4 + \ldots + blah$ for:

   a) The sum of the first n square numbers.

   b) The sum of the first n powers of 2, starting with 2^0.

   c) The sum of the first n odd powers of 2, (so start with $2^1 + 2^3$..)

9. And one lonely problem about modular arithmetic (poor fellow). We've so far spent a lot of time trying to get numbers into the "standard" representation. For instance, if we were working modulo 8, we would prefer to write [2] instead of [18]. And instead of $[-4]$, we might opt to write [4]. However, sometimes, writing things in different ways makes them easy to compute.

   Compute $[108]^2$ modulo 109 using a calculator. (Ans: [1]). Now notice that $[108] = [-1]$, so we could also compute $[108]^2 = [-1]^2 = [1]$. That was easy. Using a modification of approach, compute the following without a calculator:

   a) $[2010]^2$ modulo 2016.

   b) $[n-1]^9$ modulo n.

7 Polynomials - Due October 19

Solve the following from Aaron's notes

1. 5-2
2. 5-3
3. 5-6
4. Prove that for all natural numbers n:

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

5. Consider the sequence defined recursively by $a_1 = 2$ and $a_n = 3a_{n-1} + 5$.
   (a) Write down what this sequence is modulo 10. Explain why you know it repeats.
   (b) Now give an argument why modulo any n this sequence will also eventually loop back onto itself.
   (c) ($\star$) Modulo 10 you should have seen that the whole sequence starting from a_1 repeated. Do you think this will always be the case?
6. Recall that the Fibonacci numbers are defined by $a_1 = 1, a_2 = 1$, and $a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$.
   (a) As a warm up, write down the Fibonacci numbers mod 10. (i.e. just write the ones digit). You should see that they repeat eventually.
   (b) Now prove that for any n, modulo n, the sequence of Fibonacci numbers repeats at some point, starting again with $1, 1, 2, 3$, etc. (Hint: There are two steps to this - think about first why the sequence must necessarily get stuck in some loop. and then then try to argue why this loop must cycle through the whole sequence. Come by my office hours to talk about this. Monday after class - Tuesday 11-12, or some other time on Tuesday or Wednesday - send me an email and we can set something up!)

8 Polynomials - Oct 26

From Aaron's notes:

1. 5-4
2. 5-5
3. We say that an element x in a ring R is called a **unit** if it has a multiplicative inverse. Describe the set of *units* in the following rings:
   - $\mathbb{Z}$ (Hint: there are 2)
   - $\mathbb{Z}/12\mathbb{Z}$
   - $\mathbb{Q}[x]$ (Hint: there are infinitely many)
   - The ring of Gaussian integers $\mathbb{Z}[i]$ (See Aaron's notes 4-7)
   - $F[x]$ when F is a field.
4. Factor the polynomial $x^8 - 1$ in $\mathbb{F}_2[x]$. (Remember that in $\mathbb{F}_2$, we have that $1 = -1$. So this is the same as factoring $x^8 - 1$). In the end, make sure all of your coefficients are either 0 or 1.
5. Use the Euclidean algorithm over $\mathbb{F}_2$ to compute the a gcd in $\mathbb{F}_2[x]$ of
   $$f(x) = x^6 + x^2 + 1, \quad g(x) = x^5 + x^4 + 1$$
   Remember, that $-1 = 1$ in this field, and $2 = 0$ so this should simplify your calculations.
6. Find the prime factorization of $x^3 + x^2 + x$ in $\mathbb{F}_3[x]$ where $\mathbb{F}_3$ is the field with three elements $\{-1, 0, 1\}$.
7. Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1$ in $\mathbb{Z}/7\mathbb{Z}[x]$. Determine the quotient and remainder upon dividing $f(x)$ by $g(x)$. (Note: you'll probably be tempted to write something like $5/3$. But we are in $\mathbb{Z}/7\mathbb{Z}$ so there aren't fractions per se. But $5/3$ should be $5(1/3)$ and 3 does have a multiplicative inverse. Figure out what it is and use this to solve this problem. This is a good problem to work on with a friend!)
8. Let $f(x)$ be a polynomial with rational coefficients. i.e. $f(x) \in \mathbb{Q}[x]$ Suppose that there is a rational number a such that $f(a) = 0$. We call this a rational **root**.
   (a) Write down a polynomial $f(x)$ with rational coefficients so that $a = 5$ is a root.
   (b) Write down a polynomial $g(x)$ with rational coefficients so that $a = \sqrt{5}$ is a root.
   (c) Write down a polynomial $h(x)$ with rational coefficients so that $a = 2i$ is a root.
   (d) Write down a polynomial $p(x)$ with rational coefficients so that $a = \sqrt{5} + \sqrt{2}$ is a root. (This is the hardest one!)

9 Exam 2 Prep

The exam will have 6 questions as before. Here is a short description:

9.1 Problem 1 (Complex Numbers)

This problem will have basic computational questions about complex numbers. I might ask you to compute the magnitude of a complex number (its length) or multiply two numbers. You'll have to convert to polar coordinates - you'll be expected to know your angles - e.g. what is the angle for the number $1+\sqrt{3}i$. You'll be asked to compute roots of complex numbers. This might be a multi-step process. Some sample questions to look at include the homework questions from last time and the following:

- Let $z = 2+3i$ and let $w = (4, 60^o)$ be complex numbers. (Obviously the second is in polar form). Compute $z+w$ and write the answer in the form $a+bi$.
- What are the solutions x to the equation $x^3 = w$? (You can write your answer in polar form. Hint: there are three answers)
- What is $1/w$. Write your answer in both polar and standard coordinates.

9.2 Problem 2 (Complex Numbers)

This problem will also be about complex numbers, but will be a bit more theoretical in nature. For instance, if I give you a picture and have plotted a number z could you plot z^2, $1/z$, $3z$, and the three cube roots of z?

I might ask you to compute something like $\overline{z/w}$ if $z = (r, \theta)$ and $w = (s, \phi)$. This is a hard question and is related to the homework you recently got back.

I might ask you to compute the 10th power of $3(\cos 20^o + i \sin 20^0)$. Make sure you know how to do this.

9.3 Problem 3 (A segue question relating complex numbers and polynomials)

Our main point in defining the complex numbers was that we wanted to solve the equation $x^2 = -1$. Now with i, we can factor x^2+1 and get $(x+i)(x-i)$. I might ask you to think about what happens when you look at a factored polynomial like $(x-2i)(x+i)$. Where are its roots - can you draw them? What about the roots of $x^6 - 1 = 0$. If you sketched these what would it look like? You should definitely be able to write down all of these explicitly. How does this help you factor your polynomial? Don't worry - I won't make you write long technical expressions. But it'll be important to understand what's going on. Some things to think about.

- If the three roots of x^3-1 are $1, w_1$ and w_2, can you explain to me why $(x-1)(x-w_1)(x-w_2) = (x^3-1)$? In other words, what does factoring have to do with solving equations?
- As extra practice, make sure you can find w_1 and w_2. Is there any relationship between w_1 and w_2? (For instance is one the negative of the other?)

9.4 Problem 4 (Polynomials and Rings)

In this problem I will ask for a definition of one of the following: degree of a polynomial, what it means to be a prime polynomial, or what a zero divisor is in a ring. (See Worksheet 8)

I might give you a list of rings and ask which ones are fields. For example, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Q}[x], \mathbb{C}[x]$. I might ask you to find some zero divisors in a ring if it has some. Finally I might ask you to factor something in the ring of Gaussian integers $\mathbb{Z}[i]$. By the way, is the ring $\mathbb{Z}[i]$ a field? (This was defined on the previous homework assignment)

9.5 Problem 5 (Polynomials over weird rings)

I'll ask you some questions about polynomials over finite rings, like $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. I might ask you to work out with $(x+1)^3$ is. Or I might give you a polynomial and ask you how you know it is prime, or not prime. I'll ask you to do some polynomial long division over $\mathbb{Q}$. At least one problem from the most recent homework (due on Exam day) will be on the exam.

9.6 Problem 6 (Grab bag)

I'll ask you why $\mathbb{Z}/4\mathbb{Z}$ is not a field. I might give you a list of polynomials and ask whether or not they are prime. I might throw in that problem from the homework about whether $b^2 - 4ac$ is positive or negative. I might have some true or false questions like "the polynomial $x + 1$ is always prime in $F[x]$ no matter what field we work in.

10 Homework 10 - Due November 9th

From Aaron's notes:

1. 6-2 (You'll want to go and carefully check the requirements in the **definition** of a degree function.)
2. 6-3 and 6-4 (this problem is optional - the gcds are: $1, 7, 1001$ and $1, x^8-x^6+x^2-1$ respectively. I really recommend trying these, especially the part where you are asked to write the gcd as a combination of the two original elements. This has the benefit that you can check if you are correct - so you can just multiply everything out. Feel free to use a computer/calculator. This won't be graded - if you have questions please email me.)
3. Let $f(x)$ be in any polynomial ring $F[x]$. Suppose that the degree of $f(x)$ is 3. Prove that $f(x)$ factors over F if and only if it has a root r in F. (Hint: This is an if and only if statement, so you'll want to write your proof in two parts. The first should have the form "If f has a root r then.... so therefore $f(x)$ factors." The second proof should be "Suppose that $f(x)$ factors ... ".)
4. Determine whether the following polynomials factor in $\mathbb{Q}[x]$.

   $$(a)\ x^3+x+2 \quad (c)\ x^3-3x+1 \quad (e)\ x^3+x^2+x+1$$

   $$(b)\ x^3+x-3 \quad (d)\ x^3-3x+2 \quad (f)\ x^3+x^2+x+2$$

   (Hint: The rational root test and the previous problem should help!)
5. Which of the above polynomials factor over $\mathbb{R}$? (Hint: your answer to this should be simple)
6. Check out the website `wolframalpha.com` and look at the graphs of the above polynomials and see if that matches with what you've seen.
7. Find the characteristic polynomial of

   $$(a)\ \frac{1-\sqrt{7}}{2} \quad (b)\ \frac{1+\sqrt{7}\,i}{2} \quad (c)\ \sqrt[3]{2} \quad (d)\ \sqrt{2}+\sqrt{3}i.$$

8. The polynomial x^n-1 always has 1 as a root. This means it factors as $(x-1)p(x)$.
   - What is $p(x)$?
   - When does x^n-1 have two real roots? Explain why if it does have another root r, $p(r)=0$ (where $p(x)$ is defined above.)
   - Can x^n-1 have more than two real roots?

11 Factoring Due November 16th

1. In calculus class, you learned about derivatives of differentiable functions. For polynomials it was easy to calculate what the derivative should be, and we saw that, for instance

$$\frac{d}{dx}x^n = nx^{n-1} \tag{1}$$

In algebra, where were might be working over some number system like $\mathbb{Q}$ or even $\mathbb{Z}_2$ talking about continuity, limits etc isn't really possible. So instead, we opt to use Equation 1 as a **definition** of the derivative of a polynomial. But wait - you ask - that only tells us how to take the derivative of something of the form x^n. That's true. So I'll also tell you that the derivative function is **linear** meaning that

$$\frac{d}{dx}(f+g) = \frac{d}{dx}f + \frac{d}{dx}g, \quad \frac{d}{dx}(cf) = c\frac{d}{dx}f, \quad c \text{ a constant.}$$

   (a) The Leibniz rule, that $\frac{d}{dx}(fg) = \frac{df}{dx}g + \frac{dg}{dx}f$ is of course true for polynomials (It's true for any differentiable function). Prove this in the case that $f(x) = ax^n + bx^2$ and $g(x) = cx^m + dx^2$. This is meant to give you an idea of how the general proof should go. Extra credit if you can write a complete proof of the Leibniz rule in general.

   (b) Now suppose $(x-r)^2$ is a factor of $f(x)$. When this happens, we say that r is a double root of $f(x)$. When this is true, show that r is a root of both $f(x)$ and $\frac{df}{dx}$.

   (c) Explain why the converse is also true. If r is a root of $\frac{df}{dx}$ and $f(x)$ then $(x-r)^2$ must be a factor of $f(x)$.

   (d) If $f(x) \in \mathbb{Q}[x]$ is the characteristic polynomial of α, prove that $(x-\alpha)^2$ does not divide $f(x)$. (Hint: think about the gcd of $f(x)$ and $\frac{df}{dx}$) The point of this problem is to show that in an irreducible polynomial there are no repeated roots.

2. In class we proved that $\mathbb{Z}_p$ was a field. Remember that earlier we used a different notation $\mathbb{Z}/p\mathbb{Z}$. The main important thing to prove was the existence of multiplicative inverses. Review the way we proved this, and then consider the following problem.

   We know that $\mathbb{Z}_n$ is not a field when n is not prime. But some of the elements in $\mathbb{Z}_n$ do indeed have multiplicative inverses. Use the style of proof you studied above to prove that if a is relatively prime to n then a has a multiplicative inverse, in $\mathbb{Z}_n$.

3. Using a calculator and the Euclidean algorithm, find the multiplicative inverse of 1027 in $\mathbb{Z}_{20317}$. Check your answer: Does 1027 times your inverse wind up being 1 mod 20317?

4. Prove that if n is not a prime number then $x^{n-1} + x^{n-2} + \cdots + x + 1$ is not a prime polynomial. Hint - think about how this polynomial came up in class.

5. Aaron's notes 8-4. I recommend going online to check with wolfram alpha. I'm mostly interested in knowing what test you are using to determine whether the polynomial is prime.

6. (optional) Aaron's notes 8-5. This is an optional problem - but it will be a potential problem for the final project so it's a good one to get started on.

7. (Extra credit) and potential final project question - it's easy to find the characteristic polynomials for say, $\sqrt{3}$ and $\sqrt[3]{5}$. But what about the number $\alpha = \sqrt{3} + 2\sqrt[3]{5}$? It's not even obvious that this is algebraic, let alone what its characteristic polynomial is! Try to find the characteristic polynomial of α (It's pretty hard!)

12 Field Extension, Finite Fields, Due November 30th

1. In words, describe how you could find a field with 7^8 elements. Do *not* actually try to find this.
2. What are the polynomial in $\mathbb{Z}_7[x]$ of the form $x^2 + a$ that are prime? (Hint: just write them all down and see which ones factor. Remember that a degree two polynomial will factor if and only if it has a root...) Use your work to write down a field that has 49 elements.
3. (Optional) Number 10-1 in Aaron's notes.
4. (Not optional) 10-4 in the notes (a),(b),(c)
5. (a) Prove that $f(x) = x^3 + 2x + 1$ is prime in $\mathbb{Z}_3[x]$.

   (b) Find the inverse of $x + 1$ in $\mathbb{Z}_3[x]_{f(x)}$.
6. Find the characteristic polynomial of $(1, 2\pi/10)$ and prove that it is prime. (Hint: You may want to use the irreducible polynomials pdf posted on Canvas)
7. Find the characteristic polynomial of $(1, 2\pi/8)$ and prove that it is prime.
8. What is the number of elements in $\mathbb{Z}_2[x]_{x^3+x+1}$?
9. Is $(1, 2\pi/5)$ a constructible number?
10. For which n can $\sqrt[n]{3}$ be constructed?
11. Given that the characteristic polynomial of $\alpha = \cos(2\pi/25) + \sin(2\pi/25)i$ is

$$f(x) = x^{20} + x^{15} + x^{10} + x^5 + 1.$$

    Explain why the number α cannot be constructed. Also, explain why this showed that a general angle cannot by "divided by 5" or "pentasected".
12. Prove that a 40 degree angle is not constructible.
13. (Optional) You might enjoy looking at the exercises for the final section of Aaron's notes

13 Exam 3 Info

The exam will have 6 questions and I will write it so that time will not be an issue. The questions below are meant to help you prepare for the exam. No calculators will be allowed.

13.1 Numbers 1 - 2

These problems will be computational. For instance, you might be asked:

- How do you know that $f(x) = x^3 + 2x^2 + 1$ is prime in $\mathbb{Z}_3[x]$. Hint: Think about roots, but do NOT use the rational root test - that only works in $\mathbb{Q}[x]$.
- How many elements are in the field $\mathbb{Z}_3[x]_{f(x)}$ if $f(x) = x^3 + 2x^2 + 1$?
- Is $\mathbb{Z}_2[x]_{x^2+1}$ a field? If so, how many elements does it have?
- What is the inverse of $x + 1$ in $\mathbb{Z}_3[x]_{f(x)}$?
- In $\mathbb{Q}[x]/(x^3 + x + 1)$ what is the inverse of $x - 2$? Simplify $x^4 + x$ in this ring by writing it in the form $ax^2 + bx + c$.
- Calculate the characteristic polynomial of the complex number $\alpha = (1; 2\pi/5)$? What about $\alpha = (1; 2\pi/6)$? Finally, what about $(1; 2\pi/8)$.
- If α is a root of $x^{10} - 5x^8 - 10x^5 + 15$ is α constructible with ruler and compass?
- If α is a root of $x^{10} - 5x^8 - 10x^5 + 15x$ is α constructible with ruler and compass? (Hint: the answer to these two questions is different!)

13.2 Numbers 3

This problem is about factoring over $\mathbb{Q}$. You will be given some polynomials and asked to factor them completely (or explain why they are prime)

- You should know how to use Eisenstein, Rational Root Test and reduction to mod p.
- I'll print out a list of some polynomials that are irreducible mod p for $p = 2$ and $p = 3$ which might be useful.
- One of the problems will involve Eisenstein in disguise. This is a problem where you will have to do a change variable, like $x \to x + 1$ before you use Eisenstein. To practice this, take a look at $x^4 + 1$ and $x^6 + x^3 + 1$.
- Know when the rational root test is sufficient to imply that a polynomial is prime.

13.3 Number 4

This problem will be about polynomials and factoring. It might involve something about when polynomials factor. For instance, if you have a polynomial $f(x) \in \mathbb{Q}[x]$ of degree two - when will it have two rational roots? Is it possible for it to only have one? Can one root be real and one root be complex (i.e. not real)? Can you find some values n such that the polynomial $x^2 + 100x + n$ factors over $\mathbb{Q}$. Can you find infinitely many values? For what n does this polynomial factor over $\mathbb{R}$ and finally what about over $\mathbb{C}$.

13.4 Number 5

Conceptual questions:

- For instance, let $f(x) \in \mathbb{Q}[x]$. If $[f(x)]$ is prime after we go modulo 2 does that mean that $f(x)$ is prime?
- Same question but with composite.
- True or false: If $f(x)$ is prime in $\mathbb{Q}[x]$ then so is $f(x + 1)$.
- True or false: If $f(x)$ is prime in $\mathbb{Q}[x]$ then so is $f(x^2)$.
- You will be asked to define one of: Algebraic number, characteristic polynomial of an algebraic number.

13.5 Number 6

Some questions about finite fields. You should know how to construct a field with p^n elements. For small p and n, you should be able to use your list of irreducible polynomials to write down explicit examples. For higher numbers, you might just have to write a sentence or two about what steps you would take. What is the inverse of 14 in $\mathbb{Z}_{31}$?