Honors Algebra II, Courant Institute, Spring 2022
http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2022/HonorsAlgebraII.html

Motivation

This first class is a combination of hints about algebraic reasoning and motivation for the subject.

Modern algebra is built on powerful abstract ideas. To understand how they work, you should have an idea what they're about. General algebraic structures, such as groups and vector spaces, all are generalizations of many different specific situations. You find your way around abstract objects by thinking about specific concrete realizations and looking for their "lifts" to abstract situations. Something may seem obscure in one situation but completely natural in another. The "big picture" is not just the sequence of definitions and theorems, but the specific problems that motivate them and their application to solving concrete problems.

1 Fermat's last theorem

Fermat's last theorem is a math problem that motivated much of present day abstract algebra, directly or indirectly.

Sometime in the late 1600's in southern France, a lawyer and amateur mathematician (Fermat) was reading 1500 year old book about numbers. The book described right triangles where the "squares" (geometric squares, not second powers of integers) had sides with integer lengths. The algebraic formulation $x^2 + y^2 = z^2$, with x, y, and z being integers, had been given more recently, in the early 1600's. There are many such triples, including *pythagorean triples*, including 3,4,5 (because $3^2 + 4^2 = 5^2$) and 5, 12, 13 (because $25 + 141 = 169$). As we will see, there is a formula for all pythagorean triples.

Fermat thought about this for a while and made a note to himself that this can't happen with powers higher than 2. The note said that are no triples $x^n + y^n = z^n$ with positive integers x, y, z and $n \geq 3$. It also said that he knew a proof, but the proof was not in the note. Today, the majority expert opinion is that Fermat found a mistake in his proof, but did prove it for $n = 4$, he wrote it down later, and possibly for $n = 3$. When Fermat died, his notes were found and published.

You can wonder why Fermat's "theorem" became a central problem of mathematics while other problems from that era didn't. The *Goldbach conjecture*, for example, is just as simple: every even number $n = 2k > 2$ may be written as a sum of two prime numbers: $n = p+q$ ($4 = 2+2$, $100 = 89+11 = 83+17 = \cdots$ (p and q are not unique), etc.). One reason, I think, is that there was always "progress" toward the Fermat theorem. It is possible to prove specific cases, and to "reduce" to problem to more general abstract problems that seem interesting in themselves. Work on the Fermat problem was incredibly interesting (to mathematicians) even if it didn't solve the Fermat problem.

Here is a simple illustration, a proof that if $x^4+y^4 = z^4$ with positive integers x and y, then x or y must be divisible by 5. We use the *little Fermat* theorem and modular arithmetic described in Subsection 1.1. It is a proof by contradiction. $a \not\equiv b$ We assume that $x \not\equiv 0$ and $y \not\equiv 0 \bmod 5$ and get a contradiction. If $x \not\equiv 0$ and $y \not\equiv 0 \bmod 5$, then $x^4 \equiv 1$ and $y^4 \equiv 1 \bmod 5$ (Fermat's little theorem). Therefore, $z^4 = x^4 + y^4 \equiv 1 + 1 \equiv 2 \bmod 5$. But the equation $z^4 \equiv 2 \bmod 5$ has no solutions. The little Fermat theorem implies that $z^4 \equiv 1$ (if $z \not\equiv 0$) or $z^4 = 0$ (if $z \equiv 0$) are the only possibilities. Exercise 1 takes reasoning like this a step further.

A *diophantine equation* is an equation involving powers of several integer variables. They are named for Diophantus (dead by 300 AD), the guy who wrote the book Fermat was reading. The theory of diophantine equations makes great use of modular arithmetic, prime factorization, and little Fermat. That's one of the reasons it gets so much attention in abstract algebra. This class will use the trick of reducing mod p a few times. One is for *Eisenstein's criterion* which is a way to find integer coefficient polynomials that cannot be factored over the integers (Chapter 12 in the text).

1.1 Modular arithmetic, Fermat's little theorem

First a review of modular arithmetic then the little theorem.

All numbers in this section are assumed to be integers. We say $a = b \pmod n$ if $a = b + kn$ for some (integer) k. This might be expressed in other ways, such as $a \equiv b \pmod n$, particularly when we need to distinguish between equal mod n and equal as integers. We often neglect to say "(mod) n" when it is clear in context. We will take for granted the basic facts of modular arithmetic: $a(b + c) = ab + ac$, if $a = b$ then $ac = bc$ and $a + c = b + c$ (all (mod) n). As an example, mod 4, $3 = -1$ so $3^2 = (-1)^2 = 1$. This might be simpler than $3^2 = 9 = 1 \pmod 4$.

Arithmetic mod p (a prime) is special because $ab = 0 \pmod p$ only if $a = 0$ or $b = 0$ (or both). This is not true otherwise (example mod $n = 6$: $2 \neq 0$ and $3 \neq 0$, but $2 \cdot 3 = 0$). This is a property of prime numbers emphasized in Section 11.1 of the Artin text: if p divides ab (meaning $ab = kp$ for some k), then p divides a or p divides b (or both). Also, "$a = 0 \pmod p$" and "p divides a" are equivalent, because both mean $a = kp$ for some k.

This fact about arithmetic mod p has a consequence that is used to understand arithmetic of non-zeros mod p. If you multiply by different numbers, you get different answers. More precisely, if $c \neq 0$ then $ac \neq bc$ if $a \neq b$. On the other hand, if $c = 0$ (always mod p), then $ac = bc = 0$ no matter what a and b are. Here's the reasoning: if $a \neq b$ then $a - b \neq 0$. If $c \neq 0$ then $(a - b)c \neq 0$. But remember that if $(a - b)c = ac - bc \neq 0$, then $ac \neq bc$. That's what we wanted to show. The text calls this the *cancellation property*: if $ac = bc$ and $c \neq 0$, then you can "cancel" c and get $a = b$.

The term "Fermat's little theorem" can refer to several related facts about powers mod p. One is that any integer x has $x^p = x \pmod p$. Take, for example,

$x = 10$ and $p = 7$. You get that ten million equals ten mod 7. I can check this using Python:

```
>>> 1428570*7 + 10
10000000
```

How did Fermat check it?

Another "little Fermat" fact is that if $x \neq 0 \pmod{p}$, then $x^{p-1} = 1 \pmod{p}$. This implies $x^p = x \pmod{p}$ because if $x \neq 0$ (leaving out "(mod p)" for simplicity) then $x^p = x \cdot x^{p-1} = x \cdot 1 = x$. We are taking for granted the basic facts of modular arithmetic: if $a = b$, then $ac = bc$ and $a+c = b+c$ (all (mod p)). On the other hand, if $x = 0$, then $x^p = 0 \cdot 0 \cdot \cdots = 0$, so again $x^p = x$. As examples, $10^6 = 1$ (mod) 7 (check: $1{,}000{,}000 - 1 = 999{,}999 = 142{,}857 \cdot 7$), and $47^7 = 0$. It matters that p is prime. It might not be true that $x^{n-1} = 1 \pmod{n}$ when $x \neq 0 \pmod{n}$ if n is not prime. For example, take $x = 2$ and $n = 6$. You can calculate that $x^{n-1} = 2^5 = 32 = 2 \neq 1 \pmod{6}$. In retrospect you didn't have to calculate: any power of 2 is even mod 6 so it can not equal 1. The two versions of little Fermat are equivalent. If $x \neq 0$ then the cancellation principle, applied to $x^p = x$ yields $x^{p-1} = 1$. Conversely, $x^{p-1} = 1$ then $x^p = x$.

Later in the course there will be a proof of little Fermat that explains "why it's true". The argument here is both clever and mysterious – a proof without enlightenment. Consider the product of all $p-1$ non-zero "residues" mod p. That is $R = 1 \cdot 2 \cdot \cdots \cdot (p-1)$. Let R_x be what you by multiplying each of these by x and then multiplying the whole thing together. Re-ordering the $p-1$ factors, you see that

$$\begin{aligned} R_x &= (1 \cdot x)(2 \cdot x) \cdot \cdots \cdot (p-1)x \\ &= x^{p-1} \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1) \\ R_x &= x^{p-1} R \, . \end{aligned}$$

On the other hand, no two residues xj and xk in the R product are equal. Indeed, if $j \neq k$ and both are among $\{1, 2, \cdots, p-1\}$, then $j \not\equiv k \pmod{p}$. Therefore (using the necessary hypothesis $x \not\equiv 0$), $xj \not\equiv xk$. Thus, the residues in the R_x product are a rearrangement of the residues in the R product. Example, with $x = 3$ and $p = 7$, the R_x product is

$$\begin{aligned} (x \cdot 1) \cdot (x \cdot 2) \cdot (x \cdot 3) \cdot (x \cdot 4) \cdot (x \cdot 5) \cdot (x \cdot 6) &= 3 \cdot 6 \cdot 9 \cdot 12 \cdot 15 \cdot 18 \\ &\equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \, . \end{aligned}$$

The last line is a re-arrangement of $R = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$. Now we have $R_x = x^{p-1}R$ and $R_x = R$. Together, these give $R = x^{p-1}R$. Exercise 2 fills in a small missing detail of this argument.

2 Primes in rings of algebraic integers

Euler (possibly Fermat before him, though without leaving a clear record) introduced a new method into algebraic number theory, as it's now called. He

worked with algebraic integers rather than the usual integers, now called *rational* integers. He used a *primitive cube root of unity*

$$\zeta_3 = e^{2\pi i/3} = -\frac{1}{2} + \frac{i\sqrt{3}}{2} \ , \ \ \zeta_3^3 = 1 \ .$$

He showed that

$$x^3 + y^3 = (x+y)(x+\zeta_3 y)(x+\zeta_3^2 y) \ . \tag{1}$$

This can be verified with direct calculations, You can compare this to the fancier, more general method of exercises 3 and 4.

Euler attacked the case $n = 3$ of Fermat's last theorem using the factorization. He showed that positive integers x, y, z cannot satisfy

$$(x+y)(x+\zeta_3 y)(x+\zeta_3^2 y) = z^3 \ .$$

For this, he used prime factorization in the ring $\mathbb{Z}[\zeta_3]$, which is the ring complex numbers $a + \zeta_3 b$ with a and b being rational integers. The notation $\mathbb{Z}[\zeta_3]$ will be explained next class. Euler and others made the mistake of thinking $\mathbb{Z}[\zeta_p]$, where $\zeta_p = e^{2\pi i/p}$ is a primitive p^{th} root of unity, also has unique factorization into primes. It usually doesn't.

To start, you can assume that the prime factorizations of x, y, and z have no primes in common. For example, if $x = pa$ and $y = pb$, and $x^3 + y^3 = z^3$, then you get $p^3a^3 + p^3b^3 = z^3$, so $z^3 = (a^3 + b^3)p^3$. This implies that the factorization of z also contains p, which can be written as $z = pc$. The p factors out, leaving $a^3 + b^3 = c^3$. This argument illustrates a way Fermat thought about what we now call "mathematical induction". You want to show that there are no numbers satisfying a certain relation. You argue by contradiction. If there are solutions, there must be a smallest solution. You get a contradiction by constructing a smaller solution. In this case, you start with x, y, z and you get a, b, c, which are smaller. The smallest $n = 3$ "Fermat triple" are mutually relatively prime.

Euler showed that the three factors $x + y$, $x + \zeta_3 y$ and $x + \zeta_3^2 y$ can be taken to be relatively prime in $\mathbb{Z}[\zeta_3]$. It is common to use π for a prime in $\mathbb{Z}[\zeta_3]$ and p for a rational prime. If $\pi \in \mathbb{Z}[\zeta_3]$ is a prime factor of $x + y$, then $x + y = \alpha\pi$, for some $\alpha \in \mathbb{Z}[\zeta_3]$. If the same π is a factor of $x + \zeta_3 y$, then $x + \zeta_3 y = \beta\pi$. You can eliminate y

$$\begin{aligned} x + \quad y &= \alpha\pi \\ x + \zeta_3 y &= \beta\pi \end{aligned}$$

$$\begin{aligned} \zeta_3 x + \zeta_3 y &= \zeta_3\alpha\pi \\ x + \zeta_3 y &= \beta\pi \end{aligned}$$

$$(\zeta_3 - 1)x = (\zeta_3\alpha - \beta)\pi$$

The right side at the end is the prime π multiplied by some (algebraic) integer in $\mathbb{Z}[\zeta_3]$. This shows that either π divides $\zeta_3 - 1$ or π divides x. A simpler

calculation leads to $(\zeta_3 - 1)y = (\beta - \alpha)\pi$. Therefore, if π does not divide $\zeta_3 - 1$, then π is a common factor in both x and y. This would imply (argument omitted) that x and y have a common rational prime factor, which would be a contradiction.

That leaves the possibility that π divides $\zeta_3 - 1$. We will not rule that out, but take it as an excuse to look more at primes and prime factorization in $\mathbb{Z}[\zeta_3]$. We show that $\zeta_3 - 1$ is prime. Observe that any $\alpha = a + \zeta_3 b \in \mathbb{Z}[\zeta_3]$ has square magnitude (as a complex number) that is an integer. For this calculation, we use the fact that $\overline{\zeta_3} = \zeta_3^2$. You can verify this by calculating:

$$\overline{\zeta_3} = \overline{e^{2\pi i/3}} = e^{-2\pi i/3} = e^{4\pi i/3} = \zeta_3^2 \; .$$

Or, you could just check

$$\overline{\zeta_3} = -\frac{1}{2} - \frac{i\sqrt{3}}{2} \; , \;\; \zeta_3^2 = \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2} \right)^2 = \frac{1}{4} - 2\frac{i\sqrt{3}}{4} - \frac{3}{4} = -\frac{1}{2} - \frac{i\sqrt{3}}{2} \; .$$

We also use the identity $1 + \zeta_3 + \zeta_3^2 = 0$, but in the form $\zeta_3 + \zeta_3^2 = -1$. Exercise 6 gives a proof that isn't direct verification. With this, we calculate and get an integer answer if a and b are rational integers:

$$\begin{aligned} |\alpha|^2 &= \alpha\overline{\alpha} \\ &= (a + \zeta_3 b)\overline{(a + \zeta_3)b} \\ &= (a + \zeta_3)(a + \zeta_3^2 b) \\ &= a^2 + (\zeta_3 + \zeta_3^2)ab + \zeta_3^3 b^3 \\ &= a^2 - ab + b^2 \; . \end{aligned}$$

Finally, you can calculate

$$\begin{aligned} |\zeta_3 - 1|^2 &= (\zeta_3 - 1)(\zeta_3^2 - 1) \\ &= \zeta_3^3 - \zeta_3 - \zeta_3^2 + 1 \\ &= 1 + 1 + 1 - (1 + \zeta_3 + \zeta_3^2) \\ &= 3 \; . \end{aligned}$$

This is a rational prime. If factors in $\mathbb{Z}[\zeta_3]$ as $\zeta_3 - 1 = \alpha\beta$, then either $|\alpha| = 1$ or $|\beta| = 1$.

Similar reasoning shows that $\zeta_3^2 - 1$ also is prime. It turns out to be essentially the same prime. We say that elements α and β are *associates* if $\alpha = u\beta$, where u is a unit. A unit is an invertible element. That is, u is a unit if there is a v with $uv = 1$. The units in $\mathbb{Z}$ are just ± 1, but other algebraic number rings have more. Most statements about factorization in algebraic number rings involve units. For example, α is *irreducible* if $\alpha = \beta\gamma$ only if β and/or γ is a unit. We would have to do this in $\mathbb{Z}$ also if we worked with positive and negative integers, not only positive ones. It turns out (Exercise 8) that $\zeta_3 - 1$ and $\zeta_3^2 - 1$ are

associates. This implies that $3 = u(\zeta_3 - 1)^2$, where u is a unit in $\mathbb{Z}[]\zeta_3]$. A prime ($p = 3$ in this case) that is a power of a prime in an algebraic number ring (up to a unit) is said to be *ramified*. Only finitely many primes are ramified in any algebraic number ring (famous theorem).

3 Exercises

1. Show that $x^4 + y^4 = w^2$ is impossible if $x \not\equiv 5$ and $y \not\equiv 5$. You can do this by looking at all possible values of w^2 mod 5. Fermat proved that $x^4 + y^4 = z^4$ is impossible among positive integers by showing that $x^4 + y^4 = w^2$ is impossible.

2. Prove that $R \not\equiv 0 \pmod{p}$. It may be easier to prove the more general fact that any product of non-zero residues mod p is non-zero. You know it's true for two factors. You can use induction to prove it for more than two factors.

3. Prove Euler's factorization formula (1). *Hint.* Let x be a fixed parameter and let $f(y)$ and $g(y)$ be the polynomials $f(y) = x^3 + y^3$ and $g(y) = (x + y)(x + \zeta_3 y)(x + \zeta_3^2 y)$, which are the left and right sides of the Euler formula (1). Show that $f(y) = g(y)$ when $y = -x$, $y = -\zeta_3 x$, $y = -\zeta_3^2 x$, and $y = 0$. If $x \neq 0$ (oops!, forgot that hypothesis, which is satisfied in the target formula (1) because x is a positive integer), this makes four distinct y values where $f(y) = g(y)$. But f and g are cubics, so . . . .

4. Suppose $n \neq 3$. Find the analogue of Euler's factorization (1) that works for n. This should lead you to define what is meant by a *primitive* n^{th} root of unity. For example, for $n = 4$, $\zeta = \pm i$ are primitive fourth roots but $\zeta = -1$ is not. Your formula should work only for primitive roots.

5. Suppose R is a ring and $S \subset R$. Suppose that S is closed under addition, multiplication and additive inversion. This means that if $x \in S$ and $y \in S$ then $x + y \in S$, $xy \in S$, and $-x \in S$. Finally, suppose 1_R (the multiplicative identity of R) is in S. Show that S is a ring. Show that $\mathbb{Z}[\zeta_3] \subset \mathbb{C}$ is closed under addition, multiplication, and additive inverse and contains the multiplicative identity. Conclude that $\mathbb{Z}[\zeta_3]$ is a ring. [*Note.* This $R \subset S$ approach may seem more complicated than direct verification that $\mathbb{Z}[\zeta_3]$ is a ring, which is simple. The only benefit is that you don't have to verify that addition and multiplication are associative and distributive.]

6. The numbers ζ_n^k are the roots of the polynomial $f(x) = x^n - 1$. Any polynomial may be expressed in terms of its roots using $f(x) = \prod(x - a_k)$. Show that $f(x) = x^n - (\sum a_k)x^{n-1} + \cdots$. Use this to show that the sum of the roots of unity is equal to zero without using complex numbers.

7. The set of units in a ring R is written R^* (or $R^\times$ or something similar). Show that R^* is an abelian group (easy). Suppose that $R^* = \mathbb{Z}[\sqrt{2}]$. Show

that $R^* \cong \mathbb{Z} \times \mathbb{Z}/(2)$. More concretely, show that $x \in R^*$ is a unit if and only if $x = \pm(1 \pm \sqrt{2})^n$ for some n. *Hints.* Suppose $x = a + \sqrt{2}b$. You can show that x is a unit if and only if $N(x) = (a + \sqrt{2}b)(x - \sqrt{2}b) = a^2 - 2b^2 = \pm 1$. This implies that a unit has $|a| \leq \sqrt{2}|b| + 1$. Show that $c + \sqrt{2}d = (1 \pm \sqrt{2})(a + \sqrt{2}b)$ may be chosen to have $|d| < |b|$ unless $b = 0$. Suppose r, a, and b are integers, and $a^2 - 2b^2 = r$. Explain how to generate an infinite set of integer solutions $c^2 - 2d^2 = r$ (same r).
Comments on this exercise.

(a) R^* is infinite, while the group of units in $\mathbb{Z}[\zeta_3]$ is isomorphic to $\mathbb{Z}/(6)$, in particular, finite.

(b) There is a better proof (more general, less ad-hoc) in the textbook that uses more information about the structure of $\mathbb{Z}[\sqrt{2}]$.

(c) Famous theorem of Minkowsky: the group of units in any ring of algebraic integers is finitely generated, not just quadratic number rings treated in the text. Chapter 14 of the text has a proof that a finitely generated abelian group is isomorphic to a product of finitely many factors, each factor being $\mathbb{Z}$ or $\mathbb{Z}/(n)$ for some n.

(d) $N(x)$ is the *norm* of x. Chapter 16 of the text defines $N(x)$ for a algebraic number field, if it's "complete" (technically, a Galois extension) as the product of the symmetric images of x under the Galois group: $N(x) = \prod \sigma(x)$, $\sigma \in \text{Gal}$. In our examples, Gal $\cong \mathbb{Z}/(2)$ with one element being the identity and the other being "conjugation", either $\sqrt{2} \to -\sqrt{2}$ or $\zeta_3 \to \overline{\zeta}_3$. This leads to $N(a + \zeta_3 b) = a^2 + b^2 - ab$. The formula for $N(x)$ depends on which extension it is in, but the formulas we used are always true: $N(x) \in \mathbb{Z}$ and $N(xy) = N(x)N(y)$ if x is an algebraic integer.

8. Show that the six units in $\mathbb{Z}[\zeta_3]$ have the form $e^{2\pi ik/6}$. Find formulas for them in terms of ζ_3 and ζ_3^2. Use the identity $\zeta_3^2 - 1 = (\zeta_3 - 1)(\zeta_3 + 1)$ to show that $\zeta_3^2 - 1$ and $\zeta_3 - 1$ are conjugate.

9. Tricks with polynomials can lead to interesting identities. Here are some involving arithmetic mod p.

(a) Let $f(X) = X^n + \cdots + a_0$ be a monic polynomial over a field $\mathbb{F}$. Suppose $a_k \in \mathbb{F}$ for $k = 1, \cdots, n$ are distinct ($a_j \neq a_k$ if $j \neq k$). Suppose that these are all zeros of f, which means $f(a_k) = 0$ for $1 \leq k \leq n$. Show that $f(X) = (X - a_1) \cdot \cdots \cdot (X - a_n)$. *Hint.* One way uses induction on n and polynomial division: $f(a) = 0$ implies that $f(X) = (X - a)g(X)$ with $\deg(g) = \deg(f) - 1$. *Warning.* It is possible for polynomials to have the same values without being equal as polynomials. A proof has to avoid this pitfall.

(b) Show that, in $\mathbb{F}_p$ (the finite field $\mathbb{Z}/(p)$).

$$X^{p-1} - 1 = \prod_{a \neq 0} (X - a) \; . \tag{2}$$

The product is over all non-zero residues in $\mathbb{F}_p$.

(c) Is this identity true in $\mathbb{Z}[X]$? *Hint.* Try it, maybe with $p = 3$.

(d) Use the identity in $\mathbb{F}_p$ to show that

$$S_1(p) = \sum_{k=1}^{p-1} k$$

is divisible by p. First prove it by comparing the coefficients of X^{p-1} on both sides of (2). Then prove it using the simple formula for the sum.

(e) Prove the formula $(p-1)! = -1 \pmod{\ } p$. Verify this explicitly for $p = 7$ (calculate $7! + 1$ and find a factor of 7).