# Class Lecture Notes for Math 305, Spring 2022

Dr Holmes

March 6, 2022

These are notes on what I say in class in Math 305.

## Contents

# 1 Tuesday, January 11, 2022

Administrative preliminaries.

I discussed the definitions of $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Z}^+$:

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of integers;

$\mathbb{N} = \{0, 1, 2, \ldots\}$, the set of natural numbers (there is no general agreement in mathematical literature as to whether 0 is a natural number, but this book includes it), or non-negative integers;

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, the set of positive integers. In all of these, the use of dots is really cheating: giving a rigorous definition of these sets is rather difficult, and we appeal instead to your pre-formal understanding of these concepts.

I stated a set of axioms for the integers which I will include here (based on the axioms in the Math 287 book with two alternative approaches to order).

We begin with a set of purely algebraic axioms. Our variables range over the set $\mathbb{Z}$ of integers; we assume special integers 0 and 1 and primitive operations or addition ($+$) multiplication ($\cdot$) and additive inverse ($-$, used as a prefix unary operator).

**commutative laws:** For any $x, y \in \mathbb{Z}$, $x + y = y + x$ and $x \cdot y = y \cdot x$.

**associative laws:** For any $x, y, z \in \mathbb{Z}$, $(x+y)+z = x+(y+z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. I should add that we are only allowed to write things like $x + y + z$ or $x \cdot y \cdot z$ because we know these operations are associative. In proofs in section 1.2 you should write parentheses, and explicitly use the associative laws to move them.

You *may* use standard order of operations and read $x \cdot y + z$ as meaning $(x \cdot y) + z$ wihtout writing out the parentheses (multiplication binds more tightly than addition, unary minus binds more tightly than either).

**distributive law:** For any $x, y, z \in \mathbb{Z}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

**identity laws:** For any $x \in \mathbb{Z}$, $x + 0 = x$ and $x \cdot 1 = x$. $0 \neq 1$.

**multiplicative cancellation:** For any $x, y, z \in \mathbb{Z}$, if $x \neq 0$ and $x \cdot y = x \cdot z$, then $y = z$. This amounts to the ability to divide both sides of an equation by the same thing, but we do not have a full division operation in the integers as we do in the rationals or reals.

This is not a full axiomatization of the integers. Of course, systems like the rationals and the reals which extend the integers satisfy these axioms, but there are also systems (even ones familiar to you) which satisfy these axioms and are quite different from the integers. Arithmetic mod $p$ where $p$ is prime satisfies these axioms, and the domain of "numbers" in mod $p$ arithmetic is finite (the remainders $0, 1, \ldots p - 1$ mod $p$).

Additional axioms appropriate for the integers which rule out the system described being modular arithmetic are axioms of order. We present these (just for fun) in two different ways.

We can axiomatize order by introducing the set of positive integers $\mathbf{Z}^+$ as a primitive notion, providing some of its properties as axioms, and using it to define order relations.

1. $0 \notin \mathbb{Z}^+$.
2. For each $m \in \mathbb{Z}$ with $m \neq 0$ either $m \in \mathbb{Z}^+$ or $-m \in \mathbb{Z}^+$.
3. For each $m, n \in \mathbb{Z}^+$, we have $m + n \in \mathbb{Z}^+$ and $m \cdot n \in \mathbb{Z}^+$
4. Define $m < n$ as $n + (-m) \in \mathbb{Z}^+$.

This is a very elegant set of axioms, and it should be straightforward for you to see that they are true in the familiar system of integers, but it may be less obvious that they are enough. This might be a homework exercise.

Here is a more familiar set of axioms for order. They do follow as consequences of the algebraic and positive integer axioms if we define $<$ as above, but for this approach we "forget" about $\mathbf{Z}^+$ and take $<$ as a primitive relation (and we define $\mathbb{Z}^+$ in terms of $<$).

**transitivity:** For any $m, n, p \in \mathbb{Z}$, if $m < n$ and $n < p$ then $m < p$.

**trichotomy:** For any $m, n \in \mathbb{Z}$, exactly one of $m < n, m = n, n < m$ is true.

**additive monotonicity:** For any $m, n, p \in \mathbb{Z}$, if $m < n$ then $m + p < n + p$.

**multiplicative monotonicity:** For any $m, n, p \in \mathbb{Z}$, if $p > 0$ and $m < n$, then $m \cdot p < n \cdot p$. Our axioms are enough to show that the right things happen if $p$ is zero or negative (that might be a homework exercise).

**definition of positive integers:** We define $\mathbb{Z}^+$ as $\{x \in \mathbb{Z} : 0 < x\}$.

I stated the Well-Ordering Principle and proved two sample theorems, "each positive integer is either even or odd", and "there is no integer strictly between 0 and 1".

If $S$ is a set of integers, $x$ is a smallest element of $S$ iff $x \in S$ and $(\forall y \in S : x \leq y)$. You could try proving that a nonempty set with a smallest element has just one smallest element.

**Well-Ordering Principle:** Any nonempty set $S$ of positive integers has a smallest element.

I proved a couple of sample theorems using the Well-Ordering Principle in class. Proofs using this principle are usually indirect (proofs by contradiction); pay attention to the logical structure of what I say.

**Definition:** An integer $m$ is even iff there is an integer $x$ such that $m = 2 \cdot x$.

An integer $m$ is odd iff there is an integer $x$ such that $m = 2 \cdot x + 1$.

**Theorem:** Each positive integer is either even or odd.

**Proof:** Suppose otherwise, so there are integers which are neither even nor odd. Let $S$ be the set of all integers which are neither even nor odd. By our assumption, it is nonempty, so by the Well-Ordering Principle it has a smallest element $w$. This number $w$ will be the smallest integer which is neither even nor odd.

The integer $w$ is not 1, because $1 = 2 \cdot 0 + 1$ is odd.

So $w - 1$ is a positive integer, and because it is less than $w$ it must be either even or odd.

If $w - 1 = 2 \cdot x$ is even, then $w = 2 \cdot x + 1$ is odd.

If $w - 1 = 2 \cdot x + 1$ is odd, then $w = 2 \cdot x + 2 = 2 \cdot (x + 1)$ is even.

In either case, we get that $w$ is either odd or even, which is a contradiction, so there can be no such $w$ and the theorem must be true.

**Observation:** At a crucial point in the argument above, I cheated (or at least I appealed to your intuition), and the fact is used is important and should be proved. How do I know that if $w \neq 1$ is a positive integer that $w-1$ is a positive integer? If we have $w > 1$, we do have $w-1 > 0$. We need to rule out the possibility that $0 < w < 1$ (which, since we know what the integers are, is hard to even take into account).

**Theorem:** There is no integer $x$ such that $0 < x < 1$.

**Proof:** If there is such an integer than the set $S = \{x \in \mathbb{Z} : 0 < x < 1\}$ is nonempty and so by the Well-Ordering Principle has a smallest element $w$.

So we have $0 < w < 1$. By multiplicative monotonicity (because $w > 0$) we have $0 < w^2 < w$ and of course we then have $0 < w^2 < w < 1$. Using transitivity we see that $0 < w^2 < 1$ and $w^2 < w$, so $w^2$ belongs to the set $S$ but is smaller than $w$, which is a contradiction.

# 2 Homework 1

This is being assigned on January 13 and is due January 20.

1. Prove all parts of proposition 1.2.8 in Crisman on properties of divisibility (this is on page 4 of Crisman).

2. Prove by mathematical induction that for every $n \in \mathbb{Z}^+$, $3|(n^3 + 5n)$.

3. Prove by mathematial induction that the sum of the first $n$ odd numbers is $n^2$. Make appropriate use of summation notation.

4. Use the first set of order axioms in these notes (in which the set of positive integers is primitive) along with the algebra axioms to prove at least two of the axioms in the second set of order axioms, in which the less-than relation is primitive (you will need to use the definition of the less-than relation given with the first set of axioms). Your algebra may be somewhat informal: your use of order axioms should be careful and explicit. Extra credit will be rewarded for proving more of the order axioms in the second set.

# 3 Thursday, January 13, 2022

We begin with the principle of mathematical induction.

Mathematical induction can be presented as a proof strategy.

**Goal:** Prove $(\forall n \in \mathbb{Z}^+ : P(n))$

**basis step:** Prove $P(1)$

**induction step:**

> **induction hypothesis:** Choose a natural number $k$ arbitrarily. Assume $P(k)$.
>
> **induction goal:** Prove $P(k+1)$ (under the assumption that $P(k)$ is true).
>
> If you succeed in proving the induction goal, assuming the induction hypothesis, you have proved $(\forall k \in \mathbb{Z}^+ : P(k) \to P(k+1))$.

If you complete both steps, you can conclude $(\forall n \in \mathbb{Z}^+ : P(n))$ by mathematical induction.

One can prove theorems by mathematical induction on $\mathbb{N}$ instead of $\mathbb{Z}^+$: in this case the basis step is to prove $P(0)$.

We give an example (which also illustrates nice tools for working with summation notation).

**Theorem:** The sum of the first $n$ squares of positive integers is $\frac{n(n+1)(2n+1)}{6}$, that is,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

**Proof:** We prove this by mathematical induction on $n$.

> **basis step:** Prove $\sum_{i=1}^{1} i^2 = \frac{(1)(1+1)(2\cdot 1+1)}{6}$
>
> $\sum_{i=1}^{1} i^2 = 1^2 = 1 = \frac{(1)(1+1)(2\cdot 1+1)}{6}$ (check)
>
> **induction step:** Choose a positive integer $k$ arbitarily.
>
> Assume (ind hyp) that $\sum_{i=1}^{k} i^2 = \frac{(k)(k+1)(2k+1)}{6}$
>
> The induction goal is to prove $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(k+2)(2k+3)}{6}$

Notice that in formulating the induction goal we allowed ourselves to do a little obvious algebra after replacing $k$ with $k+1$.
$\sum_{i=1}^{k+1} i^2 = [\sum_{i=1}^{k} i^2] + (k+1)^2$ (pulling out the last term) $= \frac{(k)(k+1)(2k+1)}{6} + (k+1)^2$ (by ind hyp: **ALWAYS highlight the use of the inductive hypothesis in any proof by induction**) $= \frac{(k+1)(k)(2k+1)+6(k+1)(k+1)}{6} = \frac{(k+1)((2k^2+k)+(6k+6))}{6} = \frac{(k+1)(2k^2+7k+6)}{6} = \frac{(k+1)(k+2)(2k+3))}{6}$ (check)

The proof by induction is complete.

I was impressed with success in Math 189 last term at teaching this general approach to proofs of statement involving summations, avoiding dots, which can cause various confusions.

Next, I lectured the equivalence of math induction to the well-ordering principle.

First assume the well-ordering principle and show that math induction follows:

**Given:**

**1.** $P(1)$

**2.** $(\forall k \in \mathbb{Z}^+ : P(k) \to P(k+1))$

**3.** the well-ordering principle

**Show:** $(\forall n \in \mathbb{Z}^+ : P(n))$

**note:** Convince yourself that if we complete this plan we really have shown that WOP does the work of math induction.

**Proof:** Suppose for the sake of a contradiction that $\neg(\forall n \in \mathbb{Z}^+ : P(n))$, so there is some $x$ a positive integer such that $\neg P(x)$. Let $S$ be the set of all $x$ such that $\neg P(x)$, which we see is nonempty and so by WOP has a smallest element which we will call $w$.

$w$ is not 1, because we have assumed $P(1)$. Thus $w > 1$ (here we are using the result proved above using WOP that there is no integer strictly between 0 and 1). Thus $w - 1 > 0$ is a positive integer. Thus we have $P(w-1)$, because $w$ is the smallest positive integer such that $\neg P(w)$. But plugging $w-1$ in for $k$ in $(\forall k \in \mathbb{Z}^+ : P(k) \to P(k+1))$

gives $P(w-1) \rightarrow P(w)$, and so since we have $P(w-1)$ and $P(w-1) \rightarrow P(w)$ we have (by the rule of modus ponens) $P(w)$, but this is a contradiction.

Thus our assumption that $\neg(\forall n \in \mathbb{Z}^+ : P(n))$ is incorrect, and we have $(\forall n \in \mathbb{Z}^+ : P(n))$

This completes the proof that the well-ordering principle implies the principle of mathematical induction.

Now we argue that the principle of mathematical induction implies the well-ordering principle.

**Given:**

**1.** $S$ is a nonempty set of positive integers

**2.** the principle of math induction

**Show:** $S$ has a smallest element.

**note:** Convince yourself that this proof plan really does show that the principle of math induction does the work of the well ordering principle, if we can carry it out.

**Proof:** Assume for the sake of a contradiction that $S$ has no smallest element. We will prove by induction that $S$ is empty, completing the desired contradiction.

We do not prove by induction that for every $n$, $n \notin S$: we prove the stronger statement that for every $n$, $(\forall m \in \mathbb{Z}^+ : m \leq n \rightarrow m \notin S)$: not only is $n$ not in $S$, but no smaller positive integer is in $S$. We will describe the strategy of strong induction of which this is an example in the last section of the notes for today.

The basis step for the induction is to show $(\forall m \in \mathbb{Z}^+ : m \leq 1 \rightarrow m \notin S)$: the only positive integer less than or equal to 1 is 1 itself, so all we have to show is $1 \notin S$, and this follows from the assumption that $S$ has no smallest element: if it contained 1, 1 would be its smallest element.

Choose an arbitrary positive integer $k$. Assume $(\forall m \in \mathbb{Z}^+ : m \leq k \rightarrow m \notin S)$ as our induction hypothesis. Our induction goal is to show that $(\forall m \in \mathbb{Z}^+ : m \leq k+1 \rightarrow m \notin S)$ If $m$ is an integer $\leq k+1$, it is either less than $k$ or equal to $k$, in which cases the induction hypothesis tells

us that $m \notin S$, or (final case to be checked) $m > k$. Now, because there is no integer strictly between 0 and 1, there is also no integer strictly between $k$ and $k+1$ (we could subtract $k$ from it to get between 0 and 1). Thus, since $m > k$ and $m \leq k+1$, $m$ is simply $k+1$. We can conclude $k+1 \notin S$, because if it were in $S$ it would be the smallest element of $S$, since we have shown that nothing less than $k+1$ can belong to $S$.

So we have shown by induction that for every positive integer $n$, $(\forall m \in \mathbb{Z}^+ : m \leq n \rightarrow m \notin S)$, but this immediately implies that for every positive integer $n$, $n \notin S$, so $S$ is empty, which is a contradiction.

This means that our assumption that $S$ has no smallest element must be false: it follows from the statements given that $S$ has a smallest element.

This completes the proof that the well-ordering principle follows from the principle of mathematical induction.

The final topic of this lecture was the method of strong induction. This is a version of mathematical induction with a stronger hypothesis which is sometimes useful. We will state it and prove a theorem as an example. We state but do not prove (it might be fairly easy to see from the proof of equivalence of ordinary math induction and the well-ordering principle) that strong induction is in fact precisely equivalent in strength to ordinary induction. But it is sometimes much more convenient.

We state strong induction as a strategy of proof.

**Goal:** Prove $(\forall n \in \mathbb{Z}^+ : P(n))$

**basis step:** Prove $P(1)$

**induction step:**

**induction hypothesis:** Let $k$ be an arbitrarily chosen positive integer. Assume $(\forall m \in \mathbb{Z}^+ : m \leq k \rightarrow P(m))$: instead of assuming just $P(k)$ we assume $P(1), P(2), \ldots, P(k)$. This is a stronger hypothesis, and this is why we call this method strong induction.

**induction goal:** Prove $P(k+1)$ under the assumption of the inductive hypothesis.

If you succeed in completing the basis and induction steps, you have proved $(\forall n \in \mathbb{Z}^+ : P(n))$ by strong induction.

Here is an important example. (I am not for the moment trying to expound this in terms of product notation as I suggested in class; I might do it later, but my brain is tired after writing these notes).

**Theorem:** Each integer $\geq 2$ is a prime or a finite product of primes.

**Proof:** we prove this by strong induction.

The basis step requires us to prove that 2 is a prime or a finite product of primes. 2 is a prime (check).

We choose an arbitrary positive integer $k \geq 2$. The induction hypothesis will be that for every positive integer $m \leq k$, $m$ is a prime or a product of primes.

The induction goal is to prove that $k+1$ is a prime or a finite product of primes.

By the law of excluded middle either $k+1$ is a prime (in which case we are done, as it is then a prime or a finite product of primes) or it is composite, in which case there are $a, b$ such that $2 \leq a, b \leq k$ and $ab = k+1$. Now by inductive hypothesis, each of $a, b$ is either a prime or a finite product of primes, so $ab$ is a finite product of primes. And this completes the proof of the theorem by strong induction.

# 4 Tuesday, January 19, 2022

Today I talked about the Division Algorithm and the Euclidean Algorithm (plain and extended). I talked about this off the top of my head, and I owe you a discussion of what this material looks like in Crisman and how it might differ from what I say.

**Theorem (division algorithm):** For each $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, there are unique determined integers $q$ and $r$ such that $a = bq + r$ and $0 \leq r < b$.

Of course "$q$" and "$r$" are hints: we give these variables these names because they suggest *quotient* and **remainder**.

We prove the theorem using the Well-Ordering Theorem (and it is a positive result, we are not arguing by contradiction!)

**Proof:** Define $S$ as the set $\{a - bq : q \in \mathbb{Z} \wedge a - bq \geq 0\}$. This is the set of candidates for the remainder $r$, as it were.

It is a set of nonnegative integers, so if it is nonempty it has a least element.

If $a \geq 0$, let $q = 0$ and we see that $a - bq = a \geq 0$, so $a \in S$ and $S$ is nonempty.

If $a < 0$ let $q = a$ and we see that $a - bq = a - ba = a(1 - b)$. $a$ is negative and $1 - b$ is nonpositive (since $b$ is positive), so $a(1 - b)$ is nonnegative, and so belongs to $S$, so $S$ is nonempty.

Define $r$ as the smallest element of $S$. There is a unique $q$ such that $r = a - bq$, so $a = bq + r$.

All that remains is to show $0 \leq r < b$. We know that $r \geq 0$ because $r \in S$. Notice that $a - b(q + 1)$ must be negative, because if it were nonnegative it would be an element of $S$ smaller than $r = a - bq$.

$a - b(q+1) = a - bq - b = r - b$ so we have $r - b < 0$ so $r < b$ completing the proof.

We still need to prove that $q$ and $r$ are uniquely determined. Suppose that $a = bq - r = bQ - R$ and $0 \leq r < R < b$.

Observe that $R - r = b(Q - q)$. Now $R - r < b$, and the only way for $b(Q - q) < b$ to be true is $Q - q = 0$, so $Q = q$. Then $r = a - bq = a - bQ = R$.

**Definition:** For $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$ define $a\texttt{div}b$ and $a \,\texttt{mod}\, B$ as the unique $q$ and $r$ whose existence is proved by the division algorithm.

**Observations:** Be careful with negative values of $a$. Notice that while $100 \,\texttt{div}\, 3 = 33$ and $100 \,\texttt{mod}\, 3 = 1$, it turns out that $100 \,\texttt{div}\, 3 = -34$ and $100 \,\texttt{mod}\, 3 = 2$.

It might not be obvious that we can compute `mod` with a simple calculator. But we can. For positive $a$, $a\texttt{div}b$ is easy to compute, by computing $\frac{a}{b}$ in floating point then dropping what is after the decimal point. Then $a \,\texttt{mod}\, b = a - b(a \,\texttt{div}\, b)$.

Now we prove the Euclidean Algorithm theorem, indicating the procedure for computing the greatest common divisor of two integers, and the extended

Euclidean Algorithm theorem which shows that the gcd of two integers is an integer linear combination of those two integers.

**Definition:** Recall that for integers $a, d$, $d|a$ means that there is an integer $x$ such that $dx = a$. We say that $d$ is a divisor of $x$.

**Definition:** $d$ is a *common divisor* of $a$ and $b$ iff $d|a$ and $d|b$.

**Lemma:** For any $a, b$ which are not both zero, there is a greatest common divisor of $a$ and $b$.

**Proof:** If $a$ is not zero, every divisor of $a$ is $\leq |a|$. Thus if we do not have $a = b = 0$, we have an upper bound on common divisors of $a$ and $b$.

Any nonempty set $S$ of integers which has an upper bound $B$ has a greatest element: this follows from the W.O.P: the set $S' = \{B - x : x \in S\}$ is a set of nonnegative integers so has a smallest element $B - x$ and this $x$ will be the largest element of $S$.

It follows that the set of common divisors of $a$ and $b$ has a largest element, unless $a = b = 0$, in which case all integers fall in the set of common divisors.

**Definition:** Except in the case $a = b = 0$, we define $\texttt{gcd}(a, b)$, for integers $a, b$ as the greatest common divisor of$a$ and $b$.

**Lemma:** $\texttt{gcd}(a, b) = \texttt{gcd}(|a|, |b|)$. This justifies restricting our attention for the rest of this discussion to nonnegative $a, b$.

**Lemma:** $\texttt{gcd}(a, 0) = a$ if $a > 0$. Obvious.

**Lemma:** $\texttt{gcd}(a, b) = \texttt{gcd}(b, a \texttt{ mod } b)$ if $a > b > 0$.

**Proof of Lemma:** Let $a > b > 0$. Let $q = a \texttt{ div } b$ and let $r = a \texttt{ mod } b$.

Since $r = a - bq$, any common divisor of $a, b$ is also a divisor of $r$ and so a common divisor of $b, r$.

Since $a = bq + r$, any common divisor of $b, r$ is also a divisor of $a$, and so a common divisor of $a, b$.

It follows that $\texttt{gcd}(a, b)$ and $\texttt{gcd}(b, a \texttt{ mod } b)$ are respectively the greatest element of one and the same set, so they are equal.

**Euclidean Algorithm:** Let $a > b \geq 0$. Define a finite sequence $E$ by $E_1 = a, E_2 = b$ and $E_{i+2} = E_i \,\texttt{mod}\, E_{i+1}$ if this is nonzero, and otherwise is undefined.

It is straightforward to see that this is a strictly decreasing sequence of positive integers, and so it must end: if it were infinite, its range would be a set of positive integers with no smallest elements.

Notice that it is straightforward by the previous Lemma and induction that $\texttt{gcd}(E_i, E_{i+1}) = \texttt{gcd}(E_1, E_2)$ for each $i$ for which these terms are defined. If $E_{i+1}$ is the last term, it goes evenly into $E_i$ (that is how the sequence stops) and so $E_{i+1} = \texttt{gcd}(E_i, E_{i+1}) = \texttt{gcd}(E_1, E_2) = \texttt{gcd}(a, b)$. So if one computes this sequence by repeated application of the mod operation, the sequence ends with the greatest common divisor of the two numbers with which you start.

**Extended Euclidean Algorithm:** For any $a > b \geq 0$ integers, there are integers $x, y$ such that $ax + by = \texttt{gcd}(a, b)$ [these integers $x, y$ are not unique, but the procedure we describe will give specifix $x, y$ that work).

**Proof:** Let $a > b > 0$. Compute the sequence $E$ just as above.

Notice that $E_{i+2} = E_i - (E_i \texttt{div} E_{i+1})E_{i+1}$.

Compute two new sequences

$X_1 = 1, X_2 = 0, X_{i+2} = X_i - (E_i \texttt{div} E_{i+1})X_{i+1}$. $Y_1 = 0, Y_2 = 1, X_{i+2} = Y_i - (E_i \texttt{div} E_{i+1})Y_{i+1}$.

Prove by induction that for each $i$ for which the terms of the sequences are defined, $E_i = aX_i + bY_i$:

This is obvious for $i = 1, 2$:

$aX_1 + bY_1 = a1 + b0 = a = E_1$. $aX_2 + bY_2 = a0 + b1 = a = E_1$.

Suppose it works for $i$ and $i + 1$: then it works for $i + 2$:

$aX_{i+2} + bY_{i+2} = a(X_i - (E_i \texttt{div} E_{i+1})X_{i+1}) + b(Y_i - (E_i \texttt{div} E_{i+1})Y_{i+1}) = (aX_i + bY_i) - (E_i \texttt{div} E_{i+1})(aX_{i+1} + bY_{i+1}) = [\texttt{ind} - \texttt{hyp}]E_i - (E_i \texttt{div} E_{i+1})E_{i+1} = E_{i+2}$.

So if $E_i$ is the last term of the sequence, we have $\texttt{gcd}(a, b) = E_i = aX_i + bY_i$.

We will spend time in class examining these formal proofs (I didn't give proofs in the first lecture, just built tables, but in fact I am saying basically the same thing).

I set up the main in-class example: compute $\texttt{gcd}(1024, 137)$ (other knowledge tells us this will be 1) and find $x, y$ so that $1024x + 137y = \texttt{gcd}(1034, 137)$, which we will find is 1.

| | $x$ | $y$ | $q$ |
|---|---|---|---|
| 1024 | 1 | 0 | |
| 137 | 0 | 1 | |
| 65 | 1 | $-7$ | 7 |
| 7 | $-2$ | 15 | 2 |
| 2 | 19 | $-142$ | 9 |
| 1 | $-59$ | 441 | 3 |

The first column is the sequence $E$, the second the sequence $X$, the third the sequence $Y$. The fourth column contains the quotients used.

The final result is that $\texttt{gcd}(1024, 137) = 1 = (-59)(1024) + (441)(137)$.

I provide a spreadsheet you can use to do these calculations, but you do need to know how to do them by hand with the assistance of a calculator.

# 5 Thursday, January 21, 2022

My apologies to the class for the initial disruption. I'm working with my technically minded son on getting a scheme for delivering Zoom sessions that will be useful to students out of class: and yes, he got the web cam software to work in a flash.

I talked through some topics in Crisman related to the Tuesday lecture.

I spent some time discussing the more formal way I presented the extended Euclidean algorithm in the notes: I said the same thing in the Tuesday lecture, but I did not define the sequences used in the formal presentation.

**Theorem:** If $\texttt{gcd}(a, b)$ is defined, then $\texttt{gcd}(a, b)$ is the smallest positive integer which can be written in the form $ax + by$ where $x$ and $y$ are integers (i.e, as an integer linear combination of $a$ and $b$.)

**Proof:** By the extended Euclidean algorithm theorem, $\texttt{gcd}(a, b)$ can be written in this form.

Now suppose that $w = ax + by$ for integers $x$ and $y$, and $w$ is positive. $\texttt{gcd}(a,b)|a$ and $\texttt{gcd}(a,b)|b$, so $\texttt{gcd}(a,b)|ax$ and $\texttt{gcd}(a,b)|by$ so $\texttt{gcd}(a,b)|ax + by = w$. A positive multiple of any integer $z$ must be $\geq z$ (can you prove this?) so $\texttt{gcd}(a,b) \leq w$, so $\texttt{gcd}(a,b)$ is the smallest positive number which can be expressed in the form $ax + by$.

**Definition:** The theorem that $\texttt{gcd}(a,b) = ax + by$ for some integers $x, y$ is called the Bezout identity. I learned this preparing for this class!

**Observation:** The $x, y$ in the Bezout identity are not unique (though there is a specific one we find with the extended Euclidean algorithm (EEA)). Suppose I want $ax + by = a(x + u) + b(y - v)$. For this to be true, it is sufficient for $au = bv$ to hold. $u = b$ and $v - a$ will work, giving $a(x + b) + b(y - a)$ with the same value as $ax + by$. For this to work, it is sufficient for $au = bv$ to be a common multiple of $a$ and $b$ and this may be less than the product $ab$: $b$ is not necessarily the smallest number that can be added to $x$ here, nor $a$ the smallest number that can be subtracted from $y$.

**Definition:** We say that $a$ and $b$ are *relatively prime* iff $\texttt{gcd}(a,b) = 1$. This is a familiar concept, but it probably wasn't defined in this exact way when you first encountered it.

**Theorem (Euclid's lemma):** If $p$ is a prime and $p|ab$ then either $p|a$ or $p|b$.

Study this proof. You might be asked to write it.

Either $p|a$, in which case we are done, or $p \not| a$.

So the rest of the argument is in the case $p \not| a$: we need to show that in this case $p|b$.

Because $p$ is prime, $\texttt{gcd}(p,a) = 1$, so there are integers $x, y$ such that $px + ay = 1$.

So $b = 1b = (px + ay)b = pxb + ayb$. $pxb$ is obviously divisible by $p$, $ayb$ is divisible by $p$ because $ab$ is divisible by $p$. Thus $b = pxb + ayb$ is divisible by $p$, which is what we needed to show.

**Prop 2.4.9 part 1:** Suppose $\texttt{gcd}(ab) = 1$. If $a|c$ and $b|c$ then $ab|c$ (this theorem shows that in this case $ab$ is the least common multiple of $a$ and $b$).

**Proof:** Suppose $\texttt{gcd}(ab) = 1$. Suppose $a|c$ and $b|c$. Our goal is to show $ab|c$.

Since $a|c$ we have $x$ such that $ax = c$. Since $b|c$ we have $y$ such that $by = c$. Since $\texttt{gcd}(ab) = 1$ we have $u$ and $v$ such that $au + bv = 1$. Now $c = 1c = (au + bv)c = auc + bvc = auby + bvax = ab(uy + vx)$ which is divisible by $ab$ by inspection, so $ab|c$, which is what we needed to prove.

**Prop. 2.4.9 part 2:** Suppose $\texttt{gcd}(ab) = 1$. Suppose $a|bc$. Then $a|c$.

Since $a|bc$ we have $bc = xa$ for some $x$. Since $\texttt{gcd}(ab) = 1$ we have $ay + bz = 1$ for some $y, z$. Thus $c = 1c = (ay + bz)c = ayc + bzc = ayc + bxa = a(cy + bx)$ which is divisible by $a$ by inspection, so $a|c$, which is what we need to show.

I was setting out to prove Prop 3.7.1 at the end of class. These notes may contain a proof of that theorem before Tuesday's class: keep an eye on them.

# 6 Homework 2, assigned 1/21/2022, due 1/27/2022

In section 2.5 in Crisman, problems 3, 5 (you may use my spreadsheet, but say how you did it), 6, 7, 8 (with no more than a simple calculator; of course I cannot stop you from using the spreadsheet to check, but you do need to know how to do this by hand for in-class tests), 10 (same remark as on 8), 15 (coprime is another word for "relatively prime"), 17, 20.

# 7 A Problem Solved: Pythagorean Triples

**Definition:** A *Pythagorean triple* is a triple of natural numbers $a, b, c$ such that $a^2 + b^2 = c^2$.

**Geometric Motivation:** For any Pythagorean triple $a, b, c$ , there is a right triangle with legs $a, b$ and hypotenuse $c$. The 3,4,5 Pythagorean triple can be used as a practical method to form a right angle.

**Example:** $3^2 + 4^2 = 5^2$

**Definition:** A *primitive Pythagorean triple* is a Pythagorean triple with no common factors other than 1.

**Motivation:** If $a, b, c$ are a Pythagorean triple and $d \neq 1$ is a common factor of $a, b, c$, so $a'd = a, b'd = b, c'd = c$, then $(a'd)^2 + (b'd)^2 = (c'd)^2$ implies $a'^2 + b'^2 = c'^2$ (divide both sides by $d^2$). If we further let $d$ be the greatest common divisor of $a, b, c$, then $a', b', c'$ will be a primitive Pythagorean triple. So if we know all the primitive triples, we can obtain all the triples by multiplying by constants.

**Lemma:** In a primitive Pythagorean triple $a, b, c$, the numbers $a, b$ will neither both be odd nor both be even.

**Proof:** if $a, b$ were both even, then $a^2 + b^2 + c^2$ would be even, so $c$ would be even and $a, b, c$ would not be a primitive triple.

If $a, b$ were both odd, then $a = 2x+1$, $b = 2y+1$, and since $a^2+b^2 = c^2$ would be even, $c^2$ and so $c$ are even, so we can set $c = 2z$. Now $a^2 + b^2 = (2x + 1)^2 + (2y + 1)^2 = 4x^2 + 4x + 4y^2 + 4y + 2$ is not divisible by 4, while $(2z)^2 = 4z^2$ is divisible by 4. But these two quantities are supposed to be equal. So this situation is impossible.

**Observations:** Let $a, b, c$ be a primitive Pythagorean triple. We may safely assume that $a$ is odd and $b$ is even (if not we could switch them), and $c$ is thus odd.

Since $a^2 + b^2 = c^2$ we have $a^2 = c^2 - b^2 = (c + b)(c - b)$.

$c + b$ and $c - b$ have no common factors. Both are odd numbers. If $d$ were a prime factor of both, $d$ would be odd and $d$ would also be a factor of $2c$ (their sum) and $2b$ (their difference) and so would be a factor of both $c$ and $b$ which is impossible as we have a primitive triple.

$a^2$ is a perfect square, so every prime in its factorization has an even exponent. Any prime which goes into $a^2$ goes into only one of $c + b$ and $c - b$, and in fact we can see that the exponent of each such prime must be the same as its exponent in the expansion of $a$, and so even. And so $c + b$ and $c - b$ are perfect squares.

Set $c + b = s^2$ and $c - b = t^2$. Notice that $s$ and $t$ have no common prime factors, as any common prime factor of these would be a common factor of $b$ and $c$ by reasoning already given.

Algebra gives $c = \frac{s^2+t^2}{2}$ and $b = \frac{s^2-t^2}{2}$. $a^2 = (c + b)(c - b) = s^2t^2$ so $a = st$.

**Theorem:** Every primitive Pythagorean triple is of the form $st$, $\frac{s^2-t^2}{2}$, $\frac{s^2+t^2}{2}$, where $\texttt{gcd}(s, t) = 1$ and $s, t$ are both odd.. Moreover, all such triples are primitive Pythagorean triples.

**Proof:** The first sentence has been shown to be true in the observations above. The second sentence requires slightly more work.

That for any $s, t$ at all ($s > t$, both odd or both even) $st$, $\frac{s^2-t^2}{2}$, $\frac{s^2+t^2}{2}$ is a Pythagorean triple is just algebra.

What remains is to shown that if $\texttt{gcd}(s, t) = 1$, then this triple is primitive. It is enough to show that $\frac{s^2-t^2}{2}$, $\frac{s^2+t^2}{2}$ have no common factors. Any prime common factor of these two numbers would be a prime factor of $s^2$, the sum of these two numbers, and $t^2$, their absolute difference. But any prime which goes into $s^2$ and $t^2$ also goes into $s, t$ (by the lemma on prime factorizations proved earlier), and $s, t$ have no common prime factor.

To my mind, this is an example of the fact that proofs in number theory are often rather odd and indirect. Others might not think so.

These notes are taken from a context where the usual results about prime factorizations were assumed. We will justify our appeals to prime factorizations using two specific facts, Prop 3.7.1 and 7.7.2 from Crisman. Notes on my proofs of these results will appear here later.

**Prop. 3.7.1:** If $a^2|b^2$ then $a|b$.

**Proof:** It isn't clear to me that my proof above uses this, but it is easy enough to prove.

We remark first that it is enough to prove this result when $\texttt{gcd}(a,b) = 1$: assume the theorem in this special case, let $a, b$ be general integers, and assume $a^2|b^2$. Then if $d = \texttt{gcd}(a,b)$, we have $a = a'd$ and $b = b'd$ (because $d$ goes into $a, b$) and we have $\texttt{gcd}(a', b') = 1$, because if $a'$ and $b'$ had a nontrivial common factor $k$, $kd > d$ would go into both $a'd = a$, and $b'd = b$, and $d$ is the greatest common divisor of $a$ and $b$. So we have $a'^2d^2|b'^2d^2$, from which we have $a'^2|b'^2$, from which we have $a'|b'$ by the special case of the Theorem, from which we have $a'd = a|b = b'd$.

Now we prove the special case. Suppose that $a^2|b^2$ and $\texttt{gcd}(a,b) = 1$. Then for suitable $x, y$ we have $ax + by = 1$ so we have $b = b1 = b(ax + by) = abx + b^2y$. $a$ goes into $abx$ by inspection and it goes into $a^2$ which goes into $b^2y$ by hypothesis.

**Prop. 3.7.2:** For any integers $a, b, c$, if $\texttt{gcd}(a,b) = 1$ and $ab = c^2$ then $a$ and $b$ are perfect squares.

**Proof:** We expect, in fact that $a = \mathbf{gcd}(a,c)^2$.

Certainly $\mathbf{gcd}(a,c)^2|c^2$. Equally clearly, $\mathbf{gcd}(a,c)^2$ is relatively prime to $b$, so it goes into $a$ by theorems already shown, since $ab = c^2$ and $a, b$ have no common factors. Thus $\mathbf{gcd}(a,c)^2|a$.

Now show that $a|\texttt{gcd}(a,c) = (ax + cy)^2$ for suitable $x, y$, $= a^2x^2 + 2acy + c^2y$, and $a$ goes into the first two terms by inspection and the last because $c^2 = ab$. So $a|\mathbf{gcd}(a,c)^2$.

Two positive integers which go into each other are equal.

I am proud of this proof, it is much better than the one in Crisman!

# 8 Everything you might want to know about primes. . .well, on day one: lecture of 1/27/2022

We discuss the important notions of prime and composite number.

**Definition:** A prime number is a positive integer with exactly two positive integer divisors.

**Observations:** Every positive integer $n$ has 1 and $n$ as divisors. If $n = 1$, this fails to meet our definition, so 1 is not prime. If $n > 1$, then $n$ has at least two positive integer divisors, and will be prime just in case it has no others. So the definition given is equivalent to "$n$ is prime iff $n > 1$ and has no factors other than 1 and itself."

**Definition:** A positive integer $n$ is composite iff there are integer $a, b$ with $1 < a \leq b < n$ and $ab = n$. Notice that 1 is not composite.

**Theorem:** Every natural number $n \geq 2$ can be expressed as a prime or a finite product of primes.

**Proof:** Use the Well-Ordering Principle, and argue by contradiction.

If there is an integer $w \geq 2$ which is neither a prime nor a finite product of primes, then there is a smallest one, because the set of such integers would be a nonempty set of positive integers, and so have a smallest element.

Suppose that the Theorem is false, so this $w$ exists.

$w$ is not 1 and is not prime, so there are $a, b$ with $1 < a \leq b < w$ and $w = ab$.

Since $a < w$ $b < w$ and $a$ and $b$ are both $\geq 2$ they are each either primes or finite products of primes. But then $ab = w$ is a finite product of primes, which is a contradiction.

**Corollary:** An immediate consequence is that any integer greater than one has at least one prime divisor.

**Theorem (Euclid?):** There are infinitely many prime numbers.

**Proof:** Suppose otherwise. Then there is a finite list $p_1, \ldots, p_n$ containing all primes. Define $P$ as $\prod_{i=1}^{n} p_i$. The integer $P + 1$ is greater than 1, so it has a prime factor $q$. There must be $j$ such that $q = p_j$. Now $q|P$ because $P$ is the product of all primes, and $q|(P+1)$ by choice of $q$, so $q|(P + 1) - P = 1$, and $q|1$ is absurd.

**comments:** This proof is so well-known and (relatively) simple that some have proposed that every educated person should know it.

Here is a subtler related result.

**Theorem:** There are infinitely many primes $p$ such that $p \texttt{ mod } 4 = 3$.

**Comments:** Obviously there are no primes $p$ such that $p \texttt{ mod } 4 = 4$, and only one (2) such that $p \texttt{ mod } 4 = 2$. If $p$ is an odd prime, it will either be of the form $4k + 1$ or the form $4k + 3$. It would seem natural that there are infinitely many primes of both kinds: this is much easier to prove for 3 than for 1.

**Lemma:** If $a \texttt{ mod } 4 = 1$ and $b \texttt{ mod } 4 = 1$ then $ab \texttt{ mod } 4 = 1$.

$(4x+1)(4y+1) = 16xy+4x+4y+1 = 4(4xy+x+y)+1$. The Division Algorithm theorem tells us that the remainder is uniquely determined.

If $a \texttt{ mod } 4 = 1$ and $b \texttt{ mod } 4 = 3$ then $ab \texttt{ mod } 4 = 3$.

$(4x+1)(4y+3) = 16xy+12x+4y+3 = 4(4xy+3x+y)+3$. The Division Algorithm theorem tells us that the remainder is uniquely determined.

If $a \texttt{ mod } 4 = 3$ and $b \texttt{ mod } 4 = 3$ then $ab \texttt{ mod } 4 = 1$.

$(4x + 3)(4y + 3) = 16xy + 12x + 12y + 9 = 4(4xy + 3x + 3y + 2) + 1$. The Division Algorithm theorem tells us that the remainder is uniquely determined.

**Corollary:** Any integer of the form $4k + 3$ must have a prime divisor of the form $4k + 3$.

**Proof:** Suppose otherwise. Then the integer in question would have a prime factorization in which every prime was of the form $4y+1$, and a product of numbers of this form is of the form $4k + 1$, not $4k + 3$.

**Proof of the Main Theorem:** Suppose that there are only finitely many primes $p_1, \ldots, p_n$ of the form $4k + 3$.

Define $P$ as $\prod_{i=1}^{n} p_i$.

Either $P \,\texttt{mod}\, 4 = 1$ or $P\texttt{mod4} = 3$.

In the first case $(P+2) \,\texttt{mod}\, 4 = 3$ so $P+2$ has a prime factor $q$ of the form $4x+3$, which goes into $P$ and $P+2$, so $q|2$, which is absurd, since $q$ is an odd prime.

In the second case, $(P+4) \,\texttt{mod}\, 4 = 3$ so $P+4$ has a prime factor $q$ of the form $4x+3$, which goes into $P$ and into $P+4$, and so goes into 4, which is absurd.

This can be proved, as a student noted, without cases. Notice that $4P-1 = 4(P-1)+3$ is of the form $4k+3$, so has a prime factor $q$ of the form $4x+3$, and we observe that $q|4P$ and $q|(4P-1)$ so $q|1$, which is absurd.

**Theorem:** Each positive integer can be expressed in exactly one way as the product of a nondecreasing sequence of primes.

**Proof:** The statement in terms of a nondecreasing sequence is meant to tell us what is meant by uniqueness of factorization: applications of the associative and commutative laws of multiplication do not give different factorizations.

We prove this by contradiction using the Well-Ordering Principle.

Suppose there is some $w = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$ where $p$ and $q$ are different finite nondecreasing sequences of primes. Then there is a smallest such $w$ by the W.O.P.

We argue that $p_1$ cannot be one of the $q_i$'s, say $q_j$. If it were, then $\frac{w}{p_1} = \prod_{i=2}^{n} p_i = \prod_{i=1 \wedge i \neq j}^{m} q_i$ would be both less than $w$ and would have two different prime factorizations, which is a contradiction. (Removing the same term from two nondecreasing sequences of integers which are distinct must give distinct sequences; otherwise, adding the same term back, necessarily in the same position because the order determines it, would give the same sequence).

Now we prove using Euclid's Lemma and induction, that $p_1 | \prod_{i=k}^{m} q_i$ for all $k$ for which this makes sense.

Basis: $p_1 | \prod_{i=1}^{m} q_i = w$.

Induction step: Suppose $p_1 | \prod_{i=k}^{m} q_i$. $\prod_{i=k}^{m} q_i = (q_k)^z \prod_{i=k+z}^{m} q_i$ for some $z$ with $q_{k+z} \neq q_k$ (I overlooked this in class, but so did everyone else) [or $\prod_{i=k}^{m} q_i = (q_k)^z$, in which case we have immediately that $p_1 \neq q_k$ does not go into it, contradicting the inductive hypothesis]. These two numbers, $(q_k)^z, \prod_{i=k+z}^{m} q_i$ are relatively prime, and $p_1$ goes into their product, so by Euclid's Lemma $p_1$ goes into one of the factors. But it does not go into $(q_k)^z$, so it must go into $\prod_{i=k+z}^{m} q_i$, and so it goes into $\prod_{i=k+1}^{m} q_i$, which can differ only in having more factors.

This completes the embedded induction proof.

So set $k = m$ and we have $p_1 | \prod_{i=m}^{m} q_i = q_m$, which is absurd. And this completes the proof.

# 9 Homework 3, posted 1/28/2022, due one week from 1/27/2022

Homework 3: Use the results proved in class to describe at least five distinct primitive Pythagorean triples; do problems 14, 18, 19 on p. 34 in Crisman; as an extension of problem 19 look for patterns as to which numbers in a PPT can be divisible by 5 (for this, at least display some results of investigation; I'll be impressed if you can prove something). On p. 75 do problems 2,5,10,12,13. I like problem 20 on the next page; I'm not requiring it but Ill award EC if you do it.

# 10 Modular arithmetic lectured, Feb 1 and 3

We begin by defining the congruence relation.

**Definition (congruence mod m):** Let $m > 1$ and let $x, y$ be integers. We say $x \equiv y \bmod m$, or compactly $x \equiv_m y$, just in case $m|(x - y)$.

**Theorem:** $x \equiv y \bmod m$ if and only if $x \bmod m = y \bmod m$.

**Proof:** I suggest that you try to write the proof. It follows from the Division Algorithm theorem. You have to show the implication in both directions.

**Theorem:** $\equiv_m$ is an equivalence relation.

**Proof:** We need to prove that this relation is reflexive, symmetric, and transitive.

Let $m > 0$. Let $x, y, z$ be arbitrarily chosen integers.

We want to show $x \equiv_m x$. This means $m|(x - x)$ which is equivalent to $m|0$, which is true.

We want to show that if $x \equiv_m y$ then $y \equiv_m x$. Assume that $x \equiv_m y$. This means $m|(x - y)$ and thus for some integer $k$, $x - y = km$. But then $y - x = (-k)m$, so $m|(y - x)$, so $y \equiv_m x$.

We want to show that if $x \equiv_m y$ and $y \equiv_m z$, $x \equiv_m z$ follows. Suppose $x \equiv_m y$ and $y \equiv_m z$. Then $m|(x - y)$ and $m|(y - z)$. It follows that $m|((x - y) + (y - z))$ and $(x - y) + (y - z) = x - z$ so $m|(x - z)$ so $x \equiv_m z$.

The proof is complete.

**Theorem:** $\equiv_m$ respects addition and multiplication in the sense that if $x \equiv_m x'$ and $y \equiv_m y'$ we have $x + y \equiv_m x' + y'$ and $x \cdot y \equiv_m x' \cdot y'$.

**Proof:** Suppose $x \equiv_m x'$ and $y \equiv_m y'$. This is equivalent to there being integers $u$ and $v$ such that $x' = x + um$ and $y' = y + vm$.

Then $x'+y' = (x+um)+(y+vm) = (x+y)+m(u+v)$, so $x+y \equiv_m x'+y'$.

and $x' \cdot y' = (x+um)(y+vm) = x \cdot y+m(xv+yu+uvm)$, so $x \cdot y \equiv_m x' \cdot y'$.

This allows us to make addition and multiplication tables for mod $m$ arithmetic, with just the finite system of "numbers" from 0 to $m - 1$.

The interpretation of these "numbers" admits two possibilities: we can interpret them as congruence classes of integers, that is, equivalence classes under $\equiv_m$, or as the remainders on division by $m$. Either approach works. The numbers may be called residues, if we think of them as remainders, or residue classes, if we think of them as equivalence classes.

For mod 4 arithmetic, we have

| $+$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

as the addition table. Notice that each number has an additive inverse. This is not surprising as the original system of integers on which this is based has additive inverses. In general, the addition inverse of $a$ mod $m$ is $m - a$. For example the additive inverse of 3 mod 10 is 7.

For mod 4 arithmetic, we have

| $*$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

Notice that the facts about multiplication of numbers of the forms $4k+1$ and $4k + 3$ which we used in theorems proved earlier are encoded in this table.

Notice that we do not have multiplicative inverses for all nonzero numbers in this system: we have $x$ such that $3x = 1$ and $x$ such that $1x = 1$ but no $x$ such that $2x = 1$. We do not have multiplicative inverses in the integers, so this is not surprising.

If we look at the multiplication table for mod 5 arithmetic, something unexpected happens.

| $*$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

Each nonzero residue has a multiplicative inverse: the recprocal of 1 is 1, of 2 is 3, of 3 is 2, of 4 is 4.

This is surprising: the system ends up looking more like the rationals than like the integers.

There is a theorem of course

**Theorem:** For each residue $a$ in mod $m$ arithmetic, there is an $x$ such that $ax \equiv_m 1$ if and only if $\texttt{gcd}(a, m) = 1$.

**Proof:** If $ax \equiv_m 1$ then $ax - 1$ is divisible by $m$, so any common divisor of $ax$ and $m$ would also be a divisor of 1, so certainly $a$ and $m$ have no nontrivial common factors.

If $\texttt{gcd}(a, m) = 1$ then there are integers $x$ and $y$ such that $ax + my = 1$, so for this $x$, $ax \equiv_m 1$.

This doesnt quite say that if $\texttt{gcd}(a, m) = 1$ implies that $a$ has a multiplicative inverse mod m. The proof of this is completed by the following observation:

**Theorem:** For each residue $a$ in mod $m$ arithmetic, if $\texttt{gcd}(a, m) = 1$ and $ax \equiv_m ay$ (and so in particular if $ax = ay = 1$, which implies $\texttt{gcd}(a.m) = 1$) then $x \equiv_m y$.

**Proof:** If $\texttt{gcd}(a, m) = 1$ and $ax \equiv_m ay$, then $m|a(x - y)$, and then by theorems proved above, $m|(x - y)$, since $m$ is relatively prime to $a$, and so $x \equiv_m y$.

This has the incidental effect that the multiplicative inverse of $a$ in mod m arithmetic, if it exists, is unique (up to congruence mod m). More generally, it is a version of the cancellation property of multiplication.

**Definition:** We say that $a^{-1}$ `mod` $m$ is the unique remainder mod m such that $ax \equiv_m 1$, if it exists.

**Observation:** If $p$ is prime, $a^{-1}$ `mod` $p$ is defined for each $a$ such that $a \not\equiv_p 0$. That is, modular arithmetic mod $p$ satisfies the multiplicative inverse property.

**Proof:** We have shown above that $a^{-1}$ `mod` $m$ is defined iff $a$ and $m$ are relatively prime. A prime $p$ is relatively prime to any $a$ unless $p|a$, that is, $a \equiv_p 0$.

And this is surprising. This means in effect that division is defined in the mod p integers, whereas it is not defined in the integers as usually understood.

In general, it should be easy to convince yourself that for any m, mod m arithmetic inherits from the integers the commutative, associative and distributive laws, the identity laws. and additive inverses. It does not inherit the zero factor property: you might want to work out why the fact "if $ab = 0$ then $a = 0$ or $b = 0$" which is true in the integers does not carry over to mod m arithmetic unless m is prime. And the fact that the multiplicative inverse property characteristic of the rationals holds in mod p arithmetic is a surprise.

What mod m arithmetic does not have which distinguishes it from the arithmetic of the integers is order properties.

**Example:** Compute $12^{-1}$ `mod` 137.

Use the usual Euclidean algorithm calculation (my table) to find $x$ and $y$ so that $137x + 12y = 1$, so $12y \equiv_{137} 1$.

We get $(137)(5) + 12(-57) = 1$, so $y$ is to be $-57$...but the additive inverse of 57 in mod 137 arithmetic is 137-57 = 80, the answer. You will need to make this last move about half the time.

It is wise to check that $(80)(12)$ `mod` 137 is indeed 1.

## 10.1 Exponentiation

It is not the case that exponentiation respects congruence mod m. That is, it is not true in general that if $x \equiv_m y$ and $r \equiv_m s$ that $x^r \equiv_m y^s$. It *is* true that if $x \equiv_m y$ then $x^r \equiv_m y^r$ : this is true by repeated application of the fact that congruence respects multiplication.

Nonetheless, the pattern continues that we can efficiently compute congruence facts about large numbers by ignoring everything about them but their remainder mod m.

**Algorithm (modular exponentiation):** To compute $x^r \bmod m$, first compute $x^{r\mathtt{div}2} \bmod m$. Then if $r \bmod 2 = 0$, $x^r \bmod m = (x^{r\mathtt{div}2})^2 \bmod m$ and if $r \bmod 2 = 1$, $x^r \bmod m = ((x^{r\mathtt{div}2})^2 \cdot x) \bmod m$, in either case a small multiplication problem mod m.

This is a recursive computation: at the basis, note that we can certainly compute $x^1 \bmod m$.

In practice, I execute the algorithm by making a list of exponents obtained by starting with $r$ and successively dividing by 2, throwing away remainders, then computing the powers from 1 upward.

**Example:** Compute $32^{1153} \bmod 100$. 100 is a convenient modulus just because it is easy to take remainders on division by 100.

| | |
|---|---|
| 1153 | $76^2 \cdot 32 = 184832 \equiv 32$ |
| 576 | $76^2 = 5776 \equiv 76$ |
| 288 | $76^2 = 5776 \equiv 76$ |
| 144 | $76^2 = 5776 \equiv 76$ |
| 72 | $76^2 = 5776 \equiv 76$ |
| 36 | $24^2 = 576 \equiv 76$ |
| 18 | $32^2 = 1024 \equiv 24$ |
| 9 | $76^2 \cdot 32 = 184832 \equiv 32$ |
| 4 | $24^2 = 576 \equiv 76$ |
| 2 | $32^2 = 1024 \equiv 24$ |
| 1 | 32 |

This turned out to be a rather special example, but the pattern should be clear enough. This is known as the method of repeated squaring (with addition of an extra copy of the base at odd exponents). The number of multiplications is roughly proportional to the log base 2 of the exponent, so this will handle very large exponents with computer support (hundreds of digits are no challenge).

I'll add more notes here about Fermat's Little Theorem, $a^{p-1} \equiv_p 1$ for $p$ prime, and the way it allows much simpler computation of exponentials. I do not think it figures in your homework.

## 10.2 The Linear Congruence Theorem

In this section we look at the precise conditions under which a linear congruence

$$ax \equiv b \bmod m$$

has a solution and how many solutions it has.

First of all, we can apply the results about multiplicative inverses in moduli to solve a special case.

**Theorem:** If $\gcd(a, m) = 1$ then

$$ax \equiv b \bmod m$$

has exactly one solution $x$.

**Proof:** $\gcd(a, m) = 1$ then $a^{-1} \bmod m$ exists, which we will just write $a^{-1}$.

$ax \equiv_m b$ implies $a^{-1}ax \equiv_m a^{-1}b$ which implies $x \equiv_m a^{-1}b$. And further, $a(a^{-1}b) \equiv_m b$ is true. So there is exactly one solution for $x$, that is $(a^{-1} \bmod m) \cdot b$.

We now consider the general situation.

**Convention:** In everything that follows until the main theorem is proved, let $d = \gcd(a, m)$.

**Lemma:** If $d \not| b$, then there is no solution $x$ for $ax \equiv b \bmod m$.

**Proof:** If $ax \equiv_m b$ then $b = ax + km$ for some integer $k$ and so since $d|a$ and $d|m$ we have $d|b$. We have proved $ax \equiv_m b \rightarrow d|b$, from which the contrapositive $d \not| b \rightarrow ax \not\equiv_m b$ follows.

**Lemma:** If $d|b$ then there is at least one solution to $ax \equiv b \bmod m$.

**Proof:** If $d|b$ then all of $\frac{a}{d}, \frac{m}{d}, and \frac{b}{d}$ are integers, and $\gcd(\frac{a}{d}, \frac{m}{d}) = 1$, so there is a unique solution $x$ to $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{m}{d}$. For this $x$, we have $\frac{a}{d}x + k\frac{m}{d} = \frac{b}{d}$ for some integer $k$, so we have $ax + km = b$, so $ax \equiv_m b$.

**Main Theorem:** Let $m > 0$. Let $a, b$ be integers. Let $d = \gcd(a, b)$. If $d \not| b$ then $ax \equiv_m b$ has no solutions. Otherwise this equation has $d$ solutions.

**Proof:** Let $x$ be the unique solution to $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{m}{d}$. We know that $ax \equiv_m b$. Suppose $ay \equiv_m b$. It follows that for some $k$, $ay + km = b$. Thus $\frac{a}{d}y + k\frac{m}{d} = \frac{b}{d}$ so $\frac{a}{d}y + k\frac{m}{d} = \frac{b}{d}$, so $\frac{a}{d}y \equiv_m \frac{b}{d} - k\frac{m}{d}$. This calculation is reversible: a solution of this equation for any $k$ is a solution of the original equation. For each $k$, this equation has exactly one solution, because $\frac{a}{d}$ is relatively prime to $m$. And $k\frac{m}{d} \equiv_m k'\frac{m}{d}$ just in case $k \equiv k' \bmod d$, so there are in effect $d$ possible values for $k$, and so $d$ solutions to the original equation up to congruence.

I was having difficulty with details of this last proof under the influence of muscle relaxant on Thursday; I will be lecturing it and giving numerical examples for computation on Tuesday.

# 11 Abstract algebra definitions lectured, Feb 3

I have nothing particular of my own to say about these definitions yet. I may soon revisit this and write more notes.

The definition of group on pp. 33-4 was lectured, and some theorems on p 36 (Props 3.17-18, uniqueness of the identity and the inverse). Examples given after the definition may be instructive.

The definition of ring on p. 191 was lectured. The definitions of extensions of this notion listed at the bottom are important. Notice that the integers are a ring but not a field (because not a division ring) and the integers are an integral domain (because they do satisfy the zero factor theorem). Notice that mod p arithmetic gives a field, surprisingly, but that mod m arithmetic where m is composite gives a commutative ring which is not an integral domain (the zero factor theorem fails).

I will be happy to take questions about the questions from Judson which I ask, which are occasions for mathematical exploration.

I also may well settle down later and expand this section. I'm tired out from all the stuff I wrote about modular arithmetic!

# 12 Homework 4, due Feb 10

Homework 4: p.47 Crisman, 2, 3, 7, 12, 18, 19, p. 62 6, 10, 11, 13 (you can ask for others from 8-13), Judson, p. 40 problem 2, Judson, p. 205 problem 1 (do at least four parts)

# 13 Notes on the Linear Congruence Theorem and the Chinese Remainder Theorem, Feb 8 and Feb 10 2022

## 13.1 What are the numbers of modular arithmetic?

First, I am going to chat a little about what the objects are in mod m arithmetic.

Mod $m$ arithmetic is a finite system, with objects we usually refer to as $0, 1, \ldots, m-1$. There is some creative ambiguity in what these objects actually are.

They could be viewed as the remainders on division by $m$ (which are also called residues mod $m$). In this case, when we compute $p+q$ in mod $m$ arithmetic, we are computing $(p+q) \,\texttt{mod}\, m$ in the ordinary sense, in order to be sure our answer is a remainder, and similarly for subtraction, additive inverse and multiplication (but **not** for multiplicative inverse or division).

They could be viewed as equivalence classes of integers under the relation of congruence mod $m$. In this case, we would understand $p$ and $q$ in mod $m$ arithmetic as shorthand for $\{p+km : k \in \mathbb{Z}\}$ and $\{q+km : k \in \mathbb{Z}\}$ (where $p$ and $q$ are the integers of the same name) and when we compute $p+q$ in mod $m$ arithmetic, we are adding elements of the sets: $\{(p+km)+(q+k'm) : k, k' \in \mathbb{Z}\}$ is exactly the same set as $\{((p+q) \,\texttt{mod}\, m)+km : k \in \mathbb{Z}\}$ (writing this out shows me what a complicated idea it is that I am asking you to accept!)

In general, which approach we are using does not make any difference. When we say that an integer $x$ is to be "identified" with $p$ in the sense of modular arithmetic we can be taken as saying either that $x \,\texttt{mod}\, m = p$ (if $p$ is understood as a remainder on division by $m$) or that $x \in p$ if $p$ is understood as the equivalence class $\{p+km : k \in \mathbb{Z}\}$ where $p$ is the integer of the same name). The operations of modular arithmetic behave in the same way under either understanding.

## 13.2 The Linear Congruence Theorem, again

I recapped the proof of this via a series of lemmas. Some of these lemmas are theorems in their own right.

**Lemma 1:** Let $m > 0$. Let $a$ be a residue mod $m$ (recall that this just means, a remainder mod $m$, so $0 \leq a < m$). Suppose that $\texttt{gcd}(a, m) = 1$. Then there is a unique residue $b$ mod $m$ such that $ab \equiv_m 1$.

**Proof:** Because $\texttt{gcd}(a, m) = 1$, there are integers $x, y$ such that $ax+my = 1$. Notice that $ax \equiv_m 1$ follows. So $x \,\texttt{mod}\, m = b$ gives a residue $b$ such that $ab \equiv_m 1$ as desired.

But we need to show that there is only one. Suppose that $ax \equiv_m ay \equiv_m 1$, so $x \,\texttt{mod}\, m$ and $y \,\texttt{mod}\, m$ are both candidates to be the $b$ we are looking for. Then $m|(ax - ay)$ so $m|a(x - y)$ so by Euclid's Lemma $m|(x - y)$ so $x \equiv_m y$ so $x \,\texttt{mod}\, m = y \,\texttt{mod}\, m$: there is only one residue $b$ with the desired property.

**Definition:** Let $m > 0$. Let $a$ be a residue mod $m$. Define $a^{-1} \,\texttt{mod}\, m$ as the unique residue $b$ such that $ab \equiv_m 1$.

**Obervation:** It isn't part of the theorem stated above, but it is worth observing that if $\texttt{gcd}(a, m) = d > 1$ then there can be no $b$ such that $ab \equiv_m 1$. We would have $ax + my = 1$ for some integers $x, y$ and then $ax + my = 1$ divisible by $d$, which is absurd. So $a^{-1} \,\texttt{mod}\, m$ is defined if and only if $a$ and $m$ are relatively prime.

**Lemma 2:** Let $m > 0$. Let $a$ be a residue mod $m$ which is relatively prime to $m$. Let $b$ be a residue mod $m$. Then there is exactly one residue $x$ mod $m$ such that $ax \equiv_m b$.

**Proof:** Since $a$ is relatively prime to $m$, $a^{-1} \,\texttt{mod}\, m$ exists; we will write it just $a^{-1}$. So $a(a^{-1}b) \equiv_m (aa^{-1})b \equiv_m 1b \equiv_m b$, so $x = a^{-1}b \,\texttt{mod}\, m$ is a solution of $ax \equiv_m b$.

Now suppose that $x$ is any solution of $ax \equiv_m b$. It follows that $a^{-1}(ax) \equiv_m a^{-1}b$, and $a^{-1}(ax) \equiv_m (a^{-1}a)x \equiv_m 1x \equiv_m x$, so $x \equiv_m a^{-1}b$, and we see that $a^{-1}b \,\texttt{mod}\, m$ is the only residue which can be a solution to the equation (there are many integers $x$ such that $x \equiv_m a^{-1}b$, but of these only $a^{-1}b \,\texttt{mod}\, m$ is a remainder on division by $m$).

**Lemma 3:** Let $m > 0$. Let $a$ and $b$ be residues mod $m$ and let $d = \texttt{gcd}(a, m)$. Then $ax \equiv_m b$ has a solution $x$ if and only if $d|b$.

**Proof:** Suppose $d|b$. We have $a = a'd$ and $b = b'd$ and $m = m'd$ with $\texttt{gcd}(a', m') = 1$ (if $a'$ and $m'$ had a nontrivial common factor $e$, verify that $de > d$ would be a common factor of $a$ and $m$). Thus by Lemma 2 there is a unique residue $x$ mod $m'$ such that $a'x \equiv_{m'} b'$. For some integer $k$, $a'x+km' = b'$ by this last congruence. But then $a'dx+km'd = b'd$, that is, $ax + km = b$, so $ax \equiv_m b$. So if $d|b$ there is a solution to the congruence.

Suppose there is a solution $x$ to $ax \equiv_m b$. Then $ax + km = b$ for some integer $k$. $d|ax$ because $d|a$, and $d|km$ because $d|m$, so $d|ax + km$, so $d|b$.

So we have shown that $\texttt{gcd}(a, m)|b$ if and only if there is a solution to $ax \equiv_m b$.

**Linear Congruence Theorem:** Let $m > 0$. Let $a$ and $b$ be residues mod $m$ and let $d = \texttt{gcd}(a, m)$. Then there are exactly $d = \texttt{gcd}(a, b)$ solutions to $ax \equiv_m b \,\texttt{mod}\, m$.

Let $a'd = a, b'd = b, m'd = m$, as in the previous problem. Let $x$ be the unique solution to $a'x \equiv_{m'} b'$.

Any solution to $ax \equiv_m b$, say $y$, has $a(x - y) = a'd(x - y)$ divisible by $m = m'd$, so $a'(x - y)$ divisible by $m'$. This means that $x \equiv_{m'} y$.

Any $y$ of the form $x + m'k$ actually is a solution: we have $ax + um = b$ for some $u$, so we have $b = a(x + m'k) - am'k + um = a(x + m'k) - a'mk + um[\texttt{note}\, am' = a'm] \equiv_m a(x + m'k)$.

Any $y$ of the form $x + m'k$ has to be congruent mod $m$ to some $x + m'k$ with $0 \leq k < d$: any larger or smaller number of the form $x + m'k$ we can convert to this form by adding or subtracting some multiple of $m'd = m$. And no two of these numbers are congruent mod $m$, because any two of them differ by less than $m'd = m$. So we have exactly $d$ solutions, the remainders $x + m'k \,\texttt{mod}\, m$ for $k$ ranging from 0 to $d - 1$.

We give three examples.

1. Solve the linear congruence

$$16x \equiv_{120} = 20$$

No solution, because the gcd of 16 and 120 is 8, which does not go into 20.

2. Solve the linear congruence

$$77x \equiv_{120} n = 20$$

Use the Euclidean spreadsheet, or, better, build the table by hand, to find that $(-34)(120)+(53)(77) = 1$, so $(53)(77) \equiv_{120} 1$, so $77^{-1}\texttt{mod}120 = 53$.

Without any calculation, Lemma 1 or the full congruence theorem tells us there is one solution up to congruence mod 120.

Now compute the solution: multiply both sides of the congruence by 53 to get

$$77x \equiv_{120} n = 20$$

implies

$$(53)(77)x \equiv_{120} n = (20)(53)$$

which implies

$$x \equiv_{120} (20)(53)\texttt{mod}120 = 100$$

Lets check: indeed $(77)(100)\texttt{mod}120 = 20$.

3. Solve the linear congruence

$$65x \equiv_{120} 20$$

Notice that the gcd of 65 and 120 is 5, so we expect to find 5 solutions.

We begin by dividing through by the gcd.

so we are solving $13x \equiv_{24} 4$

The spreadsheet (or the manual table computation which I strongly suggest to you) will give $(6)(24) + (-11)(13) = 1$ so $(-11)(13) \equiv_{24} 1$, so $24 - 11 = 13 = 13^{-1}\texttt{mod}24$ (a numerical coincidence, 13 is its own inverse mod 24).

Thus

$$(13(13)x \equiv_{24} (13)(4) = 4$$

[multiplication by 13 didn't do much, this is a weird example]

so the only solution to $13x \equiv_{24} 4$ up to congruence mod 24 is 4 (check: $(13)(4)\texttt{mod}24 = 4$.

So the solutions to the original congruence are of the form $4 + 24k$, and these numbers are $4, 28, 52, 76, 100$ (we stop before 120 because we are looking for residues). We suggest carrying out the check for two of these as verification.

## 13.3 The Chinese Remainder Theorem

The Chinese Remainder Theorem allows us to solve simultaneous equations of the form $x \equiv_{m_1} a_1; x \equiv_{m_2} a_2; \ldots; x \equiv_{m_k} = a_k$ as long as for any $1 \leq i < j \leq k$ we have $\texttt{gcd}(m_i, m_j) = 1$.

We indicate how to solve this when there are two equations.

Suppose $\texttt{gcd}(m, n) = 1$. We want to find an $x$ such that $x \equiv_m a$ and $x \equiv_n b$. We show that we can find such an $x$, and moreover that the solution is unique up to congruence mod $mn$.

We will mix things up a little and show the uniqueness first. Suppose that $x \equiv_m a$ and $x \equiv_n b$ and $y \equiv_m a$ and $y \equiv_n b$ ($x$ and $y$ are both solutions to the system of equations). Then $m|(x-y)$ and $n|(x-y)$. But this implies, by a result already shown, that since $m, n$ are relatively prime, $mn|x-y$, so $x \equiv_{mn} y$. It should be clear that if $x \equiv_m a$ and $x \equiv_n a$ and $y \equiv_{mn} x$, then also $y \equiv_m a$ and $y \equiv_n b$. So the solution set we are looking for, if it exists, will simply be a congruence class mod $mn$ (or a remainder mod $mn$ if we think of it in that style).

Now we argue that there is a solution. Since $x \equiv_m a$, we have $x = a + km$ for some integer $k$. Thus, if $x$ is a solution we must have $a + km \equiv_n b$. This gives us $km \equiv_n b - a$. This gives us the solution $k = (b-a)(m^{-1}\texttt{mod}n)$.

We plug this back into our equation for $x$ to get $x = a + (b-a)(m^{-1}\texttt{mod}n)m$. Clearly $x \equiv_m a$, because $(b-a)(m^{-1}\texttt{mod}n)m$ is a multiple of $m$. Further, $x \equiv_n b$ because $(m^{-1}\texttt{mod}n)m \equiv_n 1$ so $x = a + (b-a)(m^{-1}\texttt{mod}n)m \equiv_n a + (b-a)(1) = b$.

We actually compute solutions by using the extended Euclidean algorithm to compute multiplicative inverses.

Solve the simultaneous equations

$$x \equiv_{11} 3$$

$$x \equiv_{18} 4$$

for $x$.

It is strategically better to use the larger of the two moduli for the first step.

$x = 4 + 18k$ for some integer $k$

so $4 + 18k \equiv_{11} 3$

so $18k \equiv_{11} -1 \equiv_{11} 10$

Now we need $18^{-1}\texttt{mod}11$ which simplified immediately to $7^{-1}\texttt{mod}11$

$(2)(11)+(-3)(7)=1$ (use the spreadsheet, but really you should do this manually for test practice) so $7^{-1}\texttt{mod}11=-3\texttt{mod}11=8$.

Now we multiply both sides of the last congruence by 8 to get $x \equiv_{11} (8)(7)x \equiv_{11} (8)(100) \equiv_{11} 80\texttt{mod}11 = 3$

so $k=3$ works

so $x=4+(18)(3)=58$

Let's check

$58\texttt{mod}11=3$

$58\texttt{mod}18=4$

as desired

The solution is unique up to congruence mod $(11)(18)=198$ so the general solution is $58+198k$.

Another solution would be 58+198 = 256. Feel free to check.

# 14 Homework 5, due Feb 17 (accepted late within reason)

Homework 5 (officially due on the 17th as usual, but likely to be accepted late within reason): Crisman p. 61 4 (I really like this; it might be very easy for you, or not), 14, 16, 17, 18, 19, 20, 21 (the rest being pleasantly computational)

# 15 Week 7 notes: a coming attraction, I hope to have them up by the 27th

## 15.1 More about modular arithmetic, theorems of Legendre, Wilson, and Fermat

Before the test, we proved that in any prime modulus, a polynomial of degree $d$ has no more than $d$ roots (Legendre's theorem).

A polynomial of degree $d$ is a function $P(x)=\Sigma_{i=0}^{d}a_ix^i$ (where we stipulate that $x^0=1$ for all $x$, including 0, and we provide that $a_d \not\equiv_p 0$).

At the basis, we have already shown that $ax \equiv_p b$ has exactly one solution if $a \not\equiv_p 0$, the solution being $x=a_p^{-1}b$ (we adopt the abbreviation $a_p^{-1}$ for

$a^{-1}\mathtt{mod}p$). This shows the result for degree 1 polynomials.

Suppose we have shown the result for all polynomials of degree $\leq d$. Let $P(x)$ be a polynomial of degree $d+1$. If $P(x)$ has no roots at all, we have that $P(x)$ has $\leq d+1$ roots, and we are done. So suppose that $P(r) \equiv_p 0$ for some root r. For any root $x$ of $P$ we would have $P(x) = P(r)$ so $\prod_{i=1}^{d+1} a_i(x^i - r^i) = 0$. Now for any $i > 0$, $x^i - r^i = (x-r)\prod_{j=0}^{i-1} x^j r^{(i-1)-j}$. For $i = 0$ the term $a_i(x^i - r^i) = 0$. So, we can express $P(x) - P(r)$ as $(x-r)Q(x)$, where the degree of $x$ is less than or equal to $d$, by factoring $x - r$ out of each term as indicated. Any root of $P(x) = 0$ is also a root of $P(x) - P(r) = (x-r)Q(x) = 0$, and so by the Zero Factor Theorem (which does hold in prime moduli) must either be equal to $r$ or a solution of $Q(x) = 0$, and by ind hyp $Q(x) = 0$ has no more than $d$ solutions, so $P(x) = 0$ has no more than $d+1$ solutions.

After the test, I discussed Wilson's theorem and Fermat's little theorem in modular arithmetic, then switched gears to abstract algebra.

**Wilson's Theorem:** If $p$ is prime, $(p-1)! \equiv_p -1$.

**Proof:** Suppose that $p$ is prime.

$(p-1)! = 1 \cdot \Pi_{i=2}^{p-2} i \cdot (p-1)$

$p - 1 \equiv_p -1$ of course.

The idea of the proof is that $\Pi_{i=2}^{p-2} i$ can be reorganized in a way which makes it clear that it is congruent to 1. Each $a$ between 2 and $p-1$ has $a^{-1}\mathtt{mod}p$ defined and also between 2 and $p-2$ inclusive. Moreover, for each such $a$, $a \neq a^{-1}\mathtt{mod}p$, because if $a = a^{-1}\mathtt{mod}p$, it follows that $a^2 \equiv_p 1$, and when $p$ is prime the only solutions to this equation are congruent to 1 or $p-1$. So $\Pi_{i=2}^{p-2} i$ can be reorganized into a product of pairs of numbers which multiply to values congruent to 1 mod $p$, and so the entire product is $\Pi_{i=2}^{p-2}$ congruent to 1 mod $p$.

$\Pi_{i=2}^{p-2} i = \Pi_{2 \leq i \leq p-1, (i^{-1}\mathtt{mod}p) > i} i \cdot (i^{-1}\mathtt{mod}p) \equiv_p \Pi_{2 \leq i \leq p-1, (i^{-1}\mathtt{mod}p) > i} 1 = 1$

Just for laughs, I provide actual summation notation for this argument. It is tricky.

So $(p-1)! = 1 \cdot \Pi_{i=2}^{p-2} i \cdot (p-1) \equiv_p 1 \cdot 1 \cdot -1 = -1$

**Inverse of Wilson's Theorem:** If $m = 4, (m-1)! \equiv_m 2$; for composite $m > 4$, $(m-1)! \equiv_m 0$.

**Proof:** That $(4-1)! = 6 \equiv_4 2$ is immediate.

> If $m > 4$ is composite, then $m = ab$ for some $2 \leq a, b \leq m-1$. If $a \neq b$, then both $a$ and $b$ appear as factors in $(m-1)! = \Pi_{i=1}^{m-1} i$, and so $ab = m | (m-1)!$ so this is congruent to 0 mod $m$. If $a$ and $b$ cannot be chosen to be distinct, then $m = p^2$ for some prime $p$ greater than 2, and so both $p$ and $2p$ appear as factors in $(m-1)! = \Pi_{i=1}^{m-1} i$, so $2p^2 = 2m | (m-1)!$ which is again congruent to 0 mod $m$.

This seems to give us a fine test for primality: unfortunately, there is no easy way to compute $(m-1)! \mathtt{mod} m$ for very large $m$ that we know of.

**Fermat's little theorem:** If $p$ is prime and $p \not| a$, $a^{p-1} \equiv_p 1$.

**Proof:** The product of all nonzero residues mod $p$ is $(p-1)!$.

> The product of all numbers $ai$ where $i$ is a nonzero residue mod $p$ is $a^{p-1}(p-1)!$.
>
> The second product is congruent mod $p$ to the product of all numbers $ai \mathtt{mod} p$, where $i$ is a nonzero residue mod $p$.
>
> But the product of all numbers $ai \mathtt{mod} p$ for $i$ a nonzero residue mod $p$ is also $(p-1)!$, because each nonzero residue $i$ mod $p$ is of the form $aj \mathtt{mod} p$ where $j$ is the nonzero residue $(a_p^{-1} i) \mathtt{mod} p$: the third product is the product of exactly the same numbers as in the first product, in a different order. So $a^{p-1}(p-1)! \equiv_p (p-1)!$, from which it follows that $a^{p-1} \equiv_p 1$ (because $(p-1)!$ is certainly not congruent to 0 mod $p$, so it has a multiplicative inverse; not to mention that we know from the previous theorem that it is in fact congruent to $-1$; so it can be cancelled)

**Corollary:** For any prime $p$ and any nonnegative integers $a, b$,

$$a^b \equiv_p (a \mathtt{mod} p)^{(b \mathtt{mod} (p-1))}.$$

This gives a much simpler method of computing large powers in arithmetic mod $p$ where $p$ is prime than repeated squaring.

## 15.2 Initial steps in abstract algebra

I may do infill in these notes as we go forward (add more detail to text I have already written).

**Definition:** A *group* is a set $G$ equipped with an operation $\circ : (G \times G) \to G$ with the following properties:

**associativity:** For any $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$

**identity:** There is an element $e$ of $G$ such that for any $a \in G$, $e \circ a = a \circ e = a$. Such an element $e$ is called an identity for the group.

**inverse:** For any identity $e$ of the group and for any element $a$ of $G$, there is an element $b$ of the group such that $a \circ b = b \circ a = e$.

**Theorem:** The identity element in a group is unique.

**Proof:** Suppose that for all $a \in G$, $e \circ a = a \circ e = a$, and also for all $a \in G$, $e' \circ a = a \circ e' = a$. It follows that $e \circ e'$ is equal both to $e$ and to $e'$, and so $e = e'$.

**Theorem:** For each $a \in G$ there is exactly one $b \in G$ such that $a \circ b = b \circ a = e$.

**Proof:** Suppose $a \circ b = b \circ a = e$ and $a \circ c = c \circ a = e$. It follows that

$b = b \circ e$ identity

$= b \circ (a \circ c)$ hypothesis

$= (b \circ a) \circ c$ associativity

$= e \circ c$ hypothesis

$= c$ identity

So there is only one inverse of $a$.

**Definition:** For each $a \in G$ we define $a^{-1}$ as the unique inverse of $a$.

**Abelian groups:** Notice that the group operation is not assumed to be commutative. If a group $G$ in addition satisifies the property "for all $a, b \in G$, $a \circ b = b \circ a$, we say that the group is *abelian*.

**Examples:** The integers or the rationals or the reals with addition as the operation make up a group. Why do the natural numbers not make up a group?

The nonzero rationals or reals with multiplication as the operation make up a group.

The residues mod $n$ (or the congruence classes mod $n$) make up a group, usually called $\mathbb{Z}_n$, with addition (mod $n$) as the operation.

The residues mod $n$ *which are relatively prime to* $n$ make up a group, which we call $U_n$, with multiplication (mod $n$) as the operation.

These are all abelian groups.

The symmetries of a triangle, discussed at length in the book, make up a group, which is our first example of a nonabelian group.

The permutations of an $n$ element set (with composition as the operation) make up a group called $S_n$ which has $n!$ elements and is nonabelian.

Matrices with nonzero determinants make up a nonabelian group (under matrix multiplication).

**Notational conventions:** We may use the usual notation for multiplication for a group, writing $ab$ instead of $a \circ b$, and possibly writing 1 instead of $e$ for the identity.

We may use additive notation, usually for an abelian group, writing $a + b$ for $a \circ b$, writing 0 for the identity and $-a$ for the inverse.

**Solving equations:** For any $a, b \in G$, the equations $ax = b$ and $xa = b$ have unique solutions.

**Proof:** We prove only the first statement. Notice that $a(a^{-1}b) = (aa^{-1})b = eb = b$, so $x = a^{-1}b$ is a solution. Now suppose that $ax = b$. It follows that $a^{-1}(ax) = a^{-1}b$ and $a^{-1}(ax) = (a^{-1}a)x = ex = x$, so i$x = a^{-1}b$, which we see is the only solution.

**Cancellation:** for any $a, b, c \in G$, if $ac = bc$ then $a = b$, and if $ca = cb$, then $a = b$.

**Proof:** In short, multiply both sides by the inverse.

**Definition (powers or multiples);** Define $g^n$ (or $ng$ if using additive notation) so that $g^0 = e$, and for positive integers $n$, $g^{n+1} = g^n g, g^{-n} = (g^n)^{-1}$.

**Theorems:** Certain familiar properties of exponents hold. We can prove $g^{m+n} = g^m g^n$ and $(g^m)^n = g^{mn}$ for $g$ any group element and $m, n$ any integers.

One thing we absolutely cannot count on is $g^n h^n = (gh)^n$: this only works if the group is abelian.

We suggest as an exercise if you haven't been assigned it already to show that if this identity holds for all $g, h, n$ that the group is actually abelian. Hint: it is enough for $(ab)^2 = a^2 b^2$ to hold for all $a, b$: use cancellations to show that this implies $ab = ba$.

A theorem which we proved in class is that $(ab)^{-1} = b^{-1}a^{-1}$ (*not* $a^{-1}b^{-1}$)

**Definition (subgroup):** If $G$ is a group and $H$ is a subset of $G$, we say that $H$ is a subgroup of $G$ if $H$ with the restriction of the same operation used on $G$ is a group.

**Theorem:** Let $G$ be a group with operation $\circ$. $H$ with the restriction of the operation $\circ \cap (H \times H)$ is a group iff for each $a, b \in h$, $a \circ b \in h$, and the identity $e \in H$, and for each $a \in H$, $a^{-1} \in H$.

**Theorem:** Let $G$ be a group with operation $\circ$. $H$ with the restriction of the operation $\circ \cap (H \times H)$ is a group iff $H$ is nonempty and for any $a, b \in H$, we have $ab^{-1} \in H$.

**Definition and Theorem:** Let $G$ be a group. Define the cyclic subgroup generated by $a$ as $\{a^n : n \in \mathbb{Z}\}$. The cyclic subgroup is a subgrup of $G$ (this is the theorem part). The size of the cyclic subgroup generated by $a$ we call the *order* of $a$ (this is either a positive integer or infinite).

**Theorem:** Cyclic subgroups are abelian groups.

**Definition:** If $G$ is a group and $a \in G$ and the cyclic subgroup generated by $a$ is all of $G$, we say that $G$ is a cyclic group and that $a$ is a generator of $G$.

# 16 Homework 6

Homework 6: Crisman, 7,7 exercises starting p. 89, 7, 9; Judson, 3.5 exercises starting p. 40, problems 5, 6 (remember, this is residues mod 12 that are relatively prime to 12 under multiplication), 7, 28, 31 (think about uniqueness of inverses), 32 (prove the contrapositive), 4.5 exercises starting p. 55, problem 1abc, 3 bg, 5.

# 17 March 1: Cyclic Groups and the Circle Group in the complex numbers

Let $G$ be a group (use multiplicative notation) and $a$ an element.

We define the cyclic subgroup of $G$ generated by $a$ as $\{a^k : k \in \mathbb{Z}$.

We show first that the cyclic subgroup generated by $a$ actually is a subgroup of $G$.

To show that it is a subgroup we need to show that it is closed under the operation: this follows from the theorem $a^k \cdot a^l = a^{k+1}$: if $x$ and $y$ are in the cyclic subgroup, then for some integers $k, l$, $x = a^k$, $y = a^l$, and so $x \cdot y = a^{k+l}$, and so $x \cdot y$ is a "power: of $a$ and belongs to the cyclic subgroup. We need to show that it contains the identity: $a^0 = e$. We need to show that if $x$ is in the subgroup, so is $x^{-1}$: If $x = a^k$, $x^{-1} = a^{-k}$ and so is also in the subgroup.

We argue that the cyclic subgroup generated by $a$ is a subset of every subgroup of $G$ which contains $a$. The lemma needed for this is that if $a \in H$, a subgroup of $G$, it follows that $a^k \in H$ for each integer $k$. You should be able to prove this lemma (by induction for positive integers and negative integers separately, with attention to how it is defined for negative integers). I rewrote my formal definition of powers in groups above to facilitate this.

We say that the order of a group is simply the size of the group (the cardinality of the set of group elements). We say that the order of an element of a group is the order of the cyclic subgroup it generates. We say that a group $G$ is a cyclic group iff it has an element $g$ such that the cyclic subgroup of $G$ generated by $g$ is $g$ itself. We then call $g$ a generator of $G$. If $G$ is a finite group, $g \in G$ is a generator of $g$ iff the order of $g$ in $G$ is $|G|$. This isn't true for infinite groups: the cyclic subgroup of the integers generated by 2 is the same size as the set of integers, but it is not the whole set, so 2 is not a generator of the integers.

Every cyclic group is abelian. This is because $a^k \cdot a^l = a^{k+l} = a^{l+k} = a^l \cdot a^k$. (I do suggest proving the exponent properties of powers by induction from the definition on your own).

This means immediately that not all groups are cyclic. In particular, no nonabelian group can be cyclic. We have already seen an example $U(8)$ of an abelian group which is not cyclic.

Every subgroup of a cyclic group is cyclic. Let $G$ be a cyclic group with generator $g$. Let $H$ be a subgroup of $G$. If $H$ contains no element of $G$ except the identity, $H$ is cyclic. If $H$ contains an element of $G$ which is not the identity, there is a $g^k \in H$ with $k \neq 0$. $g^{-k}$ is also in $H$, and one of $k$ and $-k$ is positive, so there is a smallest positive $n$ such that $g^n \in H$. Now for any $g^k \in H$, $k = nq + r$ for some integer $q$ and nonnegative integer $r < n$. $g^k = g^{nq+r} = (g^n)^q g^t \in H$. But also $g^{nq}$, and so its inverse, are in $H$, because $H$ includes the cyclic subgroup generated by $g^n$, so $g^r \in H$, so $r = 0$ (no $g^r$ for $0 < r < n$ belongs to $H$), so in fact $H$ is exactly the cyclic subgroup. generated by $g^n$. Notice here and in following results that number theory is allowing us to prove theorems in algebra.

The elements of a cyclic group of order $n$ with generator $a$ are exactly the $a^k$ with $0 \leq k \leq n-1$. It cannot be the case that all $a^k$ with $0 \leq k \leq n$ are distinct, because the group has order $n$ and this would give $n+1$ distinct elements. So we must have $0 \leq k < l \leq n$ such that $a^k = a^l$. Notice that $a^k = a^l$ implies that $a^{l-k} = e$, and of course $l - k \leq n$, We show that in fact $l - k = n$, and so $0 = k$ and $l = n$ (and all of $0 \leq k \leq n-1$ are distinct, and so make up the entire group). For any $a^m$, there are $q$ and $r$ such that $0 \leq r < l - k$ such that $a^m = a^{(l-k)q+r} = a^r$ (because $a^{l-k} = e$). But this means that every element of the group is of the form $a^r$ for some $r$ with $0 \leq r < l - k$ so there are no more than $l - k$ elements of the group, so in fact $l - k = n$, so $l = n$ and $k = 0$.

It follows that if $a^k = e$, we can argue that $a^k = a^{qn+r} = a^r$ for some $q$ and some $r$ with $0 \leq r < n$, (by the division algorithm) and of these $a^e = e$ only if $r = 0$. so we have shown that $a^k = e$ exactly if $n|k$.

This is not how I did this in class on March 1 (you may recall that I was feeling strange at the time), but this does it neatly. Notice that I have in effect argued that every cyclic group of order $n$ has the same structure as the modular addition group $\mathbb{Z}_n$.

This also gives a quick proof of a result the book appears to prove in a different way: if $G$ is of (finite) order $n$, with $a$ as a generator, the order of

$a^k$ is $\frac{n}{\texttt{gcd}(n,k)}$. The elements of the subgroup are exactly the elements $a^{kx+ny}$ with $0 \leq kx+ny < n$, by what we have already shown. Every element of the cyclic subgroup is of the form $a^{kx}$, of course, and equal to $a^{kx+ny}$ for every $y$, and one of the values $kx+ny$ will be in the range from 0 to $n-1$ inclusive by division algorithm. So a generator of this group will be $a^d$ where $d$ is the smallest possible positive $kx+ny$, that is, $\texttt{gcd}(n,k)$, so the elements of $G$ belonging to the subgroup are exactly the multiples of $\texttt{gcd}(n,k)$ in $[0,n-1]$, and there are $\frac{n}{\texttt{gcd}(n,k)}$ of these.

It is not difficult to show that the nonzero complex numbers with multiplication are a group. You can look at the discussion in the chapter for details.

What really interests us is the subgroup of $\mathbb{C}^*$ consisting of $a+bi$ with $a^2+b^2=1$.

Each of these numbers is of the form $\cos(\theta)+i\sin(\theta)$ for some $\theta$ (and then for every $\theta+2k\pi$, since sine and cosine are periodic. This is straightforward from trigonometry.

You can verify using addition identities for sine and cosine that $(\cos(\theta)+i\sin(\theta))(\cos(\phi)+i\sin(\phi)) = \cos(\theta+\phi)+i\sin(\theta+\phi)$. If you do not know this already, please take the time to verify it. It is enormously useful in calculus and differential equations.

This group is called the circle group. It is not a cyclic group, for an interesting technical reason: the cyclic subgroup generated by any element of any grup at all can be at most the size of the set of integers, and the set of real numbers in the interval $[0,2\pi)$, which is the same size as the circle group, is larger than the set of integers.

However, it contains subgroups isomorphic to every cyclic group. $(\cos(\theta)+i\sin(\theta))^n = \cos(n\theta)+i\sin(n\theta)$ for each $n \in \mathbb{Z}$. It follows that $(\cos(\frac{2\pi}{n})+i\sin(\frac{2\pi}{n}))^n = 1$, and a little thought shows that this actually is of order $n$ (no smaller power will be 1). $(\cos(\frac{m2\pi}{n})+i\sin(\frac{m2\pi}{n}))^n = 1$ will be true, and the order of this element will be $\texttt{gcd}(m,n)$. There are $n$ distinct $n$th roots of 1 in the circle group, the values of $(\cos(\frac{m2\pi}{n})+i\sin(\frac{m2\pi}{n}))^n$ for each $0 \leq m < n$; of these, the primitive $n$th roots of unity, the ones which are not also $k$th roots of unity for some positive $k < n$, are exactly those with $\texttt{gcd}(m,n) = 1$. This should give you enough information to count the primitive $n$th roots of unity for small $n$.

Now suppose that $\cos(\theta)+i\sin(\theta)^n = 1$ for some integer $n$. We argue that $\theta$ must be a rational multiple of $\frac{2\pi}{n}$. If $\theta$ is negative, we can replace $\theta$ with positive $-\theta$. We claim that in fact $\theta$ must be an integer multiple of $\frac{2\pi}{n}$.

If it isn't we can choose the largest $m$ which leaves $\theta - \frac{m2\pi}{n}$ positive (which leaves it less than $\frac{2\pi}{n}$). $(\cos(\theta - \frac{m2\pi}{n}) + i\sin(\theta - \frac{m2\pi}{n}))^n$ would still be 1, but it is quite clear from the geometry of the unit circle that this cannot be the case.

This implies that for every irrational $r$, the order of $\cos(2\pi r) + i\sin(2\pi r))$ is infinite, so the cyclic group that it generates has the same structure as the group of integers under addition. So every cyclic group has the same structure as some subgroup of the circle group: it is a kind of universal object for cyclic groups.

# 18 March 3: Permutation Groups

We consider groups of permutations of finite sets. We note that since we are really only interested in the formal structure of the groups, we can replace consideration of a general group of permutations of a set $A$ of size $n$ with permutations of the set $\{1, \ldots, n\}$.

The permutation group $S_n$ has as its elements the bijections from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$, and composition of functions as its operation. You are all aware that the composition of two bijections from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$ is a bijection from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$, that the identity map on this set is a bijection of this kind, and that such bijections have inverse functions which are bijections of this kind, and the composition of a bijection and its inverse is the identity.

You also know that the group $S_n$ has $n!$ elements. These are finite groups but rapidly become very large.

We note that any group of size $n$ is isomorphic to a subgroup of $S_n$ (which is much larger!). We prove this, more economically than we did in class, but the idea is that same. Let $G$ be a group with $n$ elements: provide a bijection $g$ from $\{1, \ldots, n\}$ to $G$ (so the elements of $G$ are exactly $g(0), g(1), \ldots, g(n)$). Notice that for each element $a$ of $G$, $g^{-1}(a)$ is a number in $\{1, \ldots, n\}$. We define a map taking elements of $G$ to permutations in $S_n$: if $a \in G$, we define $I(a)$ as the permutation which takes each $j \in \{1, \ldots, n\}$ to $g^{-1}(a \cdot g(j))$, where $\cdot$ is the group operation. We compute $I(a) \circ I(b)$ of $j \in \{1, \ldots, n\}$ to show that we have an isomorphism.

$$(I(a) \circ I(b))(j) = I(a)(I(b)(j)) =$$

$$I(a)(g^{-1}(b \cdot g(j))) = g^{-1}(a \cdot g(g^{-1}(b \cdot g(j)))) = g^{-1}(a \cdot (b \cdot g(j))) = g^{-1}((a \cdot b) \cdot g(j)) = I(a \cdot b)(j)$$

so $I(a) \cdot I(b) = I(a \cdot b)$

This shows (with obvious remarks about identity and inverses) that the permutations $I(a)$. which are basically correlated with columns in the multiplication table of $G$, make up a subgroup of $S_n$ with the same structure as $G$.

Now we talk about notations for permutation group calculations.

A standard notation for an element $f$ of $S_n$ is

$$\begin{pmatrix} 1 & \dots & n \\ f(1) & \dots & f(n) \end{pmatrix}$$

with the elements of $\{1, \dots, n\}$ listed above and the value of $f$ at each element listed below it.

In computing the composition of two permutations written in this notation (or any notation), one must remember that they have to be permutations of the same set, and that the second one is evaluated first at each number: $(f \circ g)(x)$ is $f(g(x))$, you apply $g$ then you apply $f$, which may unfortunately seem backward.

Extended examples I leave to the book, or will produce on demand in class. Typesetting this notation is nasty.

An alternative, more compact notation for permutations is cycle notation. Where $a_1, \dots, a_k$ are distinct elements of $\{1, \dots, n\}$, we define the $(a_1, \dots, a_k)$ (I write commas here but their use is optional) to denote the permutation which sends $a_k$ to $a_1$ and each other $a_i$ to $a_{i+1}$, and fixes all elements of $\{1, \dots, n\}$ which are not $a_i$'s.

A first remark is that disjoint cycle notations (where no number in one cycle appears in the other) commute. This is straightforward to see: applying the first cycle then the second or the second cycle then the first, one does the same thing, moving the numbers around the two cycles. The change in order makes no difference because applying each cycle does not change the numbers in the other cycle.

Any permutation can be written as a composition of disjoint cycles. Let $f$ be a permutation in $S_n$. The first cycle in the composition will have $a_i = f^i(1)$, where we define $f^0(x) = x$, $f(n + 1(x) = f(f^n(X))$. The second cycle in the composition (if we didnt discover that $f$ is a cycle at the first step) is defined thus: let $j$ be the first number in $\{1, \dots, n\}$ which is not in the first cyle and define the second cycle by $b_i = f^i(j)$. Continue until there are no numbers in $\{1, \dots, n\}$ not included in cycles. In a certain sense

the deconposition into cycles is unique, mod the facts that we can rotate the number in each cycle ((1423) is the same as (4231), for example) and we can write the disjoint cycles in any order.

Computing where a permutation written in cycle notation sends each number is straightforward, and it is a skill you need to compute productes of permutations expressed in cycle notation, in cycle notation. Remember always that in a composition you apply the second function, then the first.

A transposition is a cycle of length 2. Previous results and the fact that $(a_1, \ldots, a_k) = (a_1 a_k)(a_1 a_{k-1}) \ldots (a_1 a_2)$ (check examples to see that this works and how it works) show that every permutation can be written as a product (composition) of transpositions. This product is not unique. But there is a Big Theorem about this. We say that a permutation in $S_n$ is even if it can be written as a product of an even number of transpositions, and odd if it can be written as a product of an odd number of transpositions. The theorem is that every transposition is either odd or even, and no transposition is both. [we remark that in a product of transpositions in which some transposition occurs more than once, we count each occurrence as a separate transposition for purposes of the definition of odd and even transposition].

The book proves this by giving a proof (not familiar to me until I lectured it yesterday) that the identity permutation is even, and not odd (so if it is written as a product of transpositions, the number of transpositions in the product must be even),

Given this result, it is straightforward to prove that no transposition can be both odd and even. Suppose $f$ is both odd and even. Then we can write $f$ in a form $f'$, a product of an even number of transpositions, and in a form $f''$, a product of an odd number of transpositions. Writing $f''$ in reverse order gives an expressiom $f'''$ for $f^{-1}$ (each transposition is its own inverse, and multiplying inverses in the reverse order gives the inverse of a product). Now $f'f'''$ would be a product of an odd number of transpositions giving the identity, contradicting the theorem.

I will give a proof of the theorem that the identity is not an odd permutation later when I find one that I really like, or when I make better friends with the one in the book.

This theorem implies that for each $n$, the collection of even permutations in $S_n$ makes up a group, called the alternating group $A_n$ of index $n$.

# 19 Homework 7

Homework 7: 4.5 exercises (starting on p. 55): 4adf, 11, 12, 13 (I dont think the conjecture is easy), 14 (this bears on a question asked in class), 23*, 24; 5.4 exercises starting on p. 71: 1ab, 2abcd, 3abc, 8, 6* starred questions are hard and optional.