The first exam will be on Wednesday, September 19, 2018. The syllabus will be Chapters 1 – 3 in Judson.
Following are some of the concepts and results you should know:

- Know the basic language of sets, combinations of sets, and the basic results relating these. (Proposition 1.2 and Theorem 1.3).
- Know the basic language of *mappings*: *domain, codomain, image, one-to-one (or injective), onto (or surjective), composite mapping, identity map, inverse.*
- Know the basic properties of an *invertible mapping.* Specifically, Theorems 1.15 and 1.20.
- Know: *If $\alpha : A \to B$ is a mapping where A and B are nonempty finite sets with the same number of elements, then α is one-to-one if and only if it is onto.*
- The cardinality of X, denoted $|X|$, is the number of elements of X.
- Know what it means for a *relation* $\equiv$ on a set A to be an *equivalence.*
- Know the definition of the *equivalence class* $[a]$ generated by an element $a \in A$ under the equivalence $\equiv$.
- Know the *kernel* equivalence on a set A determined by a mapping $\alpha : A \to B$ and that the equivalence class $[a]$ generated by $a \in A$ in this case is $[a] = \{x \in A \mid \alpha(x) = \alpha(a)\}$.
- Know the fundamental properties of equivalence classes. Specifically, Theorems 1.25 and Corollary 1.26 relating equivalence classes and *partitions.*
- Know the *Induction Principle* and how to use it to do proofs by induction.
- Know the *Strong Induction Principle* and how to use it to do proofs by induction.
- Know the *Well-ordering principle:* Any set of positive integers which has at least one element contains a smallest element.
- Know the *Division Algorithm.*
- Know the definition of a *divides* b for integers a and b (notation: $a|b$).
- Know the definition of the *greatest common divisor* of the integers a and b (notation: $\gcd(a, b)$).
- Know the *Euclidean Algorithm* and how to use it to compute the greatest common divisor of integers a and b, and write the greatest common divisor of a and b as an integer linear combination of a and b (Example 2.12).
- Know the definition of *relatively prime integers.*
- Know the definition of *prime* number.
- Know Euclid's Lemma: If p is a prime, a and b are integers, and $p|ab$, then $p|a$ or $p|b$ (Lemma 2.13).
- Know the Prime Factorization Theorem (Fundamental Theorem of Arithmetic, Theorem 2.15).

- Know what it means for an integer a to be *congruent modulo* n to another integer b (notation $a \equiv b \mod n$).
- Know the definition of *congruence class of* a *modulo* n (notation $[a]$ or $[a]_n$ if n needs to be identified in the notation).
- Know the definition of the number system $\mathbb{Z}_n$, and how to do arithmetic in $\mathbb{Z}_n$:

$$[a] + [b] = [a + b]$$
$$[a][b] = [ab]$$

- Know the definition of $[a]$ *is invertible* in $\mathbb{Z}_n$, and know the criterion of invertibility of $[a]$: An element $[a] \in \mathbb{Z}_n$ is invertible (or has a multiplicative inverse) if and only if $\gcd(a, n) = 1$, that is, if and only if a and n are relatively prime. Moreover, if r and s are integers such that $ar + ns = 1$, then $[a]^{-1} = [r]$. (Proposition 3.4 (6)). In particular, pay attention to the proof.
- Know how to use the Euclidean algorithm to compute $[a]^{-1}$, when the inverse exists.
- Know Theorem, proved in class, which describes the conditions under which *every* nonzero congruence class in $\mathbb{Z}_n$ has an inverse. Specifically, every nonzero element of $\mathbb{Z}_n$ has an inverse if and only if n is prime.
- Know how to solve a *linear equation* $[a]x = [b]$ in $\mathbb{Z}_n$, provided $[a]^{-1}$ exists.
- Know the symmetries of simple geometric figures such as a rectangle, equilateral triangle, and square, and how to represent each as a permutation and how to use the permutations to describe the composition of the symmetries. (See Figures 3.5 and 3.6 and the discussion following them.)
- Know the definition and basic examples of groups. (Section 3.2)
- Know the basic rules of multiplication in a group G (Propositions 3.17 – 3.22)
- Know the definition of a *subgroup* and the criterion for a subset of a group to be a subgroup. (Propositions 3.30 and 3.31).

Review Exercises

Be sure that you know how to do all assigned homework exercises. The following are a few supplemental exercises similar to those already assigned as homework. These exercises are listed randomly. That is, there is no attempt to give the exercises in the order of presentation of material in the text.

1. Prove that

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}$$

for all integers $n \geq 2$.

▶ **Solution.** Let $S(n)$ be the statement

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}$$

for the integer n.

We will use induction to show that $S(n)$ is true for all integers $n \geq 2$.

Base Step. If $n = 2$ the statement $S(2)$ becomes

$$\left(1 - \frac{1}{2^2}\right) = \frac{2+1}{2 \cdot 2} = \frac{3}{4},$$

which is a true statement.

Inductive Step. For a given integer $n \geq 2$, assume that $S(n)$ is a true statement. Thus we are assuming that

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}$$

for the given integer n. If we multiply both sides of this equation by $\left(1 - \dfrac{1}{(n+1)^2}\right)$ we get

$$\begin{aligned}
\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{n^2}\right)\left(1 - \frac{1}{(n+1)^2}\right) &= \left(\frac{n+1}{2n}\right)\left(1 - \frac{1}{(n+1)^2}\right) \\
&= \frac{n+1}{2n} - \frac{1}{2n(n+1)} \\
&= \frac{(n+1)^2 - 1}{2n(n+1)} \\
&= \frac{n^2 + 2n}{2n(n+1)} \\
&= \frac{n+2}{2(n+1)} \\
&= \frac{(n+1)+1}{2(n+1)}.
\end{aligned}$$

Therefore, we have shown that if $S(n)$ is true, then so is $S(n+1)$.

By the principle of mathematical induction, $S(n)$ is true for all natural numbers $n \geq 2$. ◀

2. Prove by induction that $4^n + 2$ is divisible by 6, for every positive integer n.

▶ **Solution.** Let $S(n)$ be the statement: $4^n + 2$ *is divisible by n for the integer n.*

We will use induction to show that $S(n)$ is true for all integers $n \geq 1$.

Base Step. If $n = 1$ the statement $S(1)$ becomes: $4^1 + 2$ *is divisible by 6*, which is a true statement.

Inductive Step. For a given integer $n \geq 1$, assume that $S(n)$ is a true statement. Thus we are assuming that $4^n + 2$ is divisible by 6 for the given integer n. That is, we are assuming that, for the given integer n, $4^n + 2 = 6k$ for some integer k. Then

$$\begin{aligned}
4^{n+1} + 2 = 4^n \cdot 4 + 2 &= 4^n \cdot 4 + 8 - 6 \\
&= 4^n \cdot 4 + 2 \cdot 4 - 6 = 4(4^n + 2) - 6 \\
&= 4(6k) - 6 = 6(4k - 1).
\end{aligned}$$

Thus, we have shown that if $4^n + 2$ is divisible by 6, then $4^{n+1} + 2$ is also divisible by 6. Therefore, we have shown that if $S(n)$ is true, then so is $S(n+1)$.

By the principle of mathematical induction, $S(n)$ is true for all natural numbers $n \geq 1$. ◀

3. Decide whether each of the following functions is injective, surjective, and/or bijective.

   $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2 - 4x + 3$.

   $g : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = 4x + 5$.

   $h : \mathbb{Z} \to \mathbb{Z}$ defined by $h(x) = 4x + 5$.

   $\alpha : \mathbb{Z}_{11} \to \mathbb{Z}_{11}$ defined by $\alpha([x]) = [4x + 5]$.

   $\beta : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ defined by $\beta([x]) = [4x + 5]$.

   $\gamma : \mathbb{Z} \to \mathbb{Z}_{15}$ defined by $\gamma(x) = [4x + 5]$.

   ► **Solution.** f is neither injective or surjective. It is not injective since the equation $f(x) = 0$ has two solutions (by the quadratic formula) $x = 1$ and $x = 3$. That is $f(1) = 0 = f(3)$ but $1 \neq 3$. It is not surjective since $f(x) = x^2 - 4x + 3 = (x - 2)^2 - 1$ so $f(x) \geq -1$ and hence -2 is not in the image of f.

   g is bijective: If $g(x_1) = g(x_2)$ then $4x_1 + 5 = 4x_2 + 5$ so $4x_1 = 4x_2$ and dividing by 4 (which is possible in $\mathbb{R}$) we get $x_1 = x_2$, so g is injective. To show g is surjective, let $y \in \mathbb{R}$ be arbitrary and try to solve the equation $g(x) = y$ for $x \in \mathbb{R}$. This is $4x + 5 = y$ and solving for x gives $x = 4^{-1}(y - 5)$. Thus, $g(4^{-1}(y - 5)) = y$.

   h is injective but not surjective: Injectivity for h is similar to that of g. Namely, $4x_1 + 5 = 4x_2 + 5$ for x_1, $x_2 \in \mathbb{Z}$ implies $4x_1 = 4x_2$ which implies that $4(x_1 - x_2) = 0$. Since $4 \neq 0$ this implies that $x_1 - x_2 = 0$, that is $x_1 = x_2$. To see that h is not surjective, note that 0 is not in the image of h since $h(x) = 0$ implies that $4x - 5 = 0$ so that $4x = -5$. But -5 is not divisible by 4, so there can be no such x.

   α is bijective: The argument is essentially the same as the argument for bijectivity of g since 4^{-1} exists in $\mathbb{Z}_{11}$, because 4 and 11 are relatively prime.

   β is neither injective of surjective: It is not injective since $\beta(0) = 5 = \beta(3)$. Since $\mathbb{Z}_{12}$ is a finite set, if β were surjective, then it would also be injective. Thus, β is not surjective.

   γ is not injective, but it is surjective: It is not injective because $\gamma(0) = \gamma(15) = 5$. It is surjective since 4^{-1} exists in $\mathbb{Z}_{15}$. In fact, $4^{-1} = 4$ in $\mathbb{Z}_{15}$. Thus, if $[y] \in \mathbb{Z}_{15}$ then $\gamma(4(y - 5)) = [y]$. ◄

4. Define $f : \mathbb{Z}_{12} \to \mathbb{Z}_8$ by $f([x]_{12}) = [2x]_8$, for all $[x]_{12} \in \mathbb{Z}_{12}$, and define $g : \mathbb{Z}_{12} \to \mathbb{Z}_8$ by $g([x]_{12}) = [3x]_8$, for all $[x]_{12} \in \mathbb{Z}_{12}$. Show that f is a function, but g is not. (Note that we are using $[x]_n$ to denote the congruence class of x in $\mathbb{Z}_n$, rather than the usual $[x]$ to avoid confusion since elements of both $\mathbb{Z}_{12}$ and $\mathbb{Z}_8$ are being used.)

   ► **Solution.** If $[x]_{12} = [y]_{12}$ then $x \equiv y \pmod{12}$ so $12 \mid (x - y)$. That is, $x - y = 12t$ for some $t \in \mathbb{Z}$ so that $2x - 2y = 24t = 8(3t)$ so $[2x]_8 = [2y]_8$. This shows that f is well-defined and hence a function.

   However, $[0]_{12} = [12]_{12}$ but $[3 \cdot 0]_8 \neq [3 \cdot 12]_8$ since 8 does not divide 36. Thus, g is not well-defined and hence is not a function. (The given rule does not give a unique element of $\mathbb{Z}_8$ for every element of $\mathbb{Z}_{12}$.) ◄

5. Define $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ by $f([x]) = [x]^2$. Verify that f is a well defined function, compute the image of f, and find the partition of $\mathbb{Z}_{12}$ for the equivalence relation on $\mathbb{Z}_{12}$ determined by the function f. That is, $[x] \equiv [y]$ if and only if $f([x]) = f([y])$.

▶ **Solution.** f is well defined since if $[x] = [y]$ then $[x]^2 = [y]^2$. The following table gives the values of f:

$x \pmod{12}$	0	1	2	3	4	5	6	7	8	9	10	11
$x^2 \pmod{12}$	0	1	4	9	4	1	0	1	4	9	4	1

Thus, under the equivalence relation $\equiv$ the distinct equivalence classes are $[0] = \{0, 6\}$, $[1] = \{1, 5, 7, 11\}$, $[2] = \{2, 4, 8, 12\}$, and $[3] = \{3, 9\}$. Thus, the qequivalence partition is:

$$\{\{0, 6\}, \{1, 5, 7, 11\}, \{2, 4, 8, 10\}, \{3, 9\}\}.$$

◀

6. Find the remainder when b is divided by a if:

   (a) $a = 6$, $b = 25$

   ▶ **Solution.** $25 = 4 \cdot 6 + 1$ so the remainder is 1. ◀

   (b) $a = -6$, $b = -25$

   ▶ **Solution.** $-25 = (-6)5 + 5$ so the remainder is 5. ◀

7. This problem involves arithmetic modulo 16. All answers should only involve expressions of the form $[a]$, with a an integer and $0 \le a < 16$.

   (a) Compute $[4] + [15]$. **Answer**: $[3]$

   (b) Compute $[4] \cdot [15]$. **Answer**: $[12]$

   (c) Compute $[15]^{-1}$. **Answer**: $[15]$

   (d) List the invertible elements of $\mathbb{Z}_{16}$. **Answer:** The invertible elements are those $a]$ with $\gcd(a, 16) = 1$. Thus, they are $\{[1], [3], [5], [7], [9], [11], [13], [15]\}$

8. Let a, b, c, and d be positive integers. Determine if each of the following statements is True or False. If False, provide a counterexample.

   (a) If $a|c$ and $b|c$, then $ab|c$. **False**. Counterexample: $a = b = c = 2$.

   (b) If $\gcd(a, b) = 1$ and $\gcd(c, d) = 1$, then $\gcd(ac, bd) = 1$. **False**. Counterexample: $a = d = 2$, $b = c = 3$. Then $\gcd(a, b) = \gcd(c, d) = 1$ but $\gcd(ac, bd) = 6$.

   (c) If there exist integers r and s such that $ra + sb = d$, then $d = \gcd(a, b)$. **False**. Counterexample: $4 \cdot 3 - 5 \cdot 2 = 2$ but $\gcd(3, 2) = 1$.

   (d) Every nonempty set of positive integers contains a largest element. **False**. The set of positive integers does not contain a largest element.

9. Find the greatest common divisor $d = \gcd(803, 154)$ of 803 and 154, using the Euclidean Algorithm, and write $d = \gcd(803, 154)$ in the form $d = s \cdot 803 + t \cdot 154$.

▶ **Solution.** Use the Euclidean Algorithm:

$$\begin{aligned} 803 &= 5 \cdot 154 + 33 \\ 154 &= 4 \cdot 33 + 22 \\ 33 &= 1 \cdot 22 + 11 \\ 22 &= 2 \cdot 11 \end{aligned}$$

Thus, gcd(803, 154) = 11 and

$$\begin{aligned} 11 &= 33 - 22 \\ &= 33 - (154 - 4 \cdot 33) = 5 \cdot 33 - 154 \\ &= 5(803 - 5 \cdot 154) - 154 \\ &= 5 \cdot 803 - 26 \cdot 154. \end{aligned}$$

◀

10. If a, b, and c are elements of a group G, then solve the equation $axb = c$ for $x \in G$.

▶ **Solution.** Multiply on the left by a^{-1} and on the right by b^{-1} to get $x = exe = a^{-1}axbb^{-1} = a^{-1}cb^{-1}$. ◀

11. Let $G = \{1, -1, i, -i\} \subseteq \mathbb{C}^*$. Recall that $\mathbb{C}^*$ is the multiplicative group of nonzero complex numbers.

(a) Verify that G is a subgroup of $\mathbb{C}^*$. (Constructing a Cayley table for G may be useful.)

(b) Verify that $S = \{1, i\}$ is *not* a subgroup of G.

▶ **Solution.** The following is the multiplication table for G:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

From the table it is clear that G is closed under multiplication so G is a subgroup of $\mathbb{C}^*$ Since $i^2 = -1 \notin S$, S is *not* closed under multiplication, and hence S is not a subgroup of G.

◀

12. Suppose that G is the group defined by the following Cayley table.

$\cdot$	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	a	h	g	f	e	d	c
c	c	d	e	f	g	h	a	b
d	d	c	b	a	h	g	f	e
e	e	f	g	h	a	b	c	d
f	f	e	d	c	b	a	h	g
g	g	h	a	b	c	d	e	f
h	h	g	f	e	d	c	b	a

(a) Which element is the identity of G?

(b) What is g^{-1}?

(c) Find $C(g) = \{x \in G : xg = gx\}$.

▶ **Solution.** (a) The identity of G is a since (from the table) $ax = x = xa$ for all $x \in G$.

(b) $g^{-1} = c$ since $gc = cg = a$ and a is the identity of G.

(c) $C(g) = \{a, c, e, g\}$.

◀

13. In each case determine whether H is a subgroup of G.

(a) $H = \{0,\ 1,\ -1\}$, $G = \mathbb{Z}$ with group operation $+$.

(b) $H = \{[1],\ [3]\}$, $G = U(8)$ (Recall $U(n)$ is the set of elements of $\mathbb{Z}_n$ that have a multiplicative inverse. the group operation is multiplication modulo n.)

(c) $H = \{[1],\ [3]\}$, $G = U(16)$

(d) $H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$, $G = \mathrm{GL}_2(\mathbb{Z})$

▶ **Solution.** (a) H is not a subgroup of $\mathbb{Z}$ since it is not closed under the group operation $+$. As an example, $1 \in H$ but $2 = 1 + 1 \notin H$.

(b) The multiplication table of H as a subset of $G = U(8)$ is

·	1	3
1	1	3
3	3	1

This table shows that H is closed under multiplication in $U(8)$, $[1] \in H$, and each element is its own inverse, and hence is in H. Thus, H is a subgroup of $U(8)$.

(c) The multiplication table of H as a subset of $G = U(16)$ is

·	1	3
1	1	3
3	3	9

Therefore, H is not closed under multiplication since $[9] \notin H$, and hence H is not a subgroup of $U(16)$.

(d) Label the elements of H as $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $-I = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $-A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

The multiplication table of H as a subset of $G = \mathrm{GL}_2(\mathbb{Z})$ is

·	I	$-I$	A	$-A$
I	I	$-I$	A	$-A$
$-I$	$-I$	I	$-A$	A
A	A	$-A$	$-I$	I
$-A$	$-A$	A	I	$-I$

This table shows that H is closed under multiplication in $\mathrm{GL}_2(\mathbb{Z})$, $I \in H$, and the inverse of each element is in H. Thus, H is a subgroup of $\mathrm{GL}_2(\mathbb{Z})$.

◀

14. Let $G = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a,\, b \in \mathbb{R},\ a \neq 0 \right\}$. Show that G is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

▶ **Solution.** Check the three criteria in the subgroup test:

- $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ by choosing $a = 1$, $b = 0$.
- Suppose $A = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \in G$. Then $AB = \begin{bmatrix} ac & ad + bc \\ 0 & ac \end{bmatrix} \in G$ since $ac \neq 0$ because $a \neq 0$ and $c \neq 0$.
- If $A = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in G$, then $a \neq 0$ so $\det A = a^2 \neq 0$ and $A^{-1} = \begin{bmatrix} 1/a & -b/a^2 \\ 0 & 1/a \end{bmatrix} \in G$ since $1/a \neq 0$.

Thus, G is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. ◀