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

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 $\gamma(x) = [4x + 5]$.

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.)

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 $f([x]) = f([y])$.

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

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

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

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

   (a) Compute $[4] + [15]$.

   (b) Compute $[4] \cdot [15]$.

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

   (d) List the invertible elements of $\mathbb{Z}_{16}$.

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 $ab|c$.

   (b) If $\gcd(a, b) = 1$ and $\gcd(c, d) = 1$, then $\gcd(ac, bd) = 1$.

   (c) If there exist integers r and s such that $ra + sb = d$, then $d = \gcd(a, b)$.

   (d) Every nonempty set of positive integers contains 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 $d = s \cdot 803 + t \cdot 154$.

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

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.

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

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

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 $\mathrm{GL}_2(\mathbb{R})$.