Exam 2 will be based on:

Homework and textbook sections covered by lectures 2/3 - 3/5.
(see http://www.math.sc.edu/~boylan/SCCourses/547Sp10/547.html)
At minimum, you need to understand how to do the homework problems.

Topic List (not necessarily comprehensive):

You will need to know: theorems, results, and definitions from class.

1. Primes, irreducibles, associates.

   **Definition.** Let \( R \) be a commutative ring. Let \( a, b \in R \) with \( a \neq 0 \). Then \( a \) divides \( b \) (we write \( a \mid b \)) if and only if \( \exists c \in R \) with \( b = ac \).

   **Facts:**
   
   (i) \( u \in R^\times \iff (u) = R \).
   
   (ii) \( a \mid b \iff b \in (a) \iff (b) \subseteq (a) \).
   
   (iii) \( a \mid b \) and \( b \mid a \iff (a) = (b) \).

   **Definition.** Elements \( a \) and \( b \in R \) are associates \((a \sim b)\) if and only if \( \exists u \in R^\times \) with \( b = ua \).

   **Facts:**
   
   (i) The relation \( \sim \) is an equivalence relation on \( R \).
   
   (ii) \( a \sim b \implies (a) = (b) \).
   
   (iii) Let \( R \) be an integral domain. Then \( a \sim b \iff (a) = (b) \).

   **Definition.** Let \( R \) be a commutative ring. Then \( d \neq 0 \) in \( R \) is the greatest common divisor (gcd) of \( \{a_1, \ldots, a_n\} \subseteq R \) if and only if the following are true:
   
   (a) \( \forall i, d \mid a_i \).
   
   (b) Suppose that \( \exists c \in R \) such that \( \forall i, c \mid a_i \). Then we have \( c \mid d \).

   **Proposition.** Let \( R \) be a PID, and let \( a, b \neq 0 \) in \( R \). Then we have:
   
   (a) gcd\((a, b)\) exists in \( R \); it is unique up to multiplication by units.
   
   (b) If \( d = \gcd(a, b) \), then \( \exists s, t \in R \) with \( d = as + bt \).
Notes: Let $R$ be a PID. Then the following rules of ideal arithmetic hold:

(i) $(a) + (b) = (\gcd(a, b))$.
(ii) $(a) \cap (b) = (\operatorname{lcm}(a, b))$.
(iii) $(a)(b) = (ab)$.

Definition. Let $R$ be an integral domain. Then $q \in R$ is **irreducible** if and only if

(a) $q$ is a non-zero, non-unit.
(b) If $\exists a, b \in R$ with $q = ab$, then one of $a, b$ is a unit, and the other is associated to $q$.

Definition. Let $R$ be an integral domain. Then $p \in R$ is **prime** if and only if

(a) $p$ is a non-zero, non-unit.
(b) If $\exists a, b \in R$ with $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Theorem. Let $R$ be an integral domain.

(a) $p \in R$ is prime if and only if $(p) = pR \triangleleft R$ is a prime ideal.
(b) $c \in R$ is irreducible if and only if $(c) = cR \triangleleft R$ is maximal in the set of all principal ideals in $R$.
(c) Let $p \in R$ be prime. Then $p$ is irreducible. (prime $\implies$ irreducible)

Note: The converse of part (3) is not true in general.

Proposition. Let $R$ be a PID, and let $p \in R$. Then $p$ is irreducible if and only if $p$ is prime.

2. Unique factorization in rings.

Definition. Let $R$ be an integral domain. Then $R$ is a **unique factorization domain** (UFD) if and only if

(a) **Existence:** Every non-zero, non-unit $r \in R$ has a factorization into irreducibles in $R$: 
$\exists q_1, \ldots, q_r$ irreducibles in $R$ with $r = q_1 \cdots q_r$.
(b) **Uniqueness:** The factorization of a non-zero, non-unit $r \in R$ is unique: if 
$r = q_1 \cdots q_s = p_1 \cdots p_t$
are two factorizations into irreducibles, then we have $s = t$ (the number of irreducibles in each factorization is the same) and for all $1 \leq j \leq s$, we have $q_j \sim p_j$ (relabeling if necessary, the irreducible factors in each factorization can be put in bijection by association).
Example. \( \mathbb{Z} \) is a UFD.

Example. The ring \( R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \) is not a UFD since the two irreducible factorizations of 6 in \( R \) given by

\[
2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 + \sqrt{-5})
\]

are distinct. In particular, 2 is associated to neither \( 1 + \sqrt{-5} \) nor \( 1 - \sqrt{-5} \).

**Definition.** Let \( R \) be an integral domain. Then \( R \) satisfies the **ascending chain condition (ACC)** if and only if all ideal chains in \( R \):

\[
I_0 \subseteq I_1 \subseteq \cdots I_k \subseteq \cdots
\]

eventually stabilize. I.e., \( \exists N \geq 1 \) such that for all \( n \geq N \), we have \( I_n = I_N \).

**Definition.** Let \( R \) be an integral domain. Then \( R \) satisfies the **maximal condition (MAX)** if and only if every non-empty set of ideals in \( R \) contains a maximal element.

**Lemma.** Suppose that \( R \) is a PID. Then \( R \) satisfies ACC and MAX.

**Theorem.** Let \( R \) be a PID. Then \( R \) is a UFD.

**Note:** The converse is not generally true.

**Definition.** Let \( R \) be commutative, let \( I \triangleleft R \), and let \( a, b \in R \). Then we have

\[
a \equiv b \pmod{I} \iff a - b \in I \iff a + I = b + I.
\]

**Theorem** (Chinese Remainder Theorem). Let \( I, J \triangleleft R \) be proper, and suppose that \( I + J = R \). Then the following are true:

(a) Let \( a, b \in R \). Then \( \exists x \in R \) such that

\[
x + I = a + I \quad (x \equiv a \pmod{I}),
x + J = b + J \quad (x \equiv b \pmod{I}).
\]

(b) \( IJ = I \cap J \).

(c) \( \frac{R}{IJ} \cong \frac{R}{I} \oplus \frac{R}{J} \).
3. Ring summary:

(a) Fields $\subseteq$ Euclidean rings $\subseteq$ PIDs $\subseteq$ UFDs $\subseteq$ Integral domains $\subseteq$ Commutative rings.

(b) Examples:

• $\mathbb{Z}[i]$ is Euclidean, but not a field.
• $\mathbb{Z} \left[ \frac{1+\sqrt{-19}}{2} \right]$ is a PID, but not Euclidean.
• $\mathbb{Z}[x]$ is a UFD, but not a PID.
• $\mathbb{Z}[\sqrt{-5}]$ is an integral domain, but not a UFD.
• $\mathbb{Z}_6$ is a commutative ring, but not an integral domain.

(c) A finite integral domain is a field.

(d) If $r \in R$ is prime, then it is irreducible. On the other hand, $2$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$, but is not prime.

(e) If $I \triangleleft R$ is maximal, then it is prime. On the other hand, the principal ideal $((0, 1)) \triangleleft \mathbb{Z} \oplus \mathbb{Z}$ is prime, but not maximal.

(f) Further facts: Let $R$ be a commutative ring.

- Cancellation holds in an integral domain, but not in all commutative rings.
- gcds exist in a UFD, but not necessarily in an integral domain.
- Irreducible and prime elements agree in a UFD; in an integral domain they may not.
- Prime and maximal ideals agree in a PID; in a UFD they may not.
- The division algorithm exists in a Euclidean ring, but not in all PIDs.
- The Chinese Remainder Theorem holds in all commutative rings.

4. Polynomial rings.

**Definition.** Let $R$ be a commutative ring, let $n \geq 0$, and let $a_0, \ldots, a_n \in R$ with $a_n \neq 0$. Then

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

is a polynomial in the indeterminate $x$ with coefficients in $R$.

(a) The degree of $p(x)$ is $n = \max\{k : a_k \neq 0\}$. The degree zero polynomials are precisely the non-zero elements in $R$; the zero polynomial has degree $-\infty$.

(b) The leading coefficient is $a_n$; $p(x)$ is monic if and only if the leading coefficient is one.

(c) The constant term is $a_0$.

(d) $R[x] = \{\text{polynomials in } x \text{ with coefficients in } R\}$; $R$ is the coefficient ring of $R[x]$.

**General facts:**

- Let $R$ be a commutative ring. Then $R[x]$ is a commutative ring with zero element: $0 \in R$; identity element: $1 \in R$.
- Let $R$ be an integral domain. Then $R[x]$ is an integral domain.
Facts on degrees: Let $R$ be an integral domain.

(a) $\deg(fg) = \deg(f) + \deg(g)$.
(b) $\deg(f + g) \leq \max(\deg(f), \deg(g))$.

Proposition. Let $R$ be an integral domain. Then we have $(R[x])^\times = R^\times$.

Notes: Let $R$ be an integral domain.

(a) $f \sim g$ in $R[x]$ if and only if $\exists r \in R^\times$ with $f(x) = rg(x)$.
(b) $f(x) \in R[x]$ is irreducible if and only if whenever $a(x), b(x) \in R[x]$ have $f(x) = a(x)b(x)$, then one of these factors is in $R^\times$.

5. Unique factorization in polynomial rings.

Theorem. Let $F$ be a field. Then $F[x]$ is a Euclidean ring with norm function given by the degree. Hence, it is also a PID and a UFD; it is not a field.

Definition. Let $f(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$. Then we have

(a) The content of $f(x)$ is $c(f) = \gcd(a_0, \ldots, a_n)$.
(b) $f(x)$ is primitive if and only if $c(f) = 1$.

Notes:

- Let $f(x) \in \mathbb{Z}[x]$. Then there is a primitive $f^*(x) \in \mathbb{Z}[x]$ for which $f(x) = c(f)f^*(x)$.
- Let $g(x) \in \mathbb{Q}[x]$. Then there is a primitive $g^*(x) \in \mathbb{Z}[x]$ and $a/b \in \mathbb{Q}$ for which $g(x) = (a/b)g^*(x)$.

Theorem (Gauss’ Lemma). Let $f(x), g(x) \in \mathbb{Z}[x]$. Then we have

(a) If $f$ and $g$ are primitive, then $fg$ is primitive.
(b) $c(fg) = c(f)c(g)$; $(fg)^* = f^*g^*$.

Theorem. Let $f(x) \in \mathbb{Z}[x]$ be primitive. Suppose that $\exists g(x), h(x) \in \mathbb{Q}[x]$ with $f(x) = g(x)h(x)$. Then there exists $g_1(x), h_1(x) \in \mathbb{Z}[x]$ with

(a) $f(x) = g_1(x)h_1(x)$.
(b) $\deg(g) = \deg(g_1)$; $\deg(f) = \deg(f_1)$.

I.e., if a primitive polynomial in $\mathbb{Z}[x]$ can be factored in $\mathbb{Q}[x]$, then it can be factored in $\mathbb{Z}[x]$.

Corollary. Let $f(x) \in \mathbb{Z}[x]$ be primitive. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$. 

5
Consequence: To show that a primitive polynomial in \( \mathbb{Z}[x] \) is irreducible in \( \mathbb{Z}[x] \), it suffices to show that it is irreducible in \( \mathbb{Q}[x] \).

**Lemma.** Let \( f(x), g(x) \in \mathbb{Z}[x] \) be primitive. Then we have \( f(x) \sim g(x) \) in \( \mathbb{Z}[x] \).

**Theorem.** \( \mathbb{Z}[x] \) is a UFD.

**Notes:**
(i) More generally, one can prove that if the ring \( R \) is a UFD, then \( R[x] \) is a UFD.
(ii) \( \mathbb{Z}[x] \) is not a PID: \( (2, x) \not\triangleleft \mathbb{Z}[x] \) is not principal.

6. Irreducibility, factors, and remainders in polynomial rings.

**Definition.** Let \( f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x] \), and let \( p \) be prime. Then \( f(x) \) is \( p \)-Eisenstein if and only if

(a) For all \( 0 \leq i \leq n-1 \), we have \( p | a_i \).
(b) \( p \nmid a_n \).
(c) \( p^2 \nmid a_0 \).

**Theorem (Eisenstein’s Criterion).** Let \( f(x) \in \mathbb{Z}[x] \), and suppose that there is a prime \( p \) for which \( f(x) \) is \( p \)-Eisenstein. Then \( f(x) \) is irreducible in \( \mathbb{Q}[x] \).

**Notes:**
(i) If \( f(x) \) is primitive and \( p \)-Eisenstein, then \( f(x) \) is irreducible in \( \mathbb{Z}[x] \).
(ii) Let \( f(x) \in \mathbb{Q}[x] \), and let \( c \in \mathbb{Z} \). Then \( f(x+c) \) is irreducible in \( \mathbb{Q}[x] \) if and only if \( f(x) \) is irreducible in \( \mathbb{Q}[x] \).

**Example.** Let \( p \in \mathbb{Z} \) be prime, and let \( \Phi_p(x) = x^{p-1} + \cdots + x + 1 \). Apply the Eisenstein Criterion to \( \Phi_p(x+1) \) to show that \( \Phi_p(x) \) is irreducible.

**Definition.** Let \( R \subseteq S \) be commutative rings, and fix \( s \in S \). Then the evaluation homomorphism at \( s \) is \( \phi_s : R[x] \to S \) defined by \( \phi_s : f(x) \mapsto f(s) \). It is a ring homomorphism.

**Definition.** Let \( f(x) \in R[x] \), and let \( s \in S \). Then \( s \) is a root of \( f(x) \) if and only if \( \phi_s(f(x)) = f(s) = 0 \).

**Note:** The kernel of \( \phi_s \) is an ideal in \( R[x] \) which consists of all polynomials in \( R[x] \) which have \( s \) as a root.

**Theorem (Remainder Theorem).** Suppose that
• $F$ is a field
• $c \in F$
• $f(x) \neq 0$ in $F[x]$. 

Then there is a unique $q(x) \in F[x]$ such that $f(x) = q(x)(x - c) + f(c)$. I.e., $f(c)$ is the remainder when you divide $f(x)$ by $x - c$.

**Theorem (Factor Theorem).** Suppose that

• $F$ is a field.
• $c \in F$.
• $f(x) \neq 0$ in $F[x]$.

Then $c$ is a root of $f(x)$ if and only if $x - c \mid f(x)$.

**Corollary.** Suppose that

• $F$ is a field.
• $f(x) \neq 0$ in $F[x]$.
• $\deg(f(x)) = 2$ or $3$.

Then $f(x)$ is reducible in $F[x]$ if and only if $f(x)$ has a root in $F$.

**Theorem (Rational root theorem).** Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Suppose that $r/s \in \mathbb{Q}$ (with $\gcd(r, s) = 1$) is a root of $f(x)$. Then $r \mid a_0$ and $s \mid a_n$. 