M622, Feb. 1: Part A is about Eisenstein's Criterion, as discussed in class 01.31. **Read Part A carefully.** Part B consists of some **quiz 1 like problems. Quiz 1 is Feb. 14**.

1. **Eisenstein's Criterion.** Let R be an integral domain having a prime ideal P, let $b(x) = b_m x^m + \ldots b_1 x + b_0 \in R[x]$ with $\{a_0, \ldots, a_{m-1}\} \subseteq P$, and $a_0 \notin P^2$. Then $b(x)$ is irreducible over $R[x]$.

   Proof. Suppose R is an integral domain having a prime ideal P, $b(x) = b_m x^m + \ldots b_1 x + b_0 \in R[x]$, with $\{a_0, \ldots, a_{m-1}\} \subseteq P$, and $a_0 \notin P^2$. Assume for contradiction that $b(x)$ is reducible. Since $\gcd(b_0, \ldots, b_m) = 1$, $b(x)$ is reducible implies there exists a factorization $b(x) = c(x)e(x)$ satisfying $\deg(b(x) > \max(deg(c(x)), deg(e(x)))$.

   Let $c(x) = c_j x^j + \ldots + c_0$, and let $e(x) = e_k x^k + \ldots + e_0$, both polynomials in $R[x]$. We have $b_0 = c_0 e_0$. That $b_0 \in P$, a prime ideal of R, implies that either c_0 or e_0 is contained in P, and that $b_0 \notin P^2$ implies that exactly one of c_0, e_0 is in P. Without loss of generality, assume $c_0 \in P$ and $e_0 \notin P$. Now consider b_1. We have $b_1 = c_0 e_1 + c_1 e_0$. Since $b_1 \in P$ and $c_0 \in P$ and P is an ideal, it follows that $c_1 e_0 \in$. That P is prime and $e_0 \notin P$ implies that $c_1 \in P$.

   (*) Now (you) prove by induction that $c_0, c_1, \ldots, c_j$ are all in P. But if all coefficients of $c(x)$ are in P, $b(x) = c(x)e(x)$ implies that $b(x)$ is not monic, a contradiction...

   Your proof by induction of the statement given in (*):

2. Use Eisenstein to prove that if p is a prime number, then $\Phi(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible in $\mathbb{Z}[x]$.

   We'll use three basic mathematical facts:

   (a) For $n \in \mathbb{N}$, $x^n - 1/x - 1 = x^{n-1} + \ldots + x + 1$.

   (b) If p is a prime number, $k \in \mathbb{N}$, and $p > k > 0$, then $p | \binom{p}{k}$.

   (c) If F is a field, $b(x) \in F[x]$, and $c \in F$, then $b(x)$ is irreducible if and only if $b(x - c)$ is irreducible.

   Proof. We'll show $\Phi(x+1)$ is irreducible, and apply the second fact above: We have $\Phi(x) = x^p - 1/x - 1$. So $\Phi(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = \frac{x^p + pc(x) + 1 - 1}{x}$, $c(x) \in \mathbb{Z}[x]$, and $c(x)$ has at least one. Thus, $\Phi(x+1) = x^{p-1} + pe(x) + p$, where $e(x)$ has degree one or more. Now it follows from Eisenstein that $\Phi(x+1)$ is irreducible in $\mathbb{Z}[x]$. The third fact above gives us that $\Phi(x)$ is irreducible in $\mathbb{Z}[x]$, completing the proof. $\square$

   Question. Is $\Phi(x)$ above irreducible over $\mathbb{Q}$? Justify your answer.

Part B: Some quiz 1 like problems. Quiz 1 is Feb. 14
R is always a ring. If R is a ring with 1, $1 \neq 0$.

1. Let R be a ring, and let I and J be two ideals of R. Let IJ be the subset of R consisting of all sums of the form $i_1 j_1 + \ldots i_m j_m$, where $\{i_1, \ldots, i_m\} \subseteq I, \{j_1, \ldots, j_m\} \subseteq J$, and $m \in \mathbb{N}$. Show that IJ is an ideal of R, and IJ is contained in $I \cap J$. Provide an example of a ring R and two ideals I and J such that IJ is properly contained in $I \cap J$.

2. Suppose R is s commutative ring with 1, and I and J are two ideals satisfying $I + J = R$. Show that $IJ = I \cap J$.

3. Prove that if R is a commutative ring with 1, R is a field if and only if R has no proper, non-trivial ideal.

4. If R is an integral domain and $R[x]$ is a UFD, prove that R is a UFD.

5. Prove that if R is an integral domain, and $b \in R$ is prime in R, then b is irreducible in R.

6. In $\mathbb{Z}[i]$, $2 = (i + 1)(i - 1)$. Use this fact to show that 2 is reducible in $\mathbb{Z}[i]$. To do so, remind yourself of the definition of the following: unit, irreducible, associate.

7. In $\mathbb{Z}[\sqrt{-5}]$, $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2(3)$. Use these equations, and the definitions of unit, irreducible, associate, and Unique Factorization Domain (UFD) to explain why $\mathbb{Z}[1 + \sqrt{-5}]$ is not a UFD.

8. Let R be an ED with Euclidean norm N. Prove that $b \in R$ with $N(r) = 0$, then either $r = 0$ or r is a unit.

9. Prove that if R is an Euclidean domain, then R is a PID.

10. Suppose R is a Euclidean Domain with a Euclidean norm N, and each $m \in \mathbb{N}$, $|\{r \in R : N(r) = m\}$ is a finite set. Explain why if I is a non-trivial ideal of R, then R/I is finite.

11. Let F be a field.
    (a) $p(x) \in F[x]$ is divisible by a linear polynomial of $F[x]$ if and only if $p(x)$ has a root (= a zero) in F.
    (b) Provide a short but completely convincing proof that if $p(x)$ has degree $n \in \mathbb{N}$, then $p(x)$ has no more than n roots. Do a proof by induction on $deg(p(x))$.

12. Let R be an integral domain. State Eisenstein's Criterion, and then **prove it**. Then use Eisenstein's Criterion to show that if p is a prime number, then $\Phi(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible in $\mathbb{Z}[x]$.

13. Prove that $\mathbb{Z}[i]/(1+i)$ is a two-element field, and prove that if q is a prime integer with $p \equiv\ 3\, mod\, 4$, then $\mathbb{Z}[x]/(q)$ is a field with q^2 elements.

14. True or false? Provide a specific counterexample.

   (a) If R is a field, then every subring of R is a subfield of R.
   (b) If R is an integral domain, then every homomorphic image of R is an integral domain.
   (c) If R is an integral domain, then every subring of R containing 1 is an integral domain.
   (d) If R is a ring, I is an ideal of R, and $\phi : R \to S$ is a homomorphism, then $\phi(I)$ is an ideal of S.
   (e) If R is a commutative ring with 1, and $b \in R$ is irreducible, then b is prime.
   (f) If R is a commutative ring with 1, and $b \in R$ is prime, then b is irreducible.
   (g) If p is a prime integer, then (p) is a prime ideal in $\mathbb{Z}[i]$.
   (h) Let F be a field, and let $n \in \mathbb{N}$. Then $I_n = \{f(x) \in F[x] : deg(f(x)) \geq n\}$ is an ideal of $F[x]$, and if n is prime, then I_n is a prime ideal of $F[x]$.
   (i) $\mathbb{Z}[x]$ is a PID.
   (j) In an integral domain R, every prime ideal is a maximal ideal.
   (k) $\mathbb{Z}[x]$ is a UFD.
   (l) If R is a commutative ring with 1, with elements b and c, then $(b)(c) = (bc)$.
   (m) If F is a field, then $F[x]$ is a Euclidean Domain.