Last time we proved the following theorem:

Theorem 1: An integral domain R is UFD if and only if every non-zero, non-invertible element in R is a product of prime elements.

Definition: An integral domain R is called principal ideal domain (PID) if every ideal in R is principal, i.e. of the form aR for some $a \in R$.

Example: $\mathbb{Z}$ is a PID; every field is a PID.

Proposition 1: If R is a PID and $a \in R$ is irreducible then a is prime and aR is a maximal ideal.

Proof: Let $a \in R$ be irreducible. Then aR is a proper ideal. We will show that aR is maximal. Since maximal ideals are prime, this will complete the proof.

Suppose $aR \subsetneq I$ for some ideal I. Since R is PID we have $I = bR$ for some $b \in R$. Since $aR \subseteq I = bR$, we have $b \mid a$ so $a = b \cdot c$ for some $c \in R$. Since $I = bR \neq aR$, a and b are not associated. Since a is irreducible, a and c must be associated and b is invertible, which means that $bR = R$. So the only ideal bigger than aR is R, i.e. aR is maximal. ☒

Suppose now that R is a PID and there is $a \in R$, $a \neq 0$, $a \notin R^\times$ which is not a product of irreducible elements.

Then, in particular, a is not irreducible, so $a=bc$ and $aR \subsetneq bR$, $aR \subsetneq cR$ for some $b, c \in R$ (i.e. b, c are not associated to a). If both b, c were products of irreducible elements, then so would be $a=bc$. Thus either b or c is not a product of irreducible elements. Pick one which is not and call it a_1. So $aR \subsetneq a_1 R$ and we can repeat the same reasoning to a_1 to get a_2 s.t. $a_1 R \subsetneq a_2 R$ and a_2 is not a product of irreducible elements. Keep repeating this process to get a sequence $aR \subsetneq a_1 R \subsetneq a_2 R \subsetneq a_3 R \subsetneq \cdots$ of ideals. Let J be the union of these ideals: $J = \bigcup_{i=1}^{\infty} a_i R$. We claim that J is an ideal of R. In fact let $x, y \in J$ and $r \in R$. Then $x \in a_m R$, $y \in a_n R$ for some m, n. We may assume that $m \leq n$ (if $m > n$, the argument is the same: swap the roles of m, n). Thus $a_m R \subseteq a_n R$ and therefore $x, y \in a_n R$. Since $a_n R$ is an ideal, $x - y \in a_n R$, $rx \in a_n R$ and $0 \in a_n R$. Since $a_n R \subseteq J$, we have $0 \in J$, $x - y \in J$, $rx = xr \in J$, so J is an ideal. Since R is a PID, we have $J = dR$ for some d. Now $d \in J$ so $d \in a_k R$ for some k which implies that $dR \subseteq a_k R \subsetneq a_{k+1} R \subseteq J = dR$. This is clearly a contradiction showing that our original assumption that a is not a product of irreducible elements was wrong. This means that all non-zero, non-invertible elements in R

are products of irreducible elements. Summarizing our discussion, we proved:

Theorem 2: If R is PID then R is UFD.

Pf: Let R be PID. We just proved that if $a \in R$, $a \neq 0$, $a \notin R^\times$ then a is a product of irreducible elements. By Proposition 1 all irreducible elements in R are prime. Thus Theorem 1 implies that R is a UFD. ☒

Corollary: $\mathbb{Z}$ is a UFD.

Consider now $a, b \in R$. We have $aR \cap bR$ is an ideal so $aR \cap bR = dR$ for some d. This means that $d \in aR$ and $d \in bR$ so $a|d$ and $b|d$. Also, if $a|c$ and $b|c$ then $c \in aR \cap bR = dR$, so $d|c$. We see that:

(1) d is a multiple of a and of b

(2) any multiple of a and of b is also a multiple of d.

Thus d is a least common multiple of a and b:

$$aR \cap bR = \mathrm{lcm}(a,b)R.$$

Similarly, $aR + bR = eR$ for some $e \in R$, so $aR \subseteq eR$ and $bR \subseteq eR$, ie. $e|a$ and $e|b$. Also, if $f|a$ and $f|b$ then $aR \subseteq fR$ and $bR \subseteq fR$ so $aR + bR \subseteq fR$, ie $eR \subseteq fR$ so $f|e$. We see that:

(1) e is a common divisor of a and b

(2) if f is a common divisor of a and b then $f|e$.

Thus e is "greatest" common divisor of a and b:

$$aR+bR=\gcd(a,b)R$$