We have the following lemma.

Lemma 1.2 Let R be an I.D. Then

1. Every prime element is irreducible
2. $0 \neq p \in R$. p is a prime element $\iff (p)$ is a prime ideal
3. The gcd of $a, b \in R$ is uniquely determined up to units (if it exists)

Proof: (1) Let $p \in R$ be prime and $p = ab$ w/ $a, b \in R$.

w.t.s.: either $a \in R^\times$, or $b \in R^\times$

$p = 1 \cdot p = ab$. Hence $p \mid p = ab$. But p is prime. Therefore $p \mid a$ or $p \mid b$. w.l.o.g assume $p \mid a$. Then $pr = a$ for some $r \in R$. We then have

$$p = ab = prb$$

This implies $p(1 - rb) = 0$. Since R is an I.D and $p \neq 0$, we have that $1 = rb$ and $b \in R^\times$.

(2) ($\Rightarrow$) Let $p \in R$ be a prime elt.

Recall: I prime ideal means, $I \neq R$ and $\forall a, b \in R$ with $ab \in I$ we have either $a \in I$ or $b \in I$.

w.t.s. (p) is a prime ideal

Note $(p) \neq R$ since otherwise $1 \in (p)$

Which means $1 = rp$ for some $r \in R$

and $p \in R^{\times}$.

Let $a, b \in R$ with $ab \in (p)$

Then $ab = rp$ for some $r \in R$

and hence $p \mid ab$. But p is prime

Hence $p \mid a$ or $p \mid b$ which implies

$a \in (p)$ or $b \in (p)$

Let $p \in R$, $p \neq 0$.

$(\Leftarrow)$ Let (p) be a prime ideal, $((p) \neq (0), p \neq 0)$

w.t.s: p is a prime element

$(p) \neq R$ by defn of prime ideal

Hence $1 \notin (p)$, and $p \notin R^{\times}$.

Suppose now $p \mid ab$. Then $\exists r \in R$ s.t

$pr = ab$. Hence $ab \in (p)$

But (p) is prime ideal. Hence

either $a \in (p)$ or $b \in (p)$

which then implies $p \mid a$ or $p \mid b$

(3) Let $a, b \in R \setminus \{0\}$, $d, \tilde{d}$ are 2 gcd's of a and b. Then by defn both $d, \tilde{d} \mid a$

$d, \tilde{d} \mid b$ and hence $d \mid \tilde{d}$, $\tilde{d} \mid d$

But then $d \cdot r = \tilde{d}$ and $\tilde{d}\tilde{r} = d$

for some $r, \tilde{r} \in R$. This means that

We then have $d r \tilde{r} = d$.

Which then implies that $d(1 - r\tilde{r}) = 0 \Rightarrow r, \tilde{r} \in R^{\times}$

since R is an I.D. and $d, \tilde{d}$ are associates as wanted

⑥ If R is not an I.D. then (0) is not a prime ideal. If $ab=0$ w/ $a\neq 0, b\neq 0$ then $ab\in(0)$ but $a\notin(0)$, $b\notin(0)$.

Rmk ① In $\mathbb{Z}$ every prime is irreducible and every irreducible elt is prime

In any ID prime $\Rightarrow$ irred (Lemma 1.2)

But for general ID irred $\not\Rightarrow$ prime

eg. $R=\mathbb{Z}[\sqrt{-5}]$

$$2.3=(1+\sqrt{-5})(1-\sqrt{-5})=6$$

Hence $2\mid(1+\sqrt{-5})(1-\sqrt{-5})$ but $2\nmid(1\pm\sqrt{-5})$

so 2 is not prime. (Note: if $2\mid 1+\sqrt{-5}$

$\Rightarrow 1+\sqrt{-5}=2(a+b\sqrt{-5})$, $a,b\in\mathbb{Z}$

$\Rightarrow 2a=1$ $a\in\mathbb{Z}$ $\cancel{\mathbb{Z}}$)

On the other hand 2 is irreducible since if $2=(a+b\sqrt{-5})(c+d\sqrt{-5})$ with $a,b,c,d\in\mathbb{Z}$, then

$$a^2+b^2 5 \mid 4$$

$\Rightarrow a=\pm 2,\ b=0$ or $a=\pm 1,\ b=0$

② Also if R is not an I.D we don't necessarily have prime $\Rightarrow$ irred. either.

eg. $R=\mathbb{Z}/6\mathbb{Z}$, $p=2$

If $2\mid ab$ in R then either $2\mid a$ or $2\mid b$

Hence 2 is prime but it is not irred since $2=2.4$ but neither 2 nor 4 is a unit in R.

③. In general rings, gcds do not need to exist!

eg $R = \mathbb{Z}[\sqrt{-5}]$. let $a = 6$, $b = 2+2\sqrt{-5}$

Both 2, and $1+\sqrt{-5}$ divide a and b

Hence if gcd(a,b) existed, it had to be a multiple of 2 and $1+\sqrt{-5}$

Exercise: Show that if gcd(a,b) exists say $c+d\sqrt{-5} = \text{gcd}(a,b)$.
Then $N(c+d\sqrt{-5}) := c^2+d^2 5$ has to be exactly 12, but in $\mathbb{Z}[\sqrt{-5}]$ there are no elts of norm 12.
Hence gcd of a and b does not exist in R.

One can show for the above defined $N: \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$, $a+b\sqrt{-5} \to a^2+b^2 5$

① N is multiplicative
② if $r \mid s$ in R, then $N(r) \mid N(s)$ in $\mathbb{Z}$
③ r is a unit in R $\Leftrightarrow N(r) = 1 \Leftrightarrow r = \pm 1$.

④ If 0 were prime then lemma 1-2, ① is clearly not correct. Since 0 is not irreducible. eg $0 = 5 \cdot 0 \in \mathbb{Z}$, and neither 5 nor 0 are units in $\mathbb{Z}$.

Also (0) is a prime ideal which is not max'l
And in a PID we'll see (r) is prime $\Leftrightarrow$ (r) maximal for $r \neq 0$.

Rmk The defining properties of gcd d of $a, b \in R$, an I.D are
(i) $d \mid a$ and $d \mid b$ and
(ii) If $\tilde{d} \mid a$, $\tilde{d} \mid b$ then $\tilde{d} \mid d$.

Note that: $b \mid a$ in a ring R
$\iff a \in (b) \iff (a) \subseteq (b)$

In particular if $d \mid a$ and $d \mid b$ then (d) contains both a and b and (d) contains the ideal (a, b)
Hence (i) and (ii) can be written in terms of the language of ideals as

Let $I = (a, b)$ ideal generated by a and b then d = gcd of a and b if
(i) $(a, b) \subset (d)$
(ii) If $(\tilde{d})$ is any principal ideal containing (a, b) then $(d) \subseteq (\tilde{d})$

Hence gcd of a, b (if it exists) is a generator for the smallest principal ideal containing a and b. ie

Lemma 1.3 Let R be a PID, $a, b \in R \setminus \{0\}$
If a and b have a greatest common divisor d then $(a, b) = (d)$

Proof. R is a PID, so (a,b) is principal ideal. So $(a,b) = (c)$ for some $c \in R$.

$(a,b) = (c) \Rightarrow a, b \in (c)$ and hence $c \mid a$ and $c \mid b$

Hence c is a common divisor of a and b. Since d is gcd of a and b $c \mid d$ and $(d) \subseteq (c)$

On the other hand, $d \mid a$ and $d \mid b$ hence $a, b \in (d)$ and hence $(c) = (a,b) \subseteq (d)$

In fact we have

Thm 1.4 R be a PID. TFAE

① $d = \gcd(a,b)$

② $(d) = (a,b)$ as ideals

③ $\exists\ x, y \in R$ s.t $d = ax + by$ and $\forall\ s, t \in R$, $d \mid as + bt$

④ $\exists\ x, y \in R$ s.t $d = ax + by$ and $d \mid a$ and $d \mid b$

Pf. In fact ②, ③, ④ are equivalent in I.D.

We'll show ② ⇒ ③ ⇒ ④ ⇒ ② in an I.D

① ⇒ ② Lemma 1.3 We'll prove ④ ⇒ ①