Kenneth Ireland & Michael Rosen A Classical Introduction to Modern Number Theory (Chapter 1 Solutions)

Khang Vinh Nguyen

February 27, 2022

Exercise 1. Let a and b be nonzero integers. We can find nonzero integers q and r such that $a = qb + r$, where $0 \leq r < b$. Prove that $(a, b) = (b, r)$ (these are ideals in $\mathbb{Z}$).

Proof. Let $m \in (a, b)$, then $m = ax + by$ for some $x, y \in \mathbb{Z}$. But $a = qb + r$, so we get $m = (qb + r)x + by = rx + b(qx + y)$, so $m \in (b, r)$ by definition. Vice versa, if $m \in (b, r)$, then $m = bx + ry$ for some $x, y \in \mathbb{Z}$. Using $a = qb + r$, we get $m = bx + (a - qb)y = ay + b(x - qy)$, so $m \in (a, b)$. We conclude that $(a, b) = (b, r)$ as sets. $\square$

Exercise 2 (continuation)**.** If $r \neq 0$, we can find q_1 and r_1 such that $b = q_1 r + r_1$, with $0 \leq r_1 < r$. Show that $\gcd(a,b) = \gcd(r, r_1)$. This process can be repeated. Show that it must end in finitely many steps. Show that the last nonzero remainder must equal $\gcd(a,b)$. The process looks like

$$\begin{aligned}
a &= qb + r, & 0 &\leq r < b, \\
b &= q_1 r + r_1, & 0 &\leq r_1 < r, \\
r &= q_2 r_1 + r_2, & 0 &\leq r_2 < r_1, \\
&\vdots \\
r_{k-1} &= q_{k+1} r_k + r_{k+1}, & 0 &\leq r_{k+1} < r_k, \\
r_k &= q_{k+2} r_{k+1}.
\end{aligned}$$

Proof. From the previous exercise (and the fact that $\gcd(a,b)$ is the least positive integer d such that $(a,b) = (d)$), we get $\gcd(a,b) = \gcd(b,r) = \gcd(r,r_1) = \cdots = \gcd(r_k, r_{k+1})$.

The process eventually stops since $b, r, r_1, r_2, \ldots$ is a strictly decreasing sequence of non-negative integers (in fact, the sequence stops once it reaches zero, in this case $r_{k+2} = 0$). Otherwise, by induction, we can show that

$$r_k \leq r_{k-1} - 1 \leq \cdots \leq r_1 - (k-1) \leq r - k \leq b - (k+1), \qquad k \geq 1$$

When $k = b$, $r_k \leq -1$ cannot be non-negative, a contradiction.

Since $r_{k+2} = 0$ according to the last division, we have $r_{k+1} \mid r_k$. Therefore, $\gcd(a,b) = \gcd(r_k, r_{k+1}) = r_{k+1}$. $\square$

Exercise 3. Calculate $\gcd(187, 221), \gcd(6188, 4709), \gcd(314, 159)$.

Solution. *$\gcd(187, 221) = 17$ since

$$\begin{aligned} 221 &= 1 \cdot 187 + 34 \\ 187 &= 5 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

*$\gcd(6188, 4709) = 17$ since

$$\begin{aligned} 6188 &= 1 \cdot 4709 + 1479 \\ 4709 &= 3 \cdot 1479 + 272 \\ 1479 &= 5 \cdot 272 + 119 \\ 272 &= 2 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

*$\gcd(314, 159) = 1$

$$\begin{aligned} 314 &= 1 \cdot 159 + 155 \\ 159 &= 1 \cdot 155 + 4 \\ 155 &= 38 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

□

Exercise 4. Let $d = \gcd(a, b)$. Show how one can use the EucJidean algorithm to find numbers m and n such that $am + bn = d$ (*Hint*: In Exercise 2 we have that $d = r_{k+1}$. Express r_{k+1} in terms of r_k and r_{k-1}, then in terms of r_{k-1} and r_{k-2}, etc.)

Proof. Let the following be the Euclidean algorithm for computing $d = \gcd(a, b)$

$$
\begin{aligned}
a &= qb + r, & 0 &\le r < b,\\
b &= q_1 r + r_1, & 0 &\le r_1 < r,\\
r &= q_2 r_1 + r_2, & 0 &\le r_2 < r_1,\\
&\vdots\\
r_{k-1} &= q_{k+1} r_k + r_{k+1}, & 0 &\le r_{k+1} < r_k,\\
r_k &= q_{k+2} r_{k+1}.
\end{aligned}
$$

From Exercise 2, we know that $d = r_{k+1}$. Thus,

$$
\begin{aligned}
d = r_{k+1} &= r_{k-1} - q_{k+1} r_k\\
r_k &= r_{k-2} - q_k r_{k-1}\\
r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2}\\
&\vdots\\
r_2 &= r - q_2 r_1\\
r_1 &= b - q_1 r\\
r &= a - qb
\end{aligned}
$$

Keeping d on one side, and sequentially substituting r_i by a linear combination of r_{i-1} and r_{i-2} (according to the above), we get

$$
\begin{aligned}
d &= r_{k-1} - q_{k+1} r_k\\
&= r_{k-1} - q_{k+1}(r_{k-2} - q_k r_{k-1})\\
&= m_k r_{k-2} + n_k r_{k-1} && (m_k = -q_{k+1}, \quad n_k = 1 + q_k)\\
&= m_k r_{k-2} + n_k (r_{k-3} - q_{k-1} r_{k-2})\\
&= m_{k-1} r_{k-3} + n_{k-1} r_{k-2} && (m_{k-1} = n_k, \quad n_{k-1} = m_k - n_k q_{k-1})\\
&\vdots\\
&= m_3 r_1 + n_3 r_2\\
&= m_3 r_1 + n_3 (r - q_2 r_1)\\
&= m_2 r + n_2 r_1 && (m_2 = n_3, \quad n_2 = m_3 - n_3 q_2)\\
&= m_2 r + n_2 (b - q_1 r)\\
&= m_1 b + n_1 r && (m_1 = n_2, \quad n_1 = m_2 - n_2 q_1)\\
&= m_1 b + n_1 (a - qb)\\
&= m_0 a + n_0 b && (m_0 = n_1, \quad n_0 = m_1 - n_1 q)
\end{aligned}
$$

$\square$

Exercise 5. Find m and n for the pairs a and b given in Exercise 3

Solution. *For $\gcd(187, 221) = 17$

$$\begin{aligned} 17 &= 187 - 5 \cdot 34 \\ &= 187 - 5(221 - 187) \\ &= 6 \cdot 187 - 5 \cdot 221 \end{aligned}$$

*For $\gcd(6188, 4709) = 17$

$$\begin{aligned} 17 &= 119 - 3 \cdot 34 \\ &= 119 - 3(272 - 2 \cdot 119) \\ &= 7 \cdot 119 - 3 \cdot 272 \\ &= 7(1479 - 5 \cdot 272) - 3 \cdot 272 \\ &= 7 \cdot 1479 - 38 \cdot 272 \\ &= 7 \cdot 1479 - 38(4709 - 3 \cdot 1479) \\ &= 121 \cdot 1479 - 38 \cdot 4709 \\ &= 121(6188 - 4709) - 38 \cdot 4709 \\ &= 121 \cdot 6188 - 159 \cdot 4709 \end{aligned}$$

*For $\gcd(314, 159) = 1$

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (155 - 38 \cdot 4) \\ &= 39 \cdot 4 - 155 \\ &= 39(159 - 155) - 155 \\ &= 39 \cdot 159 - 40 \cdot 155 \\ &= 39 \cdot 159 - 40(314 - 159) \\ &= 79 \cdot 159 - 40 \cdot 314 \end{aligned}$$

□

Exercise 6. Let $a, b, c \in \mathbb{Z}$. Show that the equation $ax + by = c$ has solutions in integers iff $\gcd(a, b) \mid c$.

Proof. Suppose $ax + by = c$ has solutions in integers, then $c \in (a, b)$. Since $(a, b) = (d)$ where $\gcd(a, b) = d$, we have $c \in (d)$, or simply $\gcd(a, b) \mid c$. Elementarily, note that a, b are divisibly by $\gcd(a, b)$, so $c = ax + by$ is also divisible by $\gcd(a, b)$.

Vice versa, suppose $\gcd(a, b) \mid c$. Exercise 4 produces us a pair of integers (m, n) such that $am + bn = \gcd(a, b)$. Let $k = \frac{c}{\gcd(a,b)}$. By assumption, k is an integer. Hence, $a(km) + b(kn) = k(am + bn) = k \gcd(a, b) = c$, and so $x_0 = km, y_0 = kn$ is a solution to $ax + by = c$. $\square$

Exercise 7. Let $d = \gcd(a, b)$ and $a = da', b = db'$. Show that $\gcd(a', b') = 1$.

First Proof. Let $d' = \gcd(a', b')$, then $d' \mid a', b'$. Since $a = da'$ and $b = db'$, we have $dd' \mid a, b$. But $d = \gcd(a, b)$, so any common divisor of a, b must divide d, i.e. $dd' \mid d$. Canceling d on both side, we get $d' \mid 1$, or simply $d' = 1$ (since the greatest common divisor is defined to be always positive). $\square$

Second Proof. From Exercise 6, we know there exists some integers m, n such that $am + bn = d$. Dividing d' on both side, we get $a'm + b'n = 1$. Again, by Exercise 6, we know that $\gcd(a', b') \mid 1$. But $\gcd(a', b')$, so we get $\gcd(a', b') = 1$. $\square$

Exercise 8. Let x_0 and y_0 be a solution to $ax + by = c$. Show that all solutions have the form $x = x_0 + t\frac{b}{d}, y = y_0 - t\frac{a}{d}$ where $d = (a, b)$ and $t \in \mathbb{Z}$.

Proof. Suppose (x, y) are any solution to $ax+by = c$. Then $a(x-x_0)+b(y-y_0) = 0$, or

$$\frac{b}{d}(y - y_0) = -\frac{a}{d}(x - x_0)$$

Note that $\frac{b}{d} \mid -\frac{a}{d}(x - x_0)$, but $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (Exercise 7), so $\frac{b}{d} \mid x - x_0$. Let $x - x_0 = t\frac{b}{d}$ and substitute into the previous equation, we get

$$\begin{aligned} \frac{b}{d}(y - y_0) &= -\frac{a}{d}(x - x_0) \\ \frac{b}{d}(y - y_0) &= -\frac{a}{d} \cdot t \cdot \frac{b}{d} \\ y - y_0 &= -t\frac{a}{d} \end{aligned}$$

Thus any solution is always of the form $x = x_0 + t\frac{b}{d}, y = y_0 - t\frac{a}{d}$ for some $t \in \mathbb{Z}$. On the other hand, for all $t \in \mathbb{Z}$

$$a\left(x_0 + t\frac{b}{d}\right) + b\left(y_0 - t\frac{a}{d}\right) = ax_0 + t\frac{ab}{d} + by_0 - t\frac{ba}{d} = c$$

So those are all (integer) solutions of $ax + by = c$. $\square$

Exercise 9. Suppose that $u, v \in \mathbb{Z}$ and that $\gcd(u, v) = 1$. If $u \mid n$ and $v \mid n$, show that $uv \mid n$. Show that this is false if $\gcd(u, v) \neq 1$.

Proof. If $\gcd(u, v) \neq 1$, then $u = v = n = 2$ should suffice (as $4 \nmid 2$). As for $\gcd(u, v) = 1$, let $n = ux = vy$ for some $x, y \in \mathbb{Z}$. In particular, we have $v \mid ux$. Yet $\gcd(u, v) = 1$, so we get $v \mid x$. In other words, $uv \mid ux = n$. $\square$

Exercise 10. Suppose that $\gcd(u, v) = 1$. Show that $\gcd(u+v, u-v)$ is either 1 or 2.

Proof. Let $d = \gcd(u+v, u-v)$, then $d \mid u+v, u-v$, and so

$$d \mid (u+v) + (u-v) = 2u$$
$$d \mid (u+v) - (u-v) = 2v$$

Hence, $d \mid \gcd(2u, 2v)$. Since $\gcd(u, v) = 1$, Exercise 6 implies that there exists some $m, n \in \mathbb{Z}$ such that $um + vn = 1$. Multiplying 2 on both side, we get $(2u)m + (2v)n = 2$, so $\gcd(2u, 2v) \mid 2$. Combining the previous result, we get $d \mid 2$, so either $d = 1$ or $d = 2$. $\square$

Remark 10.1. There is another way to show $\gcd(au, av) = a\gcd(u, v)$, assuming $a \geq 0$. Suppose $d \mid au, av$, let $t = \gcd(d, a)$. By Exercise 7, $\gcd\left(\frac{d}{t}, \frac{a}{t}\right) = 1$, so since $d \mid au$, we get $\frac{d}{t} \mid \frac{a}{t}u$, and thus, $\frac{d}{t} \mid u$. Similarly, $\frac{d}{t} \mid v$, so $\frac{d}{t} \mid \gcd(u, v)$. Multiplying both side by t, we get $d \mid t\gcd(u, v) \mid a\gcd(u, v)$. Vice versa, suppose $d \mid a\gcd(u, v)$. Again, let $t = \gcd(a, d)$, then we get $\frac{d}{t} \mid \frac{a}{t}\gcd(u, v)$, so $\frac{d}{t} \mid \gcd(u, v)$. In particular, $\frac{d}{t} \mid u$, so by multiplying t on both side, we get $d \mid tu \mid au$. Similarly, $d \mid av$.

What we have just shown is that $d \mid au, av$ iff $d \mid a\gcd(u, v)$. But $d \mid au, av$ iff $d \mid \gcd(au, av)$, so $d \mid \gcd(au, av)$ iff $d \mid a\gcd(u, v)$. Thus,

$$\gcd(au, av) = |\gcd(au, av)| = |a\gcd(u, v)| = a\gcd(u, v)$$

Exercise 11. Show that $\gcd(a, a+k) \mid k$

Proof. Like previous exercise, let $d = \gcd(a, a+k)$. Then $d \mid a, a+k$, so $d \mid (a+k) - a = k$. $\square$

Exercise 12. Suppose that we take several copies of a regular polygon and try to fit them evenly about a common vertex. Prove that the only possibilities are six equilateral triangles, four squares, and three hexagons.

Proof. Since the vertex angle of an regular n-gon is $\frac{n-2}{n}\pi$, so if there are k copies that can fit around a vertex, then we have

$$k\left(\frac{n-2}{n}\pi\right) = 2\pi$$
$$k(n-2) = 2n$$

Necessarily, $(n-2) \mid 2n = 2(n-2)+4$, so we get $(n-2) \mid 4$. Note that $n-2 \geq 1$, so the only possibilities are $n-2 \in \{1, 2, 4\}$. Equivalently, $n \in \{3, 4, 6\}$.

1. If $n = 3$: then $k = 2n/(n-2) = 6$. So we can fit 6 equilateral triangles around a vertex.

2. If $n = 4$: then $k = 2n/(n-2) = 4$. So we can fit 4 squares around a vertex.

3. If $n = 6$: then $k = 2n/(n-2) = 3$. So we can fit 3 regular hexagons around a vertex.

$\square$

Exercise 13. Let $n_1, n_2, \ldots, n_s \in \mathbb{Z}$. Define the greatest common divisor d of $n_1, n_2, \ldots, n_s$ and prove that there exist integers $m_1, m_2, \ldots, m_s$ such that $n_1m_1 + n_2m_2 + \cdots + n_sm_s = d$.

Proof. Let $(n_1, n_2, \ldots, n_s) = \{z_1n_1 + z_2n_2 + \cdots + z_sn_s : z_1, z_2, \ldots, z_s \in \mathbb{Z}\}$. Since $|n_1| \in (n_1, n_2, \ldots, n_s)$, there exists some positive integers in $(n_1, n_2, \ldots, n_s)$. By well-ordering principle, let d' to be the smalllest such. We will show that $d = d'$, and hence, there exists integers $m_1, m_2, \ldots, m_s$ such that $n_1m_1 + n_2m_2 + \cdots + n_sm_s = d$.

Since $d = \gcd(n_1, n_2, \ldots, n_s)$, then given $d' = n_1m_1 + n_2m_2 + \cdots + n_sm_s$, we must have $d \mid d'$. On the other hand, d' must divide each n_i $(i = \overline{1, s})$. In other words, d' is a common divisor, so by definition, $d' \mid d$. Both d and d' are positive, so we must have $d = d'$. $\square$

Exercise 14. Discuss the solvability of $a_1x_1 + a_2x_2 + \cdots + a_rx_r = c$ in integers (*Hint*: Use Exercise 13 to extend the reasoning behind Exercise 6.)

Solution. Suppose there exists some $x_1, x_2, \ldots, x_r$ such that $a_1x_1 + a_2x_2 + \cdots + a_rx_r = c$, then $\gcd(a_1, a_2, \ldots, a_r) \mid c$ since $\gcd(a_1, a_2, \ldots, a_r)$ divides each a_i for $1 \leq i \leq r$. Vice versa, suppose $\gcd(a_1, a_2, \ldots, a_r) \mid c$. Then by Exercise 13, there exists some integers $m_1, m_2, \ldots, m_r$ such that $a_1m_1 + a_2m_2 + \cdots + a_rm_r = \gcd(a_1, a_2, \ldots, a_r)$. Denote $k = c/\gcd(a_1, a_2, \ldots, a_r)$, which is an integer by assumption. We thus get

$$\begin{aligned} a_1(km_1) + a_2(km_2) + \cdots + a_r(km_r) &= k(a_1m_1 + a_2m_2 \cdots + a_rm_r) \\ &= k \gcd(a_1, a_2, \ldots, a_r) = c \end{aligned}$$

In other words, there exists a solution to $a_1x_1 + a_2x_2 + \cdots + a_rx_r = c$ $\square$

Remark 14.1. One can solve such equation as follows:

1. We group the first $r-1$ variables so that $(a_1x_1 + \cdots + a_{r-1}x_{r-1}) + a_rx_r = c$.
2. For the first group $a_1x_1 + \cdots + a_{r-1}x_{r-1}$, it is always a multiple of $d = \gcd(a_1, \ldots, a_{r-1})$ and vice versa, so we can set it to dy for some integer y.
3. Since $\gcd(a_1, \ldots, a_r) = \gcd(\gcd(a_1, \ldots, a_{r-1}), a_r) = \gcd(d, a_r)$ and $\gcd(a_1, \ldots, a_r) \mid c$, there exists a solution to $dy + a_rx_t = c$.
4. Fixing y, we repeat the process for $a_1x_1 + \cdots + a_{r-1}x_{r-1} = dy$. Note that $d = \gcd(a_1, \ldots, a_{r-1})$ so there exists a solution to $a_1x_1 + \cdots + a_{r-1}x_{r-1} = d$. Scaling by y gives us a solution.

However, there is no closed form for the solutions.

Exercise 15. Prove that $a \in \mathbb{Z}$ is the square of another integer iff $\operatorname{ord}_p a$ is even for all primes p. Give a generalization.

Proof. We prove that $a > 0$ is an r-th power of some integer iff $\operatorname{ord}_p a$ is divisible by r for all primes p. Suppose $a = b^r$ for some $b \in \mathbb{Z}$. Then $\operatorname{ord}_p a = \operatorname{ord}_p b^r = r \operatorname{ord}_p b$ by unique factorization. Thus, $r \mid \operatorname{ord}_p a$ for each prime p. Vice versa, suppose $r \mid \operatorname{ord}_p a$. Let $\beta_p = \frac{\operatorname{ord}_p a}{r}$, and $b = \prod_p p^{\beta_p}$ (the sign of b is so that a has the same sign as b^r). We then have $b^r = \prod_p p^{r\beta_p} = \prod_p p^{\operatorname{ord}_p a} = a$. $\square$

Exercise 16. If $\gcd(u,v)=1$ and $uv=a^2$ (with $u,v\geq 0$), show that both u and v are squares.

First proof. Let $b=\gcd(u,a)$ and $c=\gcd(v,a)$. We will show that $u=b^2$ and $v=c^2$. By Exercise 4, there exists some $x,y\in\mathbb{Z}$ such that $b=ux+ay$. Squaring on both side, we get

$$\begin{aligned} b^2 &= u^2x^2+2uaxy+a^2y^2 \\ &= u^2x^2+2uaxy+uvy^2 \\ &= u(ux^2+2axy+vy^2) \end{aligned}$$

Hence, $u\mid b^2$. On the other hand, there also exists some $m,n\in\mathbb{Z}$ such that $um+vn=1$. Multiplying u on both side we get $u=u^2m+uvn=u^2m+a^2n$. Note that $b=\gcd(u,a)$, so $b^2\mid u^2,a^2$. From there, we have $b^2\mid u^2m+a^2n=u$. We conclude that $u=b^2$ (both are non-negative). Similarly, $v=c^2$. □

Second proof. Let $u=\prod_p p^{\mu_p}, v=\prod_p p^{\nu_p}$ be the factorizations of u,v. Since $\gcd(u,v)=1$, we must have $\mu_p\nu_p=0$ at each prime p (i.e. the exponent of p in u,v cannot both be non-zero). Yet $uv=a^2$, so $\mu_p+\nu_p$ must be divisible by 2. Since one of them is zero, it must be that the other must be divisible 2. In either case, μ_p,ν_p are always even for each prime p. By Exercise 15, u,v must be squares. □

Exercise 17. Prove that the square root of 2 is irrational, i.e., that there is no rational number $r = a/b$ such that $r^2 = 2$.

Proof. Suppose otherwise, that a/b is a rational number such that $(a/b)^2 = 2$. Equivalently, $a^2 = 2b^2$. Consider the exponent of the prime factor 2 on both side, we have $2 \operatorname{ord}_2 a = 1 + \operatorname{ord}_2 b$, which is impossible since the left-hand side (LHS) is even, while the right-hand side (RHS) is odd. $\square$

Exercise 18. Prove that $\sqrt[n]{m}$ is irrational if m is not the n-th power of an integer.

Proof. Suppose otherwise, that a/b is a rational number such that $(a/b)^n = m$. Equivalently, $a^n = mb^n$. Since m is not the n-th power of an integer, Exercise 15 (or rather the generalization) tells us that, for some prime p, $\operatorname{ord}_p m$ is not divisible by n. Consider the exponent of p on both side of $a^n = mb^n$, we must have $n \operatorname{ord}_p a = \operatorname{ord}_p m + n \operatorname{ord}_p b$. In other words, $n(\operatorname{ord}_p a - \operatorname{ord}_p b) = \operatorname{ord}_p m$, so $\operatorname{ord}_p m$ must be divisible by n, contradicting the previous assertion. Therefore, $\sqrt[n]{m}$ is irrational. $\square$

Exercise 19. Define the least common multiple of two integers a and b to be an integer m such that $a \mid m, b \mid m$, and m divides every common multiple of a and b. Show that such an m exists. It is determined up to sign. We shall denote it by $\operatorname{lcm}(a, b)$ (or $[a, b]$).

Proof. Let P be the intersection of $a\mathbb{Z} = \{an : n \in \mathbb{Z}\}$ and $b\mathbb{Z} = \{bn : n \in \mathbb{Z}\}$. Note that $|ab| \in P$, so there exists some positive integer in P. By well-ordering principle, there exists the smallest such $m > 0$. Since $m \in a\mathbb{Z}$, m is a multiple of a. Similarly, m is a multiple of b.

To show m is the least common multiple of a and b, we need to show $m \mid \ell$ for any ℓ that is a common multiple of both a and b. Let $m = q\ell + r, 0 \leq r < \ell$ be the Euclidean division of m by ℓ. Since $a \mid m, \ell$, we also have $a \mid m - q\ell = r$. Similarly, $b \mid r$. However, m is the least positive integer that is a multiple of both a and b, so $r = 0$ necessarily. We conclude that $m \mid \ell$.

Now if $\ell \mid m$ additionally, then we must have $|\ell| = |m|$, i.e. the least common multiple is uniquely defined up to its sign. $\square$

Exercise 20. Prove the following

1. $\operatorname{ord}_p \operatorname{lcm}(a,b) = \max(\operatorname{ord}_p a, \operatorname{ord}_p b)$
2. $\gcd(a,b)\operatorname{lcm}(a,b) = ab$ (assuming a, b are non-negative)
3. $\gcd(a+b, \operatorname{lcm}(a,b)) = \gcd(a,b)$

Proof. Part 1: let $m = \operatorname{lcm}(a,b)$, then $a \mid m$. Using factorization, this means that $p^{\operatorname{ord}_p a} \mid p^{\operatorname{ord}_p m}$, or simply $\operatorname{ord}_p a \leq \operatorname{ord}_p m$ for each prime p. Similarly, $\operatorname{ord}_p b \leq \operatorname{ord}_p m$, so $\max(\operatorname{ord}_p a, \operatorname{ord}_p b) \leq \operatorname{ord}_p m$. On the other hand, the number $\ell = \prod_p p^{\max(\operatorname{ord}_p a, \operatorname{ord}_p b)}$ is a common multiple of a and b (note there are finite many prime with positive exponent) since $\operatorname{ord}_p \ell \geq \operatorname{ord}_p a, \operatorname{ord}_p b$ by definition, so $m \mid \ell$. In particular, $\operatorname{ord}_p m \leq \operatorname{ord}_p \ell = \max(\operatorname{ord}_p a, \operatorname{ord}_p b)$. Hence, $\operatorname{ord}_p m = \max(\operatorname{ord}_p a, \operatorname{ord}_p b)$.
Part 2: by similar argument, we also have $\operatorname{ord}_p \gcd(a,b) = \min(\operatorname{ord}_p a, \operatorname{ord}_p b)$ for each prime p. Using the identity $\max(u,v)+\min(u,v) = u+v$ (wlog, assume $u \geq v$, then $\max(u,v)+\min(u,v) = u+v$), we get

$$\begin{aligned}
\operatorname{ord}_p(ab) &= \operatorname{ord}_p a + \operatorname{ord}_p b \\
&= \min(\operatorname{ord}_p a, \operatorname{ord}_p b) + \max(\operatorname{ord}_p a, \operatorname{ord}_p b) \\
&= \operatorname{ord}_p \gcd(a,b) + \operatorname{ord}_p \operatorname{lcm}(a,b)
\end{aligned}$$

As p prime varies, this means $\gcd(a,b)\operatorname{lcm}(a,b) = ab$ (as $a, b \geq 0$).
Part 3: we first show the distribution law $\gcd(x, \operatorname{lcm}(y,z)) = \operatorname{lcm}(\gcd(x,y), \gcd(x,z))$. Indeed, at each prime p

$$\begin{aligned}
\operatorname{ord}_p \gcd(x, \operatorname{lcm}(y,z)) &= \min(\operatorname{ord}_p x, \max(\operatorname{ord}_p y, z)) \\
&= \max(\min(\operatorname{ord}_p x, \operatorname{ord}_p y), \min(\operatorname{ord}_p x, \operatorname{ord}_p z)) \\
&= \operatorname{lcm}(\gcd(x,y), \gcd(x,z))
\end{aligned}$$

The second-to-last equality is due to distribution law on maximum and minimum. From there, we have

$$\begin{aligned}
\gcd(a+b, \operatorname{lcm}(a,b)) &= \operatorname{lcm}(\gcd(a+b,a), \gcd(a+b,b)) \\
&= \operatorname{lcm}(\gcd(b,a), \gcd(a,b)) = \gcd(a,b)
\end{aligned}$$

The second-to-last equality equality is due to Exercise 1. $\square$

Exercise 21. Prove that $\operatorname{ord}_p(a+b) \geq \min(\operatorname{ord}_p a, \operatorname{ord}_p b)$ with equality holding if $\operatorname{ord}_p a \neq \operatorname{ord}_p b$.

Proof. Let $u = \operatorname{ord}_p a, v = \operatorname{ord}_p b$, then $a = p^u m, b = p^v n$ for some $p \nmid m, n$. Without loss of generality (WLOG), suppose $u \geq v$. We then have $a + b = p^v(p^{u-v}m + n)$, so $\operatorname{ord}_p(a + b) \geq v = \min(u, v) = \min(\operatorname{ord}_p a, \operatorname{ord}_p b)$. If $u \neq v$, then $p^{u-v}m$ is divisible by p, but n is not, so $p^{u-v}m + n$ is not divisible by p. Hence, $\operatorname{ord}_p(a + b) = v$, i.e. equality holds. $\square$

Exercise 22. Almost alI the previous exercises remain valid if instead of the ring $\mathbb{Z}$ we consider the ring $k[x]$. Indeed, in most we can consider any EucJidean domain. Convince yourself of this fact. For simplicity we shall continue to work in $\mathbb{Z}$

Proof. Recall that a Euclidean domain D is an integral domain with a function $\lambda : D\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ (non-negative integer) such that if $a, b \in R, b \neq 0$, there exists $q, r \in R$ such that $a = qb + r$, and either $r = 0$ or $\lambda(r) < \lambda(b)$ (the function is not required to be compatible with other structure on D).

1. Exercise 3, 5, 12, 17, 18 are explicitly stated in $\mathbb{Z}$, so there's no generalization to Euclidean domain.

2. Exercise 1, 2, 4 depends directly on the fact that D is Euclidean domain.

3. Exercise 6, 7, 8, 9, 11, 13, 14 rely on the fact that D is a PID (or rather a Bézout domain, where every finitely generated ideal is principal, not *every* ideal is principal).

4. Exercise 10 (generalization) works in any commutative ring with unity: if $(u, v) = (1) = D$, then $(2) \subseteq (u + v, u - v)$ (thus if $(d) = (u + v, u - v)$, then $d \mid 2$).

   The proof is as follows: given $r \in D$, then there exists some $m, n \in D$ such that $um + vn = r$. We then get

   $$\begin{aligned} 2r &= (2u)m + (2v)n = [(u + v) + (u - v)]m + [(u + v) - (u - v)]n \\ &= (u + v)(m + n) + (u - v)(m - n) \end{aligned}$$

   Therefore, $2r \in (u + v, u - v)$.

5. Exercise 16 (generalization) works in any commutative ring R with unity: suppose I, J, K are ideals such that $IJ = K^2$ and $I + J = R$, then $I = (I + K)^2, J = (J + K)^2$.

   The proof is as follows:

   (a) Suppose $i \in I$, then there exists $j \in J$ such that $i + j = 1$. Thus, $i = i^2 + ij$. But $ij \in IJ = K^2$, so we can represent $ij = \sum_\alpha k_\alpha l_\alpha$ for some $k_\alpha, l_\alpha \in K$. In other words, $i = i^2 + \sum_\alpha k_\alpha l_\alpha$. Since $I, K \subseteq I + K$, we know that $i \in I^2 + K^2 \subseteq (I + K)^2$.

   (b) Vice versa, note that an element of $(I + K)^2$ is always of the form

   $$\sum_\alpha (i_\alpha + k_\alpha)(j_\alpha + l_\alpha) = \sum_\alpha i_\alpha j_\alpha + \sum_\alpha (i_\alpha l_\alpha + j_\alpha k_\alpha) + \sum_\alpha k_\alpha l_\alpha$$

   for some $i_\alpha, j_\alpha \in I; k_\alpha, l_\alpha \in K$. In the latter sum (with 3 terms): the first term is in $I^2 \subseteq I$, the second term is in $IK \subseteq I$, and the last term is in $K^2 = IJ \subseteq I$. Thus, $(I + K)^2 \subseteq I^2 + IK + K^2 \subseteq I + I + I = I$.

Since we have both inclusion of I and $(I+K)^2$ into one another, we get $I = (I+K)^2$. Similarly, $J = (J+K)^2$.

When $R = \mathbb{Z}$ and $I = (u), J = (v), K = (a)$ (with $IJ = (uv), K^2 = (a^2), I + J = (\gcd(u,v)) = (1)$), we get the original exercise.

6. Exercise 15, 19, 20a, 21 work in a UFD.

7. However, 20b and 20c need a modification (both works in Bézout domain)

   (a) Part 20b: show that $(a,b) \cdot [(a) \cap (b)] = (ab)$.

   To prove, let $(d) = (a,b), (m) = (a) \cap (b)$. Then $\frac{ab}{d} = a\frac{b}{d}$, so $\frac{ab}{d} \in (a)$. Similarly, $\frac{ab}{d} \in (b)$, so $\frac{ab}{d} \in (m)$ necessarily. In other words, $ab \in (dm)$. On the other hand, suppose $d = ax + by$ and $m = az = bw$ for some $x, y, z, w \in D$. Then $dm = (ax)(bw) + (by)(az) = ab(xw + yz)$, so $dm \in (ab)$. We conclude that $(ab) = (dm) = (d)(m) = (a,b) \cdot [(a) \cap (b)]$.

   (b) Part 20c: $(a+b) + [(a) \cap (b)] = (a,b)$.

   To prove, we need the identity $(x) + [(y) \cap (z)] = (x,y) \cap (x,z)$. Note if $I = (p_i : 1 \leq i \leq n)$ and $J = (q_j : 1 \leq j \leq m)$ are finitely generated ideals, then $IJ = (p_i q_j : 1 \leq i \leq n, 1 \leq j \leq m)$, so

$$\begin{aligned}
(x,y)(y,z)(z,x) &= (x^2y, x^2z, y^2z, y^2x, z^2x, z^2y, xyz) \\
&= (x,y,z)(xy, yz, zx) \\
&= (x,y,z)[(xy, zx) + (yz)] \\
&= (x,y,z)[(x)(y,z) + (yz)]
\end{aligned}$$

   Yet by part (20b) (and the fact that D is a PID), we have $(x,y)(z,x) = [(x,y) + (z,x)][(x,y) \cap (z,x)] = (x,y,z)[(x,y) \cap (z,x)]$ and $(yz) = (y,z)[(y) \cap (z)]$. Therefore,

$$\begin{aligned}
(x,y,z)[(x,y) \cap (z,x)](y,z) &= (x,y)(y,z)(z,x) \\
&= (x,y,z)[(x)(y,z) + (yz)] \\
&= (x,y,z)[(x)(y,z) + (y,z)[(y) \cap (z)]] \\
&= (x,y,z)(y,z)[(x) + [(y) \cap (z)]]
\end{aligned}$$

   We can cancel ideals in a PID, which helps us get the identity $(x,y) \cap (z,x) = (x) + [(y) \cap (z)]$. If one to go by normal route, let $I = (x,y,z)(y,z) = (q) \neq (0)$, then $(q)[(x,y) \cap (z,x)] = (q)[(x) + [(y) \cap (z)]]$. If $a \in (x,y) \cap (z,x)$, then there exists some $v \in D, b \in (x) + [(y) \cap (z)]$ such that $qa = (qv)b$. In other words, $a = bv$ since $q \neq 0$, so $a \in (x) + [(y) \cap (z)]$. Similarly, we also have $a \in (x,y) \cap (z,x)$ whenever $a \in (x) + [(y) \cap (z)]$.

Using the identity above, we get $(a+b) \cap [(a) \cap (b)] = (a+b, a) \cap (a+b, b) = (b, a) \cap (a, b) = (a, b)$.

$\square$

Exercise 23. Suppose that $a^2+b^2=c^2$ with $a,b,c\in\mathbb{Z}$. For example, $3^2+4^2=5^2$ and $5^2+12^2=13^2$. Assume that $\gcd(a,b)=\gcd(b,c)=\gcd(c,a)=1$. Prove that there exist integers u and v such that $c-b=2u^2$ and $c+b=2v^2$ and $\gcd(u,v)=1$ (there is no loss in generality in assuming that b and c are odd and that a is even). Consequently $a=2uv$, $b=v^2-u^2$, and $c=v^2+u^2$. Conversely show that if u and v are given, then the three numbers a, b, and c given by these formulas satisfy $a^2+b^2=c^2$.

Proof. The converse direction is rather apparent: $(2uv)^2+(v^2-u^2)^2=4u^2v^2+v^4-2v^2u^2+u^4=v^4+2v^2u^2+u^4=(v^2+u^2)^2$. As for the forward direction, note if a,b are both even, then c is also even, contradicting the pairwise co-prime condition. If a,b are both odd, then considering modulo 4: $c^2\equiv 0,1 \pmod 4$, yet $a^2+b^2\equiv 1+1\equiv 2 \pmod 4$ (since a,b are odd), contradicting $a^2+b^2=c^2$. Therefore, WLOG, we can assume that a is even, and b is odd, which makes c also odd.

Rewrite $a^2=c^2-b^2=(c-b)(c+b)$. By Exercise 10, either $\gcd(c-b,c+b)=1$, or $\gcd(c-b,c+b)=2$. Both b,c are odd, so $c-b,c+b$ are even, thus $\gcd(c-b,c+b)=2$. Dividing 4 on both side, we get

$$\left(\frac{a}{2}\right)^2=\frac{c-b}{2}\cdot\frac{c+b}{2}$$

Since $\gcd(c-b,c+b)=2$, we have $\gcd\left(\frac{c-b}{2},\frac{c+b}{2}\right)=1$. By Exercise 16, we must have $\frac{c-b}{2}=u^2, \frac{c+b}{2}=v^2$ for some $u,v\in\mathbb{Z}$. In other words, $b=v^2-u^2, c=v^2+u^2$, which makes $a=2uv$. $\square$

Exercise 24. Prove the identities

1. $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1})$.
2. For n odd, $x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \cdots + y^{n-1})$.

Proof. <u>Part 1:</u>

$$\begin{aligned}
(x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k} &= \sum_{k=0}^{n-1} x^{k+1} y^{n-1-k} - \sum_{k=0}^{n-1} x^k y^{n-k} \\
&= x^n + \sum_{k=0}^{n-2} x^{k+1} y^{n-(k+1)} - \left[\sum_{k=1}^{n-1} x^k y^{n-k} + y^n\right] \\
&= x^n + \sum_{k=1}^{n-1} x^k y^{n-k} - \sum_{k=1}^{n-1} x^k y^{n-k} - y^n \\
&= x^n - y^n
\end{aligned}$$

<u>Part 2:</u>

$$\begin{aligned}
(x+y)\sum_{k=0}^{n-1} (-1)^k x^k y^{n-1-k} &= \sum_{k=0}^{n-1} (-1)^k x^{k+1} y^{n-1-k} + \sum_{k=0}^{n-1} (-1)^k x^k y^{n-k} \\
&= x^n - \sum_{k=0}^{n-2} (-1)^{k+1} x^{k+1} y^{n-(k+1)} + \left[\sum_{k=1}^{n-1} (-1)^k x^k y^{n-k} + y^n\right] \\
&= x^n + \sum_{k=1}^{n-1} (-1)^k x^k y^{n-k} + \sum_{k=1}^{n-1} (-1)^k x^k y^{n-k} + y^n \\
&= x^n + y^n
\end{aligned}$$

□

Exercise 25. If $a^n - 1$ is a prime for $a, n > 1$, show that $a = 2$ and that n is a prime. Primes of the form $2^p - 1$ are called *Mersenne primes*. For example, $2^3 - 1 = 7$ and $2^5 - 1 = 31$. It is not known if there are infinitely many Mersenne primes (as of October 2020, there are 50 Mersenne prime found).

Proof. If $a \neq 2$, then $a^n - 1 = (a-1)(a^{n-1} + \cdot + 1)$ is a factorization of it (Exercise 24). Since $a \neq 2$, we have $a - 1 \geq 2$. Since $a, n > 1$, $a^{n-1} + \cdot + 1 > 1$. Thus, $a^n - 1$ cannot be a prime by definition.

If n is not a prime, then let $n = uv$ be a factorization with $u, v > 1$. We then have $a^n - 1 = (a^u)^v - 1 = (a^u - 1)(a^{u(v-1)} + \cdots + 1)$ (Exercise 24. Since $a, u > 1$, $a^u - 1 > 1$. Since $v > 1$, $a^{u(v-1)} + \cdots + 1 > 1$. Hence, $a^n - 1$ cannot be a prime by definition.

We conclude that $a = 2$ and n is prime, given $a^n - 1$ is a prime. $\square$

Exercise 26. If $a^n + 1$ is a prime for $a, n > 1$, show that a is even and that n is a power of 2. Primes of the form $2^{2^t} + 1$ are called Fermat primes. For example, $2^{2^1} + 1 = 5$ and $2^{2^2} + 1 = 17$. It is not known if there are infinitely many Fermat primes (as of 2021, there are only 5 Fermat prime found, namely $2^{2^t} + 1$ for $0 \leq t \leq 4$).

Proof. Suppose a is odd, then a^n is also odd, and thus $a^n + 1$ is even. Since $a > 1$, we have $a^n + 1 \geq a + 1 \geq 4$. Thus, $a^n + 1$ cannot be a prime, since the only even prime is $2 < 4$. On the other hand, if n is not a power of 2, i.e. $n = 2^d m$ for some $m > 1$ odd. By Exercise 24, $a^n + 1 = (a^{2^d})^m + 1 = (a^{2^d} + 1)(a^{2^d(m-1)} - a^{2^d(m-2)} + \cdots + 1)$. Again, since $a > 1$, $a^{2^d} + 1 \geq a + 1 \geq 3$. And since $a, m > 1$, $a^{2^d(m-1)} > a^{2^d(m-2)} > \cdots > a^{2^d} > 1$, so $a^{2^d(m-1)} - a^{2^d(m-2)} + \cdots + 1 = (a^{2^d(m-1)} - a^{2^d(m-2)}) + \cdots + (a^{2^d \cdot 2} - a^{2^d}) + 1 > 1$. By definition, $a^n + 1$ cannot be a prime. $\square$

Exercise 27. For all odd n show that $8 \mid n^2 - 1$. If $3 \nmid n$, show that $6 \mid n^2 - 1$.

Proof. Suppose $n = 2k + 1, k \in \mathbb{Z}$, then $n^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k = 4k(k + 1)$. However, one of k or $k + 1$ must be even, so $n^2 - 1$ must be divisible by $4 \cdot 2 = 8$. Suppose $n = 3k \pm 1, k \in \mathbb{Z}$ (since $n \equiv \pm 1 \pmod 3$ whenever n is not divisible by 3), then $n^2 - 1 = (3k \pm 1)^2 - 1 = 9k^2 \pm 6k = 3k(3k \pm 2)$. In particular, $3 \mid n^2 - 1$. We have proved $8 \mid n^2 - 1$ (for n odd), so since $\gcd(3, 8) = 1$, we get $24 \mid n^2 - 1$ (Exercise 9). $\square$

Exercise 28. For all n show that $30 \mid n^5 - n$ and that $42 \mid n^7 - n$.

Proof. *Using the factorization $30 = 2 \cdot 3 \cdot 5$, we prove $n^5 - n$ is divisible by $2, 3, 5$ separately. Note that $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n-1)(n+1)(n^2+1)$, so since $n-1, n, n+1$ are 3 consecutive integers, one of them must be divisible by 2 and one of them must be divisible by 3. As for $5 \mid n^5 - n$, consider the following case

1. If $n \equiv 0, \pm 1 \pmod 5$, then $n(n-1)(n+1)$ is divisble by 5, so $n^5 - n$ is divisible by 5.

2. If $n \equiv \pm 2 \pmod 5$, then $n^2 + 1 \equiv 2^2 + 1 \equiv 0 \pmod 5$, so $n^5 - n = n(n-1)(n+1)(n^2+1) \equiv 0 \pmod 5$.

*Similarly as above, we prove $n^7 - n$ is divisible by $2, 3, 7$ separately. Note that $n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1) = n(n-1)(n+1)(n^2+n+1)(n^2-n+1)$, so $n^7 - n$ is divisble by 2 and 3 with the same argument previously. As for $7 \mid n^7 - n$, consider the following case

1. If $n \equiv 0, \pm 1 \pmod 7$, then $n(n-1)(n+1)$ is divisble by 7, so $n^7 - n$ is divisible by 7.

2. If $n \equiv 2 \pmod 7$, then $n^2 + n + 1 \equiv 2^2 + 2 + 1 \equiv 0 \pmod 7$, so $n^7 - n \equiv 0 \pmod 7$.

3. If $n \equiv -2 \pmod 7$, then $n^2 - n + 1 \equiv (-2)^2 + 2 + 1 \equiv 0 \pmod 7$, so $n^7 - n \equiv 0 \pmod 7$.

4. If $n \equiv 3 \pmod 7$, then $n^2 - n + 1 \equiv 3^2 - 3 + 1 \equiv 0 \pmod 7$, so $n^7 - n \equiv 0 \pmod 7$.

5. If $n \equiv -3 \pmod 7$, then $n^2 + n + 1 \equiv (-3)^2 - 3 + 1 \equiv 0 \pmod 7$, so $n^7 - n \equiv 0 \pmod 7$.

$\square$

Exercise 29. Suppose that $a, b, c, d \in \mathbb{Z}$ and that $\gcd(a, b) = \gcd(c, d) = 1$. If $(a/b) + (c/d) =$ an integer, show that $b = \pm d$.

Proof. Since $(a/b) + (c/d) = (ad + bc)/(bd)$ is an integer, we have $bd \mid ad + bc$. In particular, $d \mid ad + bc$, so $d \mid bc$. Yet $\gcd(c, d) = 1$, so we need $d \mid b$. Similarly, $b \mid d$, so we conclude $|b| = |d|$, or $b = \pm d$ simply. $\square$

Exercise 30. Prove that $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is not an integer.

Proof. Let $2^k \leq n$ be the largest power of 2 not exceeding n. Then it is also the only number $\leq n$ that is divisble by such power 2^k. Indeed, if $2^k \mid m \leq n$, then $m = 2^k d$ for some $d \geq 1$. If $d \geq 2$, then $n \geq m \geq 2^{k+1}$, contradicting the maximality of k.

We then split the sum into $\frac{1}{2^k}$ and the remaining ones $\frac{p}{q} = \sum_{i \neq 2^k} \frac{1}{i}$ ($\gcd(p, q) = 1$). By the previous remark, each i can be divisible by at most 2^{k-1}, so q (which divide $\mathrm{lcm}_{i \neq 2^k} i$) is also divisible by at most 2^{k-1}. If we suppose $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is an integer, then $\frac{1}{2^k} + \frac{p}{q}$ is that same integer. By Exercise 29, we thus have $q = \pm 2^k$, a contradiction. $\square$

Exercise 31. Show that 2 is divisible by $(1+i)^2$ in $\mathbb{Z}[i]$.

Proof. $(1+i)^2 = 1 + 2i + i^2 = 2i$, so $-i(1+i)^2 = 2$, i.e. $(1+i)^2 \mid 2$. $\square$

Exercise 32. For $\alpha = a + bi \in \mathbb{Z}[i]$, we defined $\lambda(\alpha) = a^2 + b^2$. From the properties of λ deduce the identity $(a^2 + b^2)(c^2 = d^2) = (ac - bd)^2 + (ad + bc)^2$.

Proof. Since λ is multiplicative $\lambda((a+bi)(c+di)) = \lambda(a+bi)\lambda(c+di) = (a^2 + b^2)(c^2 + d^2)$. On the other hand, $(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac-bd)+(ad+bc)i$, so $\lambda((a+bi)(c+di)) = (ac-bd)^2+(ad+bc)^2$. Comparing the 2 results, we get the desired identity. $\square$

Exercise 33. Show that $\alpha \in \mathbb{Z}[i]$ is a unit iff $\lambda(\alpha) = 1$. Deduce that 1, -1, i, and $-i$ are the only units in $\mathbb{Z}[i]$.

Proof. If $\alpha \in \mathbb{Z}[i]$ is a unit, then there exists some $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$. Applying λ to both side and use multiplicativity, we get $\lambda(\alpha)\lambda(\beta) = \lambda(1) = 1$. Note that $\lambda(\alpha)$ is always an integer for any Gaussian integer α, so we get $\lambda(\alpha) \mid 1$, i.e. $\lambda(\alpha) = 1$ since $\lambda(\alpha) \geq 0$ is a sum of square. Vice versa, suppose $\lambda(\alpha) = 1$. If $\alpha = a + bi$, consider the product of α and its conjugate: $\alpha\overline{\alpha} = (a + bi)(a - bi) = (a^2 + b^2) + (a(-b) + ba)i = \lambda(\alpha) = 1$. By definition, α is a unit.

By the previous result, the units of $\mathbb{Z}[i]$ are of the form $a + bi$ for $a^2 + b^2 = 1$. Since $a^2 \leq a^2 + b^2 = 1$, we have $-1 \leq a \leq 1$.

1. If $a = \pm 1$, then $b = 0$. The corresponding units are ± 1.
2. If $a = 0$, then $b = \pm 1$. The corresponding units are $\pm i$.

$\square$

Exercise 34. Show that 3 is divisible by $(1-\omega)^2$ in $\mathbb{Z}[\omega]$.

Proof. Recall that $\omega^2+\omega+1=0$, so $(1-\omega)^2 = 1-2\omega+\omega^2 = -3\omega$. Also recall that $\omega^3=1$, so $3 = 3\omega^3 = -\omega^2(1-\omega)^2$, so $(1-\omega^2) \mid 3$. $\square$

Exercise 35. For $\alpha = a+b\omega \in \mathbb{Z}[\omega]$, we defined $\lambda(\alpha) = a^2-ab+b^2$. Show that α is a unit iff $\lambda(\alpha)=1$. Deduce that $\pm 1, \pm\omega, \pm\omega^2$ are the only units in $\mathbb{Z}[\omega]$.

Proof. First we verify that $\overline{\omega} = \omega^2$. Indeed, $\omega^2 = \left(\frac{-1+\sqrt{-3}}{2}\right)^2 = \frac{1-3-2\sqrt{-3}}{4} = \frac{-1-\sqrt{-3}}{2} = \overline{\omega}$.

Next, we verify λ is multiplicative.

$$\begin{aligned}
\lambda(a+b\omega)\lambda(c+d\omega) &= (a^2-ab+b^2)(c^2-cd+d^2)\\
&= a^2c^2 - a^2cd + a^2d^2 - abc^2 + abcd - abd^2 + b^2c^2 - b^2cd + b^2d^2\\
&= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + abcd - a^2cd - b^2cd - abc^2 - abd^2\\
\lambda((a+b\omega)(c+d\omega)) &= \lambda(ac + bd\omega^2 + (bc+ad)\omega)\\
&= \lambda((ac-bd) + (bc+ad-bd)\omega)\\
&= (ac-bd)^2 - (ac-bd)(bc+ad-bd) + (bc+ad-bd)^2\\
&= a^2c^2 - 2abcd + b^2d^2 - abc^2 - a^2cd + abcd + b^2cd + abd^2 - b^2d^2\\
&\qquad + b^2c^2 + a^2d^2 + b^2d^2 + 2abcd - 2b^2cd - 2abd^2\\
&= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + abcd - a^2cd - b^2cd - abc^2 - abd^2
\end{aligned}$$

*Now suppose $\alpha = a+b\omega$ is a unit, i.e. $\alpha\beta = 1$ for some $\beta \in \mathbb{Z}[\omega]$. Then $\lambda(\alpha)\lambda(\beta) = \lambda(1) = 1$, so $\lambda(\alpha) \mid 1$ (since $\lambda(\alpha)$ is always an integer). But $\lambda(\alpha) = a^2-ab+b^2 = \left(a-\frac{b}{2}\right)^2 + \frac{3b^2}{4} \geq 0$, so $\lambda(\alpha)=1$. On the other hand, if $\lambda(\alpha)=1$, then note that

$$\begin{aligned}
\alpha\overline{\alpha} &= (a+b\omega)(a+b\overline{\omega})\\
&= a^2 + b^2\omega\overline{\omega} + ab(\omega+\overline{\omega})\\
&= a^2+b^2-ab = \lambda(\alpha) = 1
\end{aligned}$$

By definition, α is a unit.

*To find all units of $\mathbb{Z}[\omega]$, we need to solve $a^2-ab+b^2=1$ for $a,b\in\mathbb{Z}$. Rewrite it into $\left(a-\frac{b}{2}\right)^2 + \frac{3b^2}{4} = 1$, then normalize it by multiplying both side by 4, we get $(2a-b)^2 + 3b^2 = 4$. Since $3b^2$ is a multiple of 3 that is between 0 and 4, we consider the following cases

1. $3b^2 = 0$, or $b=0$: then $(2a-b)^2 = 4a^2 = 4$, so $a=\pm 1$. These correspond to the units ± 1.

2. $3b^2 = 3$, or $b = \pm 1$: then $(2a - b)^2 = 1$, so $2a - b = \pm 1$.

   (a) If $b = 1$, then $a \in \{0, 1\}$. These correspond to the units $\omega, 1 + \omega = -\omega^2$.

   (b) If $b = -1$, then $a \in \{0, -1\}$. These correspond to the units $-\omega, -1 - \omega = \omega^2$.

$\square$

Exercise 36. Define $\mathbb{Z}[\sqrt{-2}]$ as the set of complex numbers of the form $a + b\sqrt{-2}$, where $a, b \in \mathbb{Z}$. Show that $\mathbb{Z}[\sqrt{-2}]$ is a ring. Define $\lambda(\alpha) = a^2 + 2b^2$ for $\alpha = a + b\sqrt{-2}$. Use λ to show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

Proof. *$\mathbb{Z}[\sqrt{-2}]$ is a ring since

1. For any $a + b\sqrt{-2}, c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ (equivalently, $a, b, c, d \in \mathbb{Z}$), we have

$$\begin{aligned}(a + b\sqrt{-2}) + (c + d\sqrt{-2}) &= (a + c) + (b + d)\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}] \\ (a + b\sqrt{-2})(c + d\sqrt{-2}) &= (ac - 2bd) + (ad + bc)\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]\end{aligned}$$

2. Commutativity, associativitiy, and distributivity hold as these are just complex arithmetics.

3. Identities: since $0 = 0 + 0 \cdot \sqrt{-2}, 1 = 1 + 0 \cdot \sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$

$$\begin{aligned}(a + b\sqrt{-2}) + (0 + 0\sqrt{-2}) &= a + b\sqrt{-2} \\ (a + b\sqrt{-2})(1 + 0\sqrt{-2}) &= a + b\sqrt{-2}\end{aligned}$$

4. Additive inverse: $(a + b\sqrt{-2}) + [(-a) + (-b)\sqrt{-2}] = 0$

*To show $\mathbb{Z}[\sqrt{-2}]$, for any $\alpha = a + b\sqrt{-2}$ and $\beta = c + d\sqrt{-2} \neq 0$. Let

$$\frac{\alpha}{\beta} = \frac{(a + b\sqrt{-2})(c - d\sqrt{-2})}{c^2 + 2d^2} = \frac{(ac + 2bd) + (bc - ad)\sqrt{-2}}{c^2 + 2d^2} = r + s\sqrt{-2}$$

for some $r, s \in \mathbb{Q}$. Pick some integer m, n such that $|m - r| \leq 1/2$ and $|n - s| \leq 1/2$ (e.g. m, n are respectively the nearest integers to r, s). Let $\rho = m + n\sqrt{-2}$ and $\delta = \alpha - \rho\beta$ (both in $\mathbb{Z}[\sqrt{-2}]$), then $\lambda\left(\frac{\alpha}{\beta} - \rho\right) = (m - r)^2 + 2(n - s)^2 \leq 3/4 < 1$, so $\lambda(\delta) = \lambda(\beta)\lambda\left(\frac{\alpha}{\beta} - \rho\right) < \lambda(\beta)$ (note that λ is the square of the absolute value on $\mathbb{C}$). $\square$

Exercise 37. Show that the only units in $\mathbb{Z}[\sqrt{-2}]$ are 1 and -1.

Proof. If $\alpha = a + b\sqrt{-2}$ is a unit, then $\alpha\beta = 1$ for some $\beta \in \mathbb{Z}[\sqrt{-2}]$. Since the absolute value of a complex number is multiplicative, we have $|\alpha| \cdot |\beta| = 1$, or equivalently, $\lambda(\alpha)\lambda(\beta) = |\alpha|^2|\beta|^2 = 1$. But $\lambda(\alpha) = a^2 + 2b^2$ is a non-negative integer, so we get $\lambda(\alpha) = 1 = a^2 + 2b^2$. In particular, $2b^2 \leq 1$, so $b = 0$ necessarily. From there, we get $a = \pm 1$, so the only *possible* units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1. Checking $1^2 = (-1)^2 = 1$, we conclude that these are the only units. $\square$

Exercise 38. Suppose that $\pi \in \mathbb{Z}[i]$ and that $\lambda(n) = p$ is a prime in $\mathbb{Z}$. Show that π is a prime in $\mathbb{Z}[i]$. Show that the corresponding result holds in $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\sqrt{-2}]$.

Proof. We will show that such holds in any Euclidean domain D with Euclidean function $\lambda : D \to \mathbb{Z}_{\geq 0}$ such that λ is multiplicative, and α is a unit whenever $\lambda(\alpha) = 1$. Indeed, suppose $\pi \in D$ such that $\lambda(\pi) = p$ a prime. Then π must be irreducible, as whenever $\pi = \alpha\beta$, we have $\lambda(\alpha)\lambda(\beta) = \lambda(\pi) = p$. Since $\lambda(\alpha), \lambda(\beta) \geq 0$, we must have either $\lambda(\alpha) = 1$, or $\lambda(\beta) = 1$. In other words, either α or β is a unit.

So π is irreducible. We need to show that π is prime from this fact. Indeed, an Euclidean domain is always a PID, so whenever $\pi \mid \alpha\beta$, yet $\pi \nmid \alpha$, we let $(\gamma) = (\pi, \alpha)$. Since $(\gamma) \supseteq (\pi)$, we have $\gamma \mid \pi$. π is irreducible so either $(\pi, \alpha) = (\gamma) = (\pi)$, or $(\pi, \alpha) = (\gamma) = (1)$. The first case implies that $(\pi) \supseteq (\alpha)$, or simply $\pi \mid \alpha$, contradicting the assumption. Thus, $(\pi, \alpha) = (1)$, and so there exists $x_0, y_0 \in D$ such that $\pi x_0 + \alpha y_0 = 1$. Multiplying both side by β, we get $\pi(\beta x_0) + (\alpha\beta)y_0 = \beta$. Since $\pi \mid \alpha\beta$, we have $\pi \mid \pi(\beta x_0) + (\alpha\beta)y_0 = \beta$. By definition, π is a prime. $\square$

Exercise 39. Show that in any integral domain a prime element is irreducible.

Proof. Let $p \in R$ be a prime element. Suppose $p = ab$, then $p \cdot 1 = ab$, so $p \mid ab$. By definition, we can assume WLOG that $p \mid a$. Let $a = pc$ for some $c \in R$. Then $p = ab = pcb$, so $1 = cb$ (since R is an integral domain). In other words, b is a unit in R. In summary, any factorization $p = ab$ of a prime element has either a or b be a unit. By definition, p must be irreducible. $\square$