2.3 The Euclidean Algorithm

1. (a) \( \text{gcd}(143, 227) \)

\[
\begin{align*}
227 &= 1 \cdot 143 + 84 \\
143 &= 1 \cdot 84 + 59 \\
84 &= 1 \cdot 59 + 25 \\
59 &= 2 \cdot 25 + 9 \\
25 &= 2 \cdot 9 + 7 \\
9 &= 1 \cdot 7 + 2 \\
7 &= 3 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0 \\
\text{gcd}(143, 227) &= 1
\end{align*}
\]

(b) \( \text{gcd}(306, 657) \)

\[
\begin{align*}
657 &= 2 \cdot 306 + 45 \\
306 &= 6 \cdot 45 + 36 \\
45 &= 1 \cdot 36 + 9 \\
36 &= 4 \cdot 9 + 0 \\
\text{gcd}(306, 657) &= 9
\end{align*}
\]

(c) \( \text{gcd}(272, 1479) \)

\[
\begin{align*}
1479 &= 5 \cdot 272 + 119 \\
272 &= 2 \cdot 119 + 34 \\
119 &= 3 \cdot 34 + 17 \\
34 &= 2 \cdot 17 + 0 \\
\text{gcd}(272, 1479) &= 17
\end{align*}
\]
2. (a) \( \text{gcd}(57, 72) = 57x + 72y \)

\[ 72 = 1 \cdot 56 + 16 \]
\[ 56 = 3 \cdot 16 + 8 \]
\[ 16 = 2 \cdot 8 + 0 \quad \text{gcd} = 8 \]

\[ \because 8 = 56 - 3 \cdot 16 \]
\[ = 56 - 3(72 - 56) \]
\[ = (4)56 - (3)72 \]

(6) \( \text{gcd}(24, 138) = 24x + 138y \)

\[ 138 = 5 \cdot 24 + 18 \]
\[ 24 = 1 \cdot 18 + 6 \]
\[ 18 = 3 \cdot 6 + 0 \quad \text{gcd} = 6 \]

\[ \therefore 6 = 24 - 18 \]
\[ = 24 - (138 - 5 \cdot 24) \]
\[ = (6)24 - 138 \]

(6) \( \text{gcd}(119, 272) = 119x + 272y \)

\[ 272 = 2 \cdot 119 + 34 \quad \therefore 17 = 119 - 3 \cdot 34 \]
\[ 119 = 3 \cdot 34 + 17 \]
\[ 34 = 17 \cdot 2 + 0 \]
\[ \text{gcd} = 17 \]
(d) \[ \gcd(1769, 2378) = 1769x + 2378y \]

\[ 2378 = 1 \cdot 1769 + 609 \]
\[ 1769 = 3 \cdot 609 - 58 \]
\[ 609 = 10 \cdot 58 + 29 \]
\[ 58 = 2 \cdot 29 + 0 \]
\[ \gcd = 29 \]

\[ 29 = 609 - 10 \cdot 58 \]
\[ = 609 - 10 (3 \cdot 609 - 1769) \]
\[ = (-29) \cdot 609 + (-10) \cdot 1769 \]
\[ = (-29) (2378 - 1769) + 10 \cdot 1769 \]
\[ = (29) 1769 - (29) 2378 \]

3. \( d|a, d|b \Rightarrow d = \gcd(a, b) \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \)

**Proof:** Let \( m, n \) be s.t. \( dm = a, dn = b \)

(a) If \( d = \gcd(a, b) \), then, by Th 2.7 (since \( d > 0 \)),

\[ d = \gcd(dm, dn) = d \cdot \gcd(m, n) = d \cdot \gcd\left(\frac{a}{d}, \frac{b}{d}\right) \]

\[ \Rightarrow 1 = \gcd\left(\frac{a}{d}, \frac{b}{d}\right) \]

(b) If \( \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \), then, by Th 2.7,

\[ \gcd(a, b) = \gcd\left(b \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d \cdot \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = d \]
4. \( \gcd(a, b) = 1 \)

(a) \( \gcd(a+b, a-b) = 1 \) or 2

\begin{proof}

Let \( d = \gcd(a+b, a-b) \). \therefore by Corollary p. 25, 
d is a divisor of all linear combinations of \( a+b \) and \( a-b \).

\[ d \mid (a+b) + (a-b) \Rightarrow d \mid 2a \]
\[ d \mid (a+b) - (a-b) \Rightarrow d \mid 2b \]

\therefore \( d \mid \gcd(2a, 2b) = 2 \gcd(a, b) = 2 \)

\therefore \( d = 1 \) or 2

(b) \( \gcd(2a+b, a+2b) = 1 \) or 3

\begin{proof}

Let \( d = \gcd(2a+b, a+2b) \)

\[ d \mid 2(a+b+1) - (a+2b) \leftrightarrow d \mid 3a \]
\[ d \mid -1 \cdot (2a+b) + 2(a+2b) \leftrightarrow d \mid 3b \]

\therefore \( d \leq \gcd(3a, 3b) = 3 \gcd(a, b) = 3 \)

\therefore \( d = 1, 2, \) or 3

if \( d = 2 \), then \( d \mid 3a \Rightarrow d \mid a \), \( d \mid 3b \Rightarrow d \mid b \)

\therefore \( \text{gcd}(2, 3) = 1 \), and by Th 2.5 (Euclid's lemma)
But if \( z \mid a \) and \( z \mid b \), then \( \gcd(a, b) \neq 1 \).

\[ \therefore d \neq 2 \]

\[ \therefore d = 1 \text{ or } 3 \]

(2) \( \gcd(a + 6, a^2 + b^2) = 1 \text{ or } 2 \)

**PF:** Let \( d = \gcd(a + 6, a^2 + b^2) \)

Then \( d \mid a^2 + b^2 \iff d \mid (a + b)(a - b) + 26^2 \)

Since \( d \mid (a + b) \), let \( x \) be s.t. \( dx = a + b \)
and let \( m \) be s.t. \( dm = (a + b)(a - b) + 26^2 \)

\[ \therefore dm = dx(a - b) + 26^2 \]

\[ \therefore d \mid 26^2 \]

By Problem 20(d), on p. 26, \( \gcd(5, 6) = 1 \) and \( d \mid a + b \Rightarrow \gcd(a, d) = \gcd(b, d) = 1 \)

\[ \therefore \text{By Euclid's lemma, } d \mid 26^2 \text{ and } \gcd(d, 6) = 1 \]

means \( d \mid 26 \cdot 6 \Rightarrow d \mid 26 \Rightarrow d \mid 2 \cdot 2 \cdot 13 \)

\[ \therefore d \leq 2 \Rightarrow d = 1 \text{ or } 2 \]

(4) \( \gcd(a + 6, a^2 - 6a + b^2) = 1 \text{ or } 3 \)
\[ \text{Pf: Let } d = \gcd(a + 6, a^2 - ab + b^2) \]
\[ \therefore d \mid a^2 - ab + b^2 \Rightarrow d \mid (a + b)^2 - 3ab \]

As in (c) above, since \( d \mid (a + b) \), then
\[ d \mid 3ab. \]

Since \( d \mid a + b \) and \( \gcd(a, b) = 1 \), then by Problem 20 (d) p. 26,
\[ \gcd(a, d) = \gcd(b, d) = 1. \]

\[ \therefore \text{By Euclid's lemma, } d \mid 3ab \Rightarrow d \mid 3a \Rightarrow d \mid 3 \]

\[ \therefore d \leq 3. \] Since \( \gcd(2, 3) = 1 \), then
\[ \text{if } d = 2, \text{ then } 2 \mid 3a \Rightarrow 2 \mid ab \]
\[ \therefore 2 \mid a \text{ or } 2 \mid b, \text{ either of which contradicts } \gcd(a, d) = \gcd(b, d) = 1. \]

\[ \therefore d \neq 2 \]

\[ \therefore d = 1 \text{ or } 3 \]

5. \( a, b > 0, \eta = 1 \)

(a) If \( \gcd(a, b) = 1 \), then \( \gcd(a^n, b^\eta) = 1 \)
\( \rho_f: \ n = 1; \ \text{gcd}(a, b) = 1 \ was \ assumed \)

\( K \Rightarrow k+1: \ \text{Assume gcd}(a_k, b^{k+1}) = 1 \)

By problem 20(a) p.26,

\[ \text{gcd}(a_k, b^{k+1}) = \text{gcd}(a_k, b^k) = 1 \]

Since \( \text{gcd}(a, b) = \text{gcd}(6, a) \),

Then \( \text{gcd}(b^{k+1}, a_k) = 1 \), and

\( \text{again by} \ 20(a) \ p.26, \)

\[ \text{gcd}(b^{k+1}, a^k) = \text{gcd}(b^{k+1}, a^{k+1}) = 1 \]

(6) \( a^k | b^{k+1} \Rightarrow \ a | b \)

\( \rho_f: \ n = 1; \ \text{Clearly,} \ a' | b' = a | b \)

\( K \Rightarrow k+1: \ \text{Assume} \ a^k | b^k \Rightarrow a | b \)

3 \ s.t. \ \ x a^k = b^k \ 
3 \ y s.t. \ a y = 6

\[ x a^{k+1} = b^k = \left(\frac{b}{y}\right) 6^k = \frac{b^{k+1}}{y} \]

\[ x y a^{k+1} = 6^{k+1} \]

\[ a^{k+1} | 6^{k+1} \]
Another proof, as suggested by author

Let \( d = \gcd(a, b) \), and let \( r, s \in \mathbb{N} \) s.t.
\[
a = rd, \quad b = sd
\]
\[
\gcd(r, s) = 1 \) by problem 13 (b), p. 25
\)
\[
\therefore \gcd(r^n, s^n) = 1 \) by (a) above.
\)

But since \( a^n = r^n d^n, \quad b^n = s^n d^n \), Then
\[
since a^n | b^n, \quad Then \quad r^n \quad | \quad s^n, d^n = r^n | s^n, d^n
\]
\[
\therefore l = \gcd(r^n, s^n) = r^n, \quad so \quad r = 1.
\)
\[
\therefore \quad from \quad a = rd, \quad a = d, \quad and \quad from \quad b = sd, \quad b = s,
\]
\[
\therefore \quad 6 = s q, \quad \therefore \quad a | b
\]

\[c. \quad \gcd(a, b) = 1 \implies \gcd(a+b, ab) = 1\]

\[\text{pf: Let } c \text{ be a divisor of } a+b \text{ and } ab\]
\[\text{by 20(d), p. 26, } \gcd(a, c) = \gcd(b, c) = 1\]

Since \( c \mid ab \) and \( \gcd(c, a) = 1 \), Then by
\[\text{Euclid's lemma, } c \mid b\]

Similarly, \( c \mid ab \) and \( \gcd(c, b) = 1 \implies c \mid a\)

\[\therefore c \mid a, \quad c \mid b \] \[\therefore c \leq \gcd(a, b) = 1 \] \[\therefore c = 1\]

7. \((a) \quad a \mid b \implies \gcd(a, b) = |a|\)

\[\text{pf: (i) } a \mid a \text{ and } a \mid b \] \[\therefore a \text{ is a common divisor.}\]
Suppose $d$ is another common divisor.
\[\therefore \exists n \text{ s.t. } a = dn, \therefore |a| = |d||n|\]
Since $a \neq 0$, and $d \neq 0$, \[\therefore n \neq 0\]
\[\therefore |n| = 1, \text{ otherwise } |a| = |d|\]
\[\therefore |a| = |d||n| > |d|, \text{ so } |a| > |d|\]
and \[|a| = gcd(a, b)\].

(2) Assume \[gcd(a, b) = |a|\]
\[\therefore \exists n \text{ s.t. } b = |a|n. \text{ If } a > 0, \text{ then } |a| = a, \text{ so } b = a \cdot n = a / b\]
if $a < 0$, then \[|a| = -a \Rightarrow b = (-a)n, \therefore b = a(-n), \therefore a / b\].

(6) $a / b \iff \text{lcm}(a, b) = |b|$

\[\text{Pf.}\ (1) a / b \Rightarrow a / |b|, \text{ and clearly } b / |b|\]
Let $c$ be another common multiple
\[\therefore a / c \text{ and } b / c \text{ (and } c > 0)\]
\[6|c \Rightarrow \exists n \text{ s.t. } c = 6n, \text{ and } |n| = 1\]
\[\therefore |c| = |6||n| = 6|n| \Rightarrow |c| = 6|n| \text{ and } |c| = lcm(a, b) \text{ by def.}\]
(2) \[lcm(a, b) = |b| \Rightarrow a / |b| \text{ by def.}\]
\[\therefore 3 \text{ s.t. } a | 16|\]
if $6 > 0$, Then \[a | 6 \Rightarrow a / 6\]
if $6 < 0$, Then \[a | -6, a(-n) = 6, \therefore a / 6\].
(c) Transitivity of (a) & (b) means
\[ \gcd(a, b) \neq a \iff \text{lcm}(a, b) = 16 \]

Or, directly

(i) Assume \(\gcd(a, b) = |a|\)
\[ \therefore |a| | \text{lcm}(a, b) = |ab| = |a||b| \]
\[ \therefore \text{lcm}(a, b) = 16 \]

(ii) Assume \(\text{lcm}(a, b) = 16\)
\[ \therefore a ||b| \Rightarrow |a||b| \]
Let \(c < \) another common divisor
\[ \therefore 3 \text{ n.s.t. } a = cn \Rightarrow |a| = k|n| \]
\[ But |n| \leq 1, \therefore |c||n| \leq |c|, \therefore |a| \leq |c| \]
\[ \therefore |a| = \gcd(a, b). \]

8. (a) \(\text{lcm}(143, 227)\)

\[227 = 1 \cdot 143 + 84\]
\[143 = 2 \cdot 84 + 25\]
\[84 = 3 \cdot 25 + 9\]
\[25 = 2 \cdot 9 + 7\]
\[9 = 7 + 2\]
\[7 = 3 \cdot 2 + 1\]
\[\therefore \gcd(143, 227) = 1 \therefore \text{lcm} = 143 \cdot 227 = 32,461\]
(b) \( \text{lcm}(306, 657) \)

\[
657 = 2 \cdot 306 + 45 \\
306 = 7 \cdot 45 - 9 \\
45 = 5 \cdot 9 \\
\therefore \text{gcd} = 9, \quad \therefore \text{lcm} = \frac{306 \cdot 657}{9} = 22,338
\]

(c) \( \text{lcm}(272, 1479) \)

\[
1479 = 5 \cdot 272 + 119 \\
272 = 2 \cdot 119 + 34 \\
119 = 4 \cdot 34 - 17 \\
34 = 2 \cdot 17 \\
\text{gcd} = 17, \quad \therefore \text{lcm} = \frac{(272 \cdot 1479)}{17} = 23,664
\]

9. \( a, b \geq 0, \quad \text{gcd}(a, b) \mid \text{lcm}(a, b) \)

**Proof:** Since \( \text{gcd}(a, b) \cdot \text{lcm}(a, b) = ab \), let 
\[
d = \text{gcd}(a, b). \quad \therefore 3n \mid m \iff a = dn, b = dm
\]

\[
\therefore d \cdot \text{lcm}(a, b) = (dn)(dm)
\]

\[
\therefore \text{lcm}(a, b) = d(nm) \Rightarrow d \mid \text{lcm}(a, b)
\]
10. (a) $\gcd(a, b) = \lcm(a, b) \iff a = \pm b$

Proof: (1) Let $d = \gcd(a, b) = \lcm(a, b)$
\[ \therefore d \cdot d = a \cdot b \]
Since $d \mid a$, \exists $x$ s.t. $dx = a$.
\[ \therefore d \cdot d = d \cdot x \cdot b \Rightarrow d = x \cdot b \Rightarrow b \mid d. \]
\[ \therefore d \mid b \text{ and } b \mid d \]
\[ \therefore d = \pm b \text{ by Th. 2.2(e) on p. 21} \]
Similarly, $d = \pm a$.
\[ \therefore |d| = |a| = |b| \Rightarrow a = \pm b \]

(2) If $a = \pm b$, then $a \mid b$ and $b \mid a$

By problem (7) above,
\[ \gcd(a, b) = \lcm(a, b) = |a| = |b| \]

(b) $k > 0, \lcm(ka, kb) = k \lcm(a,b)$

Proof: $\gcd(ka, kb) \cdot \lcm(ka, kb) = K^2 |ab|$
\[ \therefore k \gcd(a, b) \cdot \lcm(ka, kb) = k^2 |ab| \]
\[ \therefore \gcd(a, b) \cdot \lcm(ka, kb) = k |ab| \]
\[ = k \gcd(a, b) \cdot \lcm(a, b) \]
\[ \therefore \lcm(ka, kb) = k \lcm(a,b) \]
(c) If \( m \) is a common multiple of \( a, b \), then \( \text{lcm}(a,b) \mid m \).

\[ \text{Proof: Let } l = \text{lcm}(a,b) \]
\[ \text{Let } q, r \text{ be s.t. } m = lq + r, 0 \leq r < l \]

If \( r = 0 \), then \( l \mid m \).

Assume \( 0 < r < l \)
\[ r = m - lq \]
Since \( m, l \) are multiples of \( a \) and \( b \), \( 3x, y, u, v \),
\[ r = ax - ayq \]
\[ r = bu - bvq \]
\[ = a(x-aq) \]
\[ = b(u-bvq) \]
\[ = r \text{ is a multiple of } a, b \]
\[ \therefore r \geq l \text{, which contradicts } r < l \]

11. Let \( a, b, c \) be s.t. no two of which are zero.
Let \( d = \gcd(a, b, c) \).

(a) \( d = \gcd(\gcd(a, b), c) \)

\[ \text{Proof: Let } f = \gcd(a, b) \text{ and let } g = \gcd(f, c) \]
\[ \therefore g \mid f \Rightarrow g \mid a, g \mid b \]
Since \( g \mid c \), then \( g \leq d \).
(2) Note that \( d \mid f \).

\[
Pf: f = ax + by, \text{some } x, y \quad (Th. 2.3)
\]
\[
a = du, \quad b = dv, \text{some } u, v.
\]
\[
\therefore f = dux + dvy, \therefore d \mid f
\]

Since \( d \mid c \), then \( d \mid g \). \therefore d \leq g.

\[\therefore (1) \land (2) \implies d = g.\]

(6) \( d = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, c), b)\)

Proofs identical to (a) above, switching letters.

12. Find \( x, y \) s.t. \( \gcd(198, 288, 512) = 198x + 288y + 512z \)

From (11) above,
\[
\gcd(198, 288, 512) = \gcd(\gcd(198, 288), 512)
\]
\[
\therefore 288 = 198 + 90 \quad \therefore 18 = 198 - 2 \cdot 90
\]
\[
198 = 2 \cdot 90 + 18 \quad = 198 - 2(288 - 198)
\]
\[
90 = 5 \cdot 18 \quad = (-2) \cdot 288 + 3 \cdot 198
\]
\[
\therefore \gcd(198, 288) = 18
\]

Now for \( \gcd(18, 512) \)
\[
512 = 28 \cdot 18 + 8
\]
18 = 2 \cdot 9 + 2 \quad \therefore 2 = 18 - 2 \cdot 8

8 = 4 \cdot 2 \quad = (18 - 2)(57 - 2 \cdot 18)

\therefore gcd(14, 57) = 2 \quad = 57 \cdot 18 - 2 \cdot 57

\therefore gcd(198, 288, 512) = 2

\therefore 2 = 57 \cdot 18 - 2 \cdot 57

= 57 \cdot [3 \cdot 198 - 2 \cdot 288] - 2 \cdot 57

= 171 \cdot 198 - 114 \cdot 288 - 2 \cdot 57