2.3 The Euclidean Algorithm

Note Title 11/1/2004

1. (a) $\gcd(143, 227)$

$$227 = 1 \cdot 143 + 84$$
$$143 = 1 \cdot 84 + 59$$
$$84 = 1 \cdot 59 + 25$$
$$59 = 2 \cdot 25 + 9$$
$$25 = 2 \cdot 9 + 7$$
$$9 = 1 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0 \qquad \therefore \gcd(143, 227) = 1$$

(b) $\gcd(306, 657)$

$$657 = 2 \cdot 306 + 45$$
$$306 = 6 \cdot 45 + 36$$
$$45 = 1 \cdot 36 + 9$$
$$36 = 4 \cdot 9 + 0 \qquad \therefore \gcd(306, 657) = 9$$

(c) $\gcd(272, 1479)$

$$1479 = 5 \cdot 272 + 119$$
$$272 = 2 \cdot 119 + 34$$
$$119 = 3 \cdot 34 + 17$$
$$34 = 17 \cdot 2 + 0 \qquad \therefore \gcd(272, 1479) = 17$$

2. (a) $\gcd(56, 72) = 56x + 72y$

$$72 = 1 \cdot 56 + 16$$
$$56 = 3 \cdot 16 + 8$$
$$16 = 2 \cdot 8 + 0 \qquad \gcd = 8$$

$$\therefore 8 = 56 - 3 \cdot 16$$
$$= 56 - 3(72 - 56)$$
$$= (4)56 - (3)72$$

(b) $\gcd(24, 138) = 24x + 138y$

$$138 = 5 \cdot 24 + 18$$
$$24 = 1 \cdot 18 + 6$$
$$18 = 3 \cdot 6 + 0 \qquad \gcd = 6$$

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

(c) $\gcd(119, 272) = 119x + 272y$

$$272 = 2 \cdot 119 + 34$$
$$119 = 3 \cdot 34 + 17$$
$$34 = 17 \cdot 2 + 0$$
$$\gcd = 17$$

$$\therefore 17 = 119 - 3 \cdot 34$$
$$= 119 - 3(272 - 2 \cdot 119)$$
$$= (3)119 - (3)272$$

(d) $\gcd(1769, 2378) = 1769x + 2378y$

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

$$\therefore\ 29 = 609 - 10\cdot 58$$
$$= 609 - 10(3\cdot 609 - 1769)$$
$$= (-29)\cdot 609 + (10)\cdot 1769$$
$$= (-29)(2378 - 1769) + 10\cdot 1769$$
$$= (39)\,1769 - (29)\,2378$$

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

Pf: Let m, n be s.t. $dm = a$, $dn = b$

(a) if $d = \gcd(a,b)$, Then, by Th. 2.7 (since $d > 0$)

$$d = \gcd(dm, dn) = d\cdot\gcd(m,n) = d\cdot\gcd\left(\frac{a}{d}, \frac{b}{d}\right)$$
$$\therefore\ 1 = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$$

(b) if $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, Then, by Th. 2.7,

$$\gcd(a,b) = \gcd\left(d\cdot\frac{a}{d}, d\cdot\frac{b}{d}\right) = |d|\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = |d|$$

4. $\gcd(a,b)=1$

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

Pf: Let $d = \gcd(a+b, a-b)$. $\therefore$ by Corollary p. 23, d is a divisor of all linear combinations of $a+b$ and $a-b$.

$\therefore$ $d \mid (a+b)+(a-b) \Rightarrow d \mid 2a$

$d \mid (a+b)-(a-b) \Rightarrow d \mid 2b$

$\therefore$ $d \leq \gcd(2a, 2b) = 2\gcd(a,b) = 2$

$\therefore$ $d = 1$ or 2

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

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

$\therefore$ $d \mid 2\cdot(2a+b) - (a+2b) \Leftrightarrow d \mid 3a$

$d \mid -1\cdot(2a+b) + 2(a+2b) \Leftrightarrow d \mid 3b$

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

$\therefore$ $d = 1, 2,$ or 3

if $d=2$, Then $d \mid 3a \rightarrow d \mid a$, $d \mid 3b \Rightarrow d \mid b$

since $\gcd(2,3)=1$, and by Th. 2.5 (Euclid's lemma)

But if $2|a$ and $2|b$, then $\gcd(a,b) \neq 1$.

$\therefore d \neq 2$

$\therefore d = 1$ or 3

(c) $\gcd(a+b, a^2+b^2) = 1$ or 2

Pf: Let $d = \gcd(a+b, a^2+b^2)$

Then $d \mid a^2+b^2 \Leftrightarrow d \mid (a+b)(a-b) + 2b^2$

Since $d \mid (a+b)$, let x be s.t. $dx = a+b$

and let m be s.t. $dm = (a+b)(a-b) + 2b^2$

$\therefore dm = dx(a-b) + 2b^2$, $\therefore d[m + x(a-b)] = 2b^2$

$\therefore d \mid 2b^2$

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

$\therefore$ By Euclid's lemma, $d \mid 2b^2$ and $\gcd(d,b) = 1$ means $d \mid 2b \cdot b \Rightarrow d \mid 2b \Rightarrow d \mid 2$.

$\therefore d \leq 2 \Rightarrow d = 1$ or 2

(d) $\gcd(a+b, a^2-ab+b^2) = 1$ or 3

Pf: Let $d = \gcd(a+b, a^2-ab+b^2)$

$\therefore d \mid a^2-ab+b^2 \Rightarrow d \mid (a+b)^2 - 3ab$

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,
$\gcd(a,d) = \gcd(b,d) = 1$.

$\therefore$ By Euclid's lemma, $d \mid 3ab \Rightarrow d \mid 3a \Rightarrow d \mid 3$

$\therefore d \le 3$. Since $\gcd(2,3)=1$, then
if $d=2$, then $2 \mid 3ab \Rightarrow 2 \mid ab$
$\therefore 2 \mid a$ or $2 \mid b$, either of
which contradicts $\gcd(a,d) =$
$\gcd(b,d) = 1$. $\therefore d \ne 2$

$\therefore d = 1$ or 3

5. $a, b > 0$, $n \ge 1$

(a) If $\gcd(a,b)=1$, then $\gcd(a^n, b^n) = 1$

Pf: $n=1$: $\gcd(a,b)=1$ was assumed

$k \Rightarrow k+1$: Assume $\gcd(a^k, b^k)=1$

By problem 20(a) p. 26,

$$\gcd(a^k, b^{k+1}) = \gcd(a^k, b^k) = 1$$

Since $\gcd(a,b)=\gcd(b,a)$,

Then $\gcd(b^{k+1}, a^k)=1$, and

$\therefore$ again by 20(a) p. 26,

$$\gcd(b^{k+1}, a^k) = \gcd(b^{k+1}, a^{k+1}) = 1$$

(b) $a^n | b^n \Rightarrow a|b$

Pf: $n=1$: Clearly, $a^1 | b^1 = a|b$

$k \Rightarrow k+1$: Assume $a^k | b^k \Rightarrow a|b$

$\exists\, x$ s.t. $xa^k = b^k$, $\exists\, y$ s.t. $ay=b$

$$\therefore xa^{k+1} = ab^k = \left(\frac{b}{y}\right) b^k = \frac{b^{k+1}}{y}$$

$$\therefore xya^{k+1} = b^{k+1}$$

$$\therefore a^{k+1} | b^{k+1}$$

Another proof, as suggested by author
Let $d = \gcd(a,b)$, and let r, s be s.t.
$a = rd$, $b = sd$
$\gcd(r,s) = 1$ by problem 13(b), p. 25
$\therefore \gcd(r^n, s^n) = 1$ by (a) above.
But since $a^n = r^n d^n$, $b^n = s^n d^n$, Then
since $a^n | b^n$, Then $r^n d^n | s^n d^n \Rightarrow r^n | s^n$
$\therefore 1 = \gcd(r^n, s^n) = r^n$, so $r = 1$.
$\therefore$ from $a = rd$, $a = d$, and from $b = sd$,
$\therefore b = sa$, $\therefore a | b$

6. $\gcd(a,b) = 1 \Rightarrow \gcd(a+b, ab) = 1$

Pf: Let c be a divisor of $a+b$ and ab
By 20(d) p. 26, $\gcd(a,c) = \gcd(b,c) = 1$

Since $c | ab$ and $\gcd(c,a) = 1$, Then by Euclid's lemma, $c | b$
Similarly, $c | ab$ and $\gcd(c,b) = 1 \Rightarrow c | a$

So, $c | a$, $c | b$. $\therefore c \leq \gcd(a,b) = 1$, $\therefore c = 1$

7. (a) $a | b \Leftrightarrow \gcd(a,b) = |a|$

Pf: (1) $a | a$ and $a | b$. $\therefore$ a is a common divisor.

Suppose d is another common divisor.
$\therefore \exists n$ s.t. $a = dn$, $\therefore |a| = |d||n|$
Since $a \neq 0$, and $d \neq 0$, $\therefore n \neq 0$
$\therefore |n| > 1$, otherwise $|a| = |d|$.
$\therefore |a| = |d||n| > |d|$, so $|a| > |d|$
and $|a| = \gcd(a, b)$.
(2) Assume $\gcd(a, b) = |a|$
$\therefore \exists n$ s.t. $b = |a|n$. If $a > 0$, Then
$|a| = a$, so That $b = an \Rightarrow a | b$
if $a < 0$, Then $|a| = -a \Rightarrow b = (-a)n$,
$\therefore b = a(-n)$, $\therefore a | b$.

(6) $a | b \Leftrightarrow \operatorname{lcm}(a, b) = |b|$

Pf: (1) $a | b \Rightarrow a \,|\, |b|$, and clearly $b \,|\, |b|$
Let c be another common multiple
$\therefore a | c$ and $b | c$ (and $c > 0$).
$b | c \Rightarrow \exists n$ s.t. $c = bn$, and $|n| \geq 1$.
$\therefore |c| = |b||n| \geq |b|$. $\therefore |c| \geq |b|$, and
$\therefore |b| = \operatorname{lcm}(a, b)$ by def.
(2) $\operatorname{lcm}(a, b) = |b| \Rightarrow a \,|\, |b|$ by def.
$\therefore \exists n$ s.t. $an = |b|$
if $b > 0$, Then $an = b \Rightarrow a | b$
if $b < 0$, Then $an = -b$, $a(-n) = b$,
$\therefore a | b$.

(c) transitivity of (a) & (b) means
$\gcd(a,b) = |a| \Leftrightarrow \operatorname{lcm}(a,b) = |b|$

Or, directly,

(1) Assume $\gcd(a,b) = |a|$
$\therefore |a| \operatorname{lcm}(a,b) = |ab| = |a||b|$
$\therefore \operatorname{lcm}(a,b) = |b|$

(2) Assume $\operatorname{lcm}(a,b) = |b|$
$\therefore a \mid |b| \Rightarrow |a| \mid |b|$
Let c be another common divisor
$\therefore \exists n$ s.t. $a = cn \Rightarrow |a| = |c||n|$
But $|n| \geq 1$. $\therefore |c||n| \geq |c|$, $\therefore |a| \geq |c|$.
$\therefore |a| = \gcd(a,b)$.

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

$$
\begin{aligned}
227 &= 1 \cdot 143 + 84 \\
143 &= 2 \cdot 84 - 25 \\
84 &= 3 \cdot 25 + 9 \\
25 &= 2 \cdot 9 + 7 \\
9 &= 7 + 2 \\
7 &= 3 \cdot 2 + 1
\end{aligned}
$$

$\therefore \gcd(143, 227) = 1 \quad \therefore \operatorname{lcm} = 143 \cdot 227 = 32{,}461$

(b) $\mathrm{lcm}(306, 657)$

$657 = 2\cdot 306 + 45$
$306 = 7\cdot 45 - 9$
$45 = 5\cdot 9$
$\therefore \gcd = 9, \quad \therefore \mathrm{lcm} = 306\cdot 657/9 = 22{,}338$

(c) $\mathrm{lcm}(272, 1479)$

$1479 = 5\cdot 272 + 119$
$272 = 2\cdot 119 + 34$
$119 = 4\cdot 34 - 17$
$34 = 2\cdot 17$
$\gcd = 17, \quad \therefore \mathrm{lcm} = (272\cdot 1479)/17 = 23{,}664$

9. $a, b > 0$. $\gcd(a,b) \mid \mathrm{lcm}(a,b)$

Pf: Since $\gcd(a,b)\cdot \mathrm{lcm}(a,b) = ab$, let $d = \gcd(a,b)$. $\therefore \exists n, m$ s.t. $a = dn$, $b = dm$

$\therefore d\cdot \mathrm{lcm}(a,b) = (dn)(dm)$

$\therefore \mathrm{lcm}(a,b) = d(nm) \Rightarrow d \mid \mathrm{lcm}(a,b)$

10. (a) $\gcd(a,b) = \text{lcm}(a,b) \iff a = \pm b$

Pf: (1) Let $d = \gcd(a,b) = \text{lcm}(a,b)$

$\therefore d \cdot d = ab$

Since $d \mid a$, $\exists x$ s.t. $dx = a$.

$\therefore d \cdot d = dxb \Rightarrow d = xb \Rightarrow b \mid d$.

$\therefore d \mid b$ and $b \mid d$

$\therefore d = \pm b$ 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,

$\gcd(a,b) = \text{lcm}(a,b) = |a| = |b|$

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

Pf: $\gcd(ka,kb) \cdot \text{lcm}(ka,kb) = k^2|ab|$

$\therefore k\gcd(a,b) \cdot \text{lcm}(ka,kb) = k^2|ab|$

$\therefore \gcd(a,b) \cdot \text{lcm}(ka,kb) = k|ab|$

$= k\gcd(a,b) \cdot \text{lcm}(a,b)$

$\therefore \text{lcm}(ka,kb) = k \cdot \text{lcm}(a,b)$

(c) If m is a common multiple of a, b, then $\text{lcm}(a,b) \mid m$

Pf: Let $l = \text{lcm}(a,b)$
Let q, r be s.t. $m = lq + r$, $0 \le r < l$

If $r = 0$, then $l \mid m$.

Assume $0 < r < l$
$\therefore r = m - lq$. Since m, l are multiples of a and b, $\exists\, x, y, u, v$

$r = ax - ayq$ $\quad$ $r = bu - bvq$
$= a(x - aq)$ $\quad$ $= b(u - vq)$

$\therefore r$ is a multiple of a, b, and
$\therefore r \ge l$, 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) $d = \gcd(\gcd(a,b), c)$

Pf: Let $f = \gcd(a,b)$ and let $g = \gcd(f,c)$

(1) $g \mid f \Rightarrow g \mid a, g \mid b$. Since $g \mid c$, then $g \le d$

(2) Note That $d \mid f$.

Pf: $f = ax + by$, some x, y (Th. 2.3)

$a = du$, $b = dv$, some u, v.

$\therefore f = dux + dvy$, $\therefore d \mid f$

Since $d \mid c$, Then $d \mid g$. $\therefore d \le g$

$\therefore (1) \,\&\, (2) \to d = g$.

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

Proofs identical to (a) above, switching letters.

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

From (11) above,

$\gcd(198, 288, 512) = \gcd(\gcd(198, 288), 512)$

$\therefore 288 = 198 + 90$

$198 = 2 \cdot 90 + 18$

$90 = 5 \cdot 18$

$\therefore \gcd(198, 288) = 18$

$\therefore 18 = 198 - 2 \cdot 90$

$= 198 - 2(288 - 198)$

$= (-2) \cdot 288 + 3 \cdot 198$

Now for $\gcd(18, 512)$

$512 = 28 \cdot 18 + 8$

$18 = 2 \cdot 8 + 2$ $\quad \therefore 2 = 18 - 2 \cdot 8$

$8 = 4 \cdot 2$ $\quad = 18 - 2(512 - 28 \cdot 18)$

$\therefore \gcd(18, 512) = 2$ $\quad = 57 \cdot 18 - 2 \cdot 512$

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

$$\therefore 2 = 57 \cdot 18 - 2 \cdot 512$$

$$= 57 \cdot [3 \cdot 198 - 2 \cdot 288] - 2 \cdot 512$$

$$= 171 \cdot 198 - 114 \cdot 288 - 2 \cdot 512$$