Number Theory Section Summary: 2.3

The Euclidean Algorithm

1. Definitions

least common multiple: The **least common multiple** of two nonzero integers a and b, denoted $\text{lcm}(a, b)$, is the positive integer m satisfying the following:

(a) $a|m$ and $b|m$;

(b) If $a|c$ and $b|c$, with $c > 0$, then $m \leq c$.

2. Theorems

Lemma: If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$ $\qquad 0 \le r < \underline{b}$

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

So $d \mid a - qb = r$; so $d \mid r$, so d is a divisor of b + r.

Now to show that it's the greatest. Consider c, another divisor of b + r. Then

$$c \mid qb + r = a.$$ So c divides a.

c was a divisor of a + b, but not the greatest: $|c| \le d$. So $d = \gcd(b,r)$, Q.E.D.

Euclidean Algorithm:

$$\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \ldots = \gcd(r_{n-1},r_n) = r_n$$

(i.e. $r_n | r_{n-1}$, so the final remainder is 0). Then $\gcd(a,b) = r_n$.

$$a = q_1 b + r_1 \qquad 0 \le r_1 < b \qquad\qquad b = q_2 r_1 + r_2 \qquad 0 \le r_2 < r_1$$

$$= q_1(q_2 r_1 + r_2) + r_1$$

$$= (q_1 q_2 + 1) r_1 + q_1 r_2 \qquad\qquad r_1 = q_3 r_2 + \boxed{r_3} \qquad 0 \le r_3 < r_2$$

$$= (q_1 q_2 + 1)(q_3 r_2 + r_3) + q_1 r_2$$

$$= [(q_1 q_2 + 1) q_3 + q_1] \underset{\overset{\uparrow}{q_4 r_3}}{r_2} + (q_1 q_2 + 1) r_3 \qquad\qquad \boxed{r_2 = q_4 r_3 + 0}$$

$$= \{[(q_1 q_2 + 1) q_3 + q_1] q_4 + (q_1 q_2 + 1)\} r_3 \qquad\qquad \underline{r_3 | a}$$

Example: (#1/2(a), p. 31) Consider 143 and 227.

- Implement the Euclidean Algorithm using Mathematica.
- Find the gcd.

$$\begin{aligned}
227 &= q\ 143 + r \\
&= 1 \cdot 143 + 84 \\
143 &= 1 \cdot 84 + 59 \\
84 &= 1 \cdot 59 + 25 \\
59 &= 2 \cdot 25 + 9 \\
25 &= 2 \cdot 9 + 7 \\
9 &= 1 \cdot 7 + 2 \\
7 &= 3 \cdot 2 + \boxed{1} \\
2 &= 2 \cdot \boxed{1} + 0
\end{aligned}$$

$$\begin{aligned}
84 &= 227 - 1 \cdot 143 \\
59 &= 143 - 1 \cdot 84 \\
25 &= 84 - 1 \cdot 59 \\
9 &= 59 - 2 \cdot 25 \\
7 &= 25 - 2 \cdot 9 \\
2 &= 9 - 1 \cdot 7 \\
1 &= 7 - 3 \cdot 2
\end{aligned}$$

$$1 = 143x + 227y$$

- Write the gcd as a linear combination of 143 and 227.

gcd

$$\boxed{r_n} = r_{n-2} - q_n r_{n-1}$$

$$\vdots$$

$$r_3 = r_1 - q_3 r_2$$

$$r_2 = b - q_2 r_1$$

$$r_1 = a - q_1 b$$

$$\begin{aligned}
1 &= 7 - 3\cdot 2 = 7 - 3(9 - 1\cdot 7)\\
&= 4\cdot 7 - 3\cdot 9\\
&= 4\cdot(25 - 2\cdot 9) - 3\cdot 9\\
&= 4\cdot 25 - 11\cdot 9\\
&= 4\cdot 25 - 11(59 - 2\cdot 25)\\
&= 26\cdot 25 - 11\cdot 59\\
&= 26(84 - 1\cdot 59) - 11\cdot 59\\
&= 26\cdot 84 - 37\cdot 59\\
&= 26\cdot 84 - 37\cdot(143 - 1\cdot 84)\\
&= 63\cdot 84 - 37\cdot 143\\
&= 63\cdot(227 - 1\cdot 143) - 37\cdot 143
\end{aligned}$$

$$\boxed{\begin{array}{c} 1 = 63\cdot \underline{227} - 100\cdot \underline{143} \\ x = 63 \qquad y = -100 \end{array}}$$

Theorem 2.7: if $k > 0$, then $\gcd(ka, kb) = k\gcd(a, b)$.

Corollary: if $k \neq 0$, then $\gcd(ka, kb) = |k|\gcd(a, b)$.

Proof: Let's prove the corollary, without recourse to Theorem 2.7 (which is proved in the process):

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

$$\begin{aligned}
\gcd(ka,kb) &= \min\{\, |kax + kby|^{\neq 0} \,/\, x,y \in \mathbb{Z} \,\}\\
&= \min\{\, |k|\,|ax + by|^{\neq 0} \,/\, x,y \in \mathbb{Z} \,\}\\
&= |k|\cdot \min\{\, |ax+by|^{\neq 0} \,/\, x,y \in \mathbb{Z} \,\}\\
&= |k| \gcd(a,b)
\end{aligned}$$

Examples: #4a,c, p. 32; #6 Assume $\gcd(a,b)=1$

#4a $\underbrace{\gcd(a+b, a-b)} = 1$ or 2.

$d = (a+b)x + (a-b)y$ for some x r y.

$\underbrace{(a+b)+(a-b)}_{d \mid \text{this}} = 2a \quad \Rightarrow \quad d \mid 2a$

$\underbrace{(a+b)-(a-b)}_{d \mid \text{this}} = 2b \quad \Rightarrow \quad d \mid 2b$

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

$\therefore \ d = 1$ or 2

Theorem 2.8: For positive integers a and b

$$\gcd(a,b)\operatorname{lcm}(a,b) = ab$$

One thing this theorem does is give us a method for calculating the lcm (since we can use the Euclidean Algorithm to find the gcd):

Example: #1a, p. 31

× Example: #10a,b, p. 32

Corollary: For positive integers a and b

$$\mathrm{lcm}(a,b) = ab \iff \gcd(a,b) = 1$$

3. Properties/Tricks/Hints/Etc.

"Gabriel Lamé (1795-1870) proved that the number of steps required in the Euclidean Algorithm is at most five times the number of digits in the smaller integer."

An improvement to the Euclidean Algorithm is achieved if, instead of choosing to work with $a = qb + r$ with $0 \leq r < b$, we work with $a = qb + r$ with $|r| < b/2$.

4. Summary

The Euclidean Algorithm gives us a tool for calculating the gcd of two integers. One variation of the algorithm (using "centered remainders" from an alternative version of the division algorithm – see problem 7, p. 20) provides a faster algorithm.

The algorithm works by replacing a pair of integers requiring a gcd by a pair of smaller integers, constrained by the fact that the smallest is greater than zero.

The least common multiple (lcm) of two integers is the first positive number appearing in both their multiplication tables, but can be found using the gcd: if they're positive and relatively prime, then the lcm is their product; but if not, then the product divided by the gcd gives us the lcm.

This makes good sense: the gcd is the "repetitious" part of the integers.

#4c $\gcd(a+b, a^2+b^2) = 1$ or 2

Hint: $a^2+b^2 = (a+b)(a-b) + 2b^2 \implies$

$$\left[\ \underset{\text{gcd}}{\overset{\parallel}{d}} = (a+b)x + (a^2+b^2)y \quad \exists x + y\ \right]$$

$$2b^2 = \underbrace{\underbrace{a^2+b^2 - (a+b)(a-b)}_{\text{a linear combination of } a+b \text{ + } a^2+b^2}}_{d \mid \text{this,}}$$

So $d \mid 2b^2$.

Similarly, $d \mid 2a^2$. [Using symmetry in a + b.]

$$\boxed{d \mid \gcd(2a^2, 2b^2) = 2\gcd(a^2, b^2)}$$

Interlude

[Now what ?!] 20f, p26 - or 20a.

20a. If $\gcd(a,b)=1$ and $\gcd(a,c)=1$, then

$$\gcd(a,bc)=1$$

$1 = ax + by = au + cv \qquad \exists x,y,u,v \in \mathbb{Z}$

$1 = (ax+by)(au+cv)$

$= a^2xu + axcv + auby + bcyv$

$1 = a[\quad] + bc[\ ]$ (a linear combination = 1; hmmm... relatively prime — gcd = 1!)

$\therefore \gcd(a,bc)=1$

$\gcd(a,b)=1$ and $\gcd(a,b)=1 \Rightarrow$

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

[Symmetrically, $\gcd(b,a^2)=1$]

$\gcd(b^2,a)=1$ and $\gcd(b^2,a)=1 \Rightarrow$

$$\boxed{\gcd(b^2,a^2)=1}$$

$d \mid 2\gcd(a^2,b^2) = 2\cdot\gcd(a,b) = 2$

$\therefore d=1$ or 2.

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

$(a+b)x + aby = \gcd(a+b,ab) \equiv d \qquad \exists x,y$

$ax + bx + aby$

$ax + b(x+ay)$

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$\underbrace{\underbrace{(a+b)^2 - 2ab}_{\text{linear combo of } (a+b) + ab}}_{d \mid \text{this}} = a^2 + b^2 \quad \Rightarrow \quad d \mid a^2+b^2$$

didn't use - but we might have!

$$(a+b)[a] + ab[-1] = a^2$$

$$\Rightarrow \quad d \mid a^2$$

Symmetrically, $d \mid b^2$

$$d \mid \underbrace{\gcd(a^2, b^2) = \gcd(a,b)}_{\text{since } \gcd(a,b)=1} = 1$$

✓

$$\therefore \ d = 1$$