3.3 Greatest Common Divisors and their Properties

GCD of integers $a$ and $b = \text{the largest integer that divides both } a \text{ and } b$\(\text{def} (a, b)\)

$(0, 0) = 0 \text{ (definition)} \quad (a, b) = (\gcd(a, b))$

To find $(a, b)$ Example $(15, 81)$

\[
\begin{array}{c}
15 \\
\downarrow \\
3 \\
\downarrow \\
\uparrow 5
\end{array} \quad \begin{array}{c}
81 \\
\downarrow \\
3 \\
\downarrow \\
\uparrow 3
\end{array} \quad \begin{array}{c}
6 \text{ GCD} = 3 \\
\text{LCM} = 3 \cdot 5 \cdot 3 \cdot 3 = \frac{81 \cdot 5}{3} = 405
\end{array}
\]

$(15, 81) = 3$

$(15/3, 81/3) = (5, 27) = 1$ This is example of Theorem: If $a$ and $b$ have $(a, b) = d$ then $(\gcd(a, b) = 1$ \(\frac{a}{d}, \frac{b}{d} \) relatively prime $a \text{ and } b \text{ are relatively prime}$

---

A linear combination of integers $a$ and $b$ is a sum of the form $ma + nb$ where $m, n$ are integers.
It turns out that the following is an important concept:

**Nonconstructive Description of \((a, b)\)**

**Theorem 3.8** \((a, b)\) is the least positive integer that is in the set of positive linear combinations \(ma + nb\) of \(a\) and \(b\).

**Proof** \(S\) is non-empty since \(1, a + b \in S\) and \(0, a + b \in S\). By well ordering \(S\) has a smallest element \(d = ma + nb\). Claim that \(d\) divides \(a\) and \(d\) divides \(b\). Dividing \(d\) into \(a\) using the division algorithm we get

\[
a = dq + r \quad 0 \leq r < d
\]

Thus \(r = a - dq = a - q(ma + nb) = (-q + (1-qm))a - qnb\). Thus \(r \in S\) positive.

But \(0 \leq r < d\) and \(d\) is smallest linear combination – so \(r = 0\) Thus \(d \mid a\).
Similarly \( a \mid b \) must now show that it is the GCD of \( a \) and \( b \). Suppose \( c \mid a \) and \( c \mid b \) then because \( d = \text{max}(a, b) \) then \( c \mid d \).

Page 99

#3 Suppose a positive, what is GCD of \( a, 2a \). Answer \( a \)

#4 Find GCD of \( a, a^2 \) Answer \( a \)

#8 Show that the GCD of an even number and an odd # is odd

3.4 The Euclidean Algorithm

**Constructive Description**

Theorem 3.4. Given \( a = r_0 \geq b = r_1 > 0 \)

Applying division algorithm repeatedly

\[ r_0 = r_1 q_1 + r_2 \]

\[ r_1 = r_2 q_2 + r_3 \]

\[ r_2 = r_3 q_3 + r_4 \]

\[ r_{n-2} = r_{n-1} q_{n-1} + r_n \]

\[ r_{n-1} = r_n q_n + r_{n+1} \]

Claim \( r_n = (a, b) \)
Example Find \((15, 81)\)

\[
81 = 15 \cdot 5 + 6
\]

\[
15 = 6 \cdot 2 + 3
\]

\[
6 = 3 \cdot 2 + 0
\]

Thus, 3 is GCD of 15 and 81.

Expression as a linear combination of 15 and 81 is

\[
3 = m \cdot 81 + n \cdot 15 = -2 \cdot 81 + 2 \cdot (45) 15 + 15 = 11(15) - 2(81)
\]

Example Find \((30, 42)\)

\[
42 = 30 \cdot 1 + 12
\]

\[
30 = 12 \cdot 2 + 6
\]

\[
12 = 6 \cdot 2 + 0
\]

6 = GCD

Expression as a linear combination of 30 and 42

\[
6 = 30 - 2(12) = 30 - 2(42 - 30, 1)
\]

\[
6 = 30 - 2(42) + 2(30)
\]

\[
6 = 3 \cdot 30 - 2(42)
\]

Expresses 6 as combo of 30 and 42

IDEA: Repeated Division gets you the GCD. Working back through the
steps gives you the GCD as a combination of the two starting numbers. 

Use Euclidean algorithm to find \((a, b)\) and then express \((a, b)\) as a combination of \(a\) and \(b\).

Illustration

\[(504, 396) = m(504) + n(396)\]

Find \(m, n\).

Solution

\[504 = 396 \cdot 1 + 108\]

\[396 = 108 \cdot 3 + 72\]

\[108 = 72 \cdot 1 + 36\] GCD

\[72 = 36 \cdot 2 + 0\]

\[36 = 108 - 72 \cdot 1 = 108 - (396 - 108 \cdot 3)\]

\[36 = 4 \cdot 108 - 396 = 4(504 - 396) - 396\]

\[36 = 4(504) - 5(396)\]
-6-

Find GCD of 15, \underline{35}, 90

90 = 35 \times 2 + 20 \quad 35 = 20 \times 1 + 15
20 = 15 \times 1 + 5 \quad 15 = 5 \times 3 + 0

\therefore 5 = (90, 35) \quad \text{GCD}(15, 5) = 5

5 = \text{GCD of } 90, 35, 15

6(b) \quad (70, 98, 105)

Prime factorization

\[
\begin{array}{c}
70 \\
\downarrow \phantom{0}
\hline
2 \\
\downarrow \\
5 \\
\downarrow \phantom{0}
\hline
35 \\
\downarrow \\
5 \\
\downarrow \phantom{0}
\hline
2 \\
\downarrow \\
7 \\
\downarrow \\
7
\end{array}
\quad 
\begin{array}{c}
98 \\
\downarrow \phantom{0}
\hline
2 \\
\downarrow \\
7 \\
\downarrow \\
49 \\
\downarrow \phantom{0}
\hline
7
\end{array}
\quad 
\begin{array}{c}
105 \\
\downarrow \phantom{0}
\hline
3 \\
\downarrow \phantom{0}
\hline
21 \\
\downarrow \phantom{0}
\hline
7
\end{array}
\]

Answer 7

\[(98, 105) = 7
\]

\[(70, 98) = 2 \cdot 7 = 14
\]

\[
(70, 98), (98, 105) = (14, 7) = 7
\]

OTHER WAY

\[(70, 98) \quad 98 = 70 \cdot 1 + 28
\]

\[(98, 105) \quad 105 = 98 \cdot 1 + 7
\]

\[
70 = 28 \cdot 2 + 14
\]

\[
98 = 7 \cdot 14 + 0
\]

\[
28 = 14 \cdot 2 + 0
\]

\[
14 \text{ gcd}
\]

\[
14 = 7 \cdot 2 + 0
\]

\[
7 \text{ gcd of } 98, 70, 28
\]

Page 110