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

Euclidean Algorithm:

$$\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \ldots = \gcd(r_n,0) = r_n$$

$\gcd(a,b) = r_n$.

Example: (Like #1/2, p. 31) Consider 309 and 897

- Implement the Euclidean Algorithm using the TI-92 calculator
- Find the gcd
- Write the gcd as a linear combination of 309 and 897.

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

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

Theorem 2.8: For positive integers a and b

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

1

$897 = q\,309 + r$

$897 = 2 \cdot 309 + 279$

$309 = q\,279 + r$

$309 = 1 \cdot 279 + 30$

$279 = q\,30 + r$

$279 = 9 \cdot 30 + 9$

$30 = q \cdot 9 + r$

$30 = 3 \cdot 9 + 3$

$9 = q\,3 + r$

$9 = 3 \cdot 3 + 0$

$897 \to a : 309 \to b$

$a - \text{floor}(a/b) \cdot b \to c$

$b \to a : c \to b$

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

Example: Like #1, p. 31: 309 and 897

Corollary: For positive integers a and b

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

---

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.

$897 = 309 \cdot 2 + 279$

$309 = 279 \cdot 1 + 30$

$279 = 30 \cdot 9 + 9$

$30 = 9 \cdot 3 + 3$

$9 = 3 \cdot 3$

$\Rightarrow$

$279 = 897 - 309 \cdot 2$

$30 = 309 - 279 \cdot 1$

$9 = 279 - 30 \cdot 9$

$3 = 30 - 9 \cdot 3$

$279 = a - 2b$

$30 = b - (a-2b)\cdot 1 = -a + 3b$

$9 = a - 2b - (-a+3b)\cdot 9 = 10a - 29b$

$3 = -a+3b - (10a-29b)\cdot 3$

$= -31a + 90b$

$$\boxed{3 = -31 \cdot 897 + 90 \cdot 309}$$

4a) Given $\gcd(a,b) = 1$ prove that

p32 $d = \gcd(a+b, a-b) = 1$ or 2

$\underbrace{(a+b) + (a-b)} = 2a$

d divides this, so $d \mid 2a$

$(a+b) - (a-b) = 2b$

similarly $d \mid 2b$

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

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

$d \leq 2$, so d is 1 or 2

4c) Given $\gcd(a,b) = 1$

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

Consider

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

d divides this, so $d \mid 2b^2$

Similarly $d \mid 2a^2$

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

By #5, p 32, $\gcd(a^2, b^2) = 1$

So $d \leq 2$, or $d = 1$ or $d = 2$.

#6 p 32 Given $\gcd(a,b) = 1$; then

$d = \gcd(a+b, ab) = 1$

$a \cdot (a+b) - ab = a^2$

d divides this, so $d \mid a^2$

Similarly, $d \mid b^2$.

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

but $\gcd(a^2, b^2) = 1$ by #5, so $d = 1$.

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

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

$\exists (x,y)$ / $ax + by = 1$

$\exists (u,v)$ / $au + cv = 1$

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

Look for a good linear combination!