Mathematics 243, section 1 – Algebraic Structures
Discussion 3 – Greatest Common Divisors
October 10, 2003

Background

From before the exam, recall that we discussed the following ideas:

- if a and b are two integers, then an integer c is a *common divisor* of a and b if $c|a$ and $c|b$.
- We say d is a *greatest common divisor*, or gcd, of a and b if all three of the following statements are true:
  1) $d \in \mathbf{Z}^+$,
  2) $d|a$ and $d|b$, and
  3) if $c|a$ and $c|b$, then $c|d$.

- For example, a greatest common divisor of $a = 240$ and $b = 504$ is $d = 24$, which we can see by factoring:

$$240 = 2^4 \cdot 3 \cdot 5 \quad \text{and} \quad 504 = 2^3 \cdot 3^2 \cdot 7$$

  However, factoring large numbers can be hard (especially if there are no small factors). Hence we want to consider today a better method for computing gcd's for large a, b, based on one of the other facts we proved before the exam:

- Given $a, b \in \mathbf{Z}$, we considered the set

$$S_{a,b} = \{ma + nb : m, n \in \mathbf{Z}\} \tag{1}$$

  We showed that if d is the smallest element in $S^+_{a,b} = S_{a,b} \cap \mathbf{Z}^+$, then d is a gcd of a, b.

Discussion Questions

A) Show that if a, b are integers and $b > 0$, then the remainder on division of a by b is one of the elements of the set $S_{a,b}$.

B) This observation suggests one method for finding the gcd, namely: Construct elements in the set $S_{a,b}$ from (1) by taking remainders, and try to identify the smallest positive element in that set by finding a remainder as small as possible. Try this for $a = 5673$ and $b = 305$. What is the smallest strictly positive number you find? Can you show there aren't any smaller elements of S?

C) A systematic procedure for doing the kind of search for small elements of S you did in B is known as *Euclid's Algorithm.* It can be phrased like this: Start with $a > b > 0$, and compute the quotient and remainder: $a = q_1 b + r_1$. Then divide r_1 into b to yield $b = q_2 r_1 + r_2$. Then divide r_2 into r_1 to yield $r_1 = q_3 r_2 + r_3$, and so on. If you "stack"

the resulting equations you will see a pattern that should help you to remember the process:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \end{aligned}$$

1) Explain why eventually you will get a remainder $r_n = 0$. (Hint: What is true about r_1 versus b, r_2 versus r_1, etc.)
2) Explain why $r_i \in S$ for all $i \geq 1$.

D) In fact,

$$r_n = 0 \text{ but } r_{n-1} \neq 0 \Rightarrow r_{n-1} = gcd(a, b).$$

Use the Euclidean Algorithm to find the gcd of

1) $a = 1400$, $b = 980$.
2) 693, $b = 414$.

Assignment

Group write-ups due Friday, October 17.