The Euclidean Algorithm

We have seen some reasons why the gcd (a, b) is important, but no good way to calculate it. We saw one method in class: find the gcd by brute force, by listing all the divisors of a and b. This is obviously impractical for large a and b. Later, we'll see that there's an easy formula if you know the prime factorizations of a and b. Unfortunately, it turns out that finding prime factorizations is not easy, so this is not a great algorithm in general.

The Euclidean algorithm gives us an efficient algorithm to calculate (a, b) for any non-negative integers a, b. [Note that $(a, b) = (|a|, |b|)$, so if we can calculate (a, b) for non-negative a, b, we can do it for any a, b.] Let r_1 be the remainder when a is divided by b. You will prove for homework that $(a, b) = (b, r_1)$. Now let r_2 be the remainder when b is divided by r_1 and apply the homework problem again, so that

$$(a, b) = (b, r_1) = (r_1, r_2).$$

Continue in this fashion until you reach a remainder of 0:

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{k-1}, r_k) = (r_k, 0). \tag{1}$$

Clearly $(r_k, 0) = r_k$, so we conclude that (a, b) is r_k, the last nonzero remainder. For example, we calculate $(2159, 1003)$:

$$\begin{aligned}
2159 &= 2 \cdot 1003 + 153, && (2)\\
1003 &= 6 \cdot 153 + 85, && (3)\\
153 &= 1 \cdot 85 + 68, && (4)\\
85 &= 1 \cdot 68 + 17, && (5)\\
68 &= 4 \cdot 17 + 0.
\end{aligned}$$

This shows that $(2159, 1003) = 17$.

1. Prove that the algorithm must terminate. That is, for any non-negative integers a and b, you will eventually get a remainder of 0. This ensures that the algorithm gives you an answer, and doesn't continue in an infinite loop forever.

2. Calculate $(1081, 1219)$.

The Euclidean algorithm can also be used to find Bézout coefficients[1] for a and b.

Each time you do division, you get an equation; those equations can be used to find the Bézout coefficients, as illustrated below. We use our earlier calculations to find Bézout coefficients for 2159 and 1003: solve each equation for r_i, and successively plug each one in:

$$\begin{aligned}
17 &= 85 - 1 \cdot 68 && \text{by (5)} \\
&= 85 - 1 \cdot (153 - 1 \cdot 85) && \text{by (4)} \\
&= 2 \cdot 85 - 1 \cdot 153 \\
&= 2 \cdot (1003 - 6 \cdot 153) - 1 \cdot 153 && \text{by (3)} \\
&= 2 \cdot 1003 - 13 \cdot 153 \\
&= 2 \cdot 1003 - 13 \cdot (2159 - 2 \cdot 1003) && \text{by (2)} \\
&= -13 \cdot 2159 + 28 \cdot 1003.
\end{aligned}$$

This proves that -13 and 28 are Bézout coefficients for 2159 and 1003. We'll see later why it's important to have an algorithm to find Bézout coefficients efficiently.

3. Find Bézout coefficients for 17 and 97.

4. Use your answer to the previous problem to find an integer n such that the remainder when $17n$ is divided by 97 is 8. (If you know modular arithmetic, this is asking you to solve the congruence $17n \equiv 8 \pmod{97}$. If you haven't seen modular arithmetic before, that's fine – we'll cover it soon.)

5. Find an integer m such that the remainder when $117m$ is divided by 367 is 61.

[1] Recall that Bézout coefficients are $u, v \in \mathbb{Z}$ such that $au + bv = (a, b)$.