Math Circles Diophantine Equations and the Euclidean Algorithm

Colin Curtis

August 9, 2020

Definition: A *Diophantine equation* is an equation of the form $ax + by = c$, where x, y are variables that we are trying to solve for. In other words, we are trying to find x and y that solve the given equation.

Definition: The *greatest common divisor (gcd)* of two numbers a and b, denoted $gcd(a, b)$, is the greatest number that divides both a and b.
Example: $gcd(5, 10) = 5$. We see this just through simple observation. $gcd(12, 7) = 1$ since 7 is a prime number.

Important Fact: if $c = gcd(a, b)$, then there exist integers x and y such that $ax + by = c$. This is important because it guarantees the existence of a solution to the Diophantine equation $ax + by = c$ if and only if $c = gcd(a, b)$.

Problem 1: Try to find integer solutions to the Diophantine equation $2x + 3y = 0$. What about $2x + 3y = 1$? Or $2x + 3y = 31$? Think about how you can get the third equation from the second equation.

Problem 2: Suppose we have a solution (x_0, y_0) to the Diophantine equation $ax + by = 1$. Let n be an arbitrary integer. Show there is a solution to the Diophantine equation $ax + by = n$. Can you give a solution? *hint:* think about the previous problem.

Euclidean Algorithm: Suppose we are trying to calculate $gcd(a, b)$, with $a \geq b$. Then write

1. $a = q_0 b + r_o$, where q_0 is the quotient and r_0 is the remainder.
2. $q_0 = q_1 r_0 + r_1$, so the old quotient is the new dividend, and the old remainder is the new divisor.
3. Continue this process, so the k^{th} iteration is given by $q_{k-1} = q_k r_{k-1} + r_k$. The amazing fact is that eventually $r_k = 0$, and then $gcd(a, b) = r_{k-1}$, namely the divisor of the step where we get remainder 0.

This is a really important algorithm that allows us to compute the gcd of two numbers really easily. What we are really doing here is saying $gcd(a, b) = gcd(b, a \text{ mod } b)$.

Problem 3: Use the Euclidean Algorithm to compute $gcd(1071, 462)$. *hint:* First write $1071 = 2(462) + 147$. Then find q, r so that $462 = 147(q) + r$

Problem 4: Use the Euclidean Algorithm to compute $gcd(383, 74)$.

Problem 5: Suppose $a|(bc)$ and $gcd(a, b) = 1$. Show $a|c$. Recall $p|q$ (p divides q) if there exists an integer k such that $pk = q$. *hint:* write out the divisibility statement and also use our important fact.

Problem 6: If $m|a$ and $m|b$, and m is a positive constant, then show that $gcd(\frac{a}{m}, \frac{b}{m}) = \frac{1}{m}gcd(a, b)$. This lets us take constants out of the gcd expression.