Euclid's Algorithm and Bézout's Identity

Dave Neary

January 15, 2021

1 Introduction

When working with large numbers, we will often want to calculate their greatest common divisor. In particular, it is often important to know if two numbers are co-prime, that is, if they have a greatest common divisor of 1. A fast algorithm for this, which dates from ancient times, is Euclid's Algorithm.

For math competitions, it will sometimes be useful to be able to find a linear combination of two numbers with integer solutions, especially when working in modular arithmetic. Based on Euclid's algorithm, we will also show how to create such a linear combination using Bézout's identity.

2 Euclid's Algorithm

The Greatest Common Divisor of two integers a, b is the largest positive integer k which evenly divides both a and b. That is, we can write $a = km$, $b = kn$ for $m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$. For smaller numbers, we will typically do this by finding the prime decomposition of the two numbers, and identifying prime numbers which are common factors of both numbers.

However, this is impractical for larger numbers. Thankfully, Euclid's algorithm gives us a simple method to systematically find the GCD of any two natural numbers.

Theorem 2.1. *Given two positive integers $a, b \in \mathbb{Z}^+$, we can find unique non-negative integers $q, r \in \mathbb{Z}^+$ (quotient and remainder) such that:*

$$a = qb + r$$

with $0 \leq r < a$

That is, we can always divide b into a to get a quotient and a remainder. We can even weaken the requirement that a and b are positive integers, if we allow negative values of q and we can find a positive $r < |b|$. For example, if we use this with $a = 89, b = 17$, we get $q = 5, r = 4$, and $89 = 5 \times 17 + 4$. What makes this into an algorithm to calculate the GCD is the following result:

Theorem 2.2. *Given positive integers a, b with $a > b$, and non-negative integers q, r such that $a = qb + r$: If $r > 0$ then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Let $k = \gcd(a, b)$. Then $a = km, b = kn, \gcd(n, m) = 1$.

We are given:

$$\begin{aligned} a &= qb + r \\ \implies r &= a - qb \\ \implies r &= k(m - qn) \end{aligned}$$

So r is a multiple of k.

Also, if $gcd(b, r) = j > k$ then $qb = jm, r = jn$ for some m, n, and then:

$$a = qb + r = j(m + n)$$

so a is also a multiple of j and k is not the GCD of a, b, which is a contradiction.

Therefore, $\gcd(a, b) = \gcd(b, r)$. □

This gives us a way to repeat this operation until r eventually reaches 0, at which case the r in the prior step is the GCD.

Let's work through an example to see it in action.

Question 2.1. *Find the GCD of 1128 and 33.*

Proof.

$$\begin{aligned} 1128 &= 34 \times 33 + 6 \\ 33 &= 5 \times 6 + 3 \\ 6 &= 2 \times 3 + 0 \end{aligned}$$

So the GCD of 1128 and 33 is 3 (the last non-zero remainder). □

Question 2.2. *Find the GCD of 6540 and 1206.*

3 Bézout's identity

Given $a, b \in \mathbb{Z}, a, b \neq 0$, we can find $n, m \in \mathbb{Z}$ such that:

$$\gcd(a, b) = ma + nb$$

In fact when both a and b are not equal to 0, we can find infinitely many such pairs (m, n).

In particular, if $\gcd(a, b) = 1$, then for all integers k, we can find $n, m \in \mathbb{Z}$ such that:

$$k = am + bn$$

And further, if $\gcd(a, b) = k$, there are no solutions to the equation $am+bn = j$ if j is not a multiple of k.

The way that we use Euclid's algorithm to generate this identity is that we start at the last step, and rearrange everything to be in terms of $\gcd(a, b)$, and then at each stel we replace the remainder term with $a - qb$.

Let's work through an example to see how it works:

Question 3.1. *Find an integer solution to:*

$$267x + 112y = 3$$

Proof. Let's start by calculating the GCD of 267 and 112 using Euclid's algorithm, and also noting the form $r = a - qb$ at each step:

$$\begin{aligned}
267 &= 2 \times 112 + 43 & 43 &= 267 - 2 \times 112 \\
112 &= 2 \times 43 + 26 & 26 &= 112 - 2 \times 43 \\
43 &= 1 \times 26 + 17 & 17 &= 43 - 1 \times 26 \\
26 &= 1 \times 17 + 9 & 9 &= 26 - 1 \times 17 \\
17 &= 1 \times 9 + 8 & 8 &= 17 - 1 \times 9 \\
9 &= 1 \times 8 + 1 & 1 &= 9 - 1 \times 8 \\
8 &= 8 \times 1 + 0 & &
\end{aligned}$$

So the GCD of 267 and 112 is 1.

Now we run through the algorithm backwards, isolating the remainder term:

$$\begin{aligned}
1 &= 9 - 1 \times 8 \\
1 &= 9 - 1 \times (17 - 1 \times 9) = 2 \times 9 - 1 \times 17 \\
1 &= 2 \times (26 - 1 \times 17) - 1 \times 17 = 2 \times 26 - 3 \times 17 \\
1 &= 2 \times 26 - 3 \times (43 - 1 \times 26) = 5 \times 26 - 3 \times 43 \\
1 &= 5 \times (112 - 2 \times 43) - 3 \times 43 = 5 \times 112 - 13 \times 43 \\
1 &= 5 \times 112 - 13 \times (267 - 2 \times 112) = 31 \times 112 - 13 \times 267
\end{aligned}$$

Now we have a general solution $1 = 31 \times 112 - 13 \times 267$, and we can generate other solutions to the same equation by adding and subtracting multiples of 112×267 as follows:

$$1 = (31 - 267k) \times 112 + (112k - 13) \times 267$$

And we can get the general solution to the question asked by multiplying every term by 3:

$$3 = (93 - 801k) \times 112 + (336k - 39) \times 267$$

which gives solutions for any $k \in \mathbb{Z}$.

□

Questions of this type often arise with different notation or ways of framing the question. Here are another example, and some exercises:

Question 3.2. *What is the inverse of 10 modulo 17?*

Proof. The multiplicative inverse of $k \pmod{n}$ in modular arithmetic is an integer which, when you multiply it by k, gives a result of $1 \pmod{n}$

In other words, we need to find a number m such that:

$$10m + 17n = 1$$

We will use Euclid's algorithm to get the GCD of 10 and 17 (which is obviously 1):

$$\begin{array}{rlrl}
17 &= 10 + 7 & \qquad 7 &= 17 - 10 \\
10 &= 7 + 3 & 3 &= 10 - 7 \\
7 &= 2 \times 3 + 1 & 1 &= 7 - 2 \times 3 \\
 & & 1 &= 7 - 2 \times (10 - 7) \\
 & & 1 &= 3 \times 7 - 2 \times 10 \\
 & & 1 &= 3 \times (17 - 10) - 2 \times 10 \\
 & & 1 &= 3 \times 17 - 5 \times 10
\end{array}$$

We have an identity, with a general term:

$$1 = (3 - 10k) \times 17 + (17k - 5) \times 10$$

with the smallest positive multiple of 10 which works being $k = 1$, $17 - 5 = 12$ And it's easy to verify that $1 = 12 \times 10 - 7 \times 17$. □

Question 3.3. *Find a solution in integers to the Diophantine equation* $61x + 23y = 1$

Question 3.4. *Find a natural number* k *such that* $(573k + 4)/719$ *is also a natural number.*

Question 3.5. *Find the smallest positive integer that ends in 2010, and is divisible by 2011.*