Problems Concerning the GCD: Modular Inverse

P. Reany

July 4, 2023

Abstract

The GCD refers to the *greatest common divisor* of a set of positive integers. The GCD of integers a and b is denoted in this paper as (a, b). The GCD of two integers is the largest (greatest) integer that evenly divides both a and b. Practical uses of the GCD are all over both mathematics and engineering. There are even practical everyday applications for it.

1 Problem 1

Use the Euclidean Algorithm to find the inverse of 7 (mod 40).

Since 7 and 40 are relatively prime, 7 has a unique inverse mod 40. So, we begin with the Euclidean Algorithm:

$$\begin{aligned} 40 &= 5 \cdot 7 + 5\,, \\ 7 &= 1 \cdot 5 + 2\,, \\ 5 &= 2 \cdot 2 + 1\,. \end{aligned} \tag{1}$$

Next, we solve these for the remainders:

$$\begin{aligned} 40 - 5 \cdot 7 &= 5\,, \\ 7 - 1 \cdot 5 &= 2\,, \\ 5 - 2 \cdot 2 &= 1\,. \end{aligned} \tag{2}$$

Now remember: The two numbers we need to end up with on the LHS are 40 and 7, and the one number we need to end up with on the RHS is unity (because we are looking for an inverse). So, let's remove the second of these by substituting it in the third, leaving:

$$\begin{aligned} 40 - 5 \cdot 7 &= 5\,, \\ 5 - 2 \cdot [7 - 1 \cdot 5] &= 1\,, \end{aligned} \tag{3}$$

which simplifies to

$$\begin{aligned} 40 - 5 \cdot 7 &= 5\,, \\ 3 \cdot 5 - 2 \cdot 7 &= 1\,. \end{aligned} \tag{4}$$

Lastly, we substitute out the 5 in the second line from the first line:

$$3 \cdot [40 - 5 \cdot 7] - 2 \cdot 7 = 1\,, \tag{5}$$

which becomes

$$3 \cdot 40 - 17 \cdot 7 = 1\,. \tag{6}$$

So, on taking this last equation mod 40, we have that

$$-17 \cdot 7 \equiv \pmod{40}\,. \tag{7}$$

However,

$$-17 \equiv 23 \pmod{40}\,. \tag{8}$$

So finally,

$$7^{-1} \equiv 23 \pmod{40}\,. \tag{9}$$