The Chinese Remainder Theorem

P. Reany

February 5, 2020

Abstract

The Chinese Remainder Theorem using undetermined coefficients.

1 Introduction

Let m_1 and m_2 be two relatively prime (coprime) positive integers. Let r_1 and r_2 be any two positive numbers less than m_1 and m_2, respectively. Then there exists a number X mod $m_1 m_2$, such that

$$X \textbf{ mod } m_1 = r_1 \quad \text{and} \quad X \textbf{ mod } m_2 = r_2 \,. \tag{1}$$

2 Solution

Proof: My proof will use Bézout's Identity. Let m_1 and m_2 be two relatively prime (coprime) positive numbers. Then there exists two integers a_1 and a_2, such that

$$a_1 m_1 + a_2 m_2 = 1 \,. \tag{2}$$

The use of this equation here seems reasonable for two reasons: 1) It is a relation between our two given coprime numbers, and 2) it establishes the existence of numbers and our problem also needs to establish the existence of a number. The similarities are too compelling to ignore!

So, how do we use Equation (2)? Our approach is to use the *method of undetermined coefficients* in the hope that X can be found as a linear combination of m_1 and m_2. We take c and d as our undetermined coefficients, getting

$$X \equiv c m_1 + d m_2 \textbf{ mod } m_1 m_2 \,. \tag{3}$$

We try to solve for c and d by use of the two constraint equations we have on X found in (1). To that end we get

$$r_1 \equiv d m_2 \textbf{ mod } m_1 \quad \text{and} \quad r_2 \equiv c m_1 \textbf{ mod } m_2 \,. \tag{4}$$

Now, multiply the first by a_2 and the second by a_1, to get

$$a_2 r_1 \equiv d a_2 m_2 \textbf{ mod } m_1 \quad \text{and} \quad a_1 r_2 \equiv c a_1 m_1 \textbf{ mod } m_2 \,. \tag{5}$$

Then substitute from (2) into both of these to get

$$a_2 r_1 = d(1 - a_1 m_1) \textbf{ mod } m_1 \quad \text{and} \quad a_1 r_2 = c(1 - a_2 m_2) \textbf{ mod } m_2 \,, \tag{6}$$

which simplifies to

$$a_2 r_1 \equiv d \textbf{ mod } m_1 \quad \text{and} \quad a_1 r_2 \equiv c \textbf{ mod } m_2 \,. \tag{7}$$

Solving for c and d and then substituting into (3), we have

$$X \equiv a_1 r_2 m_1 + a_2 r_1 m_2 \ \mathbf{mod}\, m_1 m_2 \,, \tag{8}$$

which gives us the values of c and d in terms of r_1 and r_2, which are given, and in terms of and a_1 and a_2 which can be solved for by the Euclidean algorithm, but for our needs here, it is enough to know that these numbers exist. Taking the result modulo $m_1 m_2$ keeps the value of X both positive and as small as possible. And the proof is completed.