Math From Scratch Lesson 20: The Chinese Remainder Theorem

W. Blaine Dowler

January 2, 2012

Contents

1 Relatively Prime Numbers

A quick definition: two numbers n and m are considered *relatively prime* or *coprime* if they have no common prime factors. Thus, any two prime numbers are coprime. Similarly, $32 = 2^5$ and $729 = 3^6$ are coprime because they have no common prime factors. Their greatest common factor is 1.

2 Congruence Classes

A *congruence class* $[a]$, also known as an *equivalence class*, is the set of all integers x such that $x = a \, (mod \, n)$ for a specified n. Although it is a set, it is customary to use the symbol $[a]$ as though it is a variable when we really mean an element of the set $[a]$. In modular arithmetic, the final solutions to algebra will not depend upon which specific element of $[a]$ is being used, so the "lazy" notation is used without fear of ambiguity.

3 Algebraic Units

When we first examined modular arithmetic, we learned that some elements have inverses, but others do not. In particular, all non-zero elements of $\mathbb{Z}_3$ had inverses, but several elements of $\mathbb{Z}_6$ did not. Before moving forward, we need to determine the conditions under which an element will have an inverse for a given modulus n.

Let us assume that $m < n$ and the greatest common factor of m and n is $\gcd(m, n) = g$.[1] If m has an inverse d in $\mathbb{Z}_n$, then there is some value of k for which

$$md = kn + 1$$

We will now show that this implies $\gcd(m, n) = g = 1$ any time m has such an inverse.

If $\gcd(m, n) = g$, then $m = lg$ and $n = jg$ for some l, n. Thus,

$$\begin{aligned} md &= kn + 1 \\ lgd &= kjg + 1 \\ (ld - kj)\, g &= 1 \end{aligned}$$

These steps were performed in $\mathbb{Z}$, not in $\mathbb{Z}_n$. Thus, the only possible solution to the equations is that $ld - kj = 1$ and $g = 1$. Thus, if m has an inverse in $\mathbb{Z}_n$, then $\gcd(m, n) = 1$ is required. If m has an inverse in $\mathbb{Z}_n$, then m is a *unit* of $\mathbb{Z}_n$. If n is prime, then every element of in $\mathbb{Z}_n$ is a unit.

4 Chinese Remainder Theorem

The Chinese Remainder Theorem was named for the culture that discovered the theorem centuries before anyone else. It was first published by Sun Tzu, better known for publishing *The Art of War*.

Theorem 4.1 *The Chinese Remainder Theorem states that, given coprime in-*

[1] The greatest common factor g of m and n is the largest number such that $m = k \cdot g$ and $n = l \cdot g$ for some values of k and l.

tegers n_1, n_2, n_3, ..., n_k then the system

$$\begin{aligned} x &\equiv a_1 \,(mod\ n_1) \\ x &\equiv a_2 \,(mod\ n_2) \\ x &\equiv a_3 \,(mod\ n_3) \\ &\vdots \\ x &\equiv a_k \,(mod\ n_k) \end{aligned}$$

has a solution, which is unique up to modulo $N = n_1 \cdot n_2 \cdot n_3 \cdot \ldots \cdot n_k$.

To prove the theorem we need to prove both the existence and the uniqueness of the solution x.

We start by proving the existence by constructing such a solution. Let $c_i = \frac{N}{n_i}$. As our moduli n_i are all prime, we know that all c_i are units modulo n_i, so that there exist numbers y such that $yc_i = 1 \,(mod\ n_i)$.

If $d = \gcd(a, n)$, then $ax \equiv b \,(modn)$ has a solution if and only if d divides b. This is a proof identical to that used for diophantine equations in the last lesson. This amounts to saying that $ax = kn + b$ for some k, so that $ax - kn = b$. As $\gcd(a, n) = d$, the left hand side is divisible by d, so the right hand side (b) is also divisible by d. Thus, in our example with $\gcd(c_i, n_i) = 1$, we can guarantee that $d_i c_i = 1 \,(mod\ n_i)$ for some d_i.

Knowing this, we can construct a solution x_0 as follows:

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + \ldots + a_k c_k d_k$$

When taken $mod\ n_i$, we find that $a_i c_i d_i = a_i$ by construction, while $a_j c_j d_j = 0$ for any $i \neq j$, as c_j will be a multiple of n_i. Thus, this is a general solution to our system of linear equations. We now need to prove that this is unique.

Let x be an arbitrary solution to the system. Then we know that $x \equiv a_i \equiv x_0 \,(mod\ n_i)$ for all i. Therefore, $x - x_0 \equiv 0 \,(mod\ n_i)$, showing that $x - x_0$ is divisible by n_i. Notice that the subscript i appears only on the n_i, which means every n_i divides into $x - x_0$. Since the numbers n_i are coprime, then $x - x_0$ is divisible by N, proving that this set of solutions is unique.[2]

[2] A set of solutions is unique if every solution is a part of that set. It is not required that there is only one solution.

4.1 A Concrete Example

This is fairly abstract, so we'll use a concrete example. We will be examining statements such as $x \equiv a_i \, (mod \; n_j)$ in these examples. We then choose prime numbers for the different possible values of n_j, such that $n_1 = 2$, $n_2 = 3$, $n_3 = 5$, and $n_4 = 7$. Let us reproduce one of the earliest applications of the theorem. Imagine you have an assembly of x soldiers in the Chinese army, and you do not know what x is. You ask all soldiers to pair off and count the remainder of 1. You then ask them to get into groups of 3 and have 2 remainder, and so forth. When grouped in fives, there is again one soldier left over.

We can use the Chinese Remainder Theorem to determine what the value of x is. Here is what we know:

$$\begin{aligned} x &= 1 \, (mod \; 2) \\ x &= 2 \, (mod \; 3) \\ x &= 1 \, (mod \; 5) \\ x &= 3 \, (mod \; 7) \end{aligned}$$

We can use the Chinese Remainder Theorem to start calculating x. The answer will not be unique amongst all integers, but we can quickly narrow down the options. Let us assume that the space our soldiers are in cannot hold more than 200 soldiers at a time.

We can use "brute force" to solve the problem, by listing all numbers between 1 and 200 which satisfy the first condition, then all such numbers satisfying the second condition, and so forth, and then cross referencing our lists to determine what the solution is. The Chinese Remainder Theorem effectively allows us to turn all of these conditions into a single solution, which can then be reduced to the correct modulus.

We have taken four arrangements of soldiers because the result is only unique up to modulus $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ and $2 \cdot 3 \cdot 5 \cdot 7 = 210$ is the smallest combination that is greater than the 200 soldier limit to the field. (Taking the first three gives a solution unique modulo 30, which isn't enough to guarantee the exact solution.)

First, we find our values of d_i. We find values such that $c_i d_i \equiv 1 \, (mod \; n_i)$. For the first condition, we find that $105d_1 \equiv 1 \, (mod \; 2)$. The simplest number that satisfies this condition is $d_1 = 1$. Similarly, $70d_2 \equiv 1 \, (mod \; 3)$ can be solved with $d_2 = 1$. The next condition is more challenging: $42d_3 \equiv 1 \, (mod \; 5)$ can be solved by first applying modular multiplication rules to turn it into $2d_3 \equiv 1 \, (mod \; 5)$. If $d_3 = 3$, then the condition is satisfied. The fourth and final condition is $30d_4 \equiv 1 \, (mod \; 7)$, or $2d_4 \equiv 8 \, (mod \; 7)$, which can be easily solved

by $d_4 = 4$.

Now we have our values of a_i (given in the problem), c_i (computed by multiplying all of the moduli together except n_i) and d_i (found in the previous paragraph.) We can substitute this into our general solution and get

$$x_0 = a_1c_1d_1+a_2c_2d_2+a_3c_3d_3+a_4c_4d_4 = (1)(105)(1)+(2)(70)(1)+(1)(42)(3)+(3)(30)(4) = 731$$

This is one possible solution. We can find our particular solution as $731 \equiv 101 \, (mod \; 210)$, or 101. There are 101 soldiers.

5 Next

We will next define and manipulate Euler's totient function. That function is one of the core pieces in RSA encryption.