Modular Arithmetic: The Missing Parts

Ajay Ramesh

January 28th, 2017

1 Introduction

This guide is meant to serve as a supplement to Note 6 of CS70. It provides full proofs of statements made throughout the note, which I did not understand at first glance. If you stumbled upon this document by accident, may it provide you with a better intuition of certain properties of modular arithmetic.

2 Proofs

Theorem 2.1 $a \equiv_n b \Leftrightarrow n \mid (a - b)$

$$\begin{aligned} a &= nk + r, 0 \leq r < n, k \in \mathbb{Z} \\ b &= nj + r, 0 \leq r < n, j \in \mathbb{Z} \end{aligned}$$

Both a and b can be expressed as a multiple of n with the same remainder r, since they are congruent under $mod\, n$

$$\begin{aligned} a - b &= (nk + r) - (nj + r) \\ &= nk + r - nj - r \\ &= nk - nj \\ &= n(k - j) \Leftrightarrow n \mid (a - b) \end{aligned}$$

Since $k, j \in \mathbb{Z}$, $k - j \in \mathbb{Z}$, therefore $n \mid (a - b)$

Theorem 2.2 $a \equiv_n b, c \equiv_n d \Leftrightarrow a + c \equiv_n b + d$

$$\begin{aligned}
a &= nk + r_1, 0 \leq r_1 < n, k \in \mathbb{Z} \\
b &= nj + r_1, 0 \leq r_1 < n, j \in \mathbb{Z} \\
c &= nq + r_2, 0 \leq r_2 < n, q \in \mathbb{Z} \\
d &= nz + r_2, 0 \leq r_2 < n, z \in \mathbb{Z}
\end{aligned}$$

We are representing the congruences the same way as **2.1** only with the added c and d.

$$\begin{aligned}
a + c &= (nk + r_1) + (nq + r_2) \\
b + d &= (nj + r_1) + (nz + r_2) \\
[(nk + r_1) + (nq + r_2)] &- [(nj + r_1) + (nz + r_2)] \\
(a + c) - (b + d) &= n(k + q - j - z) \\
n \mid (a + c) - (b + d) &\Leftrightarrow (a + c) \equiv_n (b + d)
\end{aligned}$$

Theorem 2.3 $a \equiv_n b, c \equiv_n d \Leftrightarrow n \mid ac \equiv_n bd$

Proved the same way as **2.2**, but with multiplication instead of addition.

Theorem 2.4 x has a multiplicative inverse $mod\, n$ iff $gcd(n, x) = 1$

We need to find $x^{-1} = a\,(mod\, n)$ for $xa \equiv 1\,(mod\, n)$, and for a to exist, $gcd(x, n) = 1$, let's see why. Recall **2.1** where we can say that $n \mid (xa - 1)$. We can use this fact to prove the above theorem.

$$\begin{aligned}
n &\mid (xa - 1) \\
xa - 1 &= nk, k \in \mathbb{Z} \\
xa &= nk + 1 \\
xa - nk &= 1 \\
\text{Let } gcd(n, x) &= c \\
c \mid (xa - nk) &= 1 \\
c &\mid 1 \\
c &= 1
\end{aligned}$$

If $gcd(n, x) = c \neq 1$ then $x^{-1} = a$ cannot exist.

Theorem 2.4.1 Mod multiplicative inverses are required for division in mod space. Let's take the following scenario as an example.

$$\text{Solve for } k \text{ in } xk \equiv_n p$$

In integer division we would divide both sides by x to isolate k. Why do we do this? Dividing both sides by x is the same as multiplying both sides by its multiplicative inverse so that the left side results in $x(x^{-1})k \equiv_n p(x^{-1})$. In integer division, the LHS would become k since $x(x^{-1}) = 1$. However, this is illegal in mod space. Instead of finding the integer multiplicative inverse like we do in integer division, we instead find the modular multiplicative inverse x^{-1} using Euclid's algorithm. In other words we are finding $a = x^{-1}$ for $xa \equiv_n 1$

Theorem 2.5 If a mod inverse exists, it is unique.

Let $xa_1 \equiv_n 1$ and $xa_2 \equiv_n 1$. We want to show that $a_1 \equiv_n a_2$

$$\begin{aligned} xa_1 \equiv_n xa_2 &\equiv_n 1 \\ n \mid (xa_1 - xa_2) \\ n \mid x(a_1 - a_2) \end{aligned}$$

In order for the last statement above to be true, $n \mid x$ or $n \mid (a_1 - a_2)$. We proved that $gcd(n, x) = 1$ if a_i exists in **2.4**. This means that $n \mid x$ is not possible. Why? $n \mid x \Leftrightarrow x = nk, k \in \mathbb{Z}$. If $gcd(n, x) = 1$ then $\frac{x}{n} \notin \mathbb{Z}$ which yields a contradiction. Therefore, $n \mid (a_1 - a_2)$ must be true. As seen in **2.1**, $n \mid (a_1 - a_2) \Leftrightarrow (a_1 \equiv_n a_2)$.