Understanding Modular Division

Overview

Recently, I reviewed some number theory topics to refresh my understanding of RSA encryption. While doing so, I came across a helpful explanation of modular division in the Stanford notes on Modular Arithmetic. This summary builds on that explanation and clarifies how division works in modular systems.

The Problem with Naive Division in Modular Arithmetic

Suppose y divides x as integers. One might assume we could divide both sides of a congruence as we do with real numbers. For example, consider the congruence:

$$10 \equiv 4 \pmod{6}$$

Dividing both sides by 2 seems to give:

$$5 \equiv 2 \pmod{6}$$

But this is clearly false, so the usual notion of division does not apply in modular arithmetic. We must instead redefine what it means to divide.

What Does Division Mean Modulo n?

Intuitively, division should *undo* multiplication. That is, to divide x by y means to find a number z such that:

$$y \cdot z \equiv x \pmod{n}$$

So, modular division becomes solving the congruence:

$$yz \equiv x \pmod{n}$$

In our earlier example:

$$2z \equiv 4 \pmod{6}$$

The question is: does this equation have a solution for z? And if so, how many solutions exist?

Conditions for Existence and Uniqueness

Let $\gcd(y, n) = d$. Then:

- If $d = 1$, there exists a **unique** solution $z \mod n$, given by:

  $$z \equiv y^{-1}x \pmod{n}$$

  where y^{-1} is the modular inverse of $y \mod n$.
- If $d > 1$, then:
  - No solution exists unless $d \mid x$.
  - If $d \mid x$, then there are exactly d distinct solutions modulo n.

Example

Consider the congruence:

$$2z \equiv 4 \pmod{6}$$

Here:

$$\gcd(2, 6) = 2 \quad \text{and} \quad 2 \mid 4$$

So, there are exactly two solutions. These are:

$$z \equiv 2 \pmod{6}, \quad z \equiv 5 \pmod{6}$$

Note: We did not immediately state the solutions as $z = 2$ and $z = 5$ because we wanted to emphasize that $z \in \mathbb{Z}_6$, meaning the solutions are considered modulo 6 and must lie within the range $0 \leq z \leq 5$.

Both satisfy the equation:

$$2 \cdot 2 = 4 \equiv 4 \pmod{6}, \quad 2 \cdot 5 = 10 \equiv 4 \pmod{6}$$

Therefore, in $\mathbb{Z}_6$, division by 2 is **not well-defined**, as it does not yield a unique result.

Conclusion

Modular division is only uniquely defined when the divisor y and the modulus n are coprime, i.e., $\gcd(y, n) = 1$. Otherwise, there may be multiple solutions or none at all, depending on whether $\gcd(y, n) \mid x$.

Proof of Uniqueness (for $\gcd(y, n) = 1$)

Before jumping into the proof, it is recommended to get familiar with the concept of Bezout's Identity.

Below is a line-by-line, fully self-contained proof of the uniqueness claim for linear Diophantine equations.

Theorem (Uniqueness Modulo the Coefficients)

Let $y, z, n, k, x \in \mathbb{Z}$ with $\gcd(y, n) = 1$, and consider the linear equation:

$$yz + nk = x \tag{1}$$

1. **(Existence)**: Equation (1) always has at least one integer solution.
2. **(Complete Description)**: If (z_0, k_0) is one solution, then every solution is given by:

$$z = z_0 + nt, \quad k = k_0 - yt, \quad \text{for some } t \in \mathbb{Z} \tag{2}$$

3. **(Uniqueness in Residue Classes)**: Among integers $0 \le z < n$, there is exactly one value satisfying (1); equivalently, the residue class $z \bmod n$ is unique. Dually, among $0 \le k < y$, the residue class $k \bmod y$ is also unique.

That is the precise sense in which "the solution is unique when $\gcd(y, n) = 1$."

1. Bézout-Based Particular Solution

Since $\gcd(y, n) = 1$, Bézout's identity guarantees the existence of integers $a, b \in \mathbb{Z}$ such that:

$$ay + bn = 1 \tag{3}$$

Multiplying both sides by x, we get a particular solution:

$$(z_0, k_0) := (ax,\, bx), \quad \text{since} \quad yz_0 + nk_0 = x \tag{4}$$

2. Homogeneous Form and Difference Equation

Let (z, k) be any solution of (1). Subtracting the particular solution (4) from (1), we obtain:

$$y(z - z_0) + n(k - k_0) = 0 \tag{5}$$

Define:

$$\Delta z := z - z_0, \quad \Delta k := k - k_0$$

So that:

$$y\,\Delta z = -n\,\Delta k \tag{6}$$

3. Key Lemma (Euclidean Lemma)

Lemma. If $\gcd(a,b)=1$ and $a \mid bc$, then $a \mid c$.

Proof. Bézout's identity gives $u,v\in\mathbb{Z}$ such that $au+bv=1$. Multiplying both sides by c gives:

$$auc+bvc=c$$

Since both terms on the left are divisible by a, so is the right-hand side: $a \mid c$.

4. Deriving the Parameter t

4.1 Show $n \mid \Delta z$: From equation (6), we know $n \mid y\,\Delta z$. Since $\gcd(y,n)=1$, the lemma implies:

$$\begin{aligned} n \mid \Delta z \quad &\Rightarrow \quad \Delta z = nt \text{ for some } t\in\mathbb{Z} \\ &\Rightarrow \quad z = z_0 + nt \end{aligned} \tag{7}$$

4.2 Determine Δk using the same t: Substitute equation (7) into equation (6):

$$y(nt) = -n\Delta k \quad\Rightarrow\quad \Delta k = -yt \quad\Rightarrow\quad k = k_0 - yt \tag{8}$$

Since every step was an equivalence, each integer t gives a valid solution, and distinct values of t give distinct ordered pairs. This proves the general form (2).

5. Uniqueness of the Residue Class

5.1 Uniqueness of $z \bmod n$: From (2), all solutions have the form $z \equiv z_0 \pmod{n}$. Conversely, any $z^* \equiv z_0 \pmod{n}$ implies $z^* = z_0 + nt$ for a unique t, and setting $k^* = k_0 - yt$ gives a valid solution.

5.2 Uniqueness of $k \bmod y$: Similarly, all solutions have $k \equiv k_0 \pmod{y}$. Any $k^* \equiv k_0 \pmod{y}$ implies $k^* = k_0 - yt$, leading to $z^* = z_0 + nt$. Thus, each residue class modulo y corresponds to exactly one solution.

6. Summary of the Proof

1. Existence of a solution follows from Bézout's identity.
2. All solutions are of the form given in equation (2).
3. The mapping $t \mapsto (z,k)$ defines a bijection $\mathbb{Z} \to \{\text{solutions}\}$.
4. Fixing $z \bmod n$ or $k \bmod y$ uniquely determines t, and therefore the entire solution.

7. Numerical Example

Solve the equation:

$$5z + 7k = 3$$

- A particular solution: $5(-4) + 7(3) = 1 \Rightarrow$ Multiply both sides by 3:

$$(z_0, k_0) = (-12, 9)$$

- General solution:

$$z = -12 + 7t, \quad k = 9 - 5t$$

- Reduce to residues:

$$z \equiv 2 \pmod{7} \quad \text{is unique}, \quad k \equiv 4 \pmod{5} \quad \text{is unique}$$

Choosing the representative $0 \leq z < 7$ forces $t = 2$, which gives:

$$z = 2, \quad k = -1$$

Final Remark

"Uniqueness" in Diophantine equations with coprime coefficients refers to uniqueness in residue classes. The coprimality condition is what enables us to cancel terms and express both variables in terms of a shared parameter t—this is the heart of the uniqueness argument.

Proof of Non-Uniqueness (for $\gcd(y, n) > 1$)

We now prove the general linear Diophantine equation

$$yz + nk = x, \quad \text{with } y, n, x \in \mathbb{Z}$$

does not yield a unique solution modulo n when $\gcd(y, n) > 1$.

1. What We Aim to Prove

Let

$$d = \gcd(y, n), \quad \text{where } d > 1.$$

Then:

1. **Necessity:** If an integer solution (z, k) exists, then $d \mid x$.
2. **Sufficiency and Parameterization:** If $d \mid x$, then:
   - A particular solution (z_0, k_0) exists.
   - All solutions are given by:

$$z = z_0 + \frac{n}{d}t, \quad k = k_0 - \frac{y}{d}t, \quad t \in \mathbb{Z}.$$

2. Why $d \mid x$ is Necessary

Since d divides both y and n, it divides every linear combination of them:

$$x = yz + nk \quad \Rightarrow \quad d \mid x.$$

Thus, if $d \nmid x$, no solution exists. For the remainder of this proof, we assume $d \mid x$.

3. Factoring Out the Common Divisor

Write:

$$y = d\bar{y}, \quad n = d\bar{n}, \quad x = d\bar{x}$$

with $\bar{y}, \bar{n}, \bar{x} \in \mathbb{Z}$. Then:

$$\gcd(\bar{y}, \bar{n}) = 1.$$

This reduces the equation to:

$$\bar{y}z + \bar{n}k = \bar{x}. \tag{$\star$}$$

4. A Bézout-Based Particular Solution

By Bézout's identity, there exist $a, b \in \mathbb{Z}$ such that:

$$\bar{y}a + \bar{n}b = 1.$$

Multiplying both sides by $\bar{x}$, we get a particular solution:

$$z_0 = \bar{x}a, \quad k_0 = \bar{x}b.$$

5. General Solution

Let (z, k) be any solution to $\star$. Then:

$$\bar{y}(z - z_0) + \bar{n}(k - k_0) = 0 \quad \Rightarrow \quad \bar{y}(z - z_0) = -\bar{n}(k - k_0).$$

Since $\gcd(\bar{y}, \bar{n}) = 1$, it follows:

$$\bar{y} \mid (k - k_0) \Rightarrow k = k_0 + \bar{y}t$$

for some $t \in \mathbb{Z}$. Substituting:

$$z = z_0 - \bar{n}t.$$

Thus, the full solution set is:

$$z = z_0 - \bar{n}t, \quad k = k_0 + \bar{y}t, \quad t \in \mathbb{Z}.$$

or, substituting back:

$$z = z_0 + \frac{n}{d}t, \quad k = k_0 - \frac{y}{d}t.$$

6. Example: Failure of Uniqueness Modulo n

Let:

$$y = 4, \quad n = 6 \Rightarrow \gcd(4, 6) = 2.$$

Choose $x = 2$, which is divisible by $d = 2$, so solutions exist.

Divide the equation by d:

$$2z + 3k = 1. \tag{1}$$

Particular Solution: Using extended Euclidean algorithm:

$$3(1) + 2(-1) = 1 \Rightarrow z_0 = -1, \quad k_0 = 1.$$

General Solution:

$$z = -1 + 3t, \quad k = 1 - 2t.$$

Return to the original equation:

$$z = -1 + 3t \Rightarrow \text{valid for } 4z + 6k = 2.$$

Compute some z values:

t	$z = -1 + 3t$	$z \mod 6$
0	-1	5
1	2	2
2	5	5
3	8	2

Observation: - $z = -1$ and $z = 5$ are both $\equiv 5 \pmod 6$ - $z = 2$ and $z = 8$ are both $\equiv 2 \pmod 6$

So we find **multiple solutions with the same residue modulo 6** — demonstrating that modular uniqueness fails.

7. Why Did This Happen?

In the general form:

$$z = z_0 + \frac{n}{d}t$$

the step size is $\frac{n}{d}$, so: - $z \bmod n$ only cycles through a subset of residue classes. - In this case, only 3 out of the 6 residues appear.

Final Insight. *If $d = 1$ (that is, $\frac{n}{d} = n$), then the additive term in the general solution is nt, which is always congruent to 0 modulo n. Consequently, every solution satisfies $z \equiv z_0 \pmod n$, ensuring uniqueness in that residue class.*

Conclusion: - Modular uniqueness **fails** when $\gcd(y,n) > 1$. - There are exactly d solutions that are congruent modulo n. - Only when $\gcd(y,n) = 1$, we recover the guarantee that:

$$z \equiv z_0 \pmod{n} \quad \text{(uniqueness mod } n\text{)}$$