Introduction to Modular Arithmetic

Mason Rogers

Brief warning for the CS fans: In computer science classes, 'mod' is an operation that takes in two inputs a and b and spits out the remainder of a after dividing by b. For instance, in CS speak, $27\%5 = 2$ and $33\%9 = 6$. This may guide your intuition for what we will soon call reducing a modulo b, but it is not a firm notion of modular arithmetic. Among other things, it fails because $a\%n + b\%n$ is in general not equal to $(a+b)\%n$, so that definition *does not play nicely* with arithmetic operations.

And on with the show: Several examples we have seen have involved working with remainders of integers after dividing by some fixed integer n. For instance, we proved that the sum of two perfect squares cannot leave remainder 3 when divided by 4, which we in turn used to prove that the only integer solution to $x^2 + y^2 = 3z^2$ is $(x, y, z) = (0, 0, 0)$. Another example arose in the exercise about the existence of sexy prime quintuplets, where we saw an intuitive argument for why (5,11,17,23,29) should be the only one. Modular arithmetic gives us a framework for handling these types of questions efficiently.

The essential idea is that if we only care about the remainders numbers leave after dividing by n, any two numbers that leave the same remainder after dividing by n behave the same under addition, subtraction, and multiplication; we don't have to worry about the bookkeeping. As an everyday example, when it is 11AM on Tuesday and our math 79SI homework is due at 3PM, we know that we have $3 + 12 - 11 = 4$ hours left to finish, not $3 - 11 = -8$. Implicitly, we add back in a multiple of 12 to bring the time interval back into the sensible range. As a more mathematical motivating example, if we want to know what remainder $4797 \cdot 1963$ will leave after dividing by 5, we can say that immediately that it will be 1 without doing any multiplication beyond $2 \cdot 3 = 6$.

We will introduce modular arithmetic with a few exercises. You may use the following result given by the long division algorithm:

Proposition. For any $n \in \mathbb{N}$ and any $x \in \mathbb{Z}$, we can write $x = qn + r$ uniquely for some $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$.

Definition. We define x and y to be congruent modulo n and write $x \equiv y \mod n$ if $n \mid (x-y)$.

Definition. We define the *residue class* of x modulo n to be the set $[x] = \{y \in \mathbb{Z} : x \equiv y \mod n\}$.

1. Intuitively, we want each residue class to consist of all the integers which leave a particular remainder after dividing by n. First, we need to show that congruence modulo n cuts $\mathbb{Z}$ up into disjoint classes in such a way that every integer belongs to exactly one residue class. To avoid getting bogged down in set theory, we assert that it suffices to prove that the following properties hold. Prove that 'congruence modulo n' satisfies:

(a) Reflexivity: $x \equiv x \mod n$ for all $x \in \mathbb{Z}$.

(b) Symmetry: $x \equiv y \mod n$ if and only if $y \equiv x \mod n$ for all $x, y \in \mathbb{Z}$.

(c) Transitivity: If $x \equiv y \mod n$ and $y \equiv z \mod n$, then $x \equiv z \mod n$.

You must use the definition of congruence modulo n to have a correct proof.

2. Now we have split $\mathbb{Z}$ up into disjoint residue classes $[r]$, where we may treat $[r]$ like a general number of form $qn + r$. We want to be able to perform the usual arithmetic operations on residue classes, which absorb the 'bookkeeping' of the non-remainder part of each integer. We thus may want to define

$$[x] + [y] = [x + y], \quad [x] - [y] = [x - y], \quad [x][y] = [xy],$$

but there is a slight possible issue with these definitions. They each depend on *choices* of x and y as representatives of their residue classes. We need to show that these operations are *well-defined* in the sense that they do not depend on our choice of $x \in [x]$ or $y \in [y]$. To do this, let $x \equiv a \mod n$ and $y \equiv b \mod n$, and prove:

(a) Addition is well-defined: $x + y \equiv a + b \mod n$.

(b) Subtraction is well-defined: $x - y \equiv a - b \mod n$.

(c) Multiplication is well-defined: $xy \equiv ab \mod n$.

3. We now know that we can perform the usual arithmetic operations on residue classes without worrying about our choice of representatives. It thus makes sense to choose the easiest representative with which to work. Do the following computations as quickly as possible, without any extraneous bookkeeping:

(a) $[4][8] \mod 5$

(b) $[1234] + [12345] \mod 10$

(c) $[6913112352][14235913451] \mod 50$

(d) $[32123] - [12321] \mod 3$

4. Let's use modular arithmetic (and a little bit of mathematical induction which we'll introduce on the fly) to prove a Fermat's little theorem, which states that for any prime p and any $a \in \mathbb{N}$, $a^p \equiv a \mod p$.

(a) Prove using the formula for binomial coefficients that $p \mid \binom{p}{k}$ for $k \in \{1, 2, \ldots, p-1\}$. Thus, $\binom{p}{k} \equiv 0 \mod p$ for all such k.

(b) Prove using the binomial theorem that for any $a \in \mathbb{Z}$, $(a+1)^p \equiv a^p + 1 \mod p$. Thus, if $a^p \equiv a \mod p$, we see that $(a+1)^p \equiv a+1 \mod p$. (This is our 'inductive step', where we prove that if Fermat's little theorem holds for a, it holds for $a+1$ too.)

(c) Observe that $1^p \equiv 1 \mod p$. (This is known as our base case.) Explain intuitively how this observation and the previous part of this problem allow you to conclude the theorem. (This is called mathematical induction, which we will introduce formally week 5.)

5. In exercise 1.1.5, we looked at an argument that there could be no sexy prime quintuplet that can be reinterpreted in terms of modular arithmetic. The argument had a flaw, which is that it assumed that divisibility by 5 is sufficient to prove that a natural number is composite (think about 5 itself), but the idea is almost correct. Formalize that argument with modular arithmetic to prove that (5,11,17,23,29) is the only sexy prime quintuplet.

6. Prove that for all $a \in \mathbb{Z}$, exactly one of $a, a+2, a+4$ is a multiple of 3. Why isn't it also true that exactly one of $a, a+2, a+4, a+6$ is a multiple of 4?

Congratulations! You now have a handle on modular arithmetic.

Bonus note for the CS fans: To tie this back to your intuition from CS, it may seem like we have shown that if $x\%n = a\%n$ and $y\%n = b\%n$, then $(x+y)\%n = (a+b)\%n$, $(x-y)\%n = (a-b)\%n$, and $(xy)\%n = (ab)\%n$. But we've actually done better. It is not true that $(x+y)\%n = x\%n + y\%n$ and so on, but we've shown that it *is* true that those expressions are congruent modulo n. We have thus shown that you can reduce modulo n before doing arithmetic, after doing arithmetic, or both, and your answer will be the same, *up to adding multiples of* n. Thus, you never have to work with numbers larger than $(n-1)^2$.