Euclidean Division

Andy Chong Sam

August 14, 2022

1 Remainder Quotient Formula

When performing integer divisions we can document a quotient (q) and a remainder (r). In this document we will use the following notation to denote each:

$$a/b = q$$
$$a \mod b = r$$

Given a dividend a, and a divisor b that results in a quotient q and a remainder r, we can derive the following expression:

$$a = bq + r \tag{1}$$

Consider a simple integer division of 25 divided by 11. Since $25/11 = 2$ and $25 \mod 11 = 3$, all pieces of the operation can be encapsulated as: $25 = (11)(2) + 3$. Expression (1) can be used to demonstrate various properties in modular arithmetic.

2 Modular Arithmetic

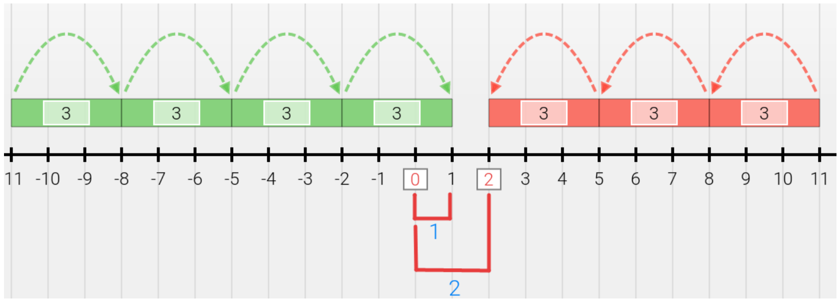
2.1 Overview

A straightforward interpretation of the modulo operation (mod) is that its output is the remainder of the division between two integers. A cyclical pattern is observed by varying x in $x \mod s$, when s is left constant.

For $x \mod 1$, the set of all possible outcomes is {0}.
For $x \mod 2$, the set of all possible outcomes is {0,1}.
For $x \mod 5$, the set of all possible outcomes is {0,1,2,3,4}.

2.2 Negative Dividends

When the dividend is a negative number, the results are less intuitive. For example, $11 \mod 3 = 2$. We have the following result when we use -11 instead: $-11 \mod 3 = 1$. One way to visualize this outcome is by imagining a number line with an emphasis on the range of mod 3, which would be $\{0, 1, 2\}$



In the case of $-11 \mod 3$ we can see that there are 4 skips needed to enter the modulo range. The distance between where the last skip lands and 0 is the modulo. In this case, this distance is 1.

In the case of $11 \mod 3$ we can see that there are 3 skips needed to enter the modulo range. The distance between where the last skip lands and 0 is the modulo. In this case, this distance is 2.

For the operation $a \mod b$ and if a is negative, then we can calculate the modulo using the following expression:

$$a + |\lfloor \frac{a}{b} \rfloor|(b) + b \tag{2}$$

2.3 Modular Addition

The property of modular addition is as follows:

$$(a + b) \mod c = (a \mod c + b \mod c) \mod c \tag{3}$$

This relationship can be derived by using expression (1). As a sidenote, recall that if a is divisible by c, and b is divisible by c, then a+b is divisible by c. We first start by restating a + b:

$$\begin{aligned}
a = cq_1 + r_1 \therefore a \mod c = r_1 \\
b = cq_2 + r_2 \therefore b \mod c = r_2 \\
a + b = (cq_1 + r_1 + cq_2 + r_2) \\
a + b = c(q_1 + q_2) + r_1 + r_2
\end{aligned}$$

Plugging the above result back into $a + b) \mod c$ we get:

$$(c(q_1 + q_2) + r_1 + r_2) \mod c$$

We can apply the following rule to simplify the above expression. If I have an operation $a \mod b$, then I know that adding a multiple of b (say kb), will result in the same modulo value: $(a + kb) \mod b = a \mod b$. We can now proceed with the following simplification:

$$\begin{aligned}
(c(q_1 + q_2) + r_1 + r_2) \mod c \\
= (r_1 + r_2) \mod c
\end{aligned}$$

On to the right hand side of expression (3), using:

$$\begin{aligned}
a = cq_1 + r_1 \therefore a \mod c = r_1 \\
b = cq_2 + r_2 \therefore b \mod c = r_2
\end{aligned}$$

So the right hand side becomes $(r_1 + r_2) \mod c$ as well.

2.4 Modular Multiplication

The property of modular multiplication is as follows:

$$(ab) \mod c = ((a \mod c)\ (b \mod c)) \mod c \tag{4}$$

This can be derived in a way similar like we did with modular addition. The left hand side can be rewritten like so:

$$\begin{aligned} &((cq_1 + r_1)(cq_2 + r_2)) \mod c \\ &= (c^2 q_1 q_2 + cq_1 r_2 + cq_2 r_1 + r_1 r_2) \mod c \\ &= (c(cq_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2) \mod c \end{aligned}$$

Since $c(cq_1 q_2 + q_1 r_2 + q_2 r_1)$ is a multiple of c, we are left with:

$$(r_1 r_2) \mod c$$

On to the right hand side of expression (4), using:

$$\begin{aligned} a = cq_1 + r_1 \therefore a \mod c = r_1 \\ b = cq_2 + r_2 \therefore b \mod c = r_2 \end{aligned}$$

We see that the right hand side of expression (4) becomes:

$$(r_1 r_2) \mod c$$

2.5 Modular Exponentiation

Modular exponentiation takes the form of evaluation a problem like $a^x \mod b$. The challenge here is that a^x could easily become a very large number, causing errors on calculators. A commonly used technique to overcome this problem is known as "fast modular exponentiation" and it involves restating x using base-2. Suppose we are trying to evaluate $7^{15} \mod 17$. The first step is to translate the exponent into base-2. The number 15 thus becomes $(1111)_2$. We can expand this base-2 number with each term representing the binary symbol {0,1} times 2 raised to the power of the place value it appears in:

$$15 = (1)(2)^3 + (1)(2)^2 + (1)(2)^1 + (1)(2)^0$$

With this expansion in mind, we can restate the original problem like so:

$$\begin{aligned} &7^{15} \mod 17 \\ &= (7^{(1)2^3+(1)2^2+(1)2^1+(1)2^0}) \mod 17 \\ &= (7^{8+4+2+1}) \mod 17 \end{aligned}$$

Finally, we can apply the algebraic rule of exponents along with modular multiplication:

$$\begin{aligned} &(7^{8+4+2+1}) \mod 17 \\ &= ((7^8 \mod 17)\ (7^4 \mod 17)\ (7^2 \mod 17)\ (7^1 \mod 17)) \mod 17 \end{aligned}$$

We have now broken the problem into individual components, thus making calculations easier and reducing the likelikhood of overflow errors.