Modular Arithmetic

Problem. What is the remainder of

$$17 \times (12 \times 19 + 5) – 23$$

when divided by 3?

To actually perform all of the calculations in this expression would take some time. Can we avoid this? It turns out that we can. But before we do this, we need to study the remainders a bit more.

Definition. We say that two numbers a and b are congruent modulo m if they have the same remainder when divided by m. We denote this by

$$a \equiv b \bmod m.$$

As we discussed above, numbers a and b have the same remainder when divided by m iff $a - b$ is divisible by m. Thus, we can say that

$$a \equiv b \bmod m \setminus \ \Leftrightarrow \setminus \ m \mid a - b.$$

In other words, a number a is congruent modulo m to all numbers $a + km$ for integer k. In particular, if r is the remainder of a when divided by m, then $a \equiv r \bmod m$.

Congruence relation has some nice and convenience properties.

Lemma. If $a \equiv b \bmod m$ then $a + c \equiv b + c \bmod m$ for any c.

In other words, we can add any integer to both sides of a relation.

The proof of this lemma is simple: $a \equiv b \bmod m$ means that $m \mid a - b$. Since $a - b = (a + c) - (b + c)$ we have $m \mid (a + c) - (b + c)$ and $a + c \equiv b + c \bmod m$.

The previous lemma generalizes as following.

Lemma. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $a + c \equiv b + d \bmod m$.

In other words, not only can we add the same number to both sides of the congruence, but we can add different, but congruent numbers. That is, we can add two congruence relations to each other.

The proof of this lemma can be written in one line:

$$a + c \equiv a + d \equiv b + d \bmod m.$$

Here we use the previous lemma twice. On the first step, we added the same number a to both sides of the congruence $c \equiv d \bmod m$ and on the second step, we added the same number d to both sides of the congruence $a \equiv b \bmod m$.

From another perspective, these two properties mean that we can substitute numbers in the sums by their congruents without changing the remainder of the sum. Using this basic property we can already show the idea of how we can simplify modular calculations.

Problem. What is the remainder of

$$14 + 41 + 20 + 13 + 29$$

when divided by 4?

Instead of computing the whole sum above and dividing by 4 with a remainder, we can apply the results we obtained. Each of the numbers in the sum is congruent to its remainder:

$$14 \equiv 2 \bmod 4,\ 41 \equiv 1 \bmod 4,\ 20 \equiv 0 \bmod 4,\ 13 \equiv 1 \bmod 4,\ 29 \equiv 1 \bmod 4.$$

Using our properties we can substitute each number by its remainder in the congruence and compute the remainder of the sum much easier:

$$14 + 41 + 20 + 13 + 29 \equiv 2 + 1 + 0 + 1 + 1 \equiv 5 \equiv 1 \bmod 4.$$

Thus the remainder of the sum is 1 when divided by 4.

It turns out that similar properties are true for multiplication as well.

Lemma. If $a \equiv b \bmod m$ then $a \times c \equiv b \times c \bmod m$ for any c.

In other words, we can multiply a congruence relation by an integer.

The proof is similar: congruence of a and b modulo m means that $m \mid (a - b)$ and then $m \mid (a - b)c$, which means that ac and bc are congruent as well.

Again, we can generalize the previous lemma.

Lemma. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $a \times c \equiv b \times d \bmod m$.

In other words, we can multiply two congruence relations by each other.

The proof is almost the same as for addition:

$$ac \equiv ad \equiv bd \bmod m.$$

Here, on the first step, we multiplied both sides of the congruence $c \equiv d \bmod m$ by the same number a and on the second step, we multiplied both sides of the congruence $a \equiv b \bmod m$ by the same number d.

Another perspective on these properties is that we can substitute numbers in the products by their congruents without changing the remainder of the product.

Now we are ready to solve the problem that asked us to calculate the remainder of

$$17 \times (12 \times 19 + 5) – 23$$

when divided by 3.

To compute the remainder, we can substitute each number by their remainder when divided by 3. As we have seen, this change does not affect the remainders of the results of arithmetic operations. This gives us

$$17 \times (12 \times 19 + 5) - 23 \equiv 2 \times (0 \times 1 + 2) - 2 \equiv 2 \bmod 3.$$

This simplifies computation a lot. When it is needed to simplify the computation even further, the following idea might be useful: we do not have to substitute numbers in the arithmetic expression by their remainders, we can use any congruent numbers. For example, in case of computations modulo 3, instead of remainders $0, 1, 2$ we can use congruents $0, 1, -1$ respectively (note that $2 \equiv -1 \bmod 3$). This introduces negative numbers, but makes the absolute values of the numbers even smaller, simplifying computations further. With this approach, the solution of the problem looks as follows:

$$17 \times (12 \times 19 + 5) - 23 \equiv -1 \times (0 \times 1 - 1) + 1 \ \equiv 2 \bmod 3.$$

In programming, this is reflected as follows. Say, you want to compute the remainder modulo m of the product of a sequence of integers. The naive way of doing this is the following.

```
def product_modulo(lst, modulo):
    product = 1
    for element in lst:
        product = product * element

    return product % modulo
```

The right way to compute it is to take every intermediate result modulo m: the code below is faster and safer as it avoids working with potentially huge numbers.

```
def product_modulo(lst, modulo):
    product = 1
    for element in lst:
        product = (product * element) % modulo

    return product
```