Some rules for modulo arithmetic

Definition Let $m > 0$ be a positive integer called the *modulus*. We say that two integers a and b are congruent modulo m if $b - a$ is divisible by m. In other words,

$$a \equiv b(\mathrm{mod} m) \iff a - b = m \cdot k \text{ for some integer} k. \tag{1}$$

Inverses in Modular arithmetic

We have the following rules for modular arithmetic:

$$\textbf{Sum rule: } \text{IF } a \equiv b (\mathrm{mod}\ m) \text{ THEN } a + c \equiv b + c (\mathrm{mod}\ m). \tag{3}$$
$$\textbf{Multiplication Rule: } \text{IF } a \equiv b (\mathrm{mod}\ m) \text{ and if } c \equiv d (\mathrm{mod}\ m) \text{ THEN } ac \equiv bd (\mathrm{mod}\ m). \tag{4}$$

Definition An inverse to a modulo m is a integer b such that

$$ab \equiv 1 (\mathrm{mod}\ m). \tag{5}$$

Addition rule

In general, when $a, b, c,$ and d are integers and m is a positive integer such that

$$a \equiv c \pmod{m}$$
$$b \equiv d \pmod{m}$$

the following is always true:

$$a + b \equiv c + d \pmod{m}.$$

And as we did in the problem above, we can apply more pairs of equivalent integers to both sides, just repeating this simple principle.

Proof of the addition rule:

Let $a - c = m \cdot k$, and $b - d = m \cdot l$ for $l, k \in \mathbb{Z}$. Adding the two equations we get:

$$\begin{aligned} mk + ml &= (a - c) + (b - d) \\ m(k + l) &= (a + b) - (c + d) \end{aligned}$$

Which is equivalent to saying $a + b \equiv c + d \pmod{m}$

Subtraction

The same shortcut that works with addition of remainders works also with subtraction.

- Exponentiation: $a^e \equiv b^e \pmod{m}$ where e is a positive integer.

Final example We calculate the table of inverses modulo 26. First note that

$$26 = 13 \cdot 2$$

so that the only numbers that will have inverses are those which are rel. prime to 26...i.e. they contain no factors of 2 or 13:

$$1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.$$

Now we write some multiples of 26

$$26, 52, 78, 104, 130, 156, 182, 208, 234...$$

A number a has an inverse modulo 26 if there is a b such that

$$a \cdot b \equiv 1 (\text{mod } 26) \text{or } a \cdot b = 26 \cdot k + 1.$$

thus we are looking for numbers whose products are 1 more than a multiple of 26. We create the following table

Table 2: inverses modulo 26

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1} (MOD m)	1	9	21	15	3	19	7	23	11	5	17	25

Conditions for an inverse of a to exist modulo m

Definition Two numbers are relatively prime if their prime factorizations have no factors in common.

Theorem Let $m \geq 2$ be an integer and a a number in the range $1 \leq a \leq m - 1$ (i.e. a standard rep. of a number modulo m). Then a has a multiplicative inverse modulo m if a and m are relatively prime.