

CONGRUENCE AND MODULUS: PART 1

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

This document discusses (i) the modulo operation $\%$, and (ii) the congruence relation \equiv_m modulo a fixed number m . These two concepts are very closely related but are different: one is a function or operation, and the second is an equivalence relation. Be careful to keep these concepts distinct.

Definition 1 (The Modulo Operation). Let m be a positive integer, and let b be any integer. Then $b \% m$ is defined to be the remainder of b when divided by m . In other words, if $b = qm + r$ with $r, q \in \mathbb{Z}$ and if $0 \leq r < m$ then $b \% m = r$.

We call m the *modulus* and $b \% m$ the *residue of b modulo m* (but a lot of people just say that $b \% m$ is “ b modulo m ”). We call $\%$ the *modulo operation*, but perhaps a better name for it is *residue operation* since it produces the residue not the modulus. This operation is not popular with number theorists who tend to prefer using congruences \equiv (see below). But the symbol $\%$ is widely used in computer programming, and it is useful to have an operation $\%$ side by side with the traditional equivalence relation \equiv .

Example 1. $17 \% 5 = 2$. As another example, $-2 \% 5 = 3$ since $-2 = (-1)5 + 3$.

Example 2. If b is non-negative then $b \% 10$ is just the last digit of b (when written in base 10). For example, $78 = 7 \cdot 10 + 8$ so $78 \% 10 = 8$. Warning: $-12 \% 10$ is not ± 2 , it is 8.

Remark 1. The operation $\%$ allows us to write the quotient-remainder equation as follows:

$$b = qm + (b \% m).$$

Obviously $b \% m$ is always in the set $\{0, 1, \dots, m - 1\}$.

Divisibility is closely related to the modulus operation. In fact, $b \% m = 0$ if and only if $m \mid b$. To see this, write $b = qm + (b \% m)$ as above. If $b \% m = 0$ then $b = qm$ so $m \mid b$. Conversely, if $m \mid b$ then $b = qm + 0$ for some m ; in other words, the remainder is zero.

Example 3. If a is an integer then $a \% 2$ is either 0 or 1. Recall, an even integer a is one where $2 \mid a$, and an odd integer a is one where $2 \nmid a$. So, by the above remark, a is even if and only if $a \% 2 = 0$. Similarly, a is odd if and only if $a \% 2 = 1$.

Example 4. If a is an integer then $a \% 1 = 0$ since every integer is divisible by 1.

Example 5. Observe that if $0 \leq a < m$ then $a \% m = a$: the modulus operation does not change the given integer a . A consequence of this observation is the identity $(b \% m) \% m = b \% m$ that holds for all $b \in \mathbb{Z}$.

Definition 2 (Congruence). If m is a positive integer, and if $a, b \in \mathbb{Z}$, then $a \equiv b \pmod{m}$ means that $m \mid (a - b)$. We can write this also as $a \equiv b \pmod{m}$ or even $a \equiv_m b$. The relation \equiv_m is called the *congruence* relation.

Example 6. Since $98 - 60 = 38$ and $19 \mid 38$, it follows that $98 \equiv 60 \pmod{19}$. Since $15 - (-5) = 20$ and $4 \mid 20$ it follows that $15 \equiv -5 \pmod{4}$.

Example 7. We have $a \equiv a - m \pmod{m}$ since $m \mid (a - (a - m))$. For example,

$$39 \equiv 33 \equiv 27 \equiv 21 \equiv 15 \equiv 9 \equiv 3 \pmod{6}.$$

Many sources use Definition 2 above to define congruences, but other sources use an alternate definition:

Alternate Definition (Congruence). Let $a, b \in \mathbb{Z}$ and let m be a positive integer. Then $a \equiv b \pmod{m}$ means that $a \% m = b \% m$. In other words, $a \equiv b \pmod{m}$ means that a and b have the same remainder when divided by m .

Definition 2 and the above alternate definition turn out to be equivalent according to the following proposition. This means you can use whichever definition is most convenient for the situation. It is handy to know both.

Proposition. Let $a, b \in \mathbb{Z}$ and let m be a positive integer. Then $m \mid (a - b)$ if and only if $a \% m = b \% m$.

Proof. Suppose that $m \mid (a - b)$ holds. So $a - b = cm$ for some $c \in \mathbb{Z}$. Thus $a = b + cm$. Now, as above, the quotient-remainder formula applied to b divided by m gives us $b = qm + (b \% m)$. So $a = b + cm = (c + q)m + (b \% m)$. Since $0 \leq b \% m < m$ this implies that $b \% m$ is the remainder when a is divided by m . Thus $a \% m = b \% m$.

Conversely, suppose that $a \% m = b \% m$. So the remainders agree (but the quotients may not): $a = qm + r$ and $b = q'm + r$. Thus $a - b = (qm + r) - (q'm + r) = (q - q')m$. Thus $m \mid (a - b)$. \square

Here is a concise version:

Proof. Suppose $m \mid (a - b)$. Since $a - b = cm$ for some $c \in \mathbb{Z}$, we get $a = b + cm$. By the quotient-remainder formula, $b = qm + (b \% m)$ for some $q \in \mathbb{Z}$. Thus $a = b + cm = (c + q)m + (b \% m)$. So $a \% m = b \% m$.

Conversely, suppose $a \% m = b \% m$. So the quotient-remainder formulas are of the form $a = qm + r$ and $b = q'm + r$. Thus $a - b = (q - q')m$. So $m \mid (a - b)$. \square

Example 8. Since $17 \% 5 = 2$ and $22 \% 5 = 2$ it follows that $17 \equiv 22 \pmod{5}$.

Example 9. As above $b \% m = (b \% m) \% m$. Thus $b \equiv (b \% m) \pmod{m}$.

Example 10. A handy way to deal with negative numbers is as follows. If $a + b = m$ then $m \mid a - (-b)$, so $-b \equiv_m a$. For example, $-5 \equiv 12 \pmod{17}$ since $5 + 12 = 17$. Likewise $-1 \equiv 3 \pmod{4}$.

As mentioned above, congruence \equiv_m is an equivalence relation:

Proposition. Let m be a positive integer. Then \equiv_m is an equivalence relation.

I will just give the concise version of the proof. You must be able to fill in the details.

Proof.

(Refl.) The identity $a \equiv_m a$ follows from $a \% m = a \% m$.

(Symm.) If $a \equiv_m b$ then $a \% m = b \% m$. Equality is symmetric, so $b \% m = a \% m$. Thus $b \equiv_m a$.

(Trans.) If $a \equiv_m b$ and $b \equiv_m c$, then $a \% m = b \% m$ and $b \% m = c \% m$. Thus $a \% m = c \% m$. So $a \equiv_m c$. \square

Remark 2. Since congruence is an equivalence relation on \mathbb{Z} , it partitions \mathbb{Z} into equivalence classes (this is a fact that you should remember from your set theory course). For example, \equiv_4 partitions \mathbb{Z} into the following four equivalence classes:

$$\begin{aligned} [0] &= \{\dots, -8, -4, 0, 4, 8, 12, \dots\} \\ [1] &= \{\dots, -7, -3, 1, 5, 9, 13, \dots\} \\ [2] &= \{\dots, -6, -2, 2, 6, 10, 14, \dots\} \\ [3] &= \{\dots, -5, -1, 3, 7, 11, 15, \dots\} \end{aligned}$$

As is typical in for a partition by equivalence classes, (i) the set \mathbb{Z} is the union of these four equivalence classes, (ii) these equivalence classes are disjoint, and (iii) two integers a and b are in the same equivalence class if and only if $a \equiv b \pmod{4}$.

Example 11. If today is Wednesday, what day of the week will it be in 47 days? Solution: observe that $47 \equiv -2 \pmod{7}$. This holds since $7 \mid (47 + 2)$. Thus advancing 47 days is the same as regressing two days. So the day will be Monday.

Example 12. It is now 7 AM. What time will it be in 100 hours? Solution: observe that $100 \% 24 = 4$ since $100 = 4 \cdot 24 + 4$. In other words, $100 \equiv 4 \pmod{24}$. Add four hours to 7 AM, so it will be 11 AM.

Historical Notes. Gauss introduced congruences and moduli into number theory in 1801.

The word *modulus* (plural *moduli*) is a Latin word meaning *measure* or *unit of measure*. So in number theory the modulus is the unit of measure that we use in congruences. More precisely, we measure according to a cycle of length equal to a given modulus. For example, clock-time is measured with a cycle of length 12; so the modulus here is 12. Days of the week are measured with a modulus of 7. The word *modulo* is a variant¹ of *modulus* meaning roughly *when measured with*. (The English word *module* comes from the Latin word *modulus*).

In everyday English, the word *residue* means “the small amount left over after the main part has been removed or used up”. This word comes from the Latin word² *residuum* “that which remains”.

The word *congruent* comes from a Latin word³ meaning “agreeing, corresponding”. In geometry, where it was used before it was used in number theory, it means that when one figure is superimposed on another they exactly coincide. In number theory it means that two numbers agree according to some modulus. For example, “17 is congruent to 2 modulo 5” means that 17 and 2 agree when measured with a cycle of length (or “modulus”) 5.

DR. WAYNE AITKEN, CAL. STATE, SAN MARCOS, CA 92096, USA
E-mail address: waitken@csusm.edu

¹In Latin, *modulo* is the ablative case of *modulus*.

²The Latin *residuum* is from the past participle of the Latin verb *resideo* “to remain”. Our words *reside* and *resident* also come from this Latin verb.

³*congruent-*, the present participle stem of the Latin verb *congruere* “meet together, agree, correspond”