Modular Arithmetic

$m \mid (a-b)$ here uses divisibility on integer.

1. Definition: For integers a, b, and $m > 1$, we say $a \equiv b \pmod m$ whenever $m \mid (a-b)$

1) $a \equiv b \pmod m$: a is congruent to b modulo m.

2). m is called modulus.

3). $a \equiv b \pmod m \iff a - b = m \cdot k$. $k \in \mathbb{Z}$.

equivalence relationship

① reflexive. $a \equiv a \pmod m$.

② symmetry. $a \equiv b \pmod m \iff b \equiv a \pmod m$ (prove if $m \mid n$ then $m \mid -n$).

③ transitivity: $a \equiv b \pmod m \wedge b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$.

2. Theorem.

1) 3.1.2: If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

Let $a \equiv b \pmod m$. Let $b \equiv c \pmod m$.

WTP: $a \equiv c \pmod m$

Since $a \equiv b \pmod m$, gives $m \mid (a-b)$. $\exists k_1 \in \mathbb{Z}$, $mk_1 = a-b$.

Since $b \equiv c \pmod m$, gives $m \mid (b-c)$. $\exists k_2 \in \mathbb{Z}$, $mk_2 = b-c$.

by linear combination of divisibility, gives.

$m \mid [a-b] + [b-c] \Rightarrow m \mid (a-c)$, which.

$a \equiv c \pmod m$. ■

2) 3.1.3. When a, b are non-negative integers, the relationship $a \equiv b \pmod m$ is equivalent to a and b leaving equal remainders upon division by m.

By quotient-remainder formula.

$\exists q_1, q_2 \in \mathbb{Z}$, $\exists r_1, r_2 \in \mathbb{Z}$, $r_1, r_2 \in \{0, 1, 2, \ldots, m-1\}$, s.t.

$a = m \cdot q_1 + r_1$; $b = m \cdot q_2 + r_2$.

Assume for contradiction $r_1 \neq r_2$.

Since $m \mid (a-b)$. $\exists k \in \mathbb{Z}$, $km = a - b = m(q_1 - q_2) + (r_1 - r_2)$.

Since $r_1 \neq r_2$, gives $r_1 - r_2 \neq 0$, $\Rightarrow m \nmid (a-b)$. contradicts ∎

Q-R formula

3). 3.1.4. For a given modulus m, each integer is congruent to exactly one of the numbers in the set $\{0, 1, 2, \dots, m-1\}$.

4). 3.1.5. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

① $(a+c) \equiv (b+d) \pmod m$. $(a+c)-(b+d) = m \cdot k$.

② $ac \equiv bd \pmod m$. $ac - bd = m \cdot k$.

Let $a \equiv b \pmod m$, $m \mid (a-b)$. $\exists k_1 \in \mathbb{Z}$. $k_1 m = a-b$.

Let $c \equiv d \pmod m$, $m \mid (c-d)$. $\exists k_2 \in \mathbb{Z}$. $k_2 m = c-d$.

① $(a-b) + (c-d) = k_1 m + k_2 m$.

$\Rightarrow (a+c) - (b+d) = m \cdot (k_1 + k_2)$. Since $k_1 + k_2 \in \mathbb{Z}$, take $k' = k_1 + k_2$.

$\Rightarrow (a+c) - (b+d) = m \cdot k$. $\Rightarrow m \mid (a+c) - (b+d) \Rightarrow (a+c) \equiv (b+d) \pmod m$

② $a = b + k_1 m$; $c = d + k_2 m$.

$a \cdot c - b \cdot d = (b + k_1 m)(d + k_2 m) - b \cdot d$

$= bd + bk_2 m + k_1 md + k_1 k_2 m^2 - bd$.

$= bk_2 m + dk_1 m + k_1 k_2 m^2$

$= m(bk_2 + dk_1 + k_1 k_2 m)$.

$\Rightarrow m \mid ac - bd \Rightarrow ac \equiv bd \pmod m$. ∎

5). 3.1.6. If $a \equiv b \pmod m$, then, for $\forall n \in \mathbb{N}$, $a^n \equiv b^n \pmod m$.

Let $a \equiv b \pmod m$.

Given Statement to prove: $\forall n \in \mathbb{N}$. $P(n)$, i.e. $a^n \equiv b^n \pmod m$.

$S = \{n \in \mathbb{N} \mid P(n)\}$.

Base Case: $n = 1$.

$a^n \equiv b^n \pmod m$. $\Rightarrow a \equiv b \pmod m$ is assumed.

live prove. B.C. is T.

Induction Step: Let $n \in \mathbb{N}$. $n \geq 1$.

Induction Hypothesis. Assume $P(n)$.

WTS: $P(n+1)$.

Since $P(n)$ is True. $a^n \equiv b^n \pmod m$.

Take $n=1$. $P(1)$ is True in B.C. $a \equiv b \pmod m$.

from theorem of modular. $a^n \cdot a \equiv b^n \cdot b \pmod m$. gives.

$a^{n+1} \equiv b^{n+1} \pmod m$. $, (n+1) \in S$.

I've shown. Induction Step is T. ∎

6).3.2.1: Every natural number is congruent to the sum of its digit modulo 9. In particular natural number is divisible by 9 iff the sum of its digit is divisible by 9.

Let $n = a_k \cdots a_2 a_1 a_0 = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k$.

Let $m = a_0 + a_1 + a_2 + \cdots + a_k$.

WTS. $n = m \pmod 9$. By 3.1.3. it's equivalent to say $9 \mid m \iff 9 \mid n$

Since. $10 \equiv 1 \pmod 9$, gives $\forall k \in \mathbb{N}. \ 10^k \equiv 1^k \pmod 9 \Rightarrow 10^k \equiv 1 \pmod 9$

From theorem 3.1.5. gives $a_0 + 10 a_1 \equiv a_0 + a_1 \pmod 9$.

Similarly, gives. $a_0 + 10 a_1 + 100 a_2 + \cdots + 10^k a_k \equiv a_0 + a_1 + a_2 + \cdots + a_k \pmod 9$.

$\Rightarrow n \equiv m \pmod 9$.