§3 Congruences.

§3.1 Definition and Basic Properties.

Definition: Let $m \in \mathbb{Z}^+$ ("<u>the modulus</u>")

We say that <u>a is congruent to b modulo m</u> if

$$m \mid b-a.$$

or $\quad b = a + km$ for some $k \in \mathbb{Z}$

or $\quad a$ and b have the same residues (remainders) modulo m.

$$(a = qm + r, \ b = q'm + r).$$

~~Example: m=6~~

Notation: $a \equiv b \pmod{m}$

Example: $m = 6$

$$4 \equiv 10 \equiv -2 \equiv 64 \equiv 6010 \pmod{6}.$$

Basic properties: $\forall a, b, c \in \mathbb{Z}, m \in \mathbb{Z}^+$ we have

1a) $a \equiv a \pmod{m}$

$(m \mid a - a = 0).$

1b) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$

$(m \mid b-a \implies m \mid -(b-a) = a-b)$

(c) If $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$ (Ex).

These properties mean that the congruence is an equivalence relation.

"Everyday" example: days of week

$\left.\begin{array}{l}\text{August } a\text{'th} \\ \text{August } b\text{'th}\end{array}\right\}$ the same day of week

$\iff a \equiv b \pmod{7}$.

Observation: $365 \equiv 1 \pmod{7}$. Therefore your birthday goes one weekday forwards from year ~~to~~ year (not on leap years).

Definition. Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$. The <u>congruence class of a mod m</u> is the set of integers which are congruent to a modulo m.

There are always m congruence classes.

Example: $m=5$. Congruence classes are

$$\{\dots,-15,-10,-5,0,5,10,15,\dots\}$$
$$\{\dots,-14,-9,-4,1,6,11,16,\dots\}$$
$$\{\dots,-13,-8,-3,2,7,12,17,\dots\}$$
$$\{\dots,-12,-7,-2,3,8,13,18,\dots\}$$
$$\{\dots,-11,-6,-1,4,9,14,19,\dots\}$$

§3.2. Modular arithmetics.

Proposition. Let $m \in \mathbb{Z}^+$. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then

(a) $a+b \equiv a'+b' \pmod{m}$

(b) $ab \equiv a'b' \pmod{m}$

Proof. We have $a = a' + u\cdot m$
$$b = b' + v\cdot m$$

(a) $$a+b = a'+um+b'+vm = a'+b'+(u+v)\cdot m$$
$\Rightarrow a+b \equiv a'+b' \pmod{m}$.

(b) $$a\cdot b = (a'+um)(b'+vm) = a'b' + a'vm + ub'm + uvm^2 = a'b' + (a'v+ub'+uvm)\cdot m$$
$\Rightarrow ab \equiv a'b' \pmod{m}$ $\boxtimes$

Example: $m=7$.

$$2068 \cdot 2988 \equiv (-32) \cdot 188 \equiv 3 \cdot 48 \equiv 3 \cdot 6 \equiv 4 \pmod 7$$

Q: Can we cancel in congruences?

A: Not always.

Example: $7 \cdot 8 \equiv 1 \cdot 8 \pmod{12}$

But $7 \not\equiv 1 \pmod{12}$.

Proposition. Let $m \in \mathbb{Z}^+$, $a, b, c \in \mathbb{Z}$ and $\gcd(c, m) = 1$. Then $ac \equiv bc \pmod m$ implies $a \equiv b \pmod m$

Proof. By EEA, $1 = s \cdot c + t \cdot m$ for some integer s, t.

$\Rightarrow 1 \equiv s \cdot c \pmod m$

$$ac \equiv bc \pmod m \Rightarrow a\underbrace{cs}_{\overset{\text{|||}}{1}} \equiv b\underbrace{cs}_{\overset{\text{|||}}{1}} \pmod m$$

$\Rightarrow a \equiv b \pmod m$. $\boxtimes$

Remark: The number s from the proof is called <u>an inverse of c mod m</u>.

Notation: $s \equiv c^{-1} \pmod m$

or $s \equiv \frac{1}{c} \pmod m$

Example: $3^{-1} \equiv 5 \pmod 7$
$5^{-1} \equiv 3 \pmod 7$

How to find inverses mod m?
(1) Guess (if numbers are small)
(2) Use E.E.A. for c and m.

Application of congruences:

Proposition: (a) A number is divisible by 9 $\Leftrightarrow$ the sum of its digits is divisible by 9.

(b) A number is divisible by 11 $\Leftrightarrow$ the alternative sum of its digits is divisible by 11.

(12345 not divisible by 9, since $9 \nmid 1+2+3+4+5$
not divisible by 11, since $11 \nmid 1-2+3-4+5$)

Proof (a). $a_0 + 10 \cdot a_1 + 100 \cdot a_2 + \ldots + 10^n a_n = m$
where $a_0, a_1, \ldots, a_n$ are digits of m

$1 \equiv 1 \pmod 9$
$10 \equiv 1 \pmod 9$
$10^2 \equiv 1^2 \pmod 9$
$\ldots$
$10^n \equiv 1^n \pmod 9$

Therefore $m \equiv a_0 + a_1 + a_2 + \dots + a_n \pmod 9$

1b) $\longrightarrow$ Ex. $\boxtimes$