

# A (mod n) Congruence Theorem and its Corollary.

NOTATION NOTE: A string of congruences can be written on one line with the "(mod n)" congruence-type designation at the end of the line.

For example: The statement:

" $77 \equiv 59 \equiv 35 \equiv 5 \pmod{6}$ " is true and is read as "77 is congruent to 59, which is congruent to 35, which is congruent to 5, all with (mod 6) congruence."

Theorem: For every positive integer  $n$  and for every integer  $a$ ,  
 $a \equiv (a+n) \pmod{n}$  and  $a \equiv (a-n) \pmod{n}$ .

Proof: Let  $n$  be any positive integer and let  $a$  be any integer. Then,  $a - (a+n) = a - a - n = -n = n \times (-1)$ .

$$\therefore a - (a+n) = n \times (-1).$$

$\therefore a \equiv (a+n) \pmod{n}$ , by definition of (mod n)-congruence.

Also,  $a - (a-n) = a - a + n = n = n \times 1$ ;  $\therefore a - (a-n) = n \times 1$ .

$\therefore a \equiv (a-n) \pmod{n}$ , by definition of (mod n)-congruence.

$\therefore$  For every positive integer  $n$  and for every integer  $a$ ,

$a \equiv (a+n) \pmod{n}$  and  $a \equiv (a-n) \pmod{n}$ , by Direct Proof.

Q.E.D.

Corollary: For every positive integer  $n$  and for every integer  $a$ ,  $a \equiv (a+4n) \pmod{n}$ .

Proof: let  $n$  be any positive integer  $n$  and let  $a$  be any integer.

By multiple applications of the Theorem above,

$$a \equiv (a+n) \equiv (a+2n) \equiv (a+3n) \equiv (a+4n) \pmod{n}.$$

$\therefore a \equiv (a+4n) \pmod{n}$ , by the transitive property of  $\pmod{n}$  congruence.

Therefore, for every positive integer  $n$  and for

every integer  $a$ ,  $a \equiv (a+4n) \pmod{n}$ ,  
by Direct Proof.

QED

Corollary: For every positive integer  $n$  and for any two integers  $a$  and  $k$ ,

$$a \equiv (a+kn) \pmod{n}.$$

Proof: The proof is left as an exercise. ■