2022-09-29

$$S = \{x \in \mathbb{Z} : x+1 \mid x-3\}$$

$\ominus$ (1) $x+1 \mid x-3 = c$

$\oplus$ (2) $x+1 \mid x+1 = b$

$$\left.\begin{array}{l} a \mid b \\ a \mid c \end{array}\right.$$

$\therefore$ (3) $x+1 \mid 4$ $\quad b-c \quad$ $a \mid b \pm c$

$$\mathrm{Div}(4) = \{\text{divisors of } 4\}$$

$$= \{\pm 1, \pm 2, \pm 4\}$$

$(2) \wedge (1) \Longrightarrow (3)$

$(2) \wedge (3) \Longrightarrow (1)$

$(2) = T$

always true

$$(1) \Longleftrightarrow (3)$$

$$\therefore \quad S = \{x : x+1 \mid 4\}$$

$$\Longleftrightarrow \quad x+1 \in \{\pm 1, \pm 2, \pm 4\} =$$

$$= \{-4, -2, -1, 1, 2, 4\}$$

$$\boxed{S = \{-5, -3, -2, 0, 1, 3\}}$$

HW 2.1 $\left.\begin{matrix} a \mid b \\ a \mid c \end{matrix}\right\} \Rightarrow a \mid b \pm c$

highlight property of arithmetic used

HW 2.2 $S = \{a : (\forall x)(a \mid x)\}$

HW 2.3 $T = \{b : (\forall y)(y \mid b)\}$

find S, T

prove correctness of your answer

Note: to prove that two sets, A and B, are equal, you need to show

$A \subseteq B$

and

$B \subseteq A$

(two separate proofs)

Be always clear, which part you are proving, what are your current assumptions and desired conclusion

Congruence

Oct 2 Oct 23

Same day of the week?

* YES b/c $7 \mid 23-2$

DEF a is CONGRUENT to b modulo m $\qquad a \equiv b \pmod{m}$

if $m \mid a-b$

---

* YES b/c $23 \equiv 2 \pmod 7$ CALENDAR ARITHMETIC

Congruence mod m is transitive:

thm $(\forall a,b,c)$ $\left.\begin{cases} a \equiv b \ (m) \\ b \equiv c \ (m) \end{cases}\right\} \Rightarrow a \equiv c \ (m)$

$\boxed{\text{DO}}$ Congruence mod m is reflexive:

$$(\forall a)\big(a \equiv a \ (m)\big)$$

$\boxed{\text{DO}}$ Congruence mod m is symmetric:

$$(\forall a, b)\Big(a \equiv b\ (m) \implies b \equiv a \ (m)\Big)$$

What properties of divisibility are we using in proving these?

Thm Congruence mod m is transitive:

$$(\forall a, b, c)\left(\begin{matrix} a \equiv b \ (m) \\ b \equiv c \ (m) \end{matrix}\right\} \implies a \equiv c \ (m)\Big)$$

conceptual hierarchy

Day 2	congruences
Day 1	divisibility
Day 0	arithmetic

Proof

Assumptions

$a \equiv b \ (m)$

$b \equiv c \ (m)$

Desired conclusion

$a \equiv c \ (m)$

TRANSLATION

$m \mid a-b \qquad (1)$

$m \mid b-c \qquad (2)$

$\overset{?}{\Rightarrow} m \mid a-c \qquad (3)$

$$(1) \wedge (2) \overset{?}{\Rightarrow} (3)$$

$$\underset{m\backslash}{(a-b)} + \underset{m\backslash}{(b-c)} \xRightarrow[2.1]{} \underset{m\backslash}{a-c}$$

We used addition property of divisibility

Quod erat demonstrandum

Q.E.D.

$m \mid a-b$

notation

$m \backslash a-b$

(if m does not fit on same line

$$(*)\quad \begin{cases} a \equiv b & (m) \\ c \equiv d & (m) \end{cases}$$

$$a \pm c \equiv b \pm d \quad (m)$$

meaning

$$a + c \equiv b + d \quad (m)$$
$$a - c \equiv b - d \quad (m)$$

HW 2.4

Prove;
State ~~property~~ of divisibility used

HW 2.5

$$a \equiv b \ (m) \Longrightarrow ax \equiv bx \ (m)$$

HW 2.6 $\quad (*) \Longrightarrow ac \equiv bd \ (m)$

What properties of congruences can we use to prove this?

(Do not use properties of basic arithmetic or properties of divisibility

HW 2.7 $\left.\begin{array}{l} a \equiv b \ (m) \\ k \geq 1 \end{array}\right\} \Rightarrow a^k \equiv b^k \ (m)$

Prove it by induction using only properties of congr.

FERMAT's Little Theorem

FLT If p is a prime number and $p \nmid a$ then $a^{p-1} \equiv 1 \ (p)$.

multiplication is <u>easy</u>

factoring is believed
to be <u>hard</u> (computationally)

this + $\boxed{\text{FLT}}$

are the basis of
the <u>RSA</u> crypto system

foundation of
$\boxed{\text{public-key cryptography}}$

---> e-commerce

"SNEAKERS" movie ← recommended

p prime

If $p \nmid a$ then $a^{p-1} \equiv 1 \ (p)$

Small cases:

$p=2 \quad 2 \nmid a \Rightarrow a \equiv 1 \ (2)$ ✓

$p=3 \quad 3 \nmid a \Rightarrow a^2 \equiv 1 \ (3)$

Proof

Lemma $(\forall x)(x \equiv 0, 1 \text{ or } -1 \bmod 3)$

$\therefore \quad x^2 \equiv 0^2 = 0$ —— then $3 \mid x^2 \therefore 3 \mid x$

or $(\pm 1)^2 = 1 \quad \bmod 3$ ✓

THM (prime property)

If p is a prime number and

$p \mid ab \Rightarrow p \mid a \vee p \mid b$

FALSE e.g. for $p = 6$

Counterexamples: $a = 4 \quad b = 9$

$a = 2 \quad b = 3$

BONUS 2.8

prove FLT for $p=5$