Modular Arithmetic

Wednesday, March 11, 2026 11:18 AM

Recall: Divisibility

On Quiz 3

Ex #718 on 3/9

+B # 728, 32, 21, 31, 33, 9

+B # 806, 814, 808

1] Exer: longest chain

Reem	Ragad
hypto. syl	MP
MP	MT
Univ Inst	hypto syl
Simplification	addition
MT	conj.
Conj.	Disj syl
addition	Resol.
Univ Gen	Simplification

+B#728, 32, 21, 31, 33, 9

Exer. longest chain

Khadija	Abeer	Fatima	Reem
PM.	MP.	MP	Ext Gen
Simp.	MT	Simp.	Ext Inst.
MT	Add	Add	Univ MP
Add	hypo-S.	MT	Univ MT
Simp L	Simpl.	Conj	Univ Inst
conjunction	Res.	hypo. sym.	Univ Gen
	dist syl		

+B # 806, 814, 808

2] Division Algorithm

Def^{n}. Let $a, b \in \mathbb{Z}^{+}$, Then, $\exists!\ q, r$ s.t.

$$a = bq + r \quad ; \quad 0 \leq r < b$$

quotient ↑ ↖ remainder (mod)

e.g.

div 100 by 23 :	$100 = \underline{4} \cdot 23 + \underline{8}$	$100 \bmod 23 = 8$
div -12 by 7 :	$-12 = \underline{-2} \cdot 7 + \underline{2}$	$-12 \bmod 7 = 2$

div 30 by 17 :	$30 = \underline{1} \cdot 17 + \underline{13}$	$30 \bmod 17 = 13$
div -24 by 5 :	$-24 = \underline{-5} \cdot 5 + \underline{1}$	$-24 \bmod 5 = 1$
div -2 by 7 :	$-2 = \underline{-1} \cdot 7 + 5$	$-2 \bmod 7 = 5$

3] Modular Arithmetic (§4.1)

Def^{n}. $a, b, m \in \mathbb{Z}$, $m > 0$

a is congruent to b modulo m if $m \mid (a-b)$

Notation:

$a \equiv b \pmod m$ denotes congruent

$a \not\equiv b \pmod m$ denotes not congruent

4] e.g.

$13 \equiv 28 \pmod 5$ Since $5 \mid (13-28)$

$37 \not\equiv 23 \pmod{10}$ Since $10 \nmid (14)$

$37 \equiv 2 \pmod 5$ Since $5 \mid (37-2)$

5] Thrm:

if $a \equiv b \pmod m \iff a \bmod m = b \bmod m$

$\iff \exists k \in \mathbb{Z},\ a = b + k \cdot m$

6] Thrm: if $a \equiv b \pmod m$

$c \equiv d \pmod m$

Then $a \pm c \equiv b \pm d \pmod m$

and $a \cdot c \equiv b \cdot d \pmod m$

e.g. $127 \times 389 \pmod 5$

$\equiv 2 \times 4$

$\equiv 8 \equiv 3 \pmod 5$

e.g. $1434 \times 2116 \pmod 7$

$\equiv (1400 + 35 - 1) \cdot (2100 + 14 + 2)$

$\equiv (-1)(2)$

$\equiv -2$

$\equiv 5 \pmod 7$
