Proposition 46 *Let* m *be a positive integer. For all natural numbers* k *and* l*,*

$$k \equiv l \pmod{m} \iff \mathrm{rem}(k, m) = \mathrm{rem}(l, m) \quad .$$

PROOF: Let m a positive integer; k and l natural numbers.

($\Rightarrow$) Assume $k \equiv l \pmod{m}$ $\iff$ $k - l = i \cdot m$ for some integer i

By div. alg. $k = q \cdot m + r \quad 0 \leq r < m$

$l = q' \cdot m + r' \quad 0 \leq r' < m$

$$\Rightarrow \underbrace{k - l}_{\substack{\| \\ i \cdot m}} = (q - q') \cdot m + (r - r')$$

Say wlog $r \geq r'$,

We have

$$i \cdot m + 0 = (q - q') \cdot m + (r - r')$$

$$0 \leq r - r' < m$$

$$\Rightarrow \quad i = q - q'$$

$$\wedge \quad 0 = r - r' \Rightarrow r = r'$$

by uniqueness of quotients and remainders

$(\Leftarrow)$ Exercise.

$\boxtimes$

Corollary 47 *Let m be a positive integer.*

1. *For every natural number n,*

$$n \equiv \operatorname{rem}(n, m) \pmod{m} .$$

Iff

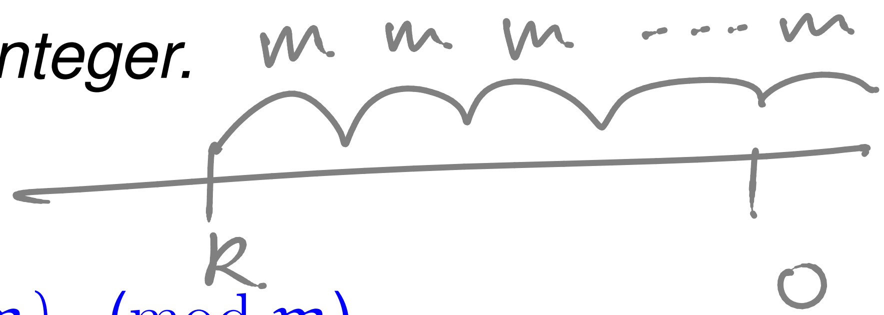
$$\underline{\operatorname{rem}}(n,m) = \underline{\operatorname{rem}}(\underline{\operatorname{rem}}(n,m), m)$$

PROOF:

<u>Exercise</u>

(use the uniqueness property of remainders).

Corollary 47 *Let m be a positive integer.*



1. *For every natural number n,*

$$\mathrm{n} \equiv \mathrm{rem}(\mathrm{n}, \mathrm{m}) \pmod{\mathrm{m}} .$$

2. *For every integer k there exists a unique integer $[\mathrm{k}]_{\mathrm{m}}$ such that*

$$0 \leq [\mathrm{k}]_{\mathrm{m}} < \mathrm{m} \quad \textit{and} \quad \mathrm{k} \equiv [\mathrm{k}]_{\mathrm{m}} \pmod{\mathrm{m}} .$$

PROOF: Let k be an integer. We proceed by cases.

Case 1: $k \geq 0$ Then take $[k]_m = \mathrm{rem}(k,m)$.

Case 2: $k < 0$

$$k \equiv k+m \equiv k+2m \equiv \cdots \equiv k+\ell m$$

Then $k \equiv k+(|k|+1)m \equiv \mathrm{rem}(k+(|k|+1)m, m) \stackrel{\text{def}}{=} [k]_m$

$\boxtimes$

Modular arithmetic

For every positive integer m, the *integers modulo* m are:

$$\mathbb{Z}_m \quad : \quad 0 \ , \quad 1 \ , \quad \ldots \ , \quad m-1 \ .$$

with arithmetic operations of addition $+_m$ and multiplication $\cdot_m$ defined as follows

$$\begin{aligned} k +_m l &= [k+l]_m &= \operatorname{rem}(k+l, m) \ , \\ k \cdot_m l &= [k \cdot l]_m &= \operatorname{rem}(k \cdot l, m) \end{aligned}$$

for all $0 \leq k, l < m$.

FACT:

NB:

$$(k +_m l) +_m p = k +_m (l +_m p)$$

$$\mathrm{rem}(\mathrm{rem}(k+l, m) + p, m) = \mathrm{rem}(k + \mathrm{rem}(l+p, m), m)$$

$$0 +_m p = p$$

Similarly for $\cdot_m$ with unit 1.

$3 \cdot_4 3 = 1$

3 is a multiplicative inverse of itself in $\mathbb{Z}_4$

Example 49 *The addition and multiplication tables for* $\mathbb{Z}_4$ *are:*

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Note that the addition table has a cyclic pattern, while there is no obvious pattern in the multiplication table.

2 does not have a multiplicative inverse.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	additive inverse
0	0
1	3
2	2
3	1

	multiplicative inverse
0	—
1	1
2	—
3	3

Interestingly, we have a non-trivial multiplicative inverse; namely, 3.

We have all multiplicative inverses.

Example 50 *The addition and multiplication tables for* $\mathbb{Z}_5$ *are:*

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Again, the addition table has a cyclic pattern, while this time the multiplication table restricted to non-zero elements has a permutation pattern.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	additive inverse
0	0
1	4
2	3
3	2
4	1

	multiplicative inverse
0	$-$
1	1
2	3
3	2
4	4

Surprisingly, every non-zero element has a multiplicative inverse.

Remark We know from FLT $i^{p-1} \equiv 1 \pmod{p}$ for $i \not\equiv 0 \pmod{p}$

$\Updownarrow$

$i \cdot (i^{p-2}) \equiv 1 \pmod{p}$

I.e. i^{p-2} is a multiplicative inverse of i

Proposition 51 *For all natural numbers* $m > 1$, *the modular-arithmetic structure*

$$(\mathbb{Z}_m, 0, +_m, 1, \cdot_m)$$

is a commutative ring.

NB Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses

.

Important mathematical jargon: Sets

Very roughly, sets are the mathematicians' data structures.
Informally, we will consider a *set* as a (well-defined, unordered) collection of mathematical objects, called the *elements* (or *members*) of the set.

Set membership

The symbol '$\in$' known as the *set membership* predicate is central to the theory of sets, and its purpose is to build statements of the form

$$x \in A$$

that are true whenever it is the case that the object x is an element of the set A, and false otherwise.

Defining sets

	of even primes		$\{2\}$
The set	of booleans	is	$\{\mathbf{true}, \mathbf{false}\}$
	$[-2..3]$		$\{-2, -1, 0, 1, 2, 3\}$

note that
$\{true, false\}$
$= \{false, true\}$.

NB

$$a \in \{x \in A \mid P(x)\} \iff [(a \in A) \wedge P(a)]$$

Set comprehension

The basic idea behind set comprehension is to define a set by means of a property that precisely characterises all the elements of the set.

Notations:

$$\{ x \in A \mid P(x) \} \quad , \qquad \{ x \in A : P(x) \}$$

Greatest common divisor

Given a natural number n, the set of its *divisors* is defined by set comprehension as follows

$$D(n) = \{ d \in \mathbb{N} : d \mid n \} \quad .$$

Example 53

1. $D(0) = \mathbb{N}$

2. $D(1224) = \left\{ \begin{array}{c} 1, 2, 3, 4, 6, 8, 9, 12, 17, 18, 24, 34, 36, 51, 68, \\ 72, 102, 136, 153, 204, 306, 408, 612, 1224 \end{array} \right\}$

Remark Sets of divisors are hard to compute. However, the computation of the greatest divisor is straightforward. :)

Going a step further, what about the *common divisors* of pairs of natural numbers? That is, the set

$$\mathrm{CD}(m, n) = \{\, d \in \mathbb{N} : d \mid m \wedge d \mid n \,\}$$

for $m, n \in \mathbb{N}$.

Example 54

$$\mathrm{CD}(1224, 660) = \{\, 1, 2, 3, 4, 6, 12 \,\}$$

Since $\mathrm{CD}(n, n) = \mathrm{D}(n)$, the computation of common divisors is as hard as that of divisors. But, what about the computation of the *greatest common divisor*?

Lemma 56 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $\mathrm{m} \equiv \mathrm{m}' \pmod{\mathrm{n}}$*. Then,*

$$\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{CD}(\mathrm{m}', \mathrm{n}) \ .$$

PROOF: Let m, m' be nat. and n pos. int.

Assume $m \equiv m' \pmod{n}$

RTP: $CD(m,n) = CD(m',n)$

$$\iff \left[\forall d.\ \left(d \mid m \wedge d \mid n\right) \iff \left(d \mid m' \wedge d \mid n\right)\right]$$

Assume $m \equiv m' \pmod{n} \iff m - m' = i \cdot n$ for some int i

Let d be arbitrary

$(d \mid m \wedge d \mid n) \Rightarrow (d \mid m' \wedge d \mid n)$

Assume $d \mid m$ and $d \mid n$

RTP: $d \mid m'$

$\iff d \mid m - in$

By Lemma

$d \mid a \wedge d \mid b \Rightarrow d \mid p \cdot a + q \cdot b$ we are done.

RTP: $d \mid n$

By assumption.

$$CD(m, n)$$

$$\|$$

$$CD(m_1, n)$$

$$\|$$

$$\underline{CD}(m_2, n)$$

$$\|$$

$$\underline{CD}(m_2, n_1)$$

$$\|$$

$$\ddots$$

$$m \equiv m_1 \pmod{n}$$

$$m_1 \equiv m_2 \pmod{n}$$

$$n_1 \equiv n \pmod{m_2}$$

$$\vdots$$