Corollary 47 *Let m be a positive integer.*

1. *For every natural number n,*

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

PROOF: Because

$$n = \underline{\mathrm{quo}}(n, m) \cdot m + \underline{\mathrm{rem}}(n,m)$$

$$0 \leq \mathrm{rem}(n,m) < m .$$

Corollary 47 *Let* m *be a positive integer.*

1. *For every natural number* n,

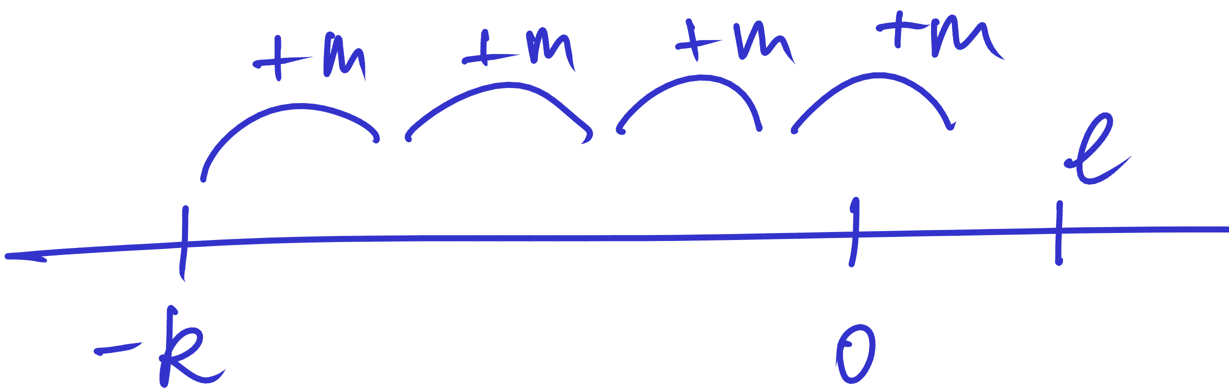
$$n \equiv \mathrm{rem}(n, m) \pmod{m} \quad .$$

2. *For every integer* k *there exists a unique integer* $[k]_m$ *such that*

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

PROOF: Because taking

$\ell = (k+1)\,m - k$



$-k \equiv \ell \equiv \underline{\mathrm{rem}}(\ell, m)$

Modular arithmetic

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

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

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 $0 \leq k, l < m$.

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.

3 is its own reciprocal in $\mathbb{Z}_4$

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.

FLT: For p prime, $i \not\equiv 0 \pmod p$

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

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.

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 .

Proposition. Let m be a positive integer. A modular integer x in $\mathbb{Z}_m$ has a reciprocal iff there exist integers i and j such that $x \cdot i + m \cdot j = 1$.

PROOF: Let m be a pos. int. and x in $\mathbb{Z}_m$.

$(\Rightarrow)$ Suppose x has a reciprocal. That is, there is some z in $\mathbb{Z}_m$ such that $x \cdot z \equiv 1 \pmod{m}$. Equivalently, $x \cdot z - 1 = m \cdot k$ for some int k. and we are done.

$(\Leftarrow)$ Assume $x \cdot i + mj = 1$ for some ints i and j. Let $z = [i]_m$. Then, RTP: $x \cdot z \equiv 1 \pmod{m}$ ... Exercise $\boxtimes$

Integer Linear Combinations

Definition. An integer ℓ is said to be an integer linear combination of two integers a and b whenever there are integers i and j such that $\ell = i \cdot a + j \cdot b$.

Proposition. Let m be a positive integer. A modular integer x in $\mathbb{Z}_m$ has a reciprocal iff 1 is an integer linear combination of m and x.

Lemma. Let a, b, c be integers.

$(c \mid a \wedge c \mid b) \iff c$ divides every integer linear combination of a and b.

PROOF Let a, b, c ints.

$(\Rightarrow)$ Assume $c \mid a$ and $c \mid b \iff a = c \cdot p$ for int p and $b = c \cdot q$ for int q.

RTP: $c \mid (ai + bj)$ for all i, j ints.

Consider

$$ai + bj = ip \cdot c + j \cdot q \cdot c = \underbrace{(i \cdot p + j \cdot q)}_{\text{int.}} \cdot c$$

for arbitrary i and j ints.

$(\Leftarrow)$ Because both a and b are int. lin. comb of a, b. Since $a = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$. $\boxtimes$

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

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

<u>NB</u>: $\{\underline{\text{true}}, \underline{\text{false}}\} = \{\underline{\text{false}}, \underline{\text{true}}\}$

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:

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

Set Equality

Two sets are equal precisely when they have the same elements

Example:

- $\{x \in \mathbb{N} : 2 \mid x \wedge x \text{ is prime}\} = \{2\}$
- For a positive integer m,
  $\{x \in \mathbb{Z} : m \mid x\} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod m\}$
- $\{d \in \mathbb{N} : d \mid 0\} = \mathbb{N}$

Equivalent predicates specify equal sets

$$\{x \in A \mid P(x)\} = \{x \in A \mid Q(x)\}$$

iff

$$\forall x \in A.\ P(x) \Leftrightarrow Q(x)$$

Example: For a positive integer m,

$$\{x \in \mathbb{Z}_m \mid x \text{ has a reciprocal in } \mathbb{Z}_m\}$$

$=$

$$\{x \in \mathbb{Z}_m \mid 1 \text{ is an integer linear combination of } m \text{ and } x\}$$

Sets of Common Divisors

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*?

Proposition For m and n natural numbers,

(1) $\underline{CD}(m, n) = \underline{CD}(n, m)$

(2) $\underline{CD}(m, n \cdot m) = \underline{D}(m)$

Corollary For a natural number ℓ,

(1) $\underline{CD}(\ell, \ell) = \underline{CD}(\ell, 0) = \underline{D}(\ell)$

(2) $\underline{CD}(1, \ell) = \{1\}$

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

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

PROOF: Let m, m' be nats. Let n be pos. int.

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

RTP: $\{d \in \mathbb{N} : d \mid m \wedge d \mid n\} = \{d \in \mathbb{N} : d \mid m' \wedge d \mid n\}$.

$\iff$

$[\forall d \in \mathbb{N}.\ (d \mid m \wedge d \mid n) \iff (d \mid m' \wedge d \mid n)]$

Let $d \in \mathbb{N}$.

$(\Longrightarrow)$ Assume $d \mid m$ and $d \mid n$

RTP: $d \mid m'$ and $d \mid n$ $\Longleftarrow$ m' is an int $\boxtimes$ lin. comb of m and n

NB: As an application of the key lemma, for a natural number m and a positive integer n, since $m \equiv \underline{\text{rem}}(m,n) \pmod n$ it follows that

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

Example:

$$\underline{CD}(34,13) = \underline{CD}(13,8) = \underline{CD}(8,5) = \underline{CD}(5,3)$$

$$= \underline{CD}(3,2) = \underline{CD}(2,1) = \underline{CD}(1,0)$$

$$= D(1) = \{1\}$$

Lemma 58 *For all positive integers m and n,*

$$\mathrm{CD}(m,n) = \begin{cases} \mathrm{D}(n) & \text{, } \textit{if } n \mid m \\ \mathrm{CD}\big(n, \mathrm{rem}(m,n)\big) & \text{, } \textit{otherwise} \end{cases}$$

Since a positive integer n is the greatest divisor in $\mathrm{D}(n)$, the lemma suggests a recursive procedure:

$$\gcd(m,n) = \begin{cases} n & \text{, if } n \mid m \\ \gcd\big(n, \mathrm{rem}(m,n)\big) & \text{, otherwise} \end{cases}$$

for computing the *greatest common divisor*, of two positive integers m and n. This is

Euclid's Algorithm

gcd

```
fun gcd( m , n )
  =  let
       val ( q , r ) = divalg( m , n )
     in
       if r = 0 then n
       else gcd( n , r )
     end
```