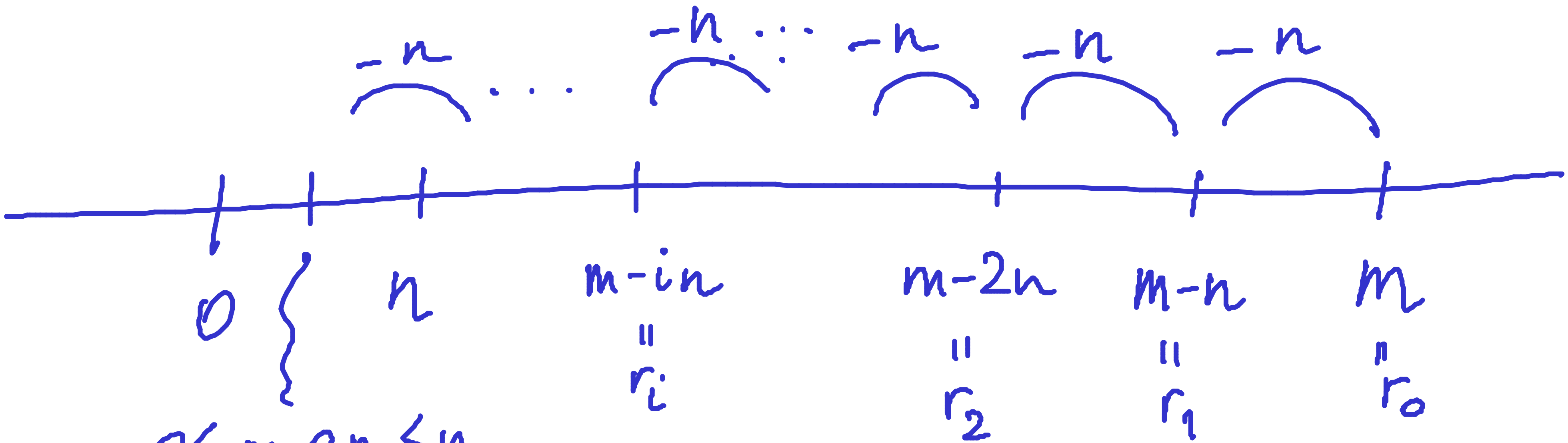
The division theorem and algorithm

Theorem 53 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $q \geq 0$*,* $0 \leq r < n$*, and* $m = q \cdot n + r$*.*

Definition 54 *The natural numbers* q *and* r *associated to a given pair of a natural number* m *and a positive integer* n *determined by the Division Theorem are respectively denoted* $\mathrm{quo}(m, n)$ *and* $\mathrm{rem}(m, n)$*.*

Proof of Theorem 53:



$$0 \le \underbrace{m-qn}_{r} < n$$

$$m = i \cdot n + r_i$$

The Division Algorithm in ML: divalg(m, n) = diviter(0, m)

```
fun divalg( m , n )
  = let
      fun diviter( q , r )
        = if r < n then ( q , r )
          else diviter( q+1 , r-n )
    in
      diviter( 0 , m )
    end
```

(*) NB: m = first arg of diviter × n + second arg of diviter

NB: Suppose (*) holds for diviter(q, r)

Then it also holds for diviter(q+1, r−n).

```
fun quo( m , n ) = #1( divalg( m , n ) )
```

$m = q \cdot n + r \overset{?}{\Longrightarrow} m = (q+1) \cdot n + (r-n)$ ✓

```
fun rem( m , n ) = #2( divalg( m , n ) )
```

Theorem 56 *For every natural number* m *and positive natural number* n*, the evaluation of* $\mathtt{divalg}(m, n)$ *terminates, outputing a pair of natural numbers* (q_0, r_0) *such that* $r_0 < n$ *and* $m = q_0 \cdot n + r_0$.

PROOF:

$r \geq 0$

$$\begin{tikzcd} & \underline{\mathrm{diviter}}(q,r) \arrow[dl, "r<n"'] \arrow[dr, "r \geq n"] & \\ (q,r) & & \underline{\mathrm{diviter}}(q+1, r-n) \end{tikzcd}$$

$r-n \geq 0$

For all calls of $\underline{\mathrm{diviter}}(a,b)$ we have $m = a \cdot n + b$

$\boxtimes$

Proposition 57 *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 be a positive integer. Consider natural numbers k and l.

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

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

Assume $k \equiv l$ Then $\underline{\mathrm{rem}}(k,m) \equiv \underline{\mathrm{rem}}(l,m)$

and $\underline{\mathrm{rem}}(k,m) = \underline{\mathrm{rem}}(l,m)$

$(\Longleftarrow)$ Exercise. $\boxtimes$

Corollary 58 *Let m be a positive integer.*

NB: $l \equiv l + a \cdot m \pmod{m}$

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*

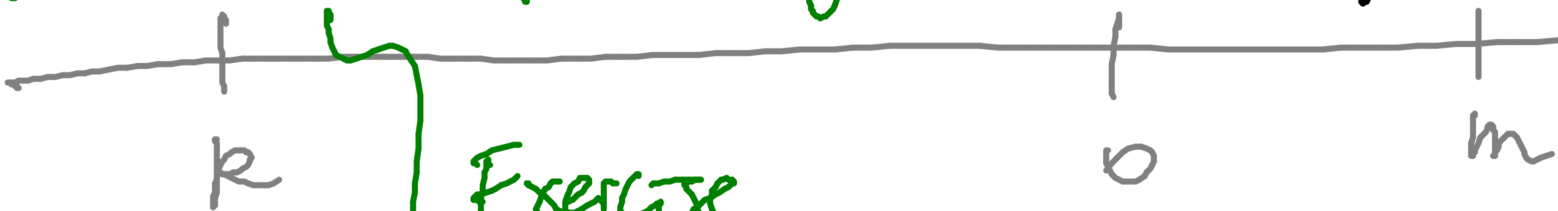
$$0 \leq [k]_m < m \quad \textit{and} \quad k \equiv [k]_m \pmod{m} \quad .$$

PROOF:

(2) Say k is a nat. Then $[k]_m = \mathrm{rem}(k, m)$.

For $k < 0$ an integer. $[k]_m = [k + am]_m$

$[k]_m = m - \mathrm{rem}(-k, m)$ if $\mathrm{rem}(-k, m) \neq 0$ for a s.t.



$k + am \geq 0$

Exercise.

$\boxtimes$

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

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

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

For k and l in $\mathbb{Z}_m$,

$$k +_m l \text{ and } k \cdot_m l$$

are the unique modular integers in $\mathbb{Z}_m$ such that

$$k +_m l \equiv k + l \pmod{m}$$

$$k \cdot_m l \equiv k \cdot l \pmod{m}$$

Example 60 *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.

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.

Example 61 *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.

Abelian group

commutative monoid

Proposition 62 *For all natural numbers* $m > 1$, *the modular-arithmetic structure*

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

distributive laws.

is a commutative ring.

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

.

Proposition 63 *Let* m *be a positive integer. A modular integer* k *in* $\mathbb{Z}_m$ *has a reciprocal if, and only if, there exist integers* i *and* j *such that* $k \cdot i + m \cdot j = 1$.

PROOF: Let m be a positive integer.

Let k be a natural number smaller than m.

($\Rightarrow$) Let l be a reciprocal of k; that is, $0 \leq l < m$ and $k \cdot l \equiv 1 \pmod{m}$. In other words $k \cdot l - 1 = j \cdot m$ for some int. j.

Then, $k \cdot l + (-j) \cdot m = 1$ and $i_0 = l$ and $j_0 = -j$ are int. with the property $k \cdot i_0 + m \cdot j_0 = 1$.

($\Leftarrow$) Assume: $\exists\, i, j$, int. $k \cdot i + m \cdot j = 1$ (*)

RTP: $\exists\, \ell$ in $\mathbb{Z}_m$. $k \cdot \ell \equiv 1 \pmod{m}$.

From (*), let i_0, j_0 be integers such that

$$k \cdot i_0 + m \cdot j_0 = 1$$

Then,

$$1 = k \cdot i_0 + m \cdot j_0 \equiv k \cdot i_0 \pmod{m}$$

and consider $\ell = [i_0]_m$ in $\mathbb{Z}_m$

So $1 \equiv k \cdot i_0 \equiv k \cdot \ell \pmod{m}$. $\boxtimes$

Integer linear combinations

Definition 64 *An integer* r *is said to be a* linear combination *of a pair of integers* m *and* n *whenever there are integers* s *and* t *such that* $s \cdot m + t \cdot n = r$.

Proposition 65 *Let* m *be a positive integer. A modular integer* k *in* $\mathbb{Z}_m$ *has a reciprocal if, and only if,* 1 *is an integer linear combination of* m *and* k.