$$m = quo(m,n)\cdot n + rem(m,n)$$

The division theorem and algorithm

Theorem 42 (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 43 *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* $\mathrm{rem}(m, n)$.

$0 \leq \quad < m$

Corollary 46 *Let* m *be a positive integer.*

1. *For every natural number* n,

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

PROOF: Let n be a natural number. We know

$n = q \cdot m + \underline{\mathrm{rem}}(n, m)$ and so $n - \mathrm{rem}(n, m) = q \cdot m$

$\square$

Corollary 46 *Let m be a positive integer.*

1. *For every natural number n,*

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

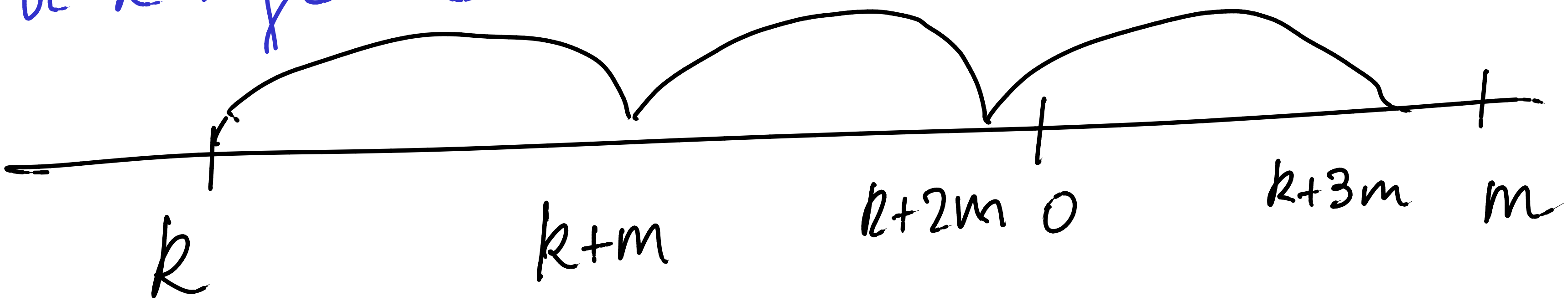
2. *For every integer k there exists a unique integer $[k]_m$ such that*

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

PROOF: of (2)

For k a natural number it follows from (1).

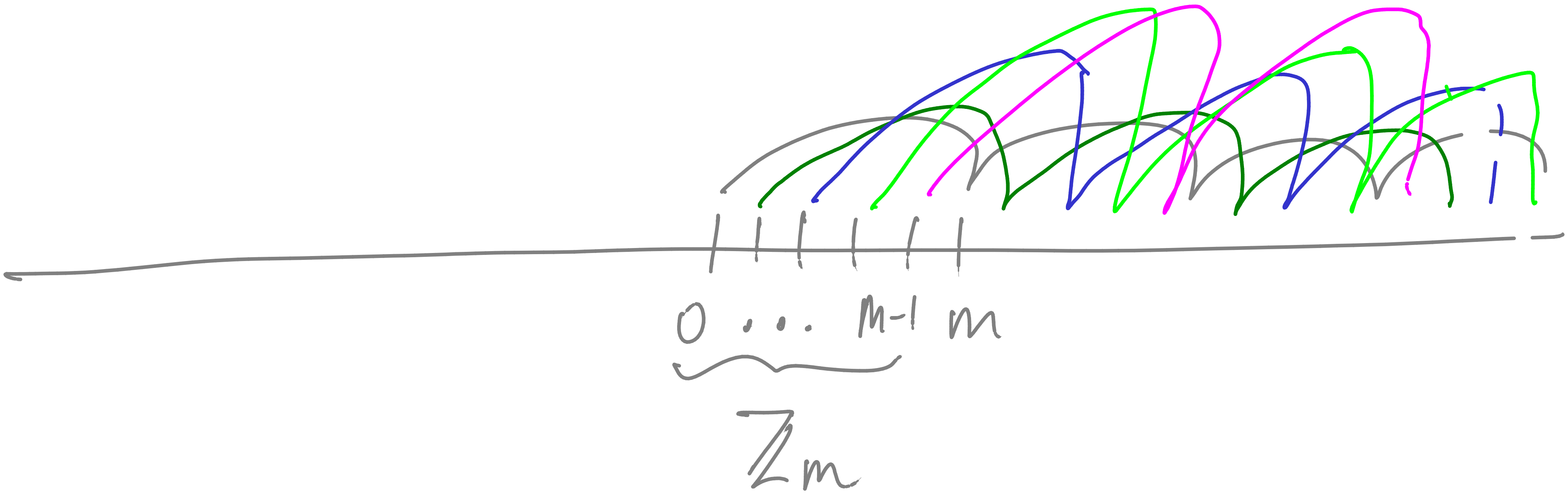
For k negative.



Consider $k + |k| \cdot m$

and take

$$[k]_m = \underline{\text{rem}}(k + |k| \cdot m, m) \qquad \square$$



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

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

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

$$3 +_4 3 = [3+3]_4 = [6]_4 = 2$$

$$3 \cdot_4 3 = [3 \cdot 3]_4 = [9]_4 = \underline{1}$$

Example 48 *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.

NB: 3 has a multiplicative inverse while 2 does not.

$$3 \cdot_4 2 = [3 \cdot 2]_4 = [6]_4 = 2$$

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.

NB: Every non-zero element has a multiplicative inverse

Example 49 *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 50 *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

$\{\ \ldots\ \}$

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

$$= \{0, 3, -1, 1, 2, -2\}$$

Ex: $\{x \in \mathbb{Z} \mid x$ is prime and even$\} = \{2\}$

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:

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

$\mathbb{N} = \{0, 1, 2, \ldots, n, \ldots\}$

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 52

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 53

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

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 55 (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' and n be as in the hypothesis.

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

That is $m - m' = k \cdot n$ for some integer k.

RTP: $(\Longrightarrow)$ $(d \mid m \wedge d \mid n) \Longrightarrow (d \mid m' \wedge d \mid n)$

$(\Longleftarrow)$ $(d \mid m' \wedge d \mid n) \Longrightarrow (d \mid m \wedge d \mid n)$

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

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

RTP: $d \mid m'$ and $d \mid n$

RTP$_1$: $d \mid m'$

Recall $m' = m - kn$

and use the lemma

RTP$_2$: $d \mid n$

Lemma:

$d \mid a \wedge d \mid b \Rightarrow d \mid a+b$

$d \mid a \Rightarrow d \mid (la)$

$(\Leftarrow)$ Analogous.

$\square$

Lemma 57 *For all positive integers* m *and* n,

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

Lemma 57 *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
```

Example 58 ($\mathrm{gcd}(13, 34) = 1$)

$$\begin{aligned}
\mathrm{gcd}(13, 34) &= \mathrm{gcd}(34, 13) \\
&= \mathrm{gcd}(13, 8) \\
&= \mathrm{gcd}(8, 5) \\
&= \mathrm{gcd}(5, 3) \\
&= \mathrm{gcd}(3, 2) \\
&= \mathrm{gcd}(2, 1) \\
&= 1
\end{aligned}$$