Boolean ~~XOR~~ and

$$(\mathbb{Z}_2, +_2, \cdot_2) \qquad 1 +_2 1 = [2]_2 = 0$$

Example 44 *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.

* correction

Proposition 46 *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' datatypes. 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	$\{\mathbf{true}, \mathbf{false}\}$
	$[-2..3]$		$\{-2, -1, 0, 1, 2, 3\}$

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.

NB! $a \in \{ x \in A \mid P(x) \} \iff (a \in A) \;\&\; P(a)$

Notations:

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

*correction

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 47

1. $D(0) = \mathbb{N}$
2. $D(1224) = \left\{ \begin{array}{c} 1, 2, 3, 4, 6, 8, 9, 12, 17, 18, 24, 34, 36, 51, 136, \\ 68, 72, 102, 153, 204, 306, 612, 408, 1224 \end{array} \right\}$

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

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

Example 48

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

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*?

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

Lemma 50 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $m \equiv m' \pmod{n}$*. Then,*

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

Could take $m' = \mathrm{rem}(m,n)$

PROOF: $\boxed{m - m' = k \cdot n}$ for some k

RTP: $(d \mid m$ & $d \mid n) \iff (d \mid m'$ & $d \mid n)$

(⇒) ① $\boxed{d \mid m}$ & $\boxed{d \mid n}$

RTP $d \mid m'$

$\Downarrow$

$d \mid kn \Rightarrow \boxed{d \mid -kn}$ ②

$m' = m - kn$

RTP $d \mid m'$ & $d \mid n$ ✓

① & ② $\Rightarrow d \mid m - kn = m'$

EXERCISE

Lemma 52 *For all positive integers* m *and* n*,*

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

$n \mid m$; That is $kn = m$

$$CD(kn, n) = D(n)$$

Lemma 52 *For all positive integers m and n,*

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

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
```

$$\underline{\mathrm{gcd}}(m,n) \overset{m<n}{=\!=} \underline{\mathrm{gcd}}(n,m) = \cdots$$

$m \geq n$

$\mathrm{gcd}(m,n)$

$\downarrow$

$\mathrm{gcd}(n,r) \quad n > r$

$\downarrow$

$\cdot$

Example 53 ($\mathrm{gcd}(13,34) = 1$)

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

Theorem 54 *Euclid's Algorithm* $\mathtt{gcd}$ *terminates on all pairs of positive integers and, for such* m *and* n, $\mathtt{gcd}(m,n)$ *is the greatest common divisor of* m *and* n *in the sense that the following two properties hold:*

(i) *both* $\mathtt{gcd}(m,n) \mid m$ *and* $\mathtt{gcd}(m,n) \mid n$, *and*

(ii) *for all positive integers* d *such that* $d \mid m$ *and* $d \mid n$ *it necessarily follows that* $d \mid \mathtt{gcd}(m,n)$.

PROOF:

NB gcd(m,n) is uniquely characterised by (i) and (ii).

$$\gcd(kn, n) \overset{\text{claim}}{=} n$$

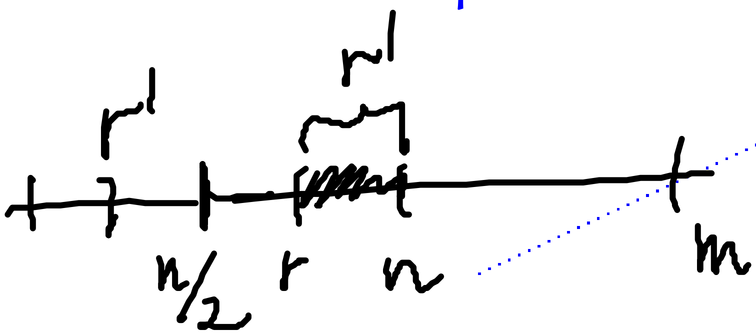
(i) $n \mid kn$ ✓ and $n \mid n$ ✓

(ii) $(d \mid kn \;\&\; d \mid n) \Rightarrow d \mid n$ ✓

$$\gcd(m,n)$$

- $n \mid m$: n
- $m = q \cdot n + r$, $q > 0,\ 0 < r < n$: $\gcd(n,r)$
  - $r \mid n$: r
  - $n = q' \cdot r + r'$, $q' > 0,\ 0 < r' < r$: $\gcd(r, r')$
- $0<m<n$: $\gcd(n,m)$

$m \geq n$



$\Big\}\ r' \leq n/2$

① $r \leq n/2 \Rightarrow r' \leq n/2$

② $r > n/2 \Rightarrow r' = n - r \leq n/2$

$$\gcd\left(\frac{m}{\gcd(m,n)}, \frac{n}{\gcd(m,n)}\right) = 1$$

Fractions in lowest terms

```
fun lowterms( m , n )
  = let
      val gcdval = gcd( m , n )
    in
      ( m div gcdval , n div gcdval )
    end
```

Some fundamental properties of gcds

Lemma 56 *For all positive integers* l, m, *and* n,

1. ***(Commutativity)*** $\gcd(m,n) = \gcd(n,m)$,
2. ***(Associativity)*** $\gcd\big(l, \gcd(m,n)\big) = \gcd(\gcd(l,m),n)$,
3. ***(Linearity)***[a] $\gcd(l \cdot m, l \cdot n) = l \cdot \gcd(m,n)$.

PROOF:

$$(m,n) \to (n,r) \to (r,r') \to \cdots \gcd(m,n)$$

$$(\ell m, \ell n) \to (\ell n, \ell r) \to (\ell r, \ell r') \to \ell \cdot \gcd(m,n)$$

$$= \gcd(\ell m, \ell n)$$

[a] Aka (Distributivity).

need to show that $\frac{(p-1)!}{m!(p-m)!} \in \mathbb{Z}$ for $0 < m < p$

Euclid's Theorem

Theorem 57 *For positive integers* k, m, *and* n, *if* $k \mid (m \cdot n)$ *and* $\gcd(k, m) = 1$ *then* $k \mid n$.

$\exists l .\ lk = m \cdot n$

PROOF:

$\gcd(k,m) = 1$

$\Rightarrow n \cdot \gcd(k,m) = n$

$\gcd(nk, nm) = \gcd(nk, lk)$

$= \gcd(n, l) \cdot k$

$\square$