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 ‘∈’ 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.

**Equality of sets:**

\[ A = B \iff \forall x. \ x \in A \iff x \in B. \]
### Defining sets

<table>
<thead>
<tr>
<th>The set</th>
<th>of even primes of booleans</th>
<th>is</th>
<th>[ -2..3 ]</th>
<th>{ 2 }</th>
<th>{ true, false }</th>
<th>{ -2, -1, 0, 1, 2, 3 }</th>
</tr>
</thead>
</table>

\[
\mathbb{N} \text{ the set of natural numbers} = \{ 0, 1, 2, \ldots, n, \ldots \}.
\]
**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:

\[ \{ x \in A \mid P(x) \} , \quad \{ x \in A : P(x) \} \]
Greatest common divisor

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

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

**Example 53**

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

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

**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

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

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

**Example 54**

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

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

$$\Rightarrow \text{hcf}$$
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,

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

PROOF: Assume $m \equiv m' \pmod{n}$, i.e. $m' = m + kn$ for some $k \in \mathbb{Z}$. RTP: $\forall d \in \mathbb{N}, d \mid m \land d \mid n \implies d \mid m' \land d \mid n$.  

($\Rightarrow$) Assume $d \mid m$ and $d \mid n$. Then $d \mid m'$ because $d \mid (m + kn)$.  

([Using $d \mid (a + b) \implies d \mid (a + 5)$])  

So $d \mid m'$ and $d \mid n$.  

($\Leftarrow$) Symmetrically
Lemma 58  For all positive integers $m$ and $n$, 

\[
\text{CD}(m, n) = \begin{cases} 
D(n), & \text{if } n \mid m \\
\text{CD}(n, \text{rem}(m, n)), & \text{otherwise}
\end{cases}
\]

by Lemma 57.1
Lemma 58  For all positive integers $m$ and $n$,

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

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

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

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

**Euclid’s Algorithm**
fun gcd( m , n )
  = let
    val ( q , r ) = divalg( m , n )
  in
    if r = 0 then n
    else gcd( n , r )
  end
Example 59 \((\gcd(13, 34) = 1)\)

\[
\gcd(13, 34) = \gcd(34, 13) \\
= \gcd(13, 8) \\
= \gcd(8, 5) \\
= \gcd(5, 3) \\
= \gcd(3, 2) \\
= \gcd(2, 1) \\
= 1
\]
Theorem 60  Euclid’s Algorithm \( \gcd \) terminates on all pairs of positive integers and, for such \( m \) and \( n \), \( \gcd(m, n) \) is the greatest common divisor of \( m \) and \( n \) in the sense that the following two properties hold:

(i) both \( \gcd(m, n) \mid m \) and \( \gcd(m, n) \mid n \), and

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

Proof:
Termination: at avg. decrease.

\[ \gcd(m, n) = D(\gcd(m, n)) \]

\[ m = q \cdot n + r \]
\[ n \mid m \]
\[ q > 0, 0 < r < n \]
\[ CD(n, r) \]
\[ r \mid n \]
\[ n = q' \cdot r + r' \]
\[ q' > 0, 0 < r' < r \]
\[ CD(r, r') \]
\[ r \mid r' \]
\[ D(r') \]

\[ \forall d. (d \mid m \land d \mid n) \]
\[ d \mid \gcd(m, n) \]
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 \( \gcd \)s

**Lemma 62** For all positive integers \( l, m, \) and \( n, \)

1. *(Commutativity)* \( \gcd(m, n) = \gcd(n, m), \)

2. *(Associativity)* \( \gcd(l, \gcd(m, n)) = \gcd(\gcd(l, m), n), \)

3. *(Linearity)* \( \gcd(l \cdot m, l \cdot n) = l \cdot \gcd(m, n). \)

**Proof:**

\( \text{aAka (Distributivity).} \)
\text{RTF. (2)} \quad \gcd(l,m,l,n) \mid l \cdot \gcd(m,n)\

\text{Note} \quad l \mid \gcd(l,m,l,n).
\text{[Because]} \quad l \mid l,m,l,n.
\quad l,l,k = \gcd(l,m,l,n) \quad (2)
\text{for some} \quad k \in \mathbb{N}. \text{Because } g(t)
\quad l,k \mid l,m,l,n
\quad k \mid m,n.
\quad k \mid \gcd(m,n)
\quad l,k \mid 2 \cdot \gcd(m,n)
\quad \therefore \quad \gcd(l,m,l,n) \quad \square
Euclid’s Theorem

**Theorem 63** For positive integers $k$, $m$, and $n$, if $k \mid (m \cdot n)$ and $\gcd(k, m) = 1$ then $k \mid n$.

**Proof:**