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. Equality of sets:

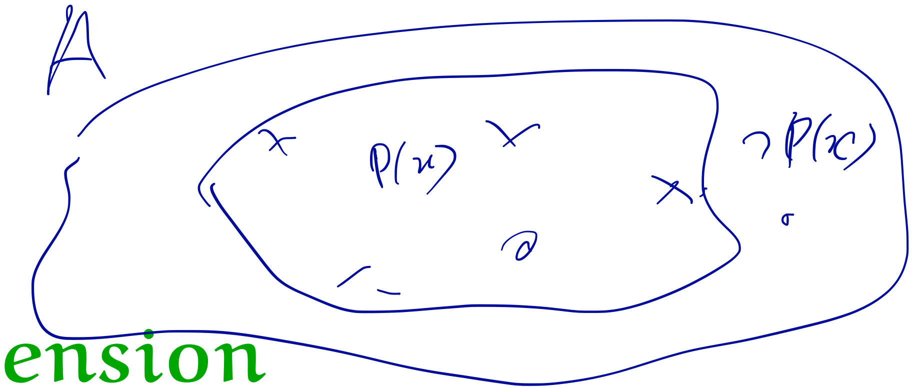
$$A = B \quad \text{iff} \quad \forall x.\ x \in A \iff x \in B .$$

Defining sets

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

$\mathbb{N}$ 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:

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

Greatest common divisor

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

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

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

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

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

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*?

$\approx$ 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,*

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

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

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

($\Rightarrow$) Assume $d \mid m$ & $d \mid n$. Then

$d \mid m'$ because $d \mid (m + kn)$.

[Using $d \mid a$ & $d \mid b \Rightarrow d \mid (a+b)$].

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

($\Leftarrow$). Symmetrically

$d \mid m$ & $n \mid m \Rightarrow d \mid m$

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

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

by Lemma 57,

$CD\left(\mathrm{rem}(m,n), n\right)$

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
```

Example 59 ($\gcd(13,34)=1$)

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

Theorem 60 *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:*

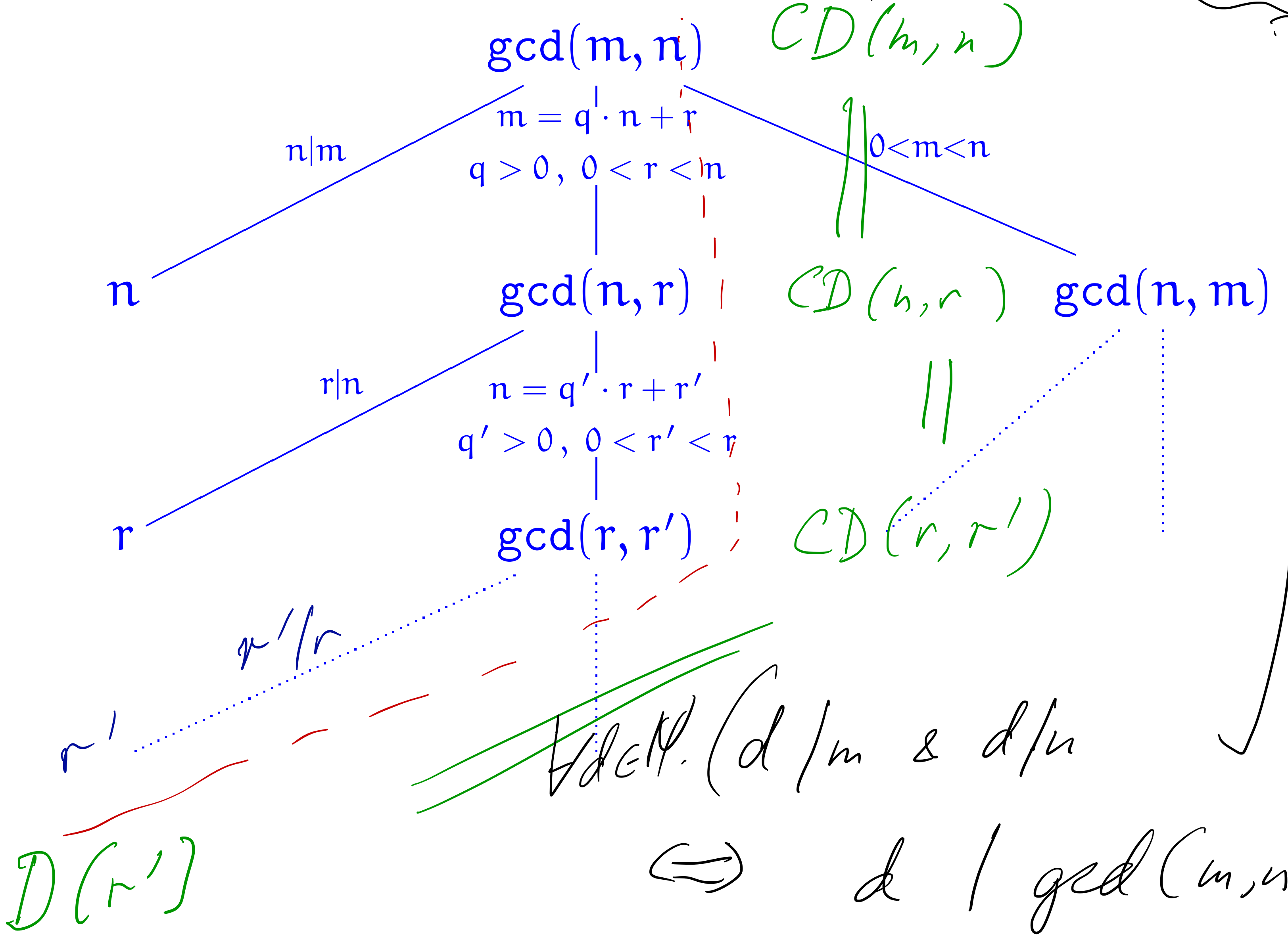
(i) *both* $\mathtt{gcd}(m, n) \mid m$ *and* $\mathtt{gcd}(m, n) \mid n$, *and*

(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:

Termination: 1st arg. decreases.

$CD(m,n) \stackrel{?}{=} D(gcd(m,n))$



$\forall d \in \mathbb{N}.\ (d \mid m\ \&\ d \mid n \iff d \mid gcd(m,n))$

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 gcds

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

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

PROOF: of (3) (1) $l \cdot \gcd(m,n) \mid \gcd(l \cdot m, l \cdot n)$

(2) $\gcd(l \cdot m, l \cdot n) \mid l \cdot \gcd(m,n)$.

(1) Have $\gcd(m,n) \mid m$, n $\therefore$ $l \cdot \gcd(m,n) \mid l \cdot m$, $l \cdot n$.

$\therefore$ $l \cdot \gcd(m,n) \mid \gcd(l \cdot m, l \cdot n)$.

[a] Aka (Distributivity).

RTP. (2) $\gcd(l\cdot m, l\cdot n) \mid l\cdot\gcd(m,n)$

Note $l \mid \gcd(l\cdot m, l\cdot n)$.

[Because $l \mid l\cdot m$, $l\cdot n$].

$\therefore$ $l\cdot k = \gcd(l\cdot m, l\cdot n)$ (1)

for some $k \in \mathbb{N}$. Because of (1),

$l\cdot k \mid l\cdot m$, $l\cdot n$

$\therefore$ $k \mid m$, n.

$\therefore$ $k \mid \gcd(m,n)$

$\therefore$ $l\cdot k \mid l\gcd(m,n)$

$\quad\ \|$

$\gcd(l\cdot m, l\cdot n)$ $\boxtimes$

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: