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

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

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.

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 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,*

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

PROOF:

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

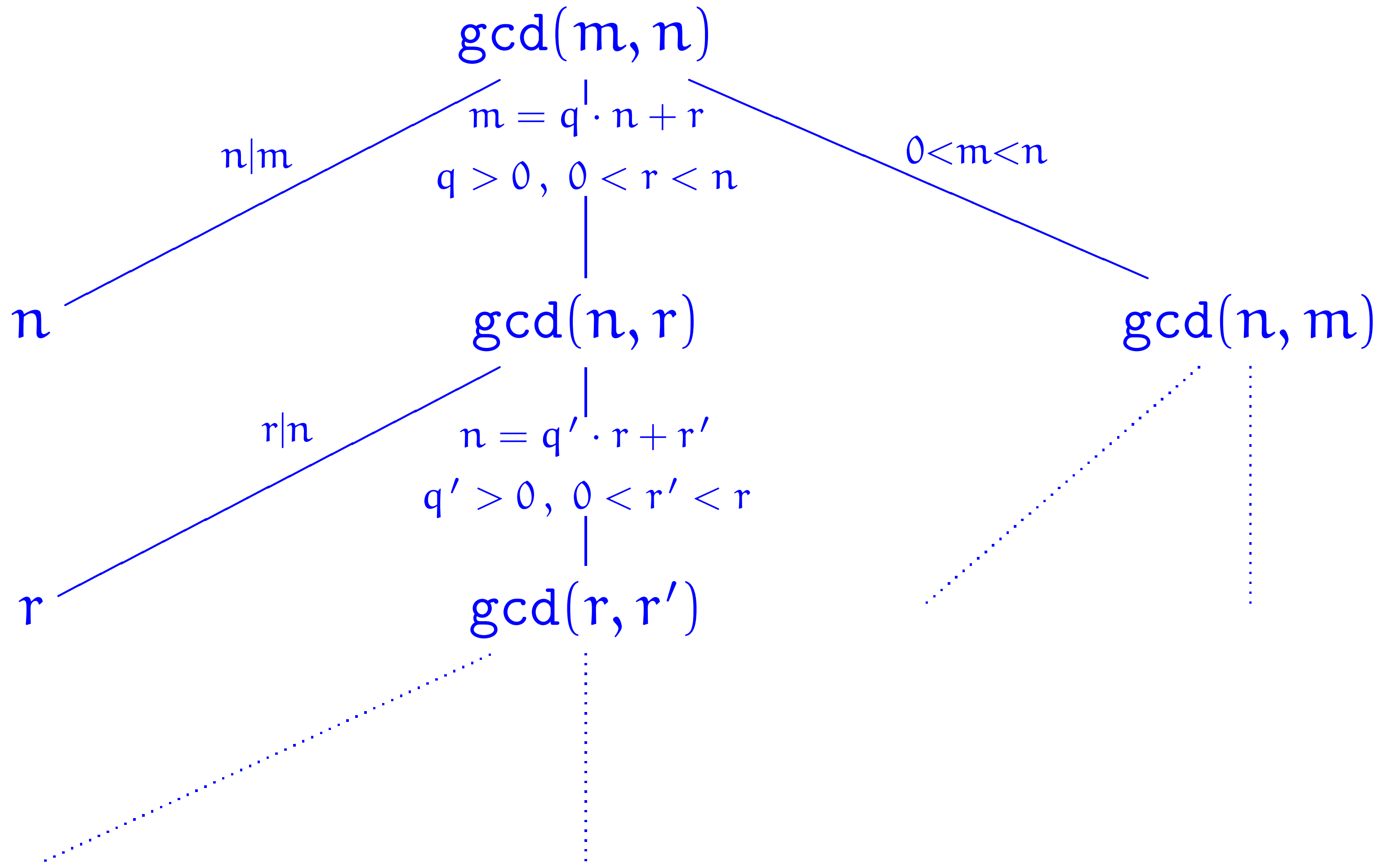
$$\begin{aligned} \mathrm{gcd}(13, 34) &= \mathrm{gcd}(34, 13) \\ &= \mathrm{gcd}(13, 8) \\ &= \mathrm{gcd}(8, 5) \\ &= \mathrm{gcd}(5, 3) \\ &= \mathrm{gcd}(3, 2) \\ &= \mathrm{gcd}(2, 1) \\ &= 1 \end{aligned}$$

Theorem 59 *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:


gcd(m, n)
n|m
m = q · n + r
q > 0 , 0 < r < n
0<m<n
n
gcd(n, r)
gcd(n, m)
r|n
n = q′ · r + r′
q′ > 0 , 0 < r′ < r
r
gcd(r, r′)

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 61 *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:

[a] Aka (Distributivity).