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

	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.

Notations:

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

Set equality

Two sets are equal precisely when they have the same elements

Examples:

- $\{ x \in \mathbb{N} : 2 \mid x \ \wedge \ x \text{ is prime} \} = \{ 2 \}$
- For a positive integer m,

$$\{ x \in \mathbb{Z} : m \mid x \} = \{ x \in \mathbb{Z} : x \equiv 0 \pmod{m} \}$$

- $\{ d \in \mathbb{N} : d \mid 0 \} = \mathbb{N}$

Equivalent predicates specify equal sets:

$$\{ x \in A \mid P(x) \} = \{ x \in A \mid Q(x) \}$$

iff

$$\forall x.\; P(x) \iff Q(x)$$

NB: Let $a \in A$, Then

$$a \in \{ x \in A \mid P(x) \} \iff P(a)$$

Equivalent predicates specify equal sets:

$$\{\, x \in A \mid P(x) \,\} = \{\, x \in A \mid Q(x) \,\}$$

iff

$$\forall x.\ P(x) \iff Q(x)$$

Example: For a positive integer m,

$$\{\ x \in \mathbb{Z}_m \mid x \text{ has a reciprocal in } \mathbb{Z}_m\ \}$$

$$=$$

$$\{\ x \in \mathbb{Z}_m \mid 1 \text{ is an integer linear combination of } m \text{ and } x\ \}$$

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 67

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

NB: $CD(m, m) = D(m)$

$d|m$ and $d|n$ $\Rightarrow$ d divides any integer linear combination of m and n

$d|m \Rightarrow d | i \cdot m$
$d|n \Rightarrow d | j \cdot n$
$\Rightarrow d | i \cdot m + j \cdot n$

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 68

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

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 71 (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:

find m'' s.t $m'' \equiv m' \pmod{n}$

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

find m' s.t $m' \equiv m \pmod{n}$

$= \mathrm{CD}(m'',n') = \cdots \quad = D(k)$

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

$$\underline{CD}(m,n) = \underline{CD}(\quad , n)$$

$$m' \text{ s.t. } m' \equiv m \pmod{n}$$

$$m' = \underline{rem}(m,n)$$

$$m' = m + i \cdot n$$

$$m' = m - n$$

$$m' = m + n$$

$$CD(m,n) = CD(m',n)$$

$$\text{with } m' < m$$

$$\underline{CD}(m,n) = \underline{CD}(m+n,n)$$

$m \equiv m' \pmod{n} \iff m - m' = kn$

$\Downarrow$

$\underline{CD}(m,n) = \underline{CD}(m',n)$ (*) $\Big\Vert$ m' is an int. linear combination of m and n

$\iff \left[\forall d \in \mathbb{N}. \ (d \mid m \wedge d \mid n) \iff (d \mid m' \wedge d \mid n) \right]$

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

($\Rightarrow$) Assume $d \mid m$ and $d \mid n$.

$\underline{RTP}$: $d \mid m'$ $\qquad$ $\underline{RTP}$: $d \mid n$ ✓

Because (*)

($\Leftarrow$) Analogous.

$\boxtimes$

Lemma 73 *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:

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

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

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

NB If $\mathtt{gcd}$ terminates on input (m, n) with output $\mathtt{gcd}(m, n)$ then $\mathrm{CD}(m, n) = \mathrm{D}\big(\mathtt{gcd}(m, n)\big)$.

NB: gcd ~ with rem.
with subtraction

Proposition 75 *For all natural numbers* m, n *and* a, b, *if* $\mathrm{CD}(m,n) = \mathrm{D}(a)$ *and* $\mathrm{CD}(m,n) = \mathrm{D}(b)$ *then* $a = b$.

Then $D(a) = D(b)$

But $a \in D(a)$ so $a \in D(b)$; i.e. $a \mid b$ } $\Rightarrow a = b$

$b \in D(b)$ so $b \in D(a)$; i.e $b \mid a$

Proposition 75 *For all natural numbers* m, n *and* a, b, *if* $\mathrm{CD}(m, n) = \mathrm{D}(a)$ *and* $\mathrm{CD}(m, n) = \mathrm{D}(b)$ *then* $a = b$.

Proposition 76 *For all natural numbers* m, n *and* k, *the following statements are equivalent:*

1. $\mathrm{CD}(m, n) = \mathrm{D}(k)$.
2.
   - $k \mid m \;\wedge\; k \mid n$, *and*
   - *for all natural numbers* d, $d \mid m \;\wedge\; d \mid n \implies d \mid k$.

Definition 77 *For natural numbers* m, n *the unique natural number* k *such that*

- $k \mid m \;\wedge\; k \mid n$, *and*
- *for all natural numbers* d, $d \mid m \;\wedge\; d \mid n \implies d \mid k$.

is called the greatest common divisor *of* m *and* n, *and denoted* $\mathrm{gcd}(m, n)$.

Theorem 78 *Euclid's Algorithm* gcd *terminates on all pairs of positive integers and, for such* m *and* n*, the positive integer* $\mathrm{gcd}(m, n)$ *is the greatest common divisor of* m *and* n *in the sense that the following two properties hold:*

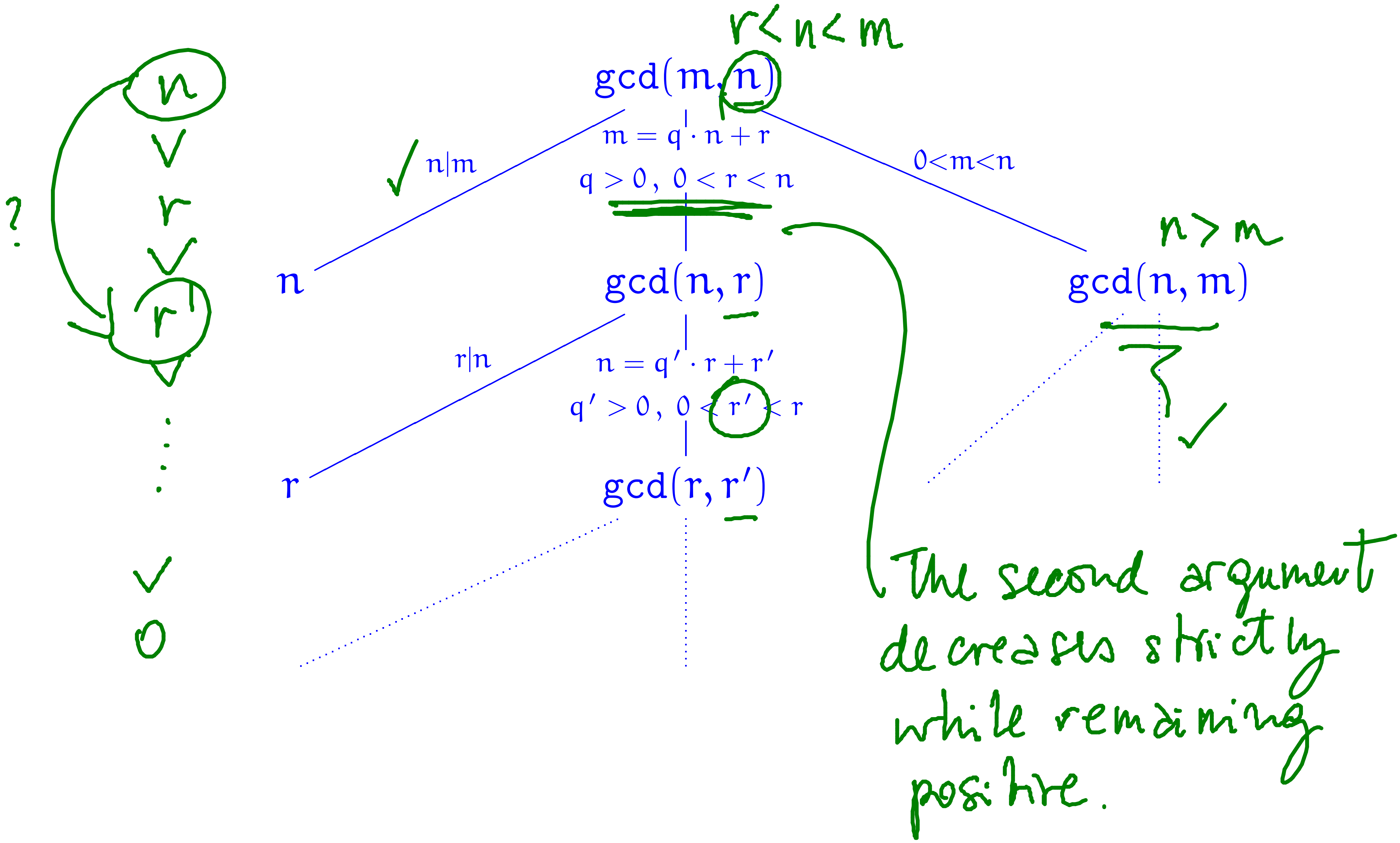
(i) *both* $\mathrm{gcd}(m, n) \mid m$ *and* $\mathrm{gcd}(m, n) \mid n$*, and*

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

PROOF: PARTIAL CORRECTNESS.

$\underline{CD}(m,n) = \underline{D}(\mathrm{gcd}(m,n)) \implies$ (i) & (ii) by Prop 76.

TERMINATION?


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′)
r<n<m
n>m
The second argument decreases strictly while remaining positive.