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

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

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

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

$\underline{\text{NB}}$: If $\underline{gcd}$ terminates on input (m,n) with output $gcd(m,n)$

Then

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

Proposition For all natural numbers m, n and a, b,

(*) $\underline{CD}(m,n) = \underline{D}(a)$ and $\underline{CD}(m,n) = \underline{D}(b)$

imply

$$a = b$$

PROOF IDEA:

Use that for all nat. numbers a and b,

$$\underline{D}(a) = \underline{D}(b) \text{ implies } a = b.$$

$\boxtimes$

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

(I) $\underline{CD}(m,n) = \underline{D}(k)$

(II) (i) $k \mid m$ and $k \mid n$

and

(ii) for all natural numbers d,

$$(d \mid m \wedge d \mid n) \Rightarrow d \mid k$$

PROOF IDEA:

(I)

equivalently

$$\{d \in \mathbb{N} \mid d|m \wedge d|n\} = \{d \in \mathbb{N} \mid d|k\}$$

equivalently

for all $d \in \mathbb{N}$, $(d|m \wedge d|n) \Leftrightarrow d|k$

equivalently

(II)

$\boxtimes$

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

(i) $k \mid m$ and $k \mid n$

and

(ii) for all natural numbers d,

$$(d \mid m \wedge d \mid n) \Rightarrow d \mid k$$

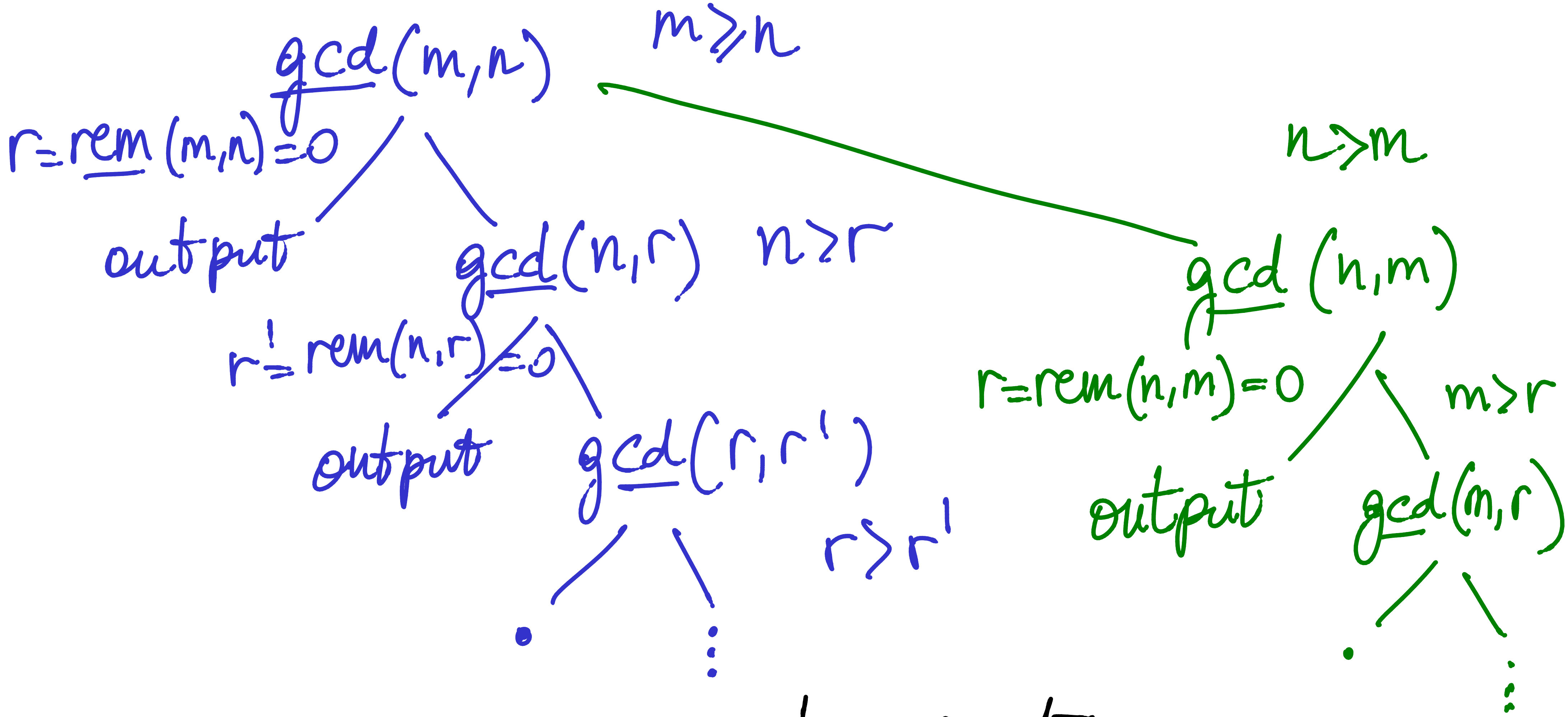
is called the **greatest common divisor** of m and n, and denoted $\gcd(m, n)$.

Theorem 60 *Euclid's Algorithm* ① $\mathtt{gcd}$ *terminates on all pairs of positive integers and,* ② *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*

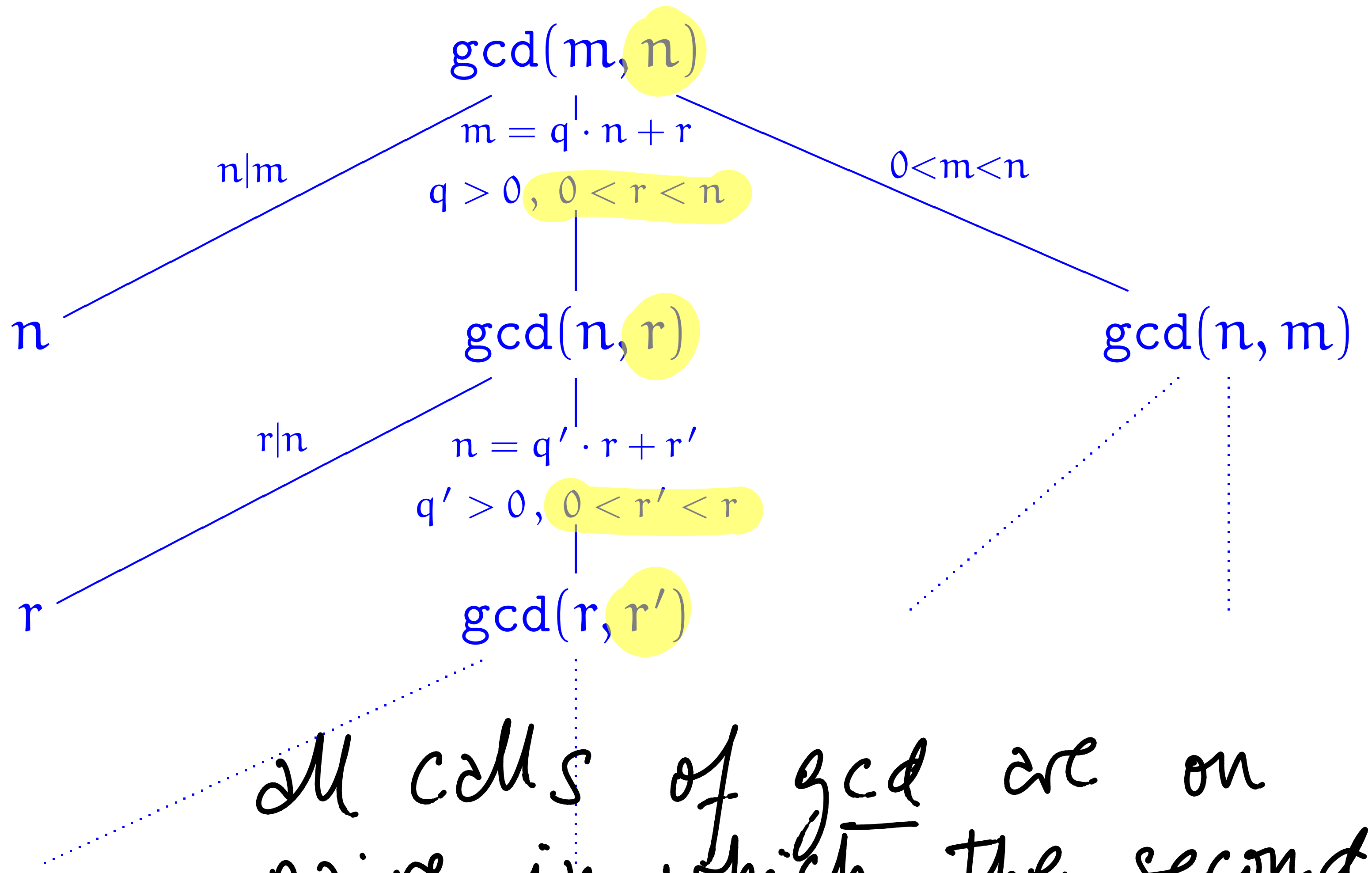
(ii) *for all positive integers* d *such that* $d \mid m$ *and* $d \mid n$ *it necessarily follows that* $d \mid \mathtt{gcd}(m, n)$*.*

PROOF:



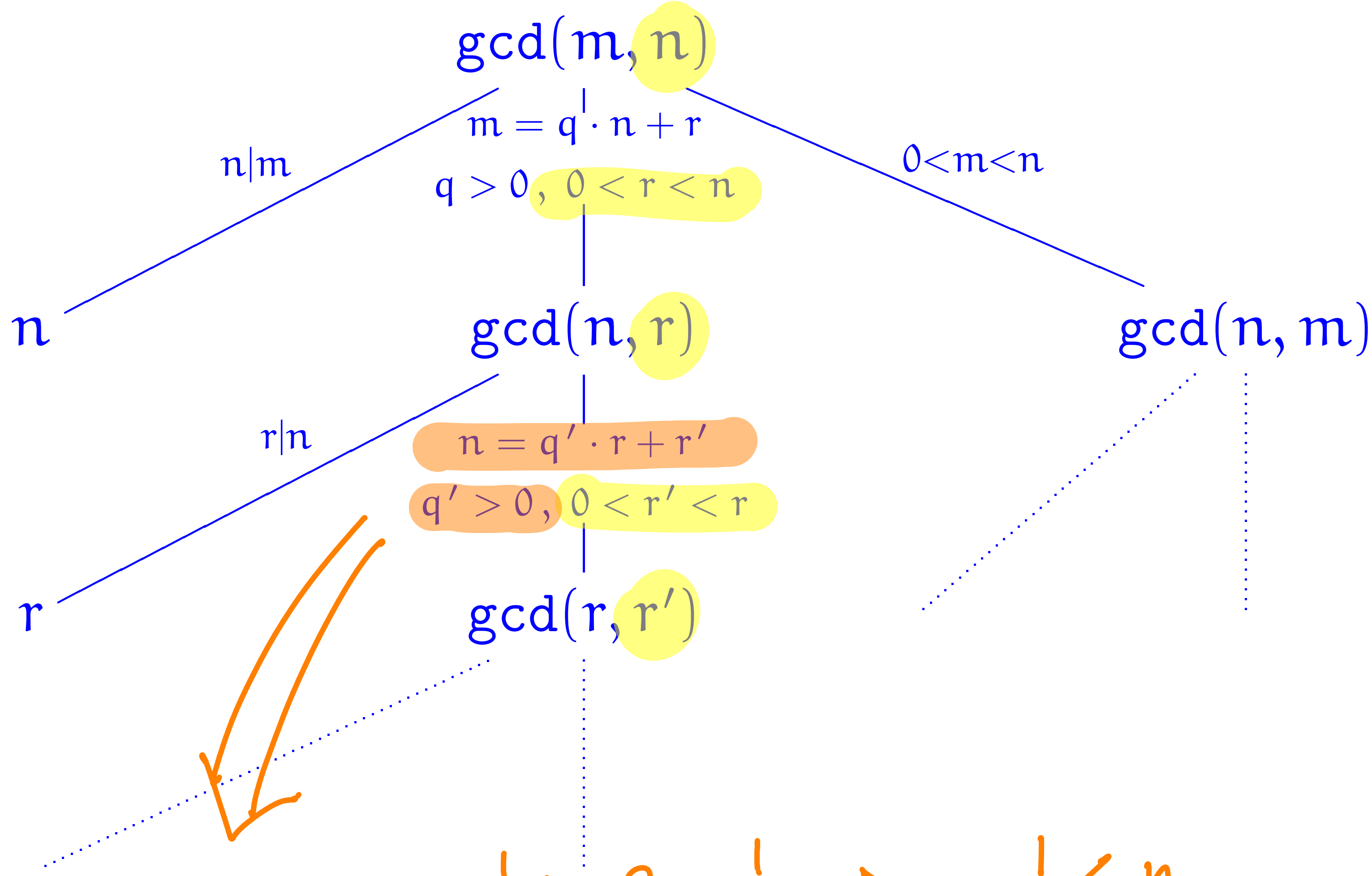
the gcd function terminates on all pairs of positive integers iff it terminates on all pairs (m,n) with $m \geq n$

$m \geqslant n$



all calls of gcd are on pairs in which the second argument decreases while remaining positive; a bounded process

$m \geqslant n$



$n \geqslant r + r' > 2r' \Rightarrow r' < \frac{n}{2}$

Fractions in lowest terms

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