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:

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

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

Euclid's Algorithm

NB: If $\gcd(m,n)$ terminates say with output k, then $\underline{CD}(m,n) = \underline{D}(k)$.

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

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

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

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

$$\Longleftrightarrow \left[\begin{array}{l} (1) \; k \mid m \wedge k \mid n \\ \wedge (2) \; \forall d \in \mathbb{N}. \; d \mid m \wedge d \mid n \Rightarrow d \mid k \end{array} \right]$$

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

$$\underline{D}(k) = \{ d \in \mathbb{N} : d \mid k \}$$

Properties (1) and (2) uniquely characterise k.

Suppose $\left[\begin{array}{l} (1)_1 \; k_1 \mid m \wedge k_1 \mid n \\ \& \; (2)_1 \; \forall d.\; d \mid m \wedge d \mid n \Rightarrow d \mid k_1 \end{array}\right]$

and $\left[\begin{array}{l} (1)_2 \; k_2 \mid m \wedge k_2 \mid n \\ \& \; (2)_2 \; \forall d.\; d \mid m \wedge d \mid n \Rightarrow d \mid k_2 \end{array}\right]$

Then, we claim, $k_1 = k_2$.

Theorem 60 *Euclid's Algorithm* gcd *terminates on all pairs of positive integers and, for such* m *and* n, $\mathrm{gcd}(m, n)$ *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*

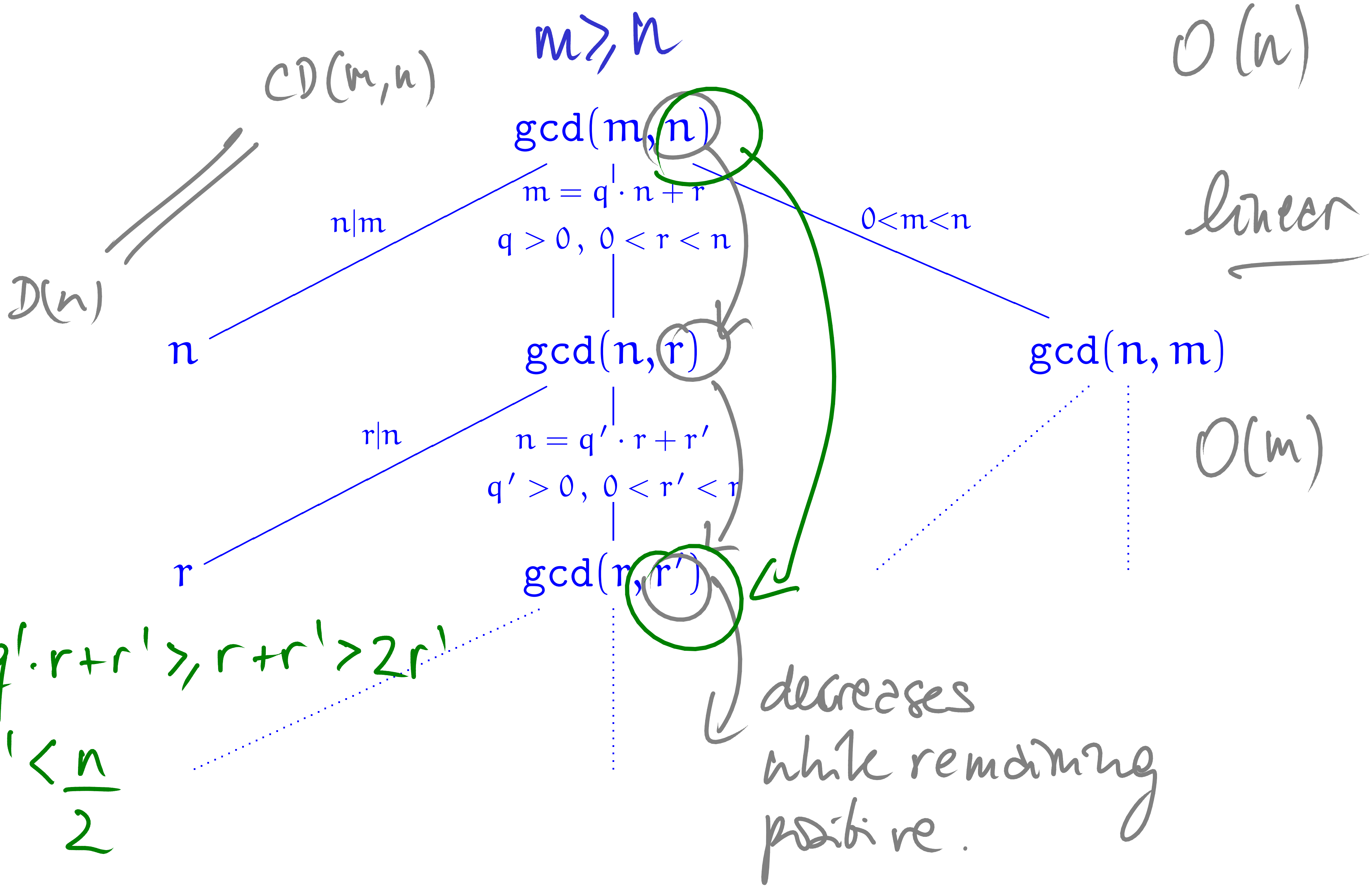
(ii) *for all positive integers* d *such that* $d \mid m$ *and* $d \mid n$ *it necessarily follows that* $d \mid \mathrm{gcd}(m, n)$.

PROOF: PROOF PRINCIPLE

To show that some k is the gcd of m and n go on to show that

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

and (2) $\forall d.\ d \mid m \wedge d \mid n \Rightarrow d \mid k$.



$$n = q' \cdot r + r' \geq r + r' > 2r'$$

$$\Rightarrow \quad r' < \frac{n}{2}$$

running time is $O(\log(\max(m,n)))$.

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)*** $\gcd(m, n) = \gcd(n, m)$,
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:

We show (1) $l \cdot \gcd(m,n) \mid lm$ and $l \cdot \gcd(m,n) \mid l \cdot n$

and (2) $\forall d.$ if $d \mid lm$ and $d \mid ln$

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

[a] Aka (Distributivity).

(1) RTP : $l \cdot \gcd(m,n) \mid l \cdot m$

Since $\gcd(m,n) \mid m$ Then $l \cdot \gcd(m,n) \mid l \cdot m$

[Lemma $a \mid b \Rightarrow a \cdot c \mid b \cdot c$]

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

---

(2) RTP : $\forall d$ if $d \mid lm$ and $d \mid ln$ Then $d \mid l \cdot \gcd(m,n)$

Let d be an arbitrary po. int. such that

① $d \mid l \cdot m$ and ② $d \mid l \cdot n$ (*) [$(a \mid b \wedge b \mid c) \Rightarrow a \mid c$]

RTP : $d \mid l \cdot \gcd(m,n)$

From ① and ②, we have $d \mid \gcd(l \cdot m, l \cdot n)$

If $\gcd(l \cdot m, l \cdot n) \mid l \cdot \gcd(m,n)$ by (*) we will be done

We want to show

$$\gcd(\ell\cdot m, \ell\cdot n) \mid \ell\cdot \gcd(m,n).$$

Exercise.

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: <u>Assume</u> $k \mid (m \cdot n)$ and $\gcd(k, m) = 1$

$$\Downarrow \qquad\qquad \Downarrow$$

$\ell \cdot k = m \cdot n$ for some k $\qquad$ $n \cdot \gcd(k, m) = n$

$$\| $$

$$\gcd(nk, nm)$$

$$k \cdot \gcd(n, \ell) = \gcd(nk, \ell \cdot k) = n \implies k \mid n. \qquad \boxtimes$$

Corollary 64 (Euclid's Theorem) *For positive integers* m *and* n*, and prime* p*, if* $\mathrm{p} \mid (\mathrm{m} \cdot \mathrm{n})$ *then* $\mathrm{p} \mid \mathrm{m}$ *or* $\mathrm{p} \mid \mathrm{n}$*.*

Now, the second part of Fermat's Little Theorem follows as a corollary of the first part and Euclid's Theorem.

PROOF: <u>Assume</u> $p \mid (m \cdot n)$

<u>case ①:</u> if $p \mid m$ then we are done.

<u>case ②</u> if $p \nmid m$ then $\underline{gcd}(p, m) = 1$

and so $p \mid n$. ☒

FLT

$$i^p \equiv i \pmod{p}$$

suppose $i \not\equiv 0 \pmod{p}$

then $p \mid (i^p - i) = (i^{p-1} - 1)\, i$

and by Euclid's Thm.

$$p \mid i^{p-1} - 1$$

That is, $i^{p-1} \equiv 1 \pmod{p}$.

NB:

$$p \mid \binom{p}{m} \qquad 0 < m < p \qquad (\text{prime } p)$$

Exercise.