$\mapsto$ to derive the gcd algorithm.

Lemma 56 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $\mathrm{m} \equiv \mathrm{m}' \pmod{\mathrm{n}}$*. Then,*

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

PROOF:

Given m and n

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

so as to compute

$$CD(m, n)$$

by computing instead

$$CD(m', n)$$

if $m > n$

$m' = m - n$

$$CD(m-n, n)$$

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

$$\text{greatest}\,\mathrm{CD}(m,n) = \begin{cases} \text{greatest}\,\mathrm{D}(n) = n & \text{, if } n \mid m \\ \text{greatest}\,\mathrm{CD}(n, \underbrace{\mathrm{rem}(m,n)}_{\exists n.\ m' \text{ s.t. } m \equiv m' \pmod{n}}) & \text{, otherwise} \end{cases}$$

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

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

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

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* $d \mid \mathtt{gcd}(m,n)$.

characterizing property of $\underline{gcd}(m,n)$

PROOF: By the previous lemma

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

which is equivalent to (1) and (2).

In fact

$$(*)$$

$$\iff$$

$$\forall d.\ d \in \underline{CD}(m,n) \iff d \in D(\gcd(m,n))$$

$$\iff \left[\forall d.\ (d \mid m \wedge d \mid n) \iff d \mid \underline{\gcd}(m,n)\right] (**)$$

Exercise Show that

$$(**) \iff [(i) \wedge (ii)]$$

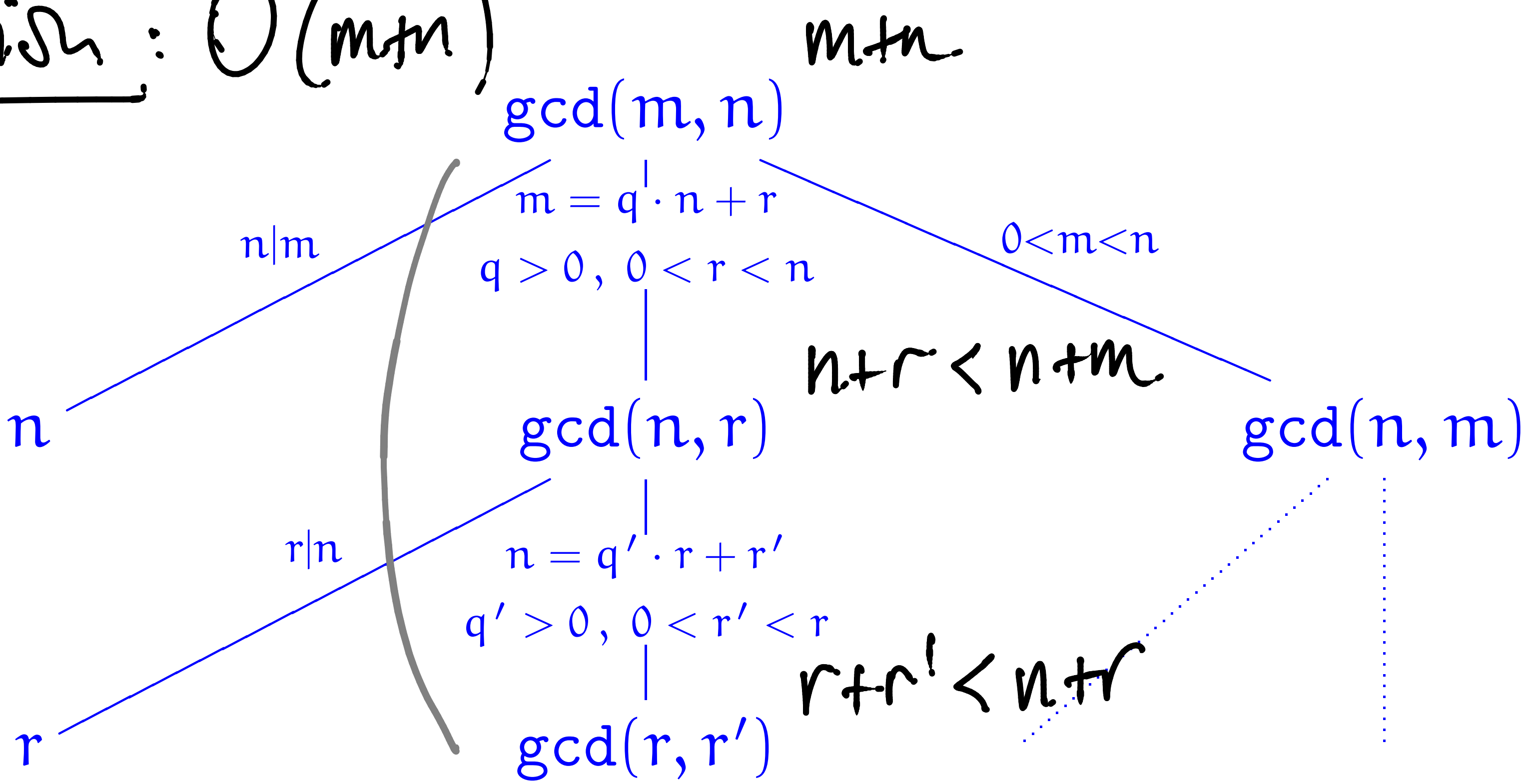
PROOF PRINCIPLE

To prove that k is the g.c.d. (m, n) we need prove

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

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

Termination: $O(m+n)$



Termination: $O(\log(\max(m,n)))$

Claim: $r' < \frac{n}{2} \iff 2r' < n$

because $2r' < r + r' < n$

There is a more precise analysis related to Fibonacci numbers. F_n

<u>Hint</u>: compute $\gcd(F_{n+1}, F_n) \ldots$

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:

Exercise

easily provable by the PROOF PRINCIPLE

[a] Aka (Distributivity).

(1) To show $\underline{gcd}(m,n) = \underline{gcd}(n,m)$

We establish the characterizing property of That $gcd(n,m)$ has $\underline{gcd}(m,n)$; That is,

(i) $\underline{gcd}(n,m) \mid m \wedge \underline{gcd}(n,m) \mid n$

(ii) $\forall d.\ d \mid m \wedge d \mid n \Rightarrow d \mid \underline{gcd}(n,m)$

This follows straightforwardly by the characterizing property of $\underline{gcd}(n,m)$. $\boxtimes$

Let l, m, n be positive integers.

RTP $\gcd(l \cdot m, l \cdot n) = l \cdot \gcd(m, n)$

Case 1 $n \mid m$:

$n \mid m \Rightarrow ln \mid lm$

$$l \cdot \gcd(m, n) = l \cdot n$$
$$\parallel$$
$$\gcd(lm, ln) = l \cdot n$$

and we are done

Case 2 otherwise: (Suppose w.l.g. that $m > n$)

$$l \cdot \gcd(m, n) = l \cdot \gcd(n, \text{rem}(m, n))$$

$$\gcd(lm, ln) = \gcd(ln, \text{rem}(lm, ln))$$
$$= \gcd(ln, l \cdot \text{rem}(m, n))$$

The property above is maintained throughout the computation and so the output of $\underline{gcd}(lm, ln)$ is l times the output of $\underline{gcd}(m, n)$ $\boxtimes$

We need to relate

$\underline{\mathrm{rem}}(m, n)$ $\qquad\qquad$ $\underline{\mathrm{rem}}(lm, ln)$

$$m = q \cdot n + \underline{\mathrm{rem}}(m,n)$$

$$0 \leq \underline{\mathrm{rem}}(m,n) < n \implies 0 \leq l \cdot \underline{\mathrm{rem}}(m,n) < ln$$

$$lm = q \cdot (ln) + l \cdot \underline{\mathrm{rem}}(m,n)$$

$$\Downarrow$$

$$l \cdot \underline{\mathrm{rem}}(m,n) = \underline{\mathrm{rem}}(lm, ln)$$

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: Let k, m, n be pos. int.

Assume $\underbrace{k \mid (m \cdot n)}_{}$ and $\underbrace{\gcd(k, m) = 1}_{(1)}$

RTP: $k \mid n$ (2)

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

$\quad\quad \gcd(nk, nm) = \gcd(nk, k \cdot i) = k \cdot \gcd(n, i)$

$(2) \Rightarrow m \cdot n = k \cdot i$ for an int i

and we are done. $\boxtimes$

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

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

PROOF: