Lemma 73 *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
```

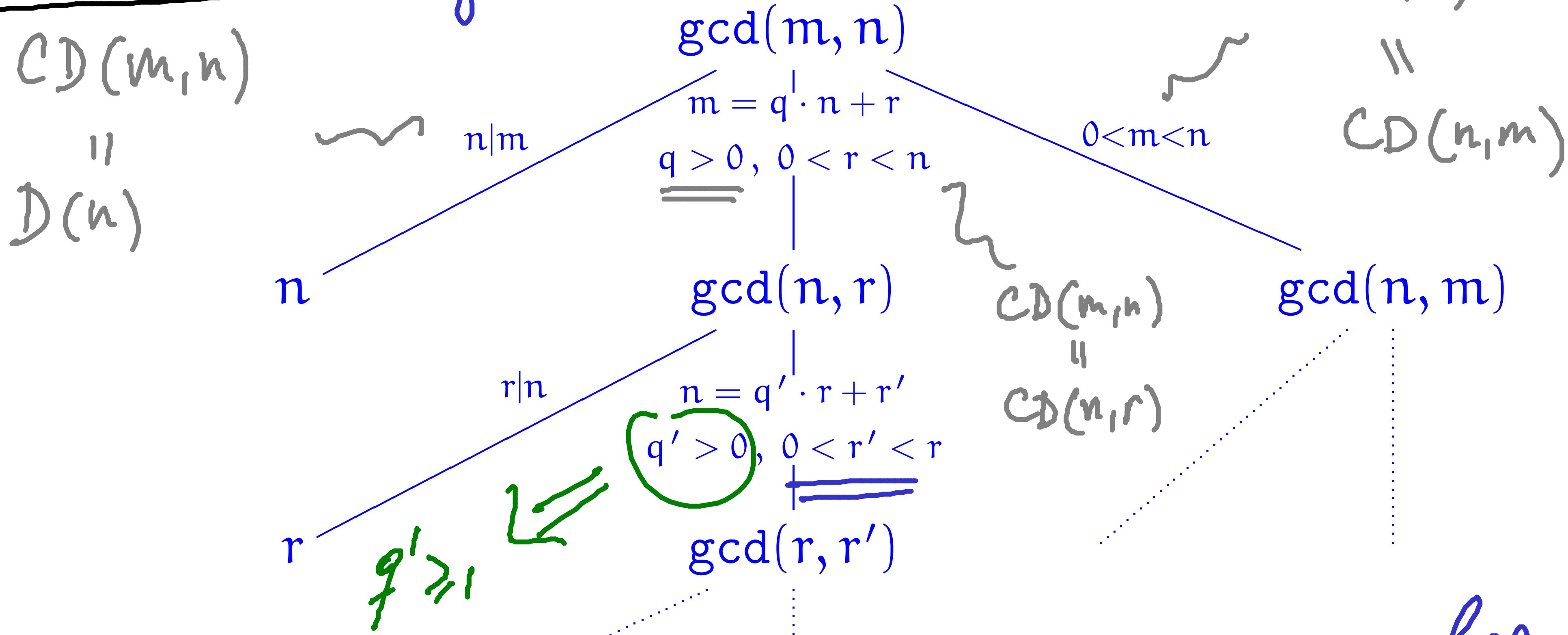
Theorem 78 *Euclid's Algorithm* gcd *terminates on all pairs of positive integers and, for such* m *and* n, *the positive integer* $\mathrm{gcd}(m, n)$ *is the greatest common divisor of* m *and* n *in the sense that the following two properties hold:*

(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: We know that if $\underline{\mathrm{gcd}}(m,n)$ terminates then $\underline{CD}(m,n) = D(\underline{\mathrm{gcd}}(m,n))$ and $\underline{\mathrm{gcd}}(m,n)$ satisfies (i) and (ii).

Termination argument.



NB: $2r' < r + r' \leq q' \cdot r + r' = n \Rightarrow r' < n/2 \Rightarrow$ log running time

NB: For each call of gcd, the second argument decreases while remaining positive.

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* $\gcd(m, n)$.

$$m/n = \frac{i \cdot \underline{gcd}(m,n)}{j \cdot \underline{gcd}(m,n)} = i/j$$

Fractions in lowest terms

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

Lemma 80 *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: Because:

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

Because: both $g\underline{cd}(\ell, g\underline{cd}(m, n))$ and $g\underline{cd}(g\underline{cd}(\ell, m), n)$ are the greatest in $\underline{CD}(\ell, m, n) = \{ d \in \mathbb{N} \mid d \mid \ell \wedge d \mid m \wedge d \mid n \}$

[a] Aka (Distributivity).

Linearity: $\gcd(\ell\cdot m, \ell\cdot n) = \ell\cdot\gcd(m,n)$.

Algorithmic proof idea:
Compares the computations of $\gcd(\ell\cdot m, \ell\cdot n)$ and $\gcd(m,n)$

$$\gcd(\ell\cdot m, \ell\cdot n) \qquad\qquad\qquad \gcd(m,n)$$

$$\ell\cdot n \qquad\qquad\qquad\qquad\qquad\qquad n$$

$$\ell\cdot m = q'\cdot \ell n + r' \qquad\qquad m = qn + r$$

$$\Downarrow$$

$$\ell m = q\cdot \ell n + \ell r$$

$$q' = q \wedge r' = \ell r$$

mathematical proof idea:

Show $\gcd(\ell \cdot m, \ell \cdot n) \stackrel{?}{=} \ell \cdot \gcd(m,n)$.

by showing

(i) $\ell \cdot \gcd(m,n) \mid \ell \cdot m \ \wedge \ \ell \cdot \gcd(m,n) \mid \ell \cdot n$ ✓

and

(ii) for all d such that $d \mid \ell \cdot m$ and $d \mid \ell \cdot n$ we have $d \mid \ell \cdot \gcd(m,n)$

(i) We know $\gcd(m,n) \mid m$ from which it follows that $\ell \cdot \gcd(m,n) \mid \ell \cdot m$.
Similarly for $\ell \cdot \gcd(m,n) \mid \ell \cdot n$.

(iv) Assume: $\underbrace{d \mid l \cdot m \quad \text{and} \quad d \mid l \cdot n}$

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

$\Downarrow$

Know:

$d \mid \gcd(lm, ln)$

$\vdots$

Know:

$l \mid (l \cdot m)$ and $l \mid (l \cdot n)$

$\vdots$

Exercise.

$\boxtimes$

Coprimality

Definition 81 *Two natural numbers are said to be* coprime *whenever their greatest common divisor is* 1.

or relative prime

Euclid's Theorem

Theorem 82 *For positive integers* k, m, *and* n, *if* $k \mid (m \cdot n)$ *and* $\gcd(k, m) = 1$ *then* $k \mid n$.

PROOF: Suppose $k \mid (m \cdot n)$. That is, $m \cdot n = k \cdot l$ for some l. Suppose also $\gcd(k, m) = 1$. Then,

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

$$\| \quad \gcd(n \cdot k, k \cdot l) = k \cdot \gcd(n, l) \qquad \Rightarrow k \mid n.$$

$\boxtimes$

Corollary 83 (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: Assume $p \mid (m \cdot n)$

<u>Case 1</u>: $p \mid m$

We are done.

<u>Case 2</u>: $p \nmid m$

Then $\underline{\gcd}(p, m) = 1$ and so $p \mid n$.

$\boxtimes$

FLT: $i^p \equiv i \pmod{p} \implies i^{p-1} \equiv 1 \pmod{p}$ if $i \not\equiv 0 \pmod{p}$

$i^p - i = (i^{p-1} - 1) \cdot i$

follows from Euclid's Thm.

Fields of modular arithmetic

Corollary 85 *For prime p, every non-zero element i of $\mathbb{Z}_p$ has $[i^{p-2}]_p$ as multiplicative inverse. Hence, $\mathbb{Z}_p$ is what in the mathematical jargon is referred to as a field.*