Lemma 73 *For all positive integers* m *and* n,

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

Since a positive integer n is the greatest divisor in $\mathrm{D}(\mathrm{n})$, the lemma suggests a recursive procedure:

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

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
```

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

Idea: $D(a) = CD(m,n) = D(b)$

$a \mid a \Rightarrow a \in D(a) = D(b) \Rightarrow a \mid b$
$b \mid b \Rightarrow b \in D(b) = D(a) \Rightarrow b \mid a$
$\Rightarrow a = b.$

Idea: $\mathrm{CD}(m,n) = \mathrm{D}(k)$

$\Leftrightarrow [\forall d \in \mathbb{N}.\ (d \mid m \wedge d \mid n) \Leftrightarrow d \mid k]$ (*)

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

(*) $\Rightarrow (\forall d \in \mathbb{N}.\ d \mid k \Rightarrow d \mid m \wedge d \mid n)$

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

since $k \mid k$

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

We have argued for (1) $\Rightarrow$ (2).

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

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

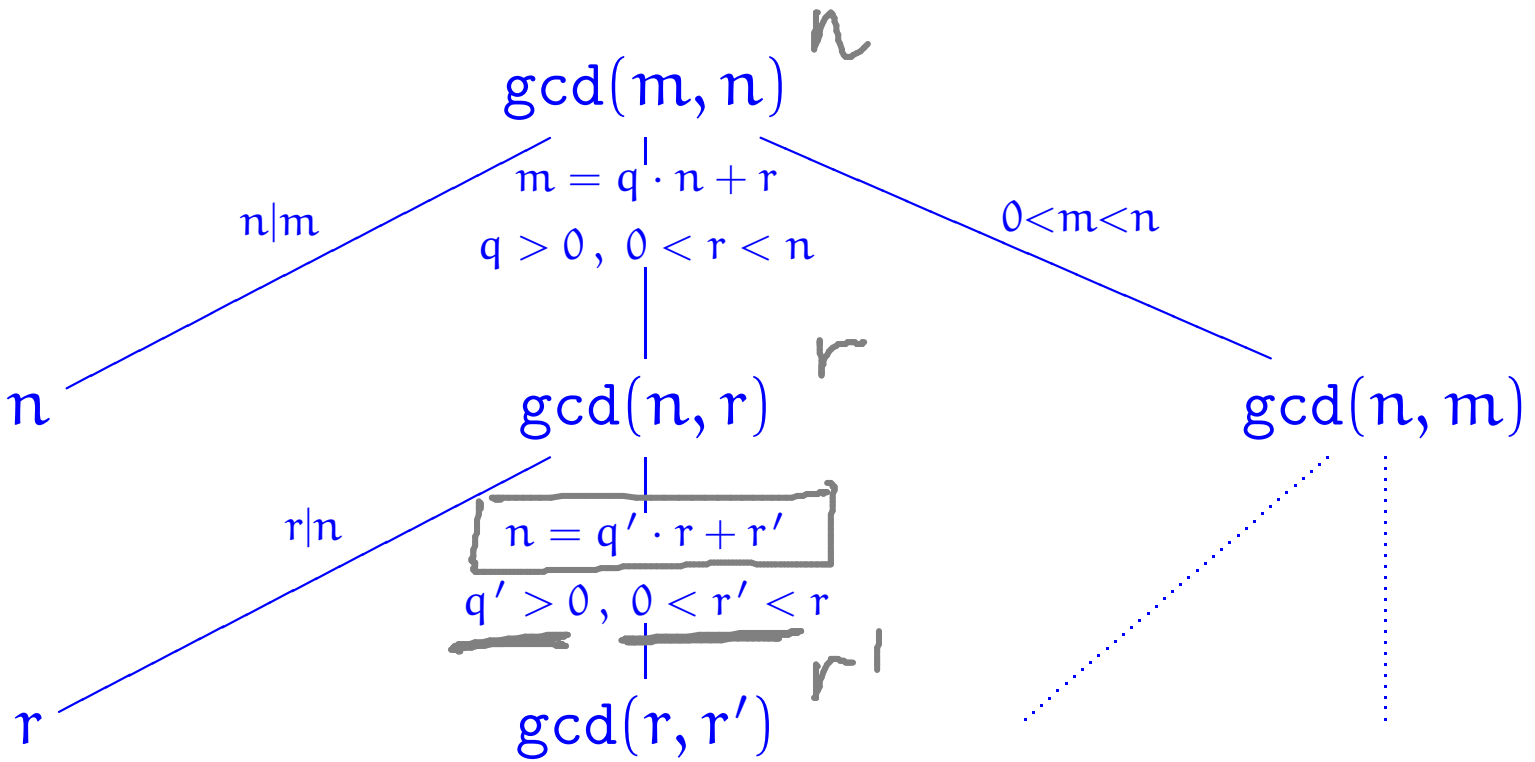
is called the greatest common divisor *of* m *and* n, *and denoted* $\mathrm{gcd}(\mathrm{m}, \mathrm{n})$.

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

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

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

PROOF: We have $CD(m,n) = D(\gcd(m,n))$ ∎ gcd terminates by construction. So the algorithm is partially correct.



$0 < \ldots < r' < r < n$

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

$r' < n/2 \rightsquigarrow$ gcd has running time $O(\log n)$

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

It is unambiguous to write gcd(l,m,n)

Lemma 80 *For all positive integers* l, m, *and* n,

1. ***(Commutativity)*** $\gcd(\mathrm{m},\mathrm{n}) = \gcd(\mathrm{n},\mathrm{m})$,
2. ***(Associativity)*** $\gcd\big(\mathrm{l},\gcd(\mathrm{m},\mathrm{n})\big) = \gcd(\gcd(\mathrm{l},\mathrm{m}),\mathrm{n})$,
3. ***(Linearity)***[a] $\gcd(\mathrm{l}\cdot\mathrm{m},\mathrm{l}\cdot\mathrm{n}) = \mathrm{l}\cdot\gcd(\mathrm{m},\mathrm{n})$.

PROOF: (1) $D(\gcd(m,n)) = CD(m,n)$

$= CD(n,m)$

$= D(\gcd(n,m))$

$\Leftarrow$

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

[a] Aka (Distributivity).

Coprimality

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

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

Assume ① $k \mid (m \cdot n)$ and ② $\gcd(k, m) = 1$

RTP: $k \mid n$

By ①, $m \cdot n = k \cdot l$ for a pos. int. l

By ②, $n = n \cdot \gcd(k, m) = \gcd(n \cdot k, n \cdot m) = \gcd(nk, lk)$

$\gcd(n, l) \cdot k$ ⊠

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: Let m, n be pos. int. Let p be a prime.

Assume $p \mid (m \cdot n)$

RTP: $p \mid m \vee p \mid n$

Cases: (1) If $p \mid m$ we are done.

(2) If $p \nmid m$ Then $\gcd(p, m) = 1$

So $p \mid n$.

$$i^p \equiv i \pmod p$$

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

If $p \nmid i$ Then $p \mid i^{p-1} - 1$;

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

$$\| \quad i^{p-2} \cdot i$$

$$\| \quad [i^{p-2}]_p \cdot i$$

multiplicative inverse of i in $\mathbb{Z}_p$.

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*.*

Extended Euclid's Algorithm

Example 86

$$
\begin{array}{rl||rcrcr||rcrcr}
 & \gcd(34,13) & 34 & = & 2\cdot & 13 & + & 8 & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 13 & = & 1\cdot & 8 & + & 5 & 5 & = & 13 & -1\cdot & 8 \\
= & \gcd(8,5) & 8 & = & 1\cdot & 5 & + & 3 & 3 & = & 8 & -1\cdot & 5 \\
= & \gcd(5,3) & 5 & = & 1\cdot & 3 & + & 2 & 2 & = & 5 & -1\cdot & 3 \\
= & \gcd(3,2) & 3 & = & 1\cdot & 2 & + & 1 & 1 & = & 3 & -1\cdot & 2 \\
= & \gcd(2,1) & 2 & = & 2\cdot & 1 & + & 0 & & & & & \\
= & 1 & & & & & & & & & & &
\end{array}
$$

$$
\begin{array}{rl||rrcl}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & = & \overbrace{-1\cdot 34+3\cdot 13} & -1\cdot & \overbrace{(2\cdot 34+(-5)\cdot 13)} \\
 & & = & -3\cdot 34+8\cdot 13 & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2 \\
 & & = & \overbrace{(2\cdot 34+(-5)\cdot 13)} & -1\cdot & \overbrace{(-3\cdot 34+8\cdot 13))} \\
 & & = & 5\cdot 34+(-13)\cdot 13 & &
\end{array}
$$

Integer linear combinations

Definition 64[a] An integer r is said to be a *linear combination* of a pair of integers m and n whenever

> there exist a pair of integers s and t, referred to as the *coefficients* of the linear combination, such that
>
> $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \ ;$$
>
> that is
>
> $$s \cdot m + t \cdot n = r \ .$$

[a] See page 195.

Theorem 87 *For all positive integers* m *and* n*,*

1. $\gcd(\mathrm{m},\mathrm{n})$ *is a linear combination of* m *and* n*, and*
2. *a pair* $\mathrm{lc}_1(\mathrm{m},\mathrm{n})$, $\mathrm{lc}_2(\mathrm{m},\mathrm{n})$ *of integer coefficients for it, i.e. such that*

$$\left[\begin{array}{cc} \mathrm{lc}_1(\mathrm{m},\mathrm{n}) & \mathrm{lc}_2(\mathrm{m},\mathrm{n}) \end{array}\right] \cdot \left[\begin{array}{c} \mathrm{m} \\ \mathrm{n} \end{array}\right] = \gcd(\mathrm{m},\mathrm{n}) \quad ,$$

can be efficiently computed.

Proposition 88 *For all integers* m *and* n*,*

1. $\begin{bmatrix} 1 & 0 \\ ? & ? \end{bmatrix} \cdot \begin{bmatrix} \mathrm{m} \\ \mathrm{n} \end{bmatrix} = \mathrm{m} \quad \wedge \quad \begin{bmatrix} 0 & 1 \\ ? & ? \end{bmatrix} \cdot \begin{bmatrix} \mathrm{m} \\ \mathrm{n} \end{bmatrix} = \mathrm{n}$;

Proposition 88 *For all integers* m *and* n,

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \ \wedge \ \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

$$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \ \wedge \ \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

implies

$$\begin{bmatrix} s_1+s_2 & t_1+t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \ ;$$

Proposition 88 *For all integers* m *and* n,

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \ \wedge \ \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

   $$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \ \wedge \ \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

   implies

   $$\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \ ;$$

3. *for all integers* k *and* s, t, r,

   $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \ \textit{implies} \ \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \ .$$

We extend Euclid's Algorithm $\mathtt{gcd}(\mathtt{m}, \mathtt{n})$ from computing on pairs of positive integers to computing on pairs of triples $((\mathtt{s}, \mathtt{t}), \mathtt{r})$ with $\mathtt{s}, \mathtt{t}$ integers and $\mathtt{r}$ a positive integer satisfying the invariant that $\mathtt{s}, \mathtt{t}$ are coefficientes expressing $\mathtt{r}$ as an integer linear combination of $\mathtt{m}$ and $\mathtt{n}$.

gcd

```
fun  gcd( m , n )
= let
    fun  gcditer(          r1   ,   c as          r2  )
    = let
        val (q,r) = divalg(r1,r2)    (* r = r1-q*r2 *)
      in
        if r = 0
        then  c
        else  gcditer(  c ,                    r  )
      end
  in
     gcditer(          m   ,          n  )
  end
```

egcd

```
fun egcd( m , n )
= let
    fun egcditer( ((s1,t1),r1) , lc as ((s2,t2),r2) )
    = let
        val (q,r) = divalg(r1,r2)   (* r = r1-q*r2 *)
      in
        if r = 0
        then lc
        else egcditer( lc , ((s1-q*s2,t1-q*t2),r) )
      end
  in
    egcditer( ((1,0),m) , ((0,1),n) )
  end
```

```
fun gcd( m , n ) = #2( egcd( m , n ) )

fun lc1( m , n ) = #1( #1( egcd( m , n ) ) )

fun lc2( m , n ) = #2( #1( egcd( m , n ) ) )
```

Multiplicative inverses in modular arithmetic

Corollary 92 *For all positive integers* m *and* n*,*

1. $\mathrm{n} \cdot \mathrm{lc}_2(\mathrm{m}, \mathrm{n}) \equiv \gcd(\mathrm{m}, \mathrm{n}) \pmod{\mathrm{m}}$*, and*
2. *whenever* $\gcd(\mathrm{m}, \mathrm{n}) = 1$*,*

   $\left[\mathrm{lc}_2(\mathrm{m}, \mathrm{n})\right]_{\mathrm{m}}$ *is the multiplicative inverse of* $[\mathrm{n}]_{\mathrm{m}}$ *in* $\mathbb{Z}_{\mathrm{m}}$.