gcd

```
fun gcd( m , n )
  =  let
       val ( q , r ) = divalg( m , n )
     in
       if r = 0 then n
       else gcd( n , r )
     end
```

$m = q \cdot n + r$

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

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

by Key Lemma

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

PROOF:

[(i) and (ii)] are equivalent

Exercise

$$\left(\forall d.\ d \mid m \wedge d \mid n \iff d \mid gcd(m,n) \right)$$

which is equivalent

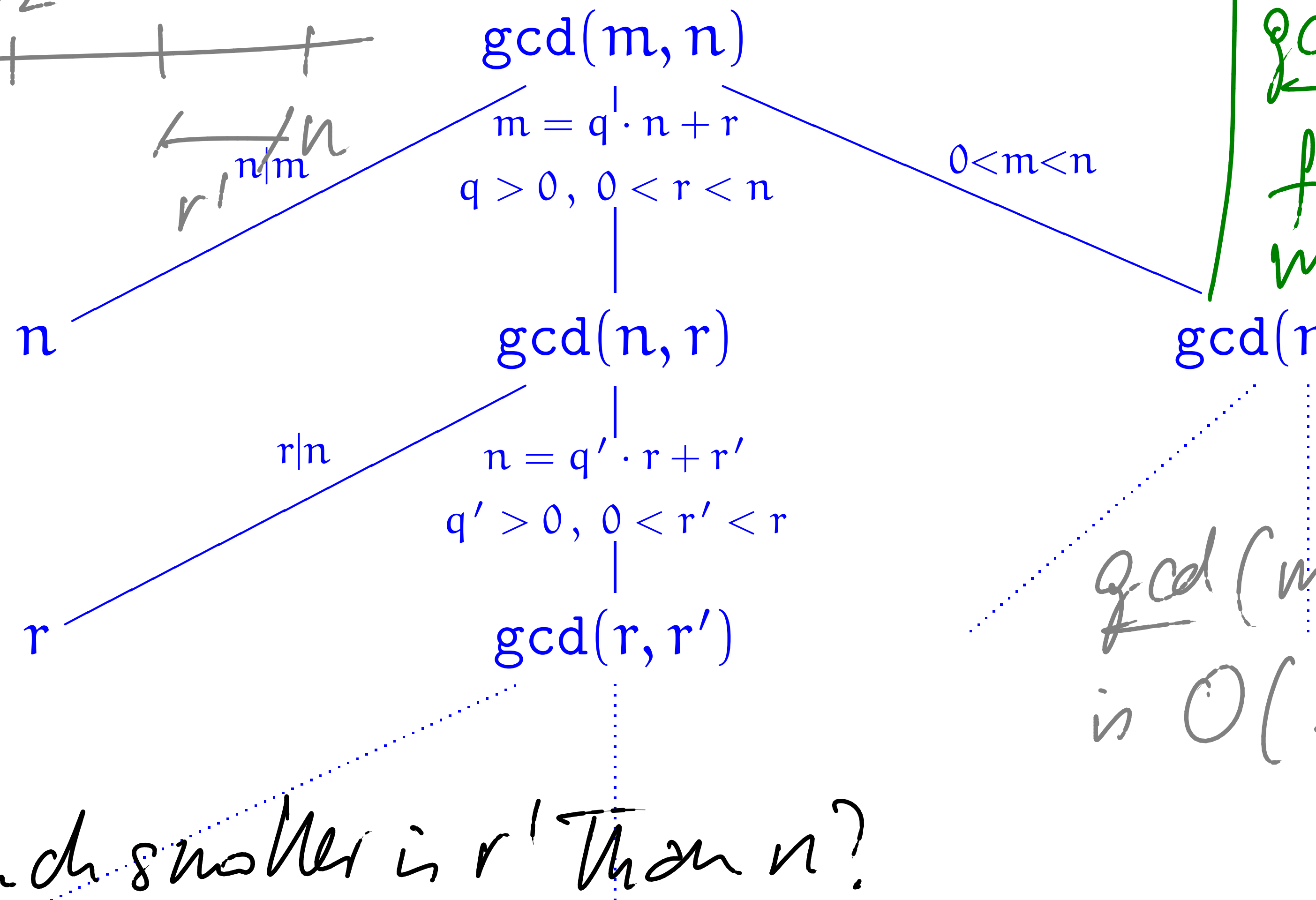
$$CD(m,n) = D(gcd(m,n))$$

Case 2

$n/2 \quad r$

$0 \qquad n \qquad r'$

$\Longrightarrow q' = 1 \Rightarrow r' = n - r \leq n/2$



Run $\underline{gcd}(F_{n+1}, F_n)$ for Fibonacci numbers.

$\underline{gcd}(m,n)$ is $O(\log(\max(m,n)))$

$\boxed{?}$ How much smaller is r' than n?

Case 1

$r' \quad r \quad n/2$

$0 \qquad n$

$r' \leq n/2$

$\underline{gcd}(m,n)$ is $O(\max(m,n))$

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* $\mathfrak{l}$, $\mathfrak{m}$, *and* $\mathfrak{n}$, Exercise

1. ***(Commutativity)*** $\gcd(\mathfrak{m},\mathfrak{n}) = \gcd(\mathfrak{n},\mathfrak{m})$, $\gcd(\ell,m,n)$
2. ***(Associativity)*** $\gcd\big(\mathfrak{l},\gcd(\mathfrak{m},\mathfrak{n})\big) = \gcd(\gcd(\mathfrak{l},\mathfrak{m}),\mathfrak{n})$,

   $\rightarrow$ PROOF by the properties of gcds
3. ***(Linearity)***[a] $\gcd(\mathfrak{l}\cdot\mathfrak{m},\mathfrak{l}\cdot\mathfrak{n}) = \mathfrak{l}\cdot\gcd(\mathfrak{m},\mathfrak{n})$.

$\gcd(n,m)$

$\gcd(m,n)$

PROOF: Consider two cases:

(1) $m \geq n$

Look at the run of $\gcd(n,m)$:

and see that $\gcd(n,m) = \gcd(m,n)$

(2) $n \leq m$

Analogous.

$\square$

[a] Aka ~~(Distributivity)~~.

Euclid's Theorem

Corollary: $p \mid \binom{p}{m}$ for p prime and $0 < m < p$

(Exercise)

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 positive integers.

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

RTP: $k \mid n$

By ② and linearity: $n \cdot \gcd(k, m) = n$

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

By ① $m \cdot n = k \cdot q$ for some integer q.

Hence, $n = \gcd(n.k, k.q) \overset{\text{by linearity}}{=} k . \gcd(n, q)$. □

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: Let m, n be positive integers and p a prime.

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

By cases: (1) $p \mid m$ and we are done.

(2) $\neg(p \mid m)$ Then $\gcd(p, m) = 1$

and by the previous Thm $p \mid n$. $\square$

NB: $k \equiv [k]_m \pmod m$

$a \equiv b \pmod m \implies k \cdot a \equiv k \cdot b \pmod m$

$\{0, 1, \ldots, p-1\}$

p prime

by Euclid's Thm

Fields of modular arithmetic

$i^p \equiv i \pmod p \implies i^{p-1} \equiv 1 \pmod p$ for i not a multiple of p

Corollary 66 *For prime* p*, every non-zero element* i *of* $\mathbb{Z}_\mathrm{p}$ *has* $[\mathrm{i}^{\mathrm{p}-2}]_\mathrm{p}$ *as multiplicative inverse. Hence,* $\mathbb{Z}_\mathrm{p}$ *is what in the mathematical jargon is referred to as a* field*.*

Fermat's Little Thm. $i^{p-1} \equiv 1 \pmod p$ $(1 \leq i < p)$

$i \cdot (i^{p-2}) \equiv 1 \pmod p$

$i \cdot [i^{p-2}]_p \equiv 1 \pmod p$

Extended Euclid's Algorithm

Example 67 ($\mathtt{egcd}(34, 13) = \big((5, -13), 1\big)$**)**

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

Extended Euclid's Algorithm

Example 67 ($\mathtt{egcd}(34, 13) = \big((5, -13), 1\big)$)

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

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

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

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

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

$\gcd(m,n) = l_1 \cdot m + l_2 \cdot n$ for some l_1 and l_2 integers.

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

I.e. $\gcd(m,n)$ is an integer linear combination of m, n