gcd

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

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:

[a] Aka (Distributivity).

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 positive integers

Assume $k \mid (m \cdot n)$ ②

Assume $\gcd(k, m) = 1$ ①

RTP: $k \mid n$

From ①: $n \cdot \gcd(k, m) = n$ and by linearity

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

From ② $m \cdot n = l \cdot k$ for some l.

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

$= k \cdot \gcd(n, l)$, by linearity.

$\boxtimes$

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

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

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

By cases consider:

(i) $p \mid m$: Then we are done

(ii) $p \nmid m$: Then $\gcd(p, m) = 1$ and by the previous theorem we have $p \mid n$.

$\boxtimes$

Fields of modular arithmetic

Corollary 66 *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 67

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

Linear integer combination of n in terms of a and b is given by ℓ, k such that $n = \ell \cdot a + k \cdot b$

Extended Euclid's Algorithm

Example 67

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

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

Linear combinations

Definition 68 *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*
>
> $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \quad ;$$
>
> *that is*
>
> $$s \cdot m + t \cdot n = r \quad .$$

Theorem 69 *For all positive integers m and n,*

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

$$\begin{bmatrix} \mathrm{lc}_1(m,n) & \mathrm{lc}_2(m,n) \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = \gcd(m,n) \quad ,$$

can be efficiently computed.

Proposition 70 *For all integers* $\mathfrak{m}$ *and* $\mathfrak{n}$,

1. $\begin{bmatrix} \overset{1}{?_1} & \overset{0}{?_2} \end{bmatrix} \cdot \begin{bmatrix} \mathfrak{m} \\ \mathfrak{n} \end{bmatrix} = \mathfrak{m} \;\wedge\; \begin{bmatrix} \overset{0}{?_1} & \overset{1}{?_2} \end{bmatrix} \cdot \begin{bmatrix} \mathfrak{m} \\ \mathfrak{n} \end{bmatrix} = \mathfrak{n}$; $\checkmark$

Proposition 70 *For all integers* m *and* n,

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

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

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

implies

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

$s_1+s_2 \quad t_1+t_2$

Proposition 70 *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*,* $k \cdot s$ $k \cdot t$

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

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 ) ) )
```

$$1 = \gcd(m,n) = lc_1 \cdot m + lc_2 \cdot n \equiv lc_2 \cdot n \pmod{m} \equiv [lc_2]_m \cdot n \pmod{m}$$

Multiplicative inverses in modular arithmetic

n^{-1} in $\mathbb{Z}_m$

Corollary 74 *For all positive integers* m *and* n*,*

1. $n \cdot lc_2(m,n) \equiv \gcd(m,n) \pmod{m}$, *and*

2. *whenever* $\gcd(m,n) = 1$,

$$\big[lc_2(m,n)\big]_m \text{ is the multiplicative inverse of } [n]_m \text{ in } \mathbb{Z}_m \ .$$

Natural Numbers and mathematical induction

We have mentioned in passing that the natural numbers are generated from zero by succesive increments. This is in fact the defining property of the set of natural numbers, and endows it with a very important and powerful reasoning principle, that of *Mathematical Induction*, for establishing universal properties of natural numbers.

Principle of Induction

Let $P(m)$ be a statement for m ranging over the set of natural numbers $\mathbb{N}$.

If

- the statement $P(0)$ holds, and
- the statement

  $$\forall n \in \mathbb{N}. \; \big(\; P(n) \implies P(n+1) \; \big)$$

  also holds

then

- the statement

  $$\forall m \in \mathbb{N}. \, P(m)$$

  holds.

Binomial Theorem

Theorem 29 *For all* $n \in \mathbb{N}$,

$$\left.(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k \quad . \right] \equiv P(n)$$

PROOF: Idea.

By induction:

~~BASE~~ CASE $(n=0)$:

RTP: $(x+y)^0 \stackrel{?}{=} \sum_{k=0}^{0} \binom{n}{k} \cdot x^{n-k} \cdot y^k$

Now $(x+y)^0 = 1$

and $\sum_{k=0}^{0} \binom{0}{k} \cdot x^{0-k} \cdot y^k = \binom{0}{0} x^{0-0} y^0 = 1$

We are done.

INDUCTIVE STEP:

$\forall n \in \mathbb{N}.\ P(n) \Rightarrow P(n+1)$

Assume $n \in \mathbb{N}$ and

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \qquad (IH)$$

RTP:

$$(x+y)^{n+1} \stackrel{?}{=} \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$$

Scratch work: $(x+y)^{n+1} = (x+y)^n \cdot (x+y)$

By (IH) $(x+y)^{n+1} = (x+y) \cdot \left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \right).$

$$(x+y)^{n+1} = x \cdot \sum_{n=0}^{k} \binom{n}{k} x^{n-k} y^{k} + y \cdot \sum_{n=0}^{k} \binom{n}{k} x^{n-k} y^{k}$$

$$= \sum_{n=0}^{k} \binom{n}{k} x^{n+1-k} y^{k} + \sum_{n=0}^{k} \binom{n}{k} x^{n-k} y^{k+1}$$

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

conjecture

(Provable by induction)

$$\sum_{k=0}^{n+1} \left[\binom{n}{k} + \binom{n}{k-1} \right] \cdot x^{n+1-k} y^{k}$$

RTP

$$(x+y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^{k}$$

Principle of Induction

from basis ℓ

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.

If

- $P(\ell)$ holds, and
- $\forall\, n \geq \ell$ in $\mathbb{N}$. $\big(P(n) \implies P(n+1) \big)$ also holds

then

- $\forall\, m \geq \ell$ in $\mathbb{N}$. $P(m)$ holds.

Principle of Strong Induction

from basis ℓ and Induction Hypothesis $P(m)$.

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.
If both

- $P(\ell)$ and
- $\forall\, n \geq \ell$ in $\mathbb{N}.\ \Big(\ \big(\forall\, k \in [\ell..n].\, P(k)\big) \implies P(n+1)\ \Big)$

hold, then

- $\forall\, m \geq \ell$ in $\mathbb{N}.\, P(m)$ holds.

Fundamental Theorem of Arithmetic

Proposition 76 *Every positive integer greater than or equal 2 is a prime or a product of primes.*

PROOF: $\forall n \geq 2.\ P(n)$ $P(n) \equiv$ n is prime or a product of prime

By strong induction:

BASE CASE $P(2)$: But 2 is prime.

IND. STEP : $\forall n \geq 2$. Assume $P(k)$ for $2 \leq k \leq n$ (SIH)

RTP $P(n+1)$:

By cases: (i) $n+1$ is prime — Then we are done.

(ii) $n+1$ is not prime —

$n+1 = a \cdot b$ for $2 \leq a, b \leq n$

By (SIH): $P(a)$ and $P(b)$ hold

That is, a is a prime or a product of primes and so is b.

Therefore $n+1$ is a product of primes. $\boxtimes$

Theorem 77 (Fundamental Theorem of Arithmetic) *For every positive integer* n *there is a unique finite ordered sequence of primes* $(p_1 \leq \cdots \leq p_\ell)$ *with* $\ell \in \mathbb{N}$ *such that*

$$n = \prod(p_1, \ldots, p_\ell) \quad .$$

PROOF: