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, $d \mid m \;\wedge\; d \mid n \implies d \mid k$.

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

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

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

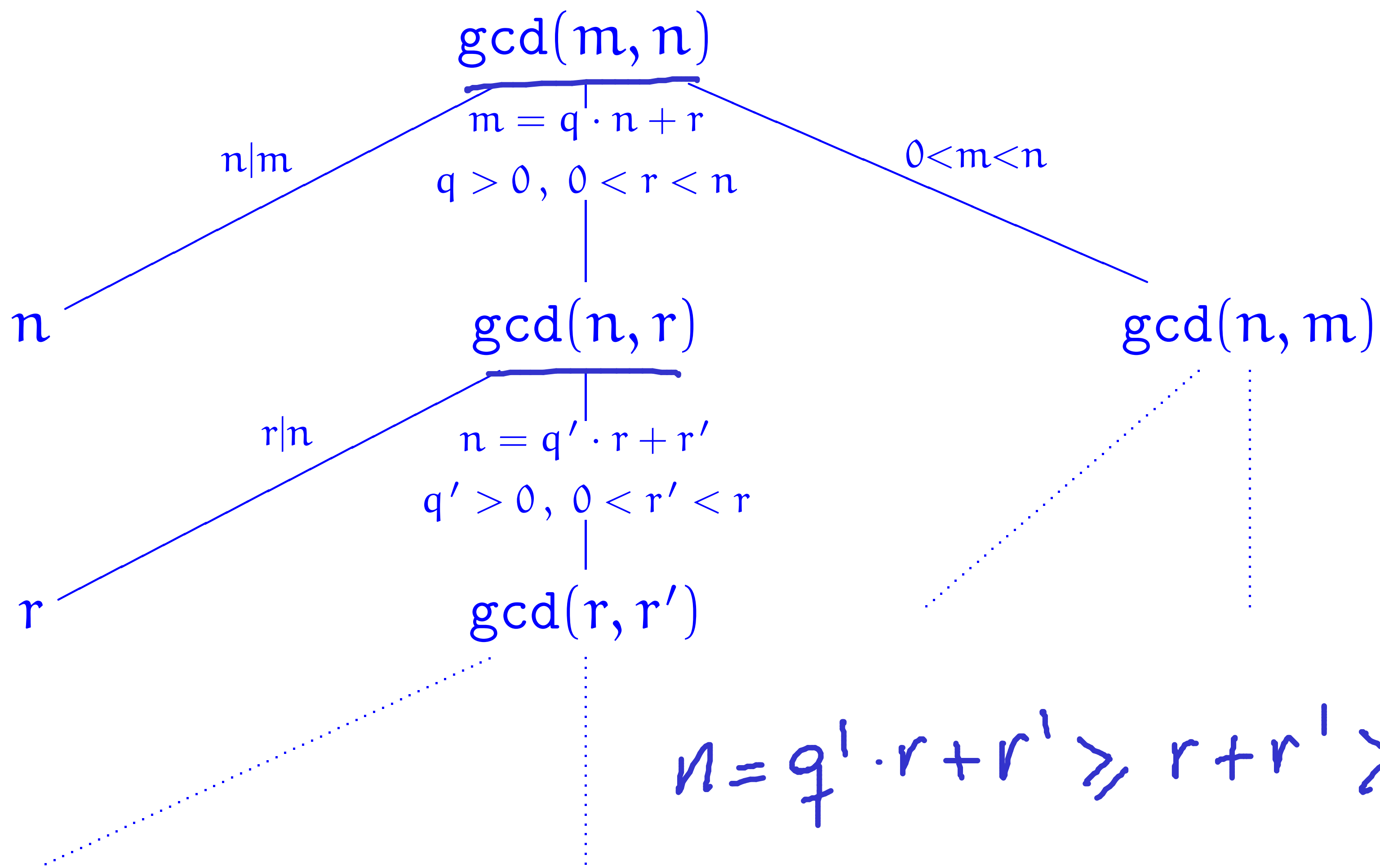
$$\mathrm{CD}(m,n) = \begin{cases} \mathrm{D}(n) & \text{, } \textit{if } n \mid m \\ \mathrm{CD}\big(n, \mathrm{rem}(m,n)\big) & \text{, } \textit{otherwise} \end{cases}$$

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



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

$$r' < n/2$$

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

1. ***(Commutativity)*** $\gcd(m, n) = \gcd(n, m)$, $\underline{\gcd}(l, m, n)$ $=$
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: (1) $\underline{CD}(m,n) = \underline{CD}(n,m)$

$$\begin{array}{ccc} \underline{CD}(m,n) & = & \underline{CD}(n,m) \\ \| & & \| \\ \underline{D}(\underline{gcd}(m,n)) & & \underline{D}(\underline{gcd}(n,m)) \end{array}$$

$$\Downarrow$$

$$\underline{gcd}(m,n) = \underline{gcd}(n,m).$$

[a] Aka (Distributivity).

(3) $\gcd(\ell\cdot m, \ell\cdot n) \overset{(*)}{=} \ell\cdot \gcd(m,n)$.

$\gcd(\ell\cdot m, \ell\cdot n)$ is characterised as the unique k such that

- $k \mid (\ell\cdot m) \wedge k \mid (\ell\cdot n)$
- $\forall d.\ d \mid (\ell\cdot m) \wedge d \mid (\ell\cdot n) \Rightarrow d \mid k$.

To show (*) we need prove that:

- $\ell\cdot\gcd(m,n) \mid (\ell m) \wedge \ell\cdot\gcd(m,n) \mid (\ell\cdot n)$
- $\forall d.\ d \mid (\ell m) \wedge d \mid (\ell n) \Rightarrow d \mid \ell\cdot\gcd(m,n)$

Exercise: use that $\gcd(m,n) \mid m \wedge \gcd(m,n) \mid n$

use that $\forall x.\ x \mid m \wedge x \mid n \Rightarrow x \mid \gcd(m,n)$.

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 positive integers.
Assume $k \mid (m \cdot n)$ and $ik + jm = 1$ for some int. i, j.
So $n = n \cdot i \cdot k + n \cdot j \cdot m$ and we are done. $\boxtimes$

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:

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

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

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

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 194.

Theorem 87 *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 88 *For all integers* m *and* n,

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

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

$$\begin{bmatrix} \overset{s_1+s_2}{\cancel{?_1}} & \overset{t_1+t_2}{\cancel{?_2}} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2$$;

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,

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

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

Example: $\mathrm{gcd}(m,n) \rightsquigarrow \mathrm{gcd}(((1,0),m),((0,1),n))$

gcd

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

coefficients expressing r as an int. lin. comb. of m and n

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
```

Terminate with $((lc_1, lc_2), \underline{gcd}(m,n))$

$\underline{gcd}(m,n) = lc_1 \cdot m + lc_2 \cdot n$

```
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,

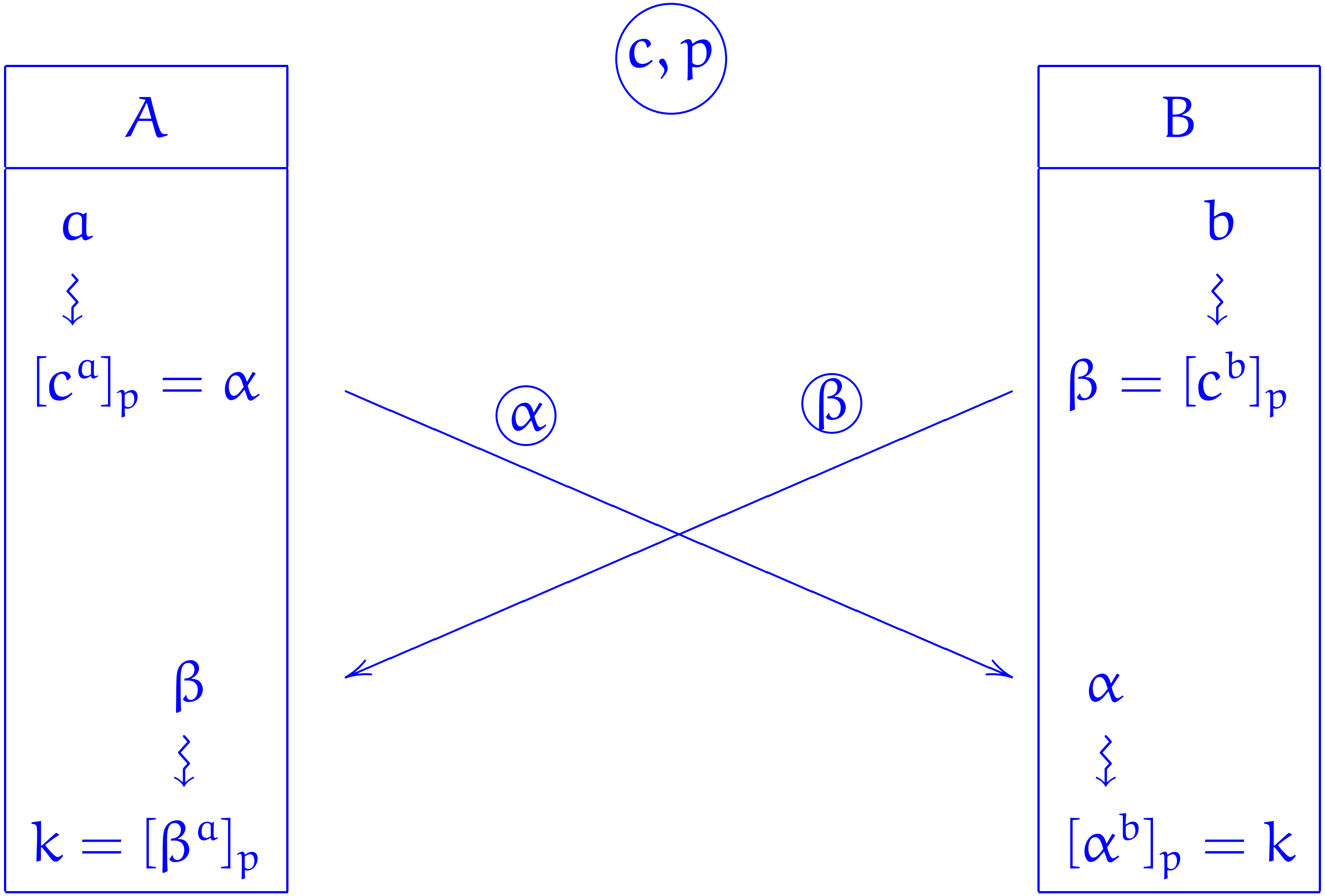
1. $n \cdot \mathrm{lc}_2(m,n) \equiv \gcd(m,n) \pmod{m}$, *and*

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

$$\big[\mathrm{lc}_2(m,n)\big]_m \text{ is the multiplicative inverse of } [n]_m \text{ in } \mathbb{Z}_m \ .$$

Diffie-Hellman cryptographic method

Shared secret key



Key exchange

Mathematical modelling:

- Encrypt and decrypt by means of modular exponentiation:

$$[k^e]_p \qquad\qquad [\ell^d]_p$$

- Encrypting-decrypting have no effect:

By Fermat's Little Theorem,

$$k^{1+c\cdot(p-1)} \equiv k \pmod{p}$$

for every natural number c, integer k, and prime p.

- Consider d, e, p such that $e \cdot d = 1 + c \cdot (p-1)$; equivalently,

$$d \cdot e \equiv 1 \pmod{p} \; .$$

$p-1$

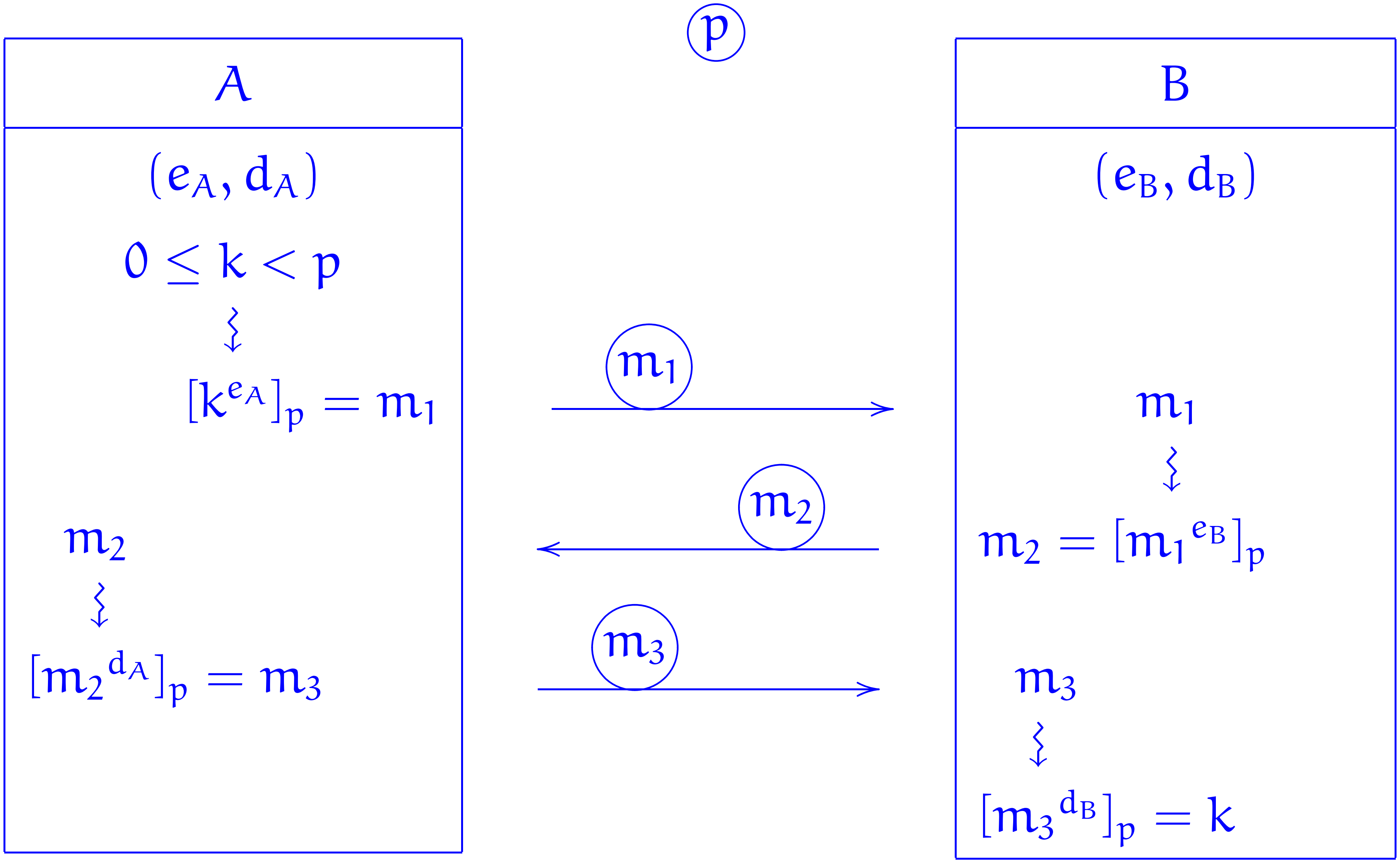
Lemma 93 *Let* p *be a prime and* e *a positive integer with* $\gcd(p-1, e) = 1$. *Define*

$$d = \left[\, \mathrm{lc}_2(p-1, e) \,\right]_{p-1} \quad .$$

Then, for all integers k*,*

$$(k^e)^d \equiv k \pmod{p} \quad .$$

PROOF:


p
A
B
(e_A, d_A)
(e_B, d_B)
$0 \leq k < p$
$[k^{e_A}]_p = m_1$
m_1
m_1
m_2
$m_2 = [{m_1}^{e_B}]_p$
m_2
$[{m_2}^{d_A}]_p = m_3$
m_3
m_3
$[{m_3}^{d_B}]_p = k$