# 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:

**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 and n be pos. int. Let p be a prime.

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

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

By cases:

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

(2) If $p \nmid m$ then $\gcd(p, m) = 1$ and by the previous Theorem we have $p \mid n$ and we are done. ☒

Remark: We proved FLT: $i^p \equiv i \pmod p$

Claim: it implies $i^{p-1} \equiv 1 \pmod p$

for $i \not\equiv 0 \pmod p$

## 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.*

Assume $i^p \equiv i \pmod p$. Then $i^p - i = (i^{p-1} - 1)\, i$ is a multiple of $p$ but further assume $p \nmid i$ we have by Euclid's Theorem $p \mid i^{p-1} - 1$, that is,

$i^{p-1} \equiv 1 \pmod p$.

Def $m$ and $n$ are said to be coprimes whenever $\gcd(m,n)=1$.

# Extended Euclid's Algorithm

## Example 67

remainders.

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

Def An integer linear combination of k m
Terms of m and n expresses it as $i \cdot m + j \cdot n$ for some $i, j$.

# Extended Euclid's Algorithm

remainders as integer linear combinations of the pair

**Example 67**

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

on which we calculate the gcd.

| | | | | |
|---|---|---|---|---|
| $\gcd(34, 13)$ | $8 =$ | $34$ | $-2\cdot$ | $13$ |
| $= \gcd(13, 8)$ | $5 =$ | $13$ | $-1\cdot$ | $8$ |
| $= \gcd(8, 5)$ | $3 =$ | $8$ | $-1\cdot$ | $5$ |
| $= \gcd(5, 3)$ | $2 =$ | $5$ | $-1\cdot$ | $3$ |
| $= \gcd(3, 2)$ | $1 =$ | $3$ | $-1\cdot$ | $2$ |

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

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

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

The gcd(m,n) is an integer linear combination of m and n.

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

# 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. $\mathrm{gcd}(m, n)$ *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*

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

*can be efficiently computed.*

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

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

**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* $s_1+s_2$

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

$t_1+t_2$

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

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

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*

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

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

   ks kt

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

# 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       [s2 t2]      [s1-q s2  t1-q t2]
        else  gcditer(  c ,                 √  r  )
      end
  in
    gcditer([1 0]  m  ,[0 1]  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 ) ) )
```

Proof of (1)

$\gcd(m,n) = l_1 \cdot m + l_2 \cdot n$

## Multiplicative inverses in modular arithmetic

$l_2 \cdot n - \gcd(m,n)$ is a multiple of $m$

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

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

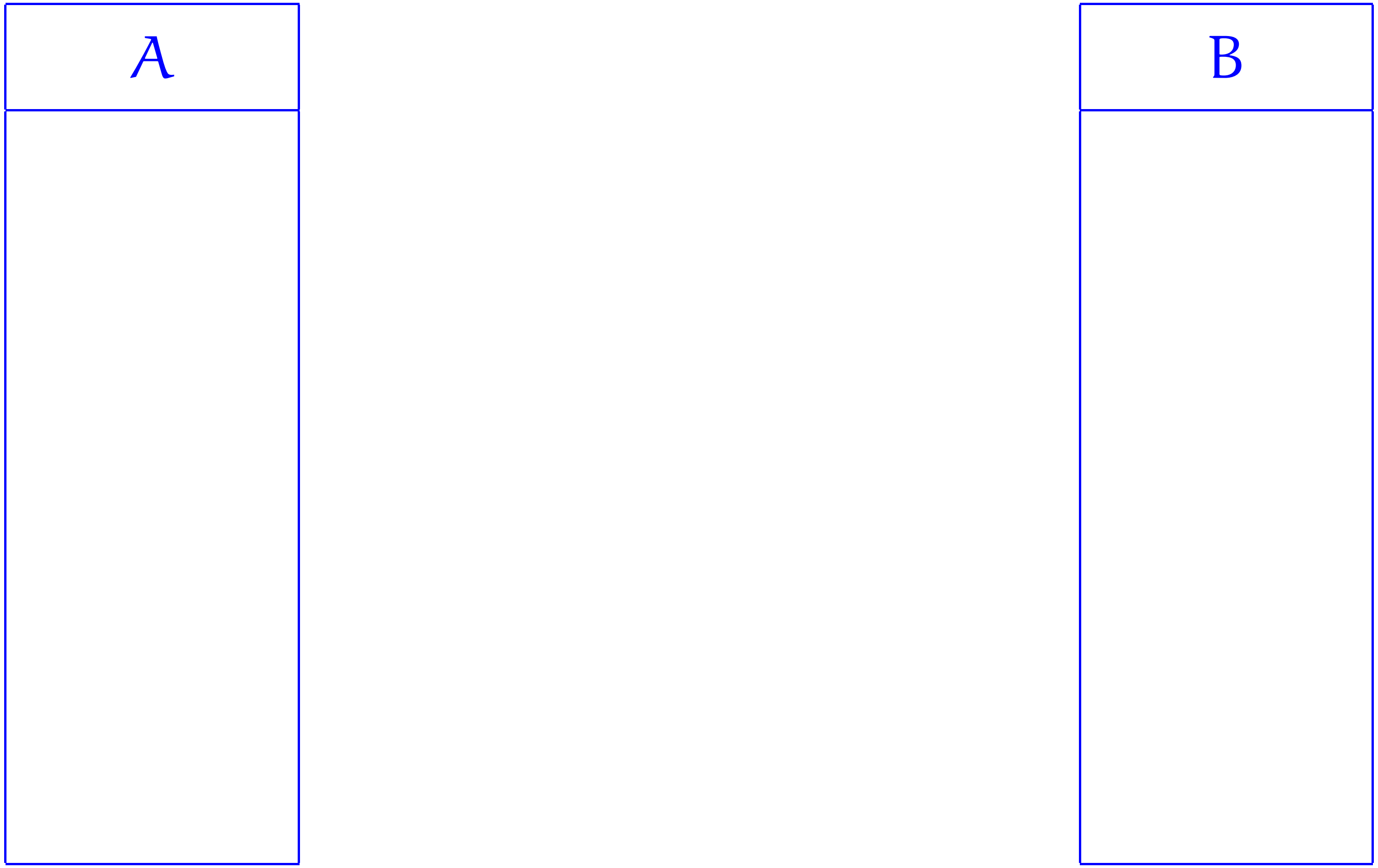
$$\big[\mathrm{lc}_2(m,n)\big]_m \text{ is the multiplicative inverse of } [n]_m \text{ in } \mathbb{Z}_m \ .$$

when $\gcd(m,n)=1$, $n \cdot \mathrm{lc}_2(m,n) \equiv 1 \pmod{m}$

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

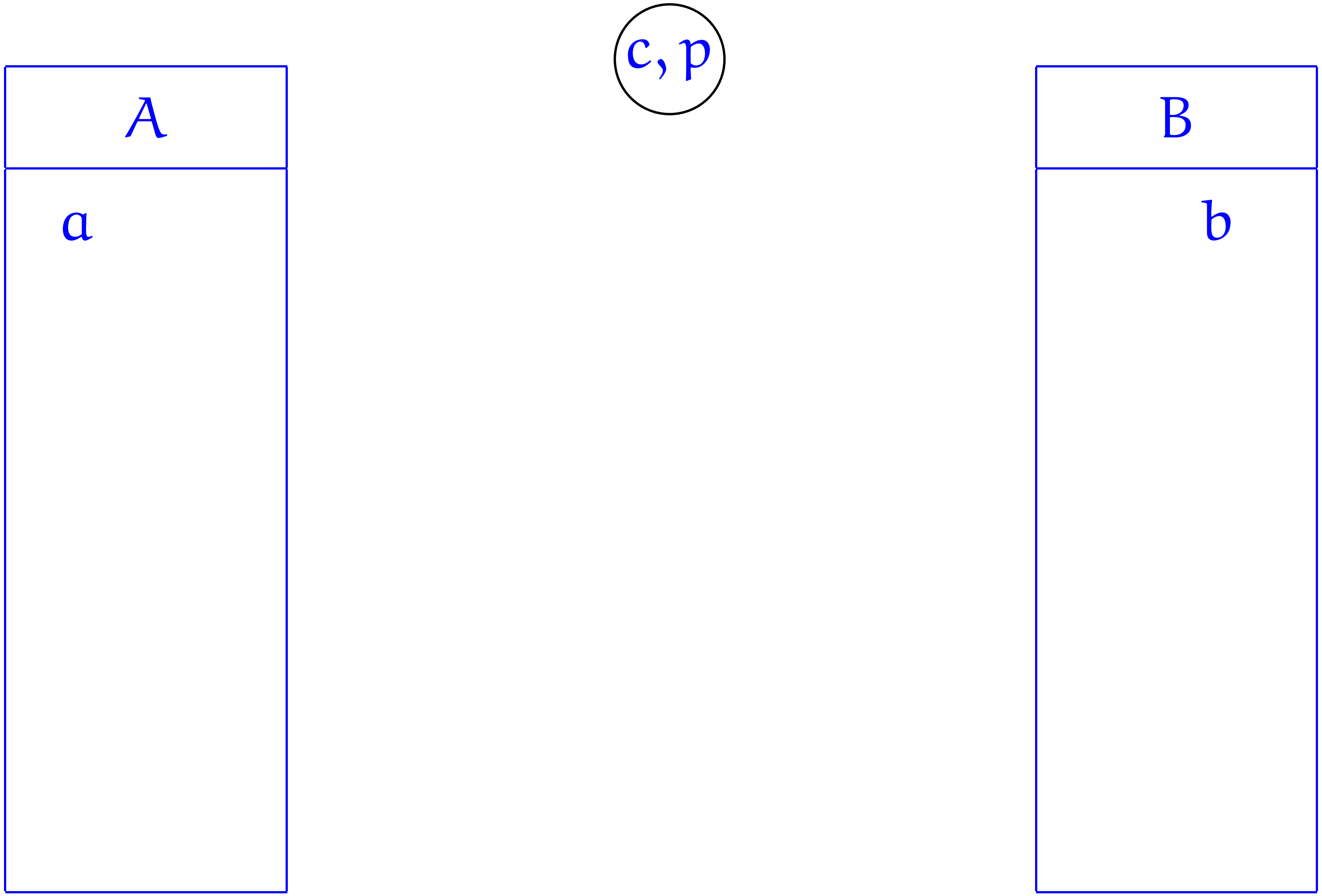
# Diffie-Hellman cryptographic method

## Shared secret key



# Diffie-Hellman cryptographic method

## Shared secret key



# Diffie-Hellman cryptographic method

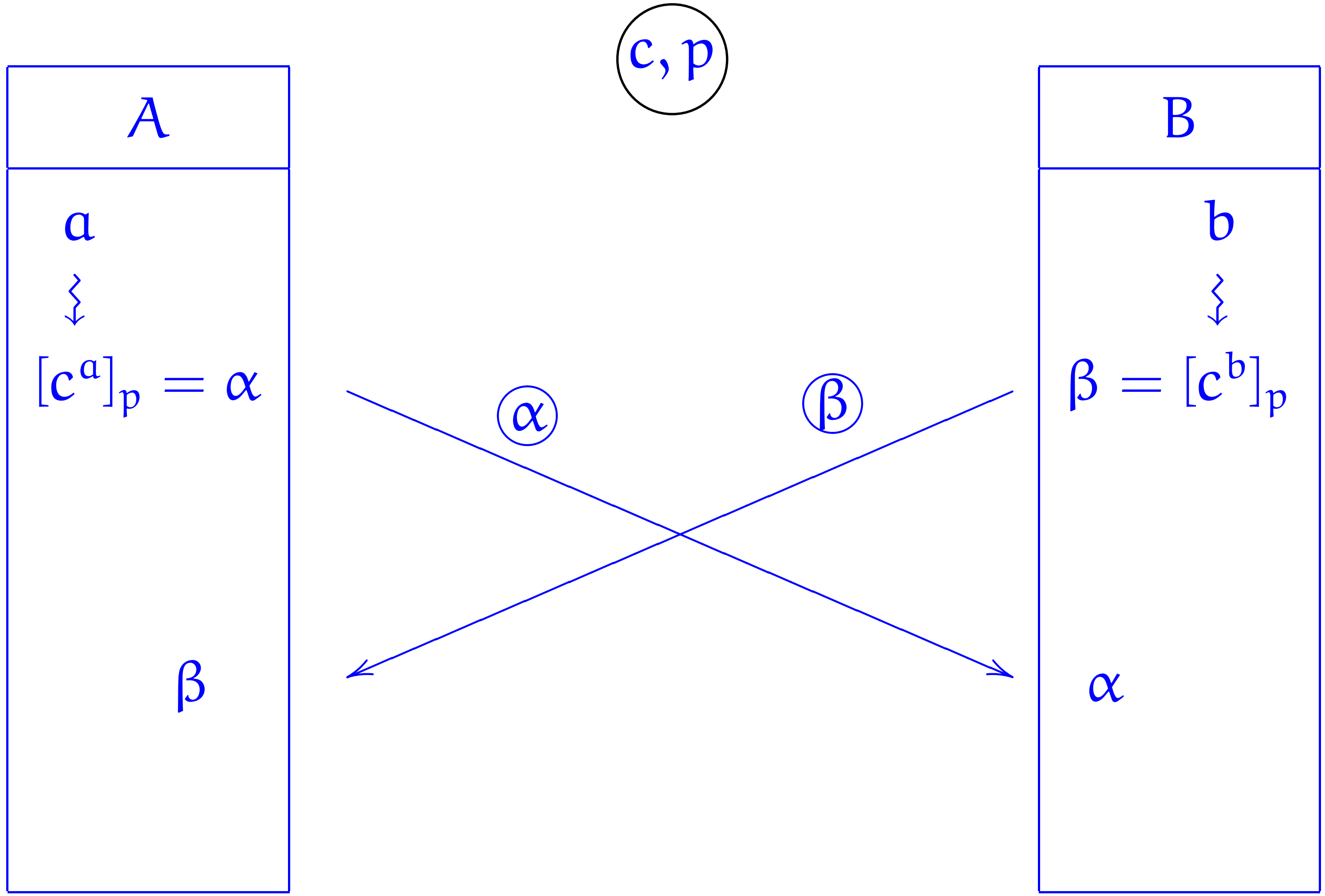
## Shared secret key

$c, p$

| A | B |
|---|---|
| $a$ | $b$ |
| $\downarrow$ | $\downarrow$ |
| $[c^a]_p = \alpha$ | $\beta = [c^b]_p$ |

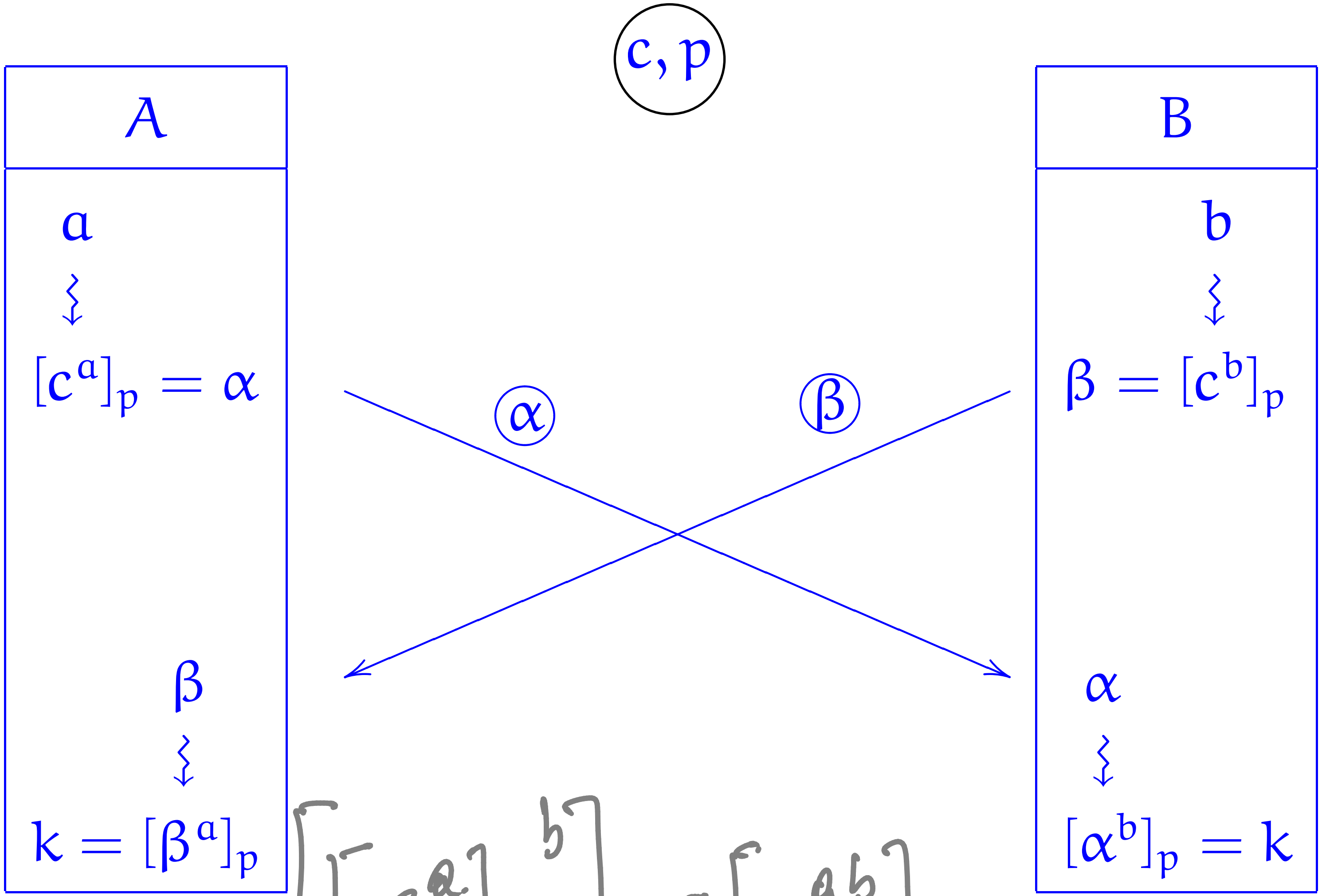
# Diffie-Hellman cryptographic method

## Shared secret key



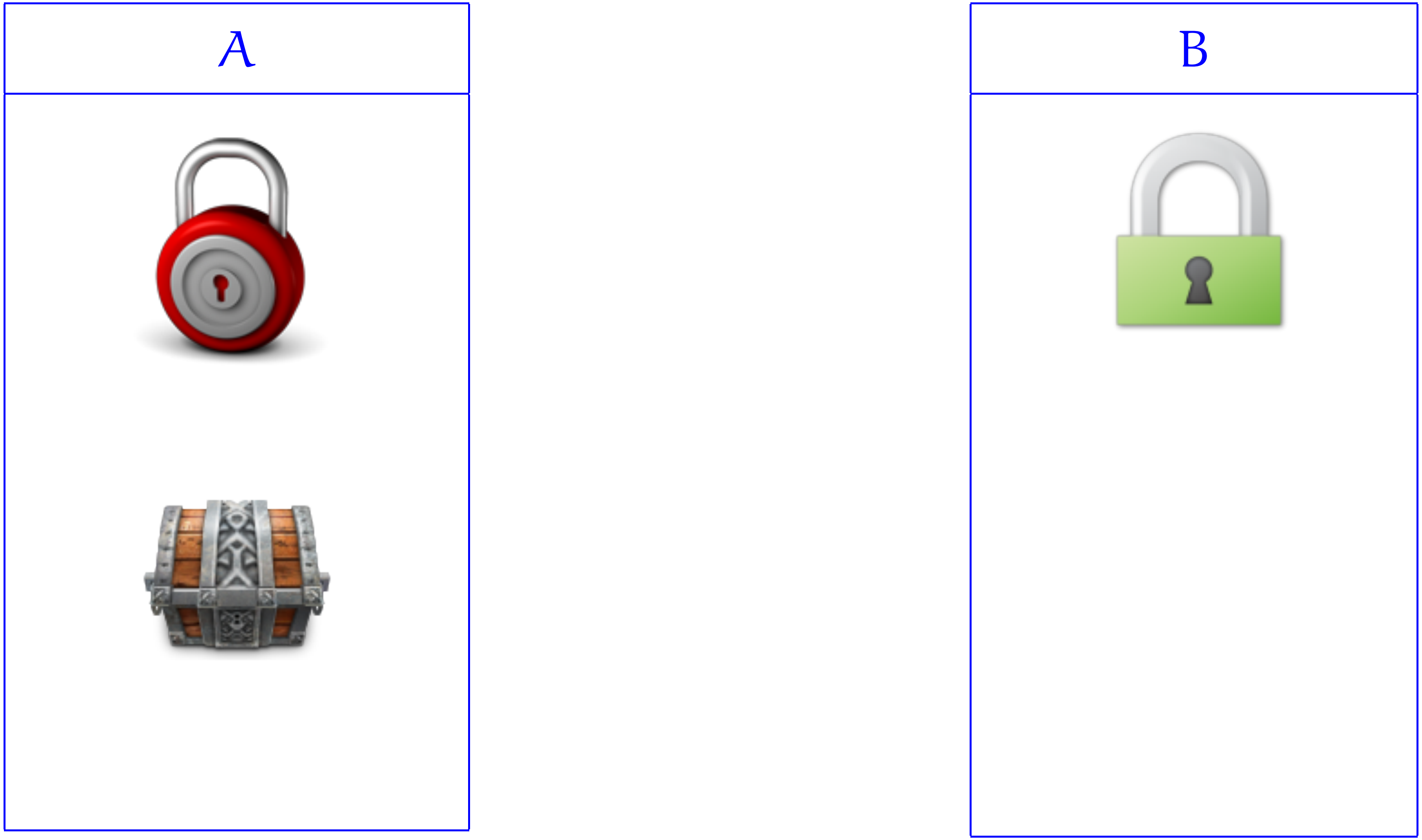
# Diffie-Hellman cryptographic method

## Shared secret key




$$[[c^a]_p^{\,b}]_p = [c^{ab}]_p = [[c^b]_p^{\,a}]_p$$

# Diffie-Hellman Key Exchange.



A

B

A

B

| A |
| --- |
| |

| B |
| --- |
|  |

| A | B |
| --- | --- |
|  | |

| A | B |
| --- | --- |
|   | |

A

B

A

B

$l_1 = \underline{lc_1}(p-1, e)$

$l_2 = \underline{lc_2}(p-1, e)$

## Key exchange

**Lemma 75** *Let* $p$ *be a prime and* $e$ *a positive integer with* $\gcd(p-1, e) = 1$. *Define*

$$d = \left[ \, lc_2(p-1, e) \, \right]_{p-1} \quad .$$

*Then, for all integers* $k$*,*

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

PROOF: Let $p$ be a prime $e$ a pos. int.

Assume $\gcd(p-1, e) = 1$

Then: $(p-1) \cdot l_1 + e \cdot l_2 = 1$ for some int. $l_1$ and $l_2$.

Rem:
Integer linear combinations.

$$r = i \cdot m + j \cdot n \qquad (*)$$

$$= (i + \ell n) m + (j - \ell m) n \quad \forall \text{ int } \ell$$

---

As $(p-1)\, l_1 + e\, l_2 = 1$

By $(*)$ it follows that

$$(p-1) \cdot \ell + e \cdot [l_2]_{p-1} = 1$$

for a non-positive int. $\ell$.

So $e \cdot d = 1 + (p-1) \cdot \ell'$ for some nat $\ell'$

So $(k^e)^d = k^{ed} = k^{1+(p-1)\cdot l'}$

$= k \cdot (k^{p-1})^{l'}$ , by FLT.

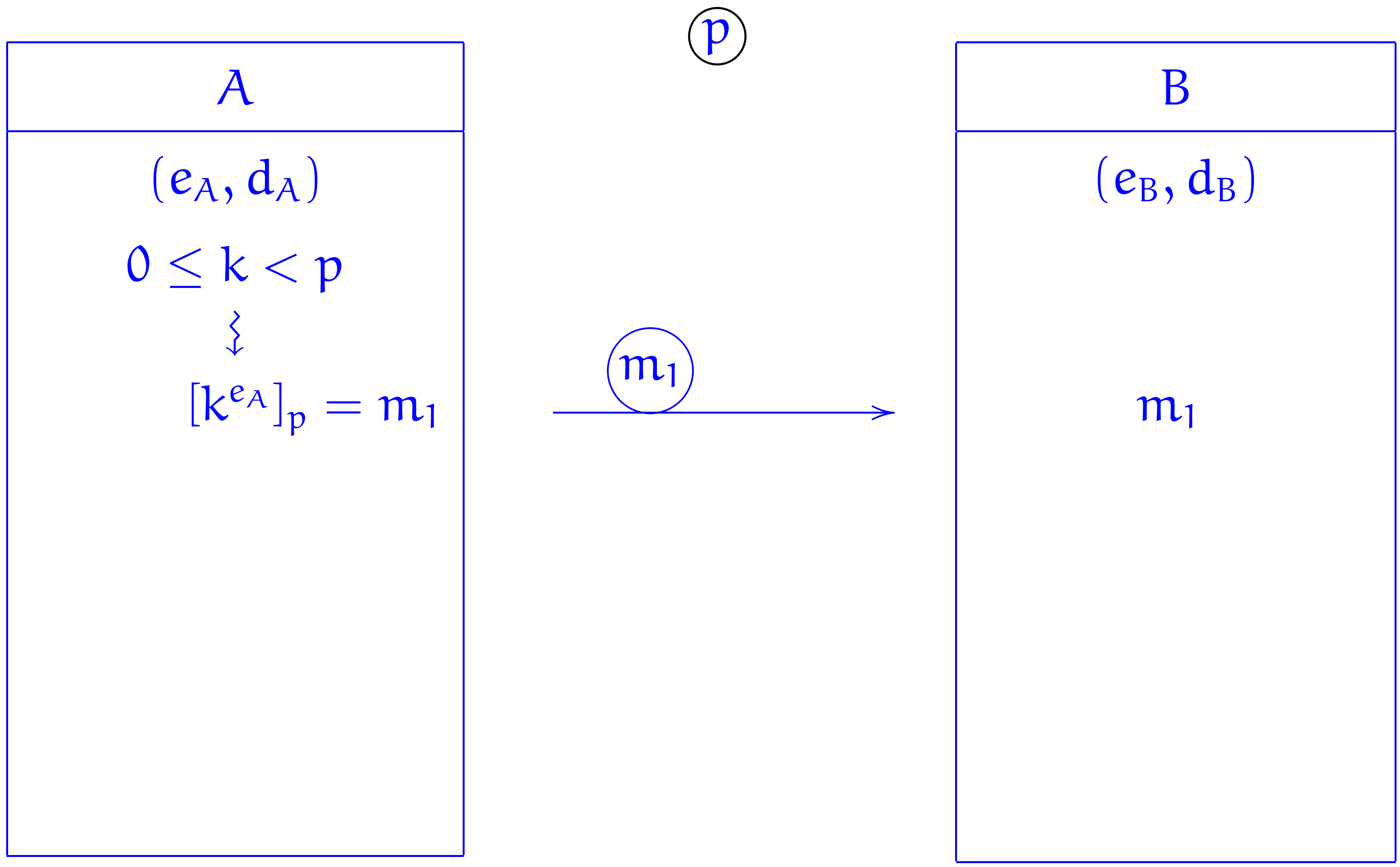
$\equiv k \cdot 1^{l'} = k \pmod{p}$

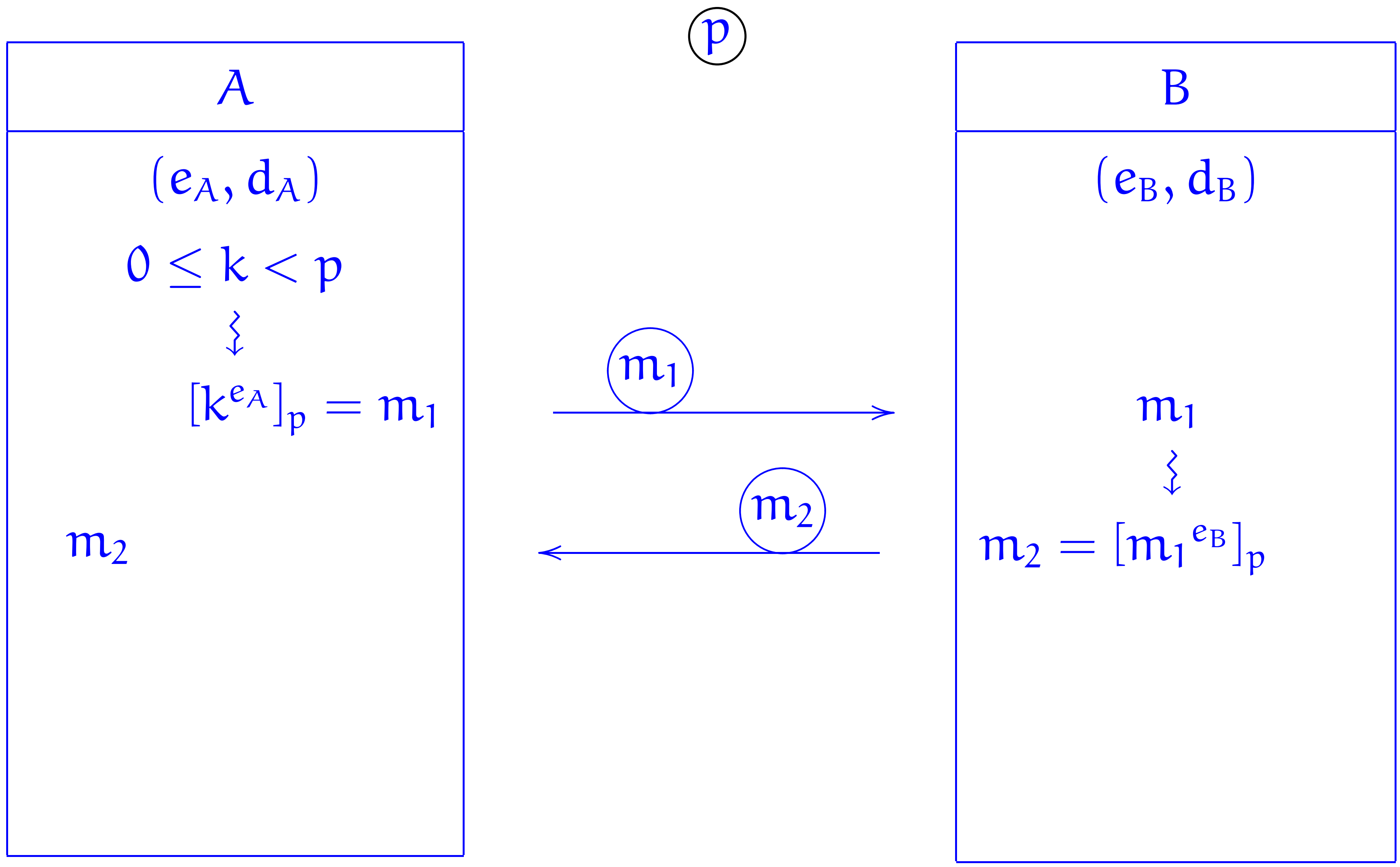
$\boxtimes$

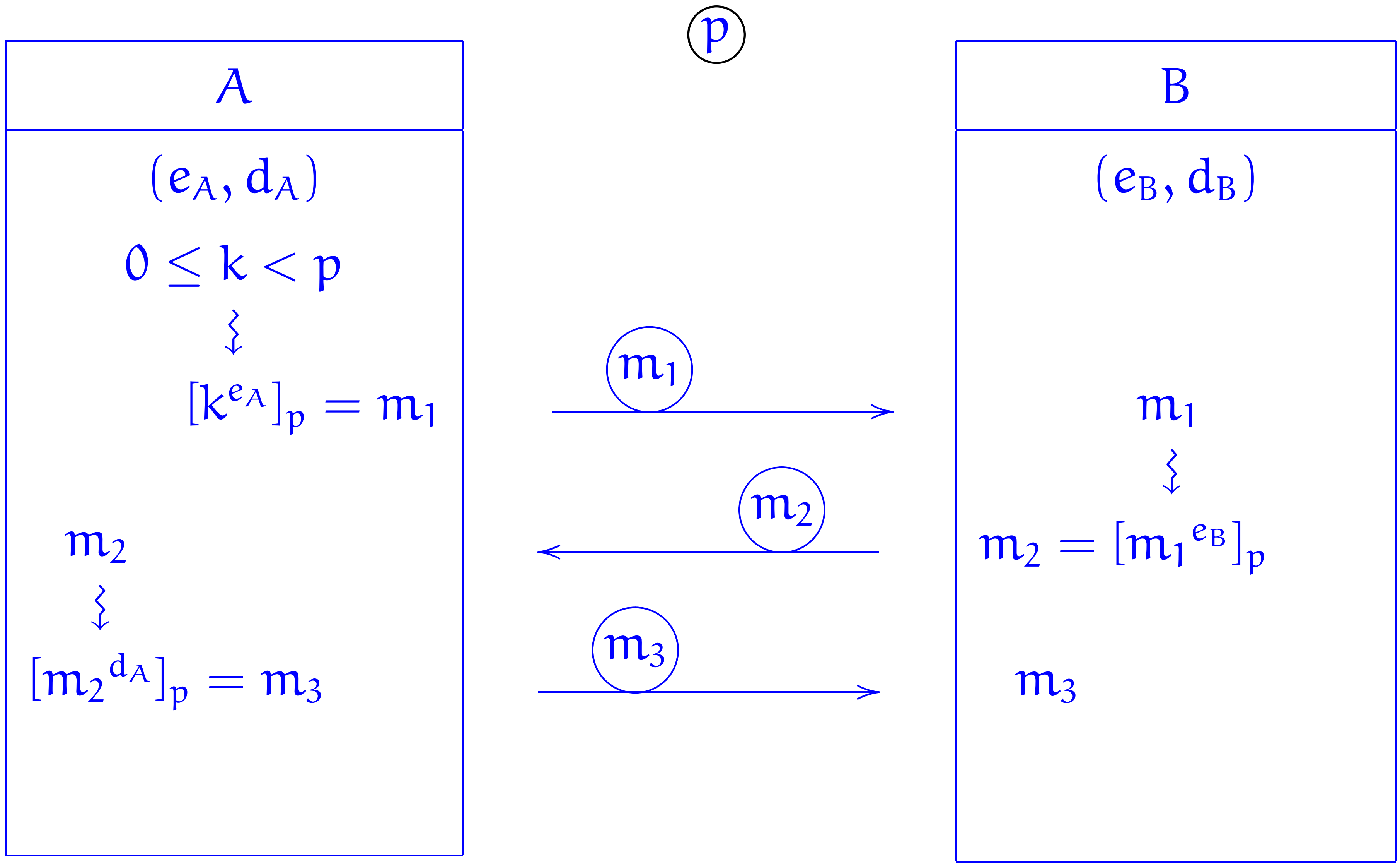
| A | B |
|---|---|
| | |

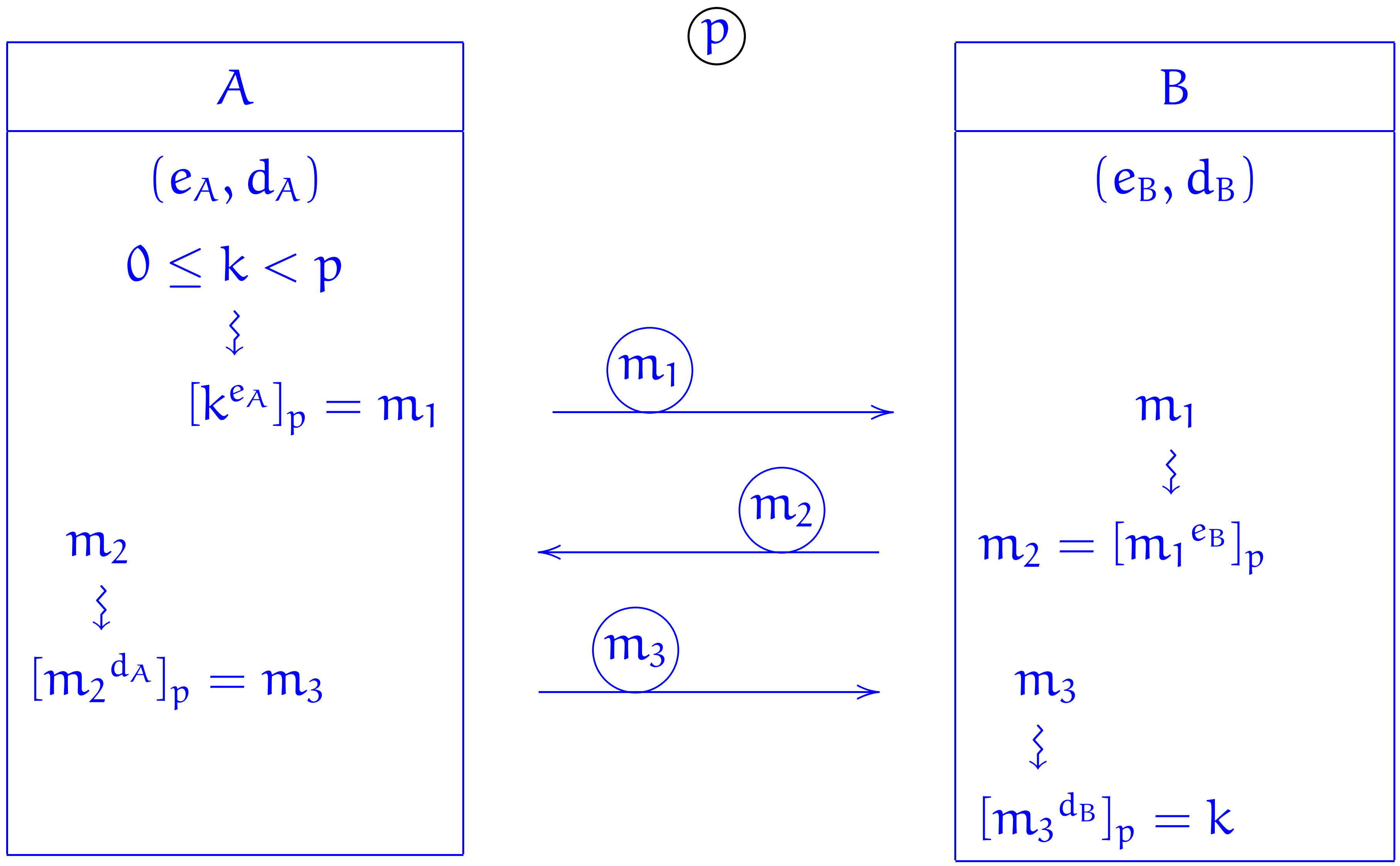
$\textcircled{p}$

| A | B |
| --- | --- |
| $(e_A, d_A)$ | $(e_B, d_B)$ |
| $0 \leq k < p$ | |


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


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


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


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