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: Assume $k \mid m \cdot n$, i.e. $m \cdot n = k \cdot i$ for nat. i.
& $\gcd(k, m) = 1$. By theorem.

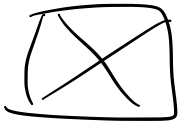
$$\gcd(n \cdot k, n \cdot m) = n$$

$$\therefore \gcd(n \cdot k, i \cdot k) = n$$

$\therefore$ By theorem,

$$k \cdot \gcd(n, i) = n.$$

$$\therefore k \mid n.$$



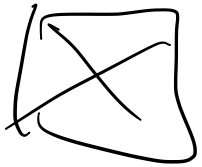
Corollary 64 (Euclid's Theorem) *For positive integers* m *and* n*, and prime* p*, if* $p \mid (m \cdot n)$ *then* $p \mid m$ *or* $p \mid n$*.*

Now, the second part of Fermat's Little Theorem follows as a corollary of the first part and Euclid's Theorem.

PROOF: Assume $p \mid m \cdot n$. If $p \mid m$ we are done. Otherwise $p \nmid m$.

$\therefore \gcd(p, m) = 1$

By Lemma 63, $p \mid n$.



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*.*

$\gcd(m,n) = \ell_1 \cdot m + \ell_2 \cdot n$ for int. ℓ_1, ℓ_2

Extended Euclid's Algorithm

Example 67

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

Extended Euclid's Algorithm

Example 67

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

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

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

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

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

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

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

Theorem 69 *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*

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

can be efficiently computed.

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

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

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

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

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

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

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,

   $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \ \textit{implies} \ \begin{bmatrix} ?_1' & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \ .$$

gcd

```
fun  gcd( m , n )
= let
    fun  gcditer(          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 ) ) )
```

Have $\gcd(m,n) = lc_1(m,n) \cdot m + lc_2(m,n) \cdot n$

Multiplicative inverses in modular arithmetic

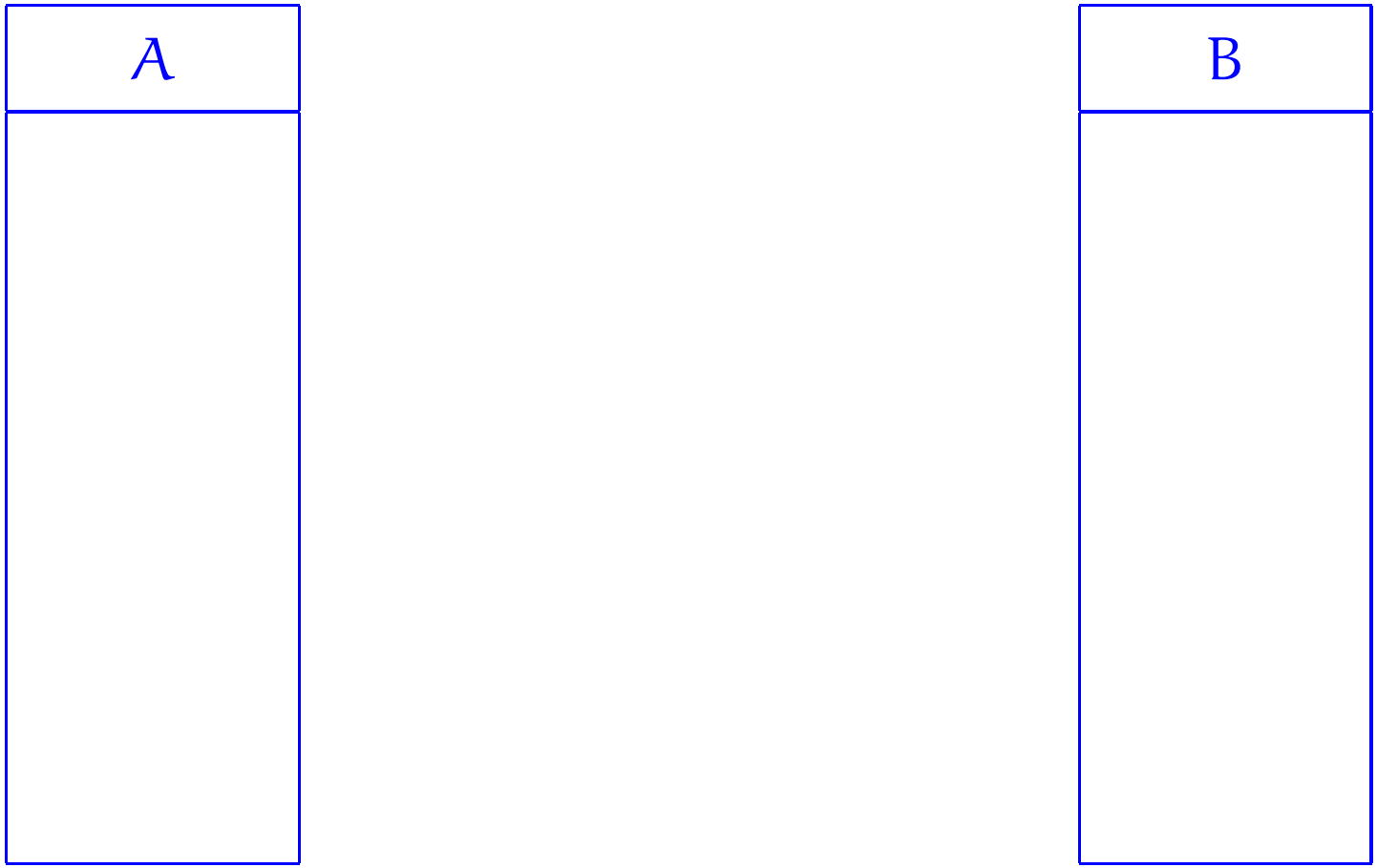
Corollary 74 *For all positive integers* m *and* n*,*

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* $\mathbb{Z}_{\mathrm{m}}$.

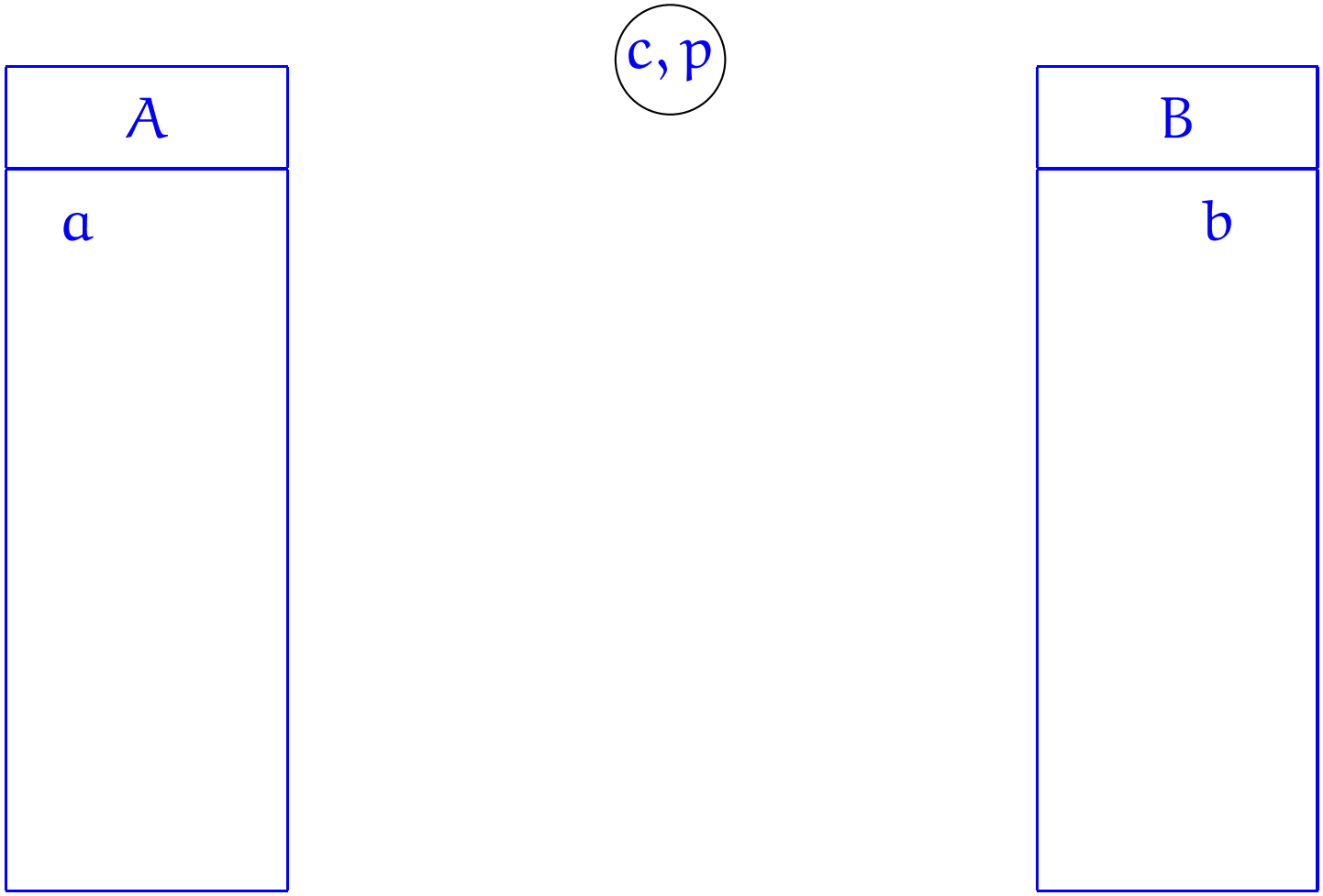
Diffie-Hellman cryptographic method

Shared secret key



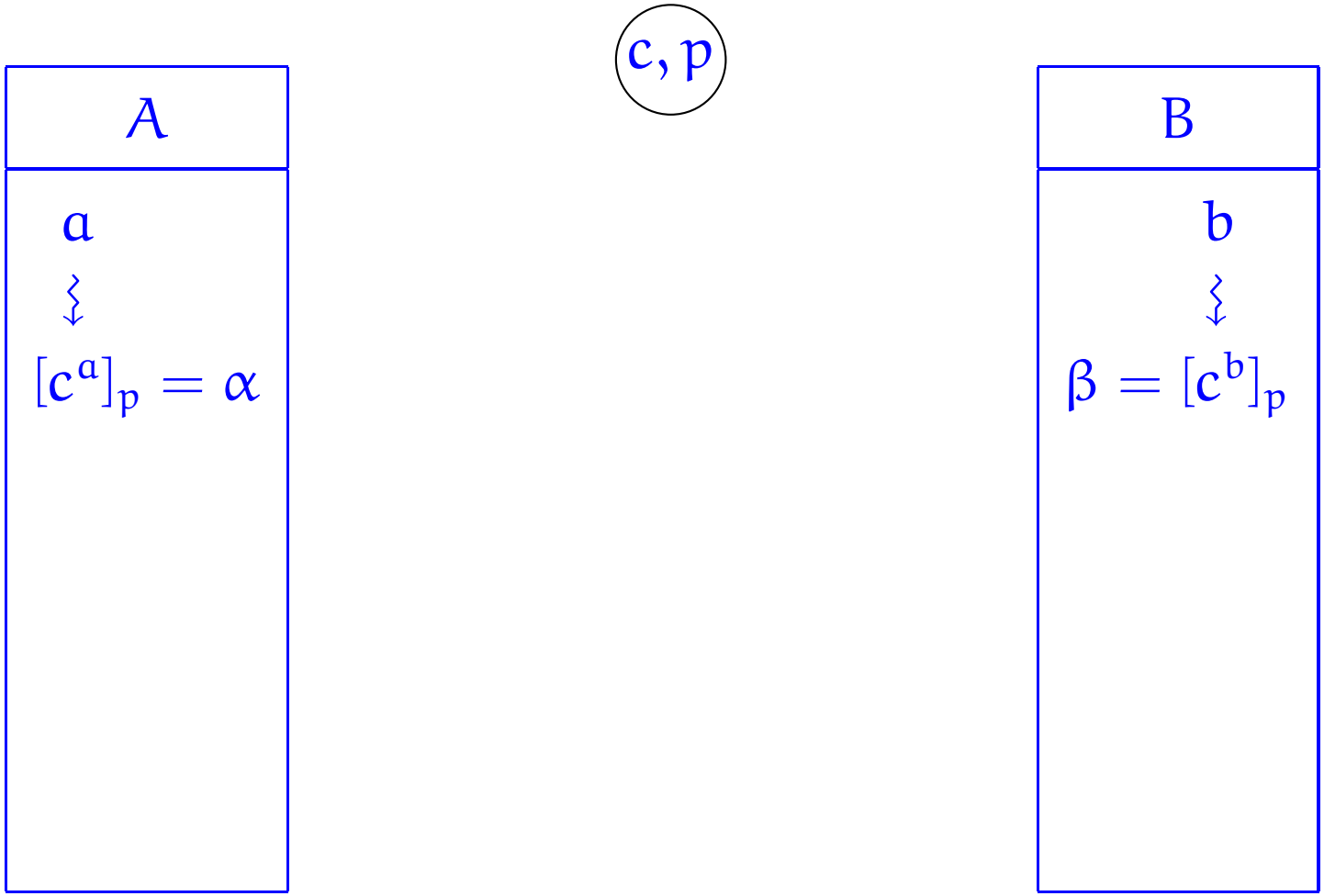
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

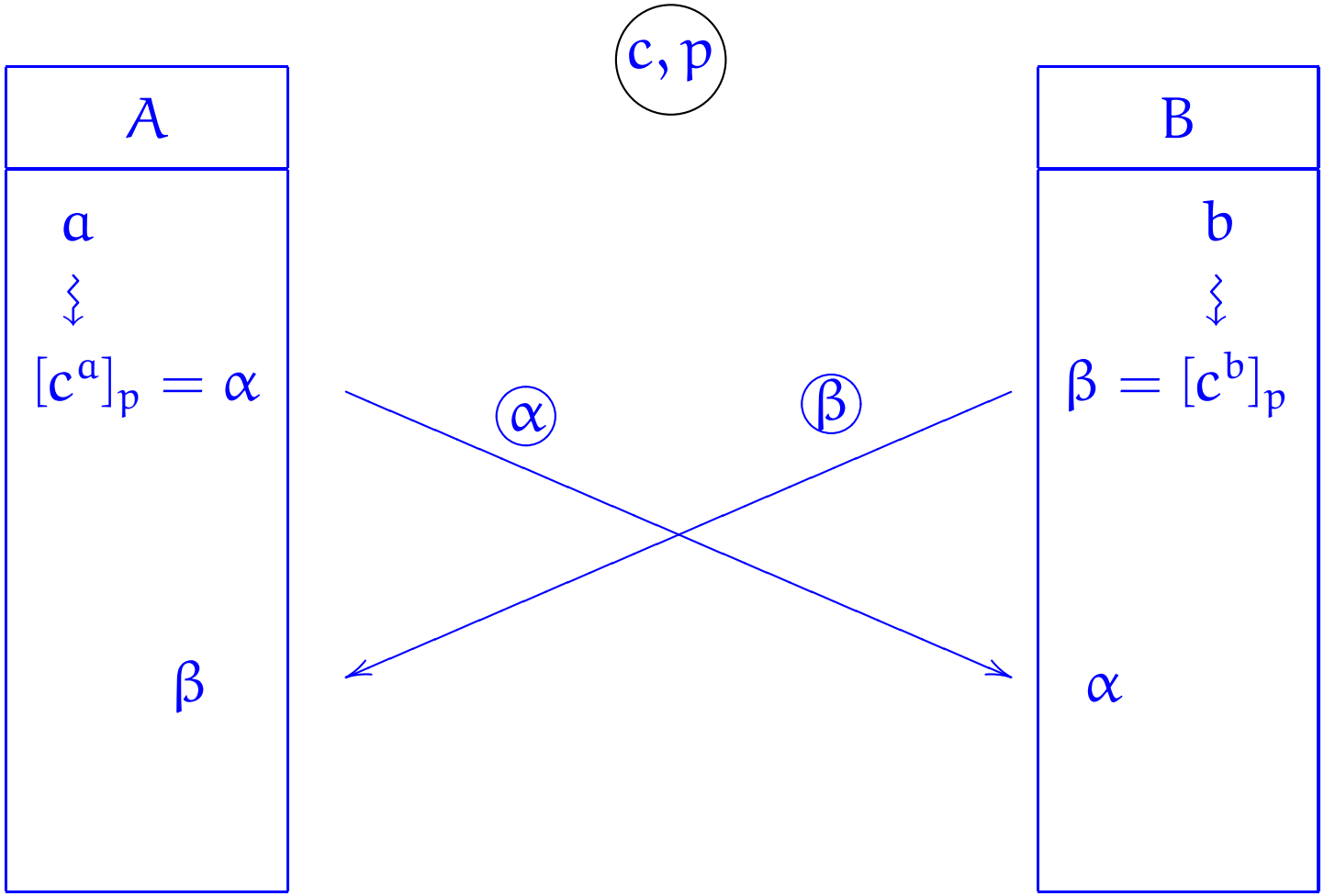
Shared secret key



Assumes discrete logarithm $\log_c$ is hard mod p — take c primitive root mod p.

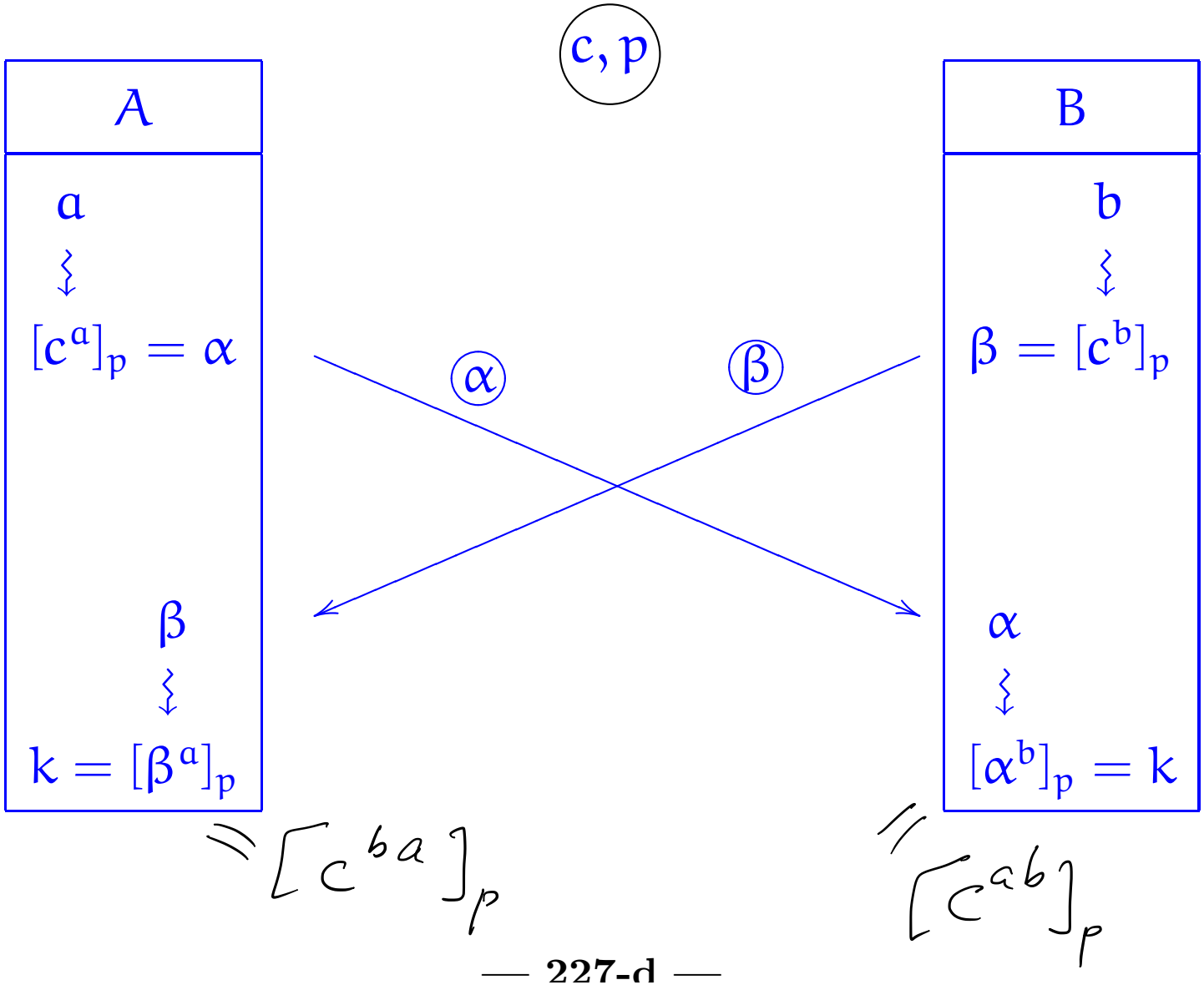
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

Shared secret key



Key exchange

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

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

Then, for all integers k,

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

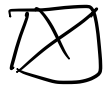
PROOF:

$1 = \gcd(p-1, e) = \mathrm{lc}_1(p-1, e) \cdot (p-1) + \mathrm{lc}_2(p-1, e) \cdot e$

$\therefore \; d \cdot e \equiv \mathrm{lc}_2(p-1, e) \cdot e \equiv 1 \pmod{(p-1)}$.

$\therefore \; d \cdot e = c \cdot (p-1) + 1$ for c nat. no.

$\therefore \; (k^e)^d = k^{d \cdot e} = k^{c \cdot (p-1) + 1} = k \cdot (k^c)^{(p-1)} \equiv k \pmod{p}$.



A

B

A

B

A

B

A

B

A

B

A

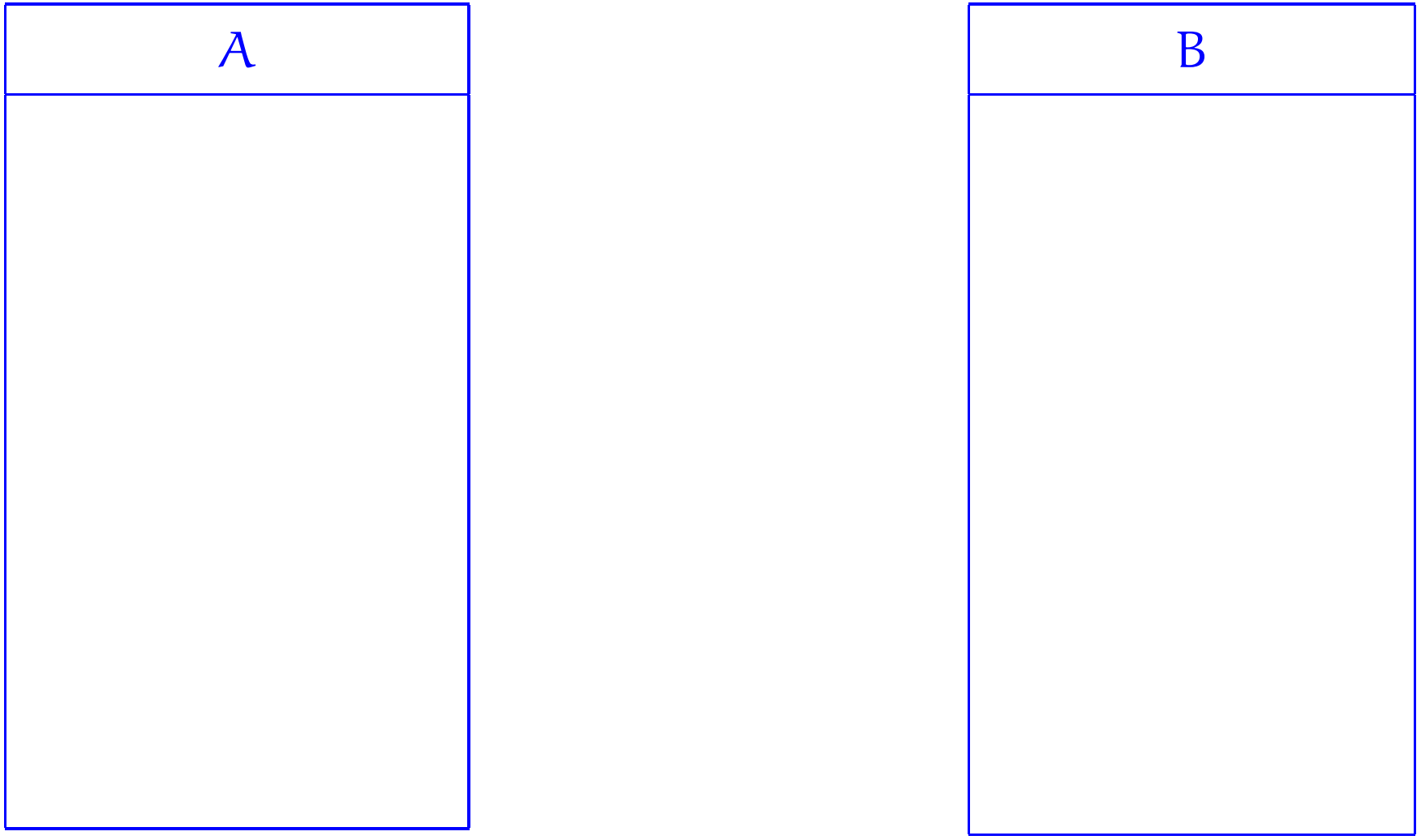
B

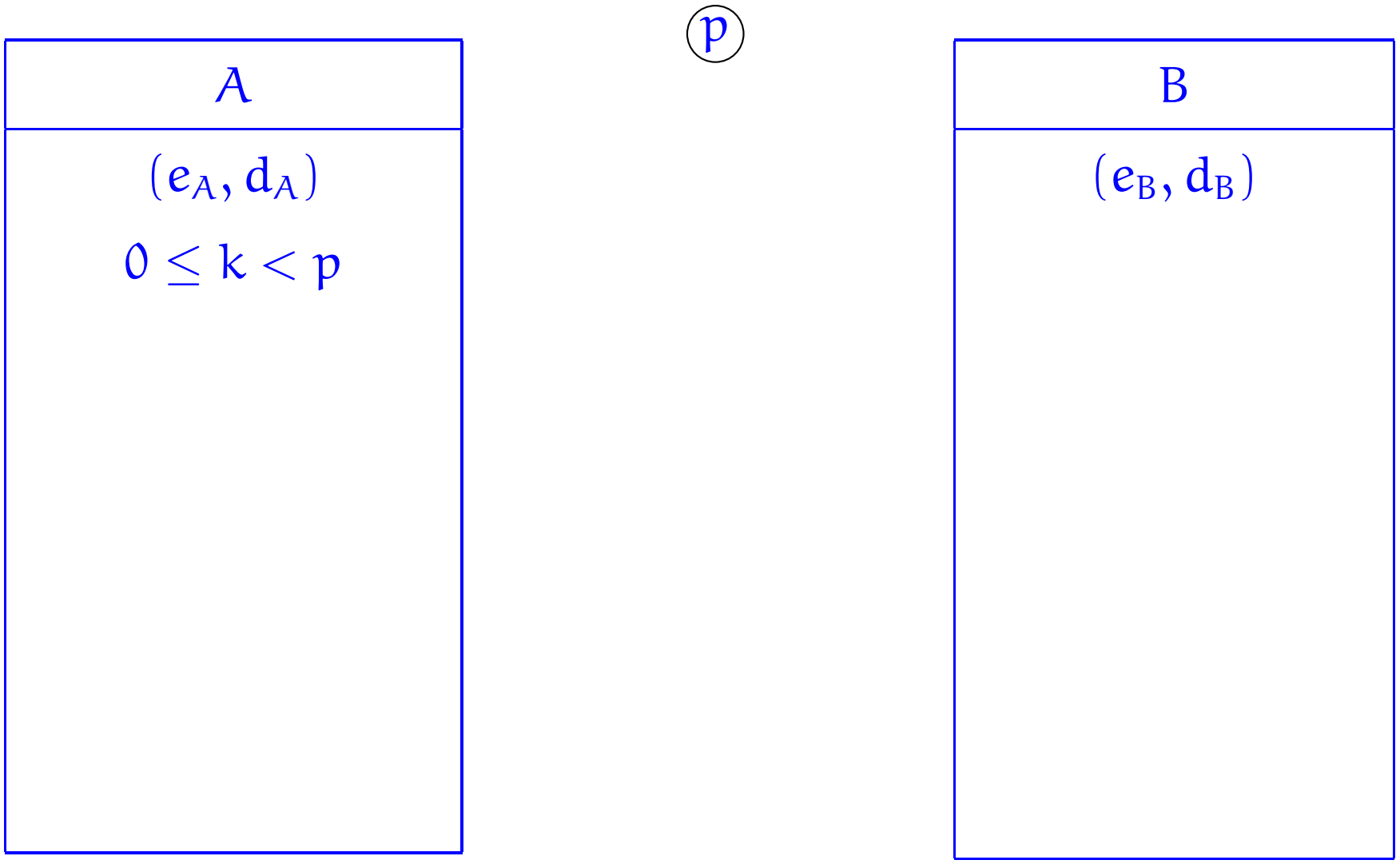
A

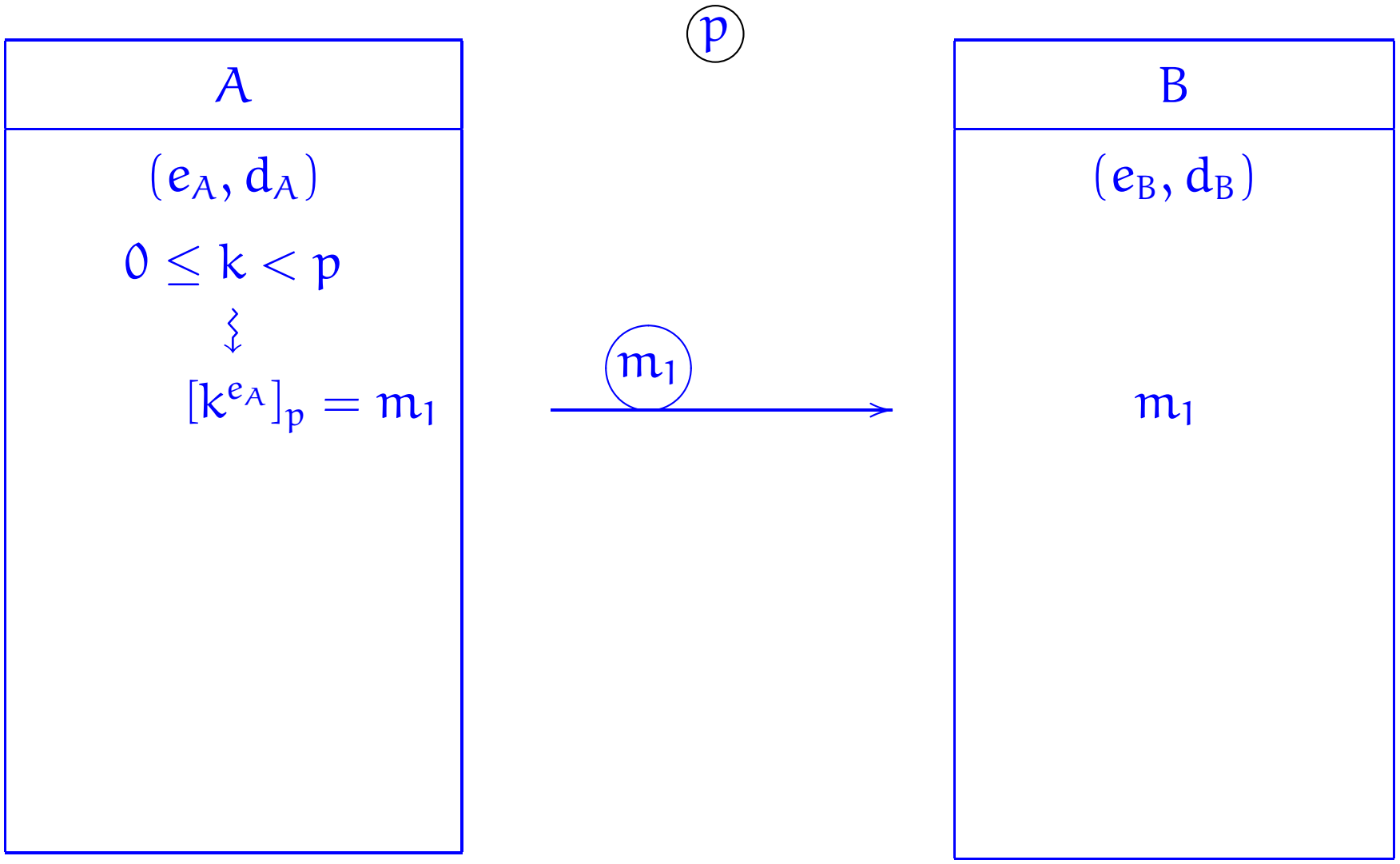
B

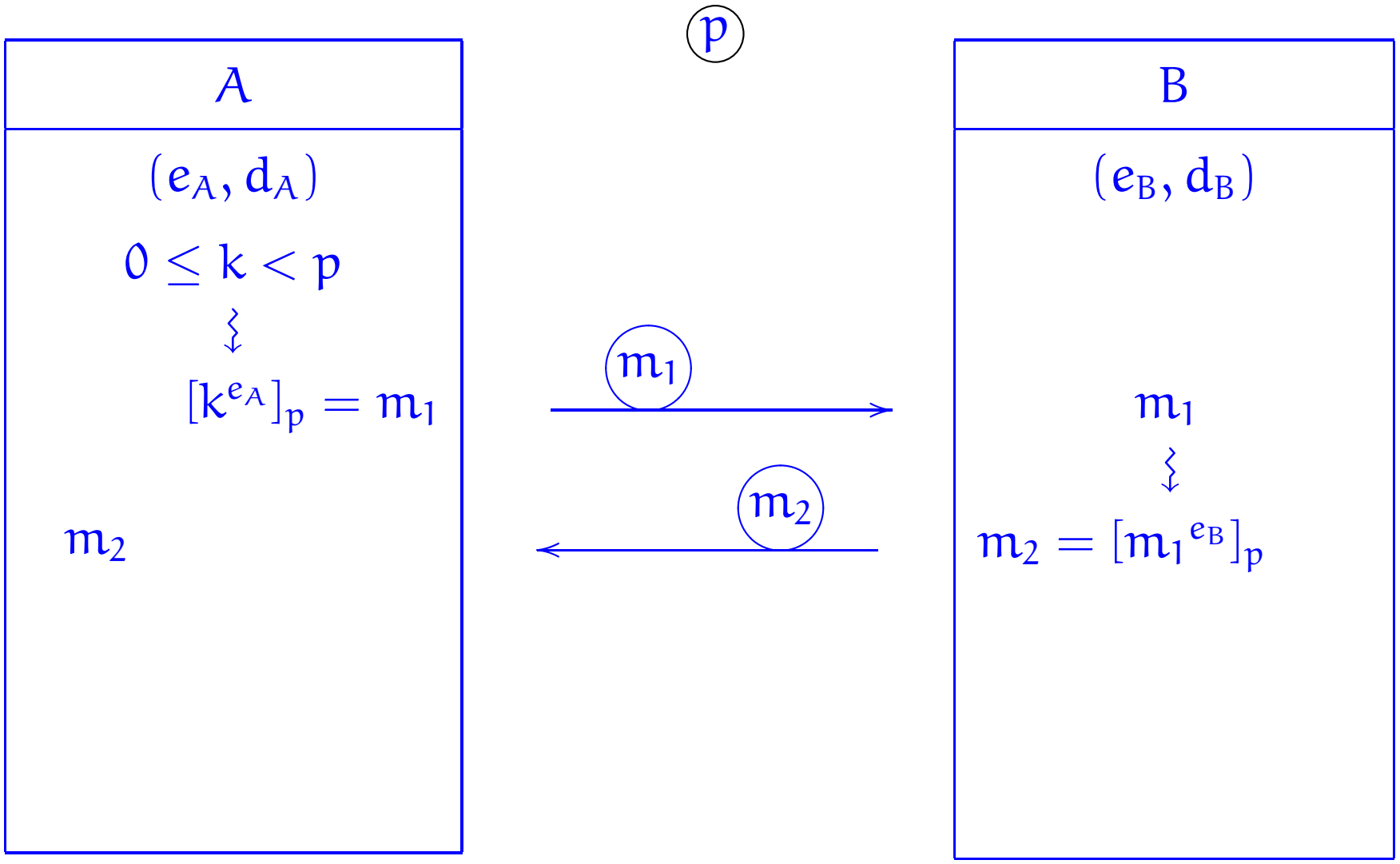
A

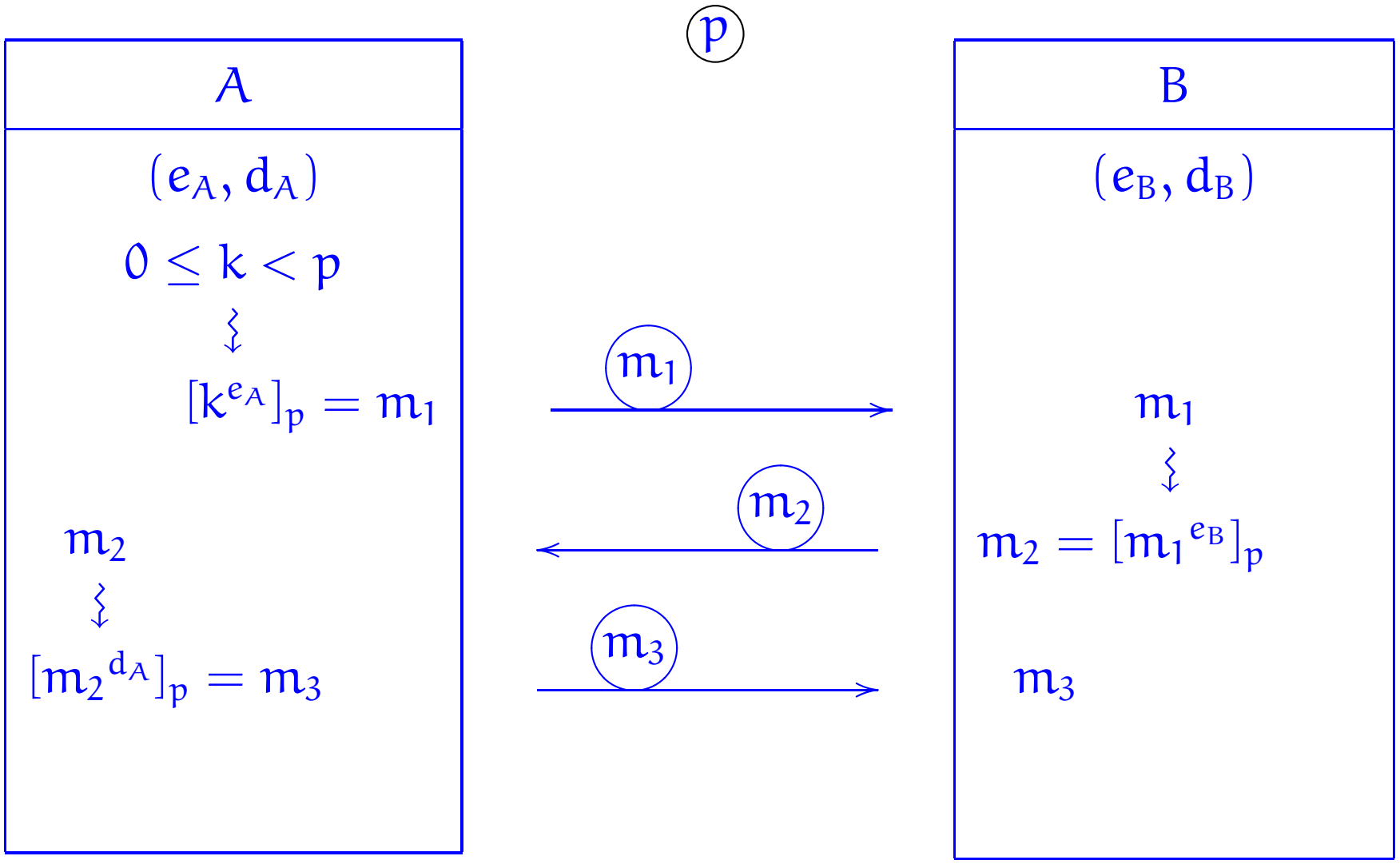
B

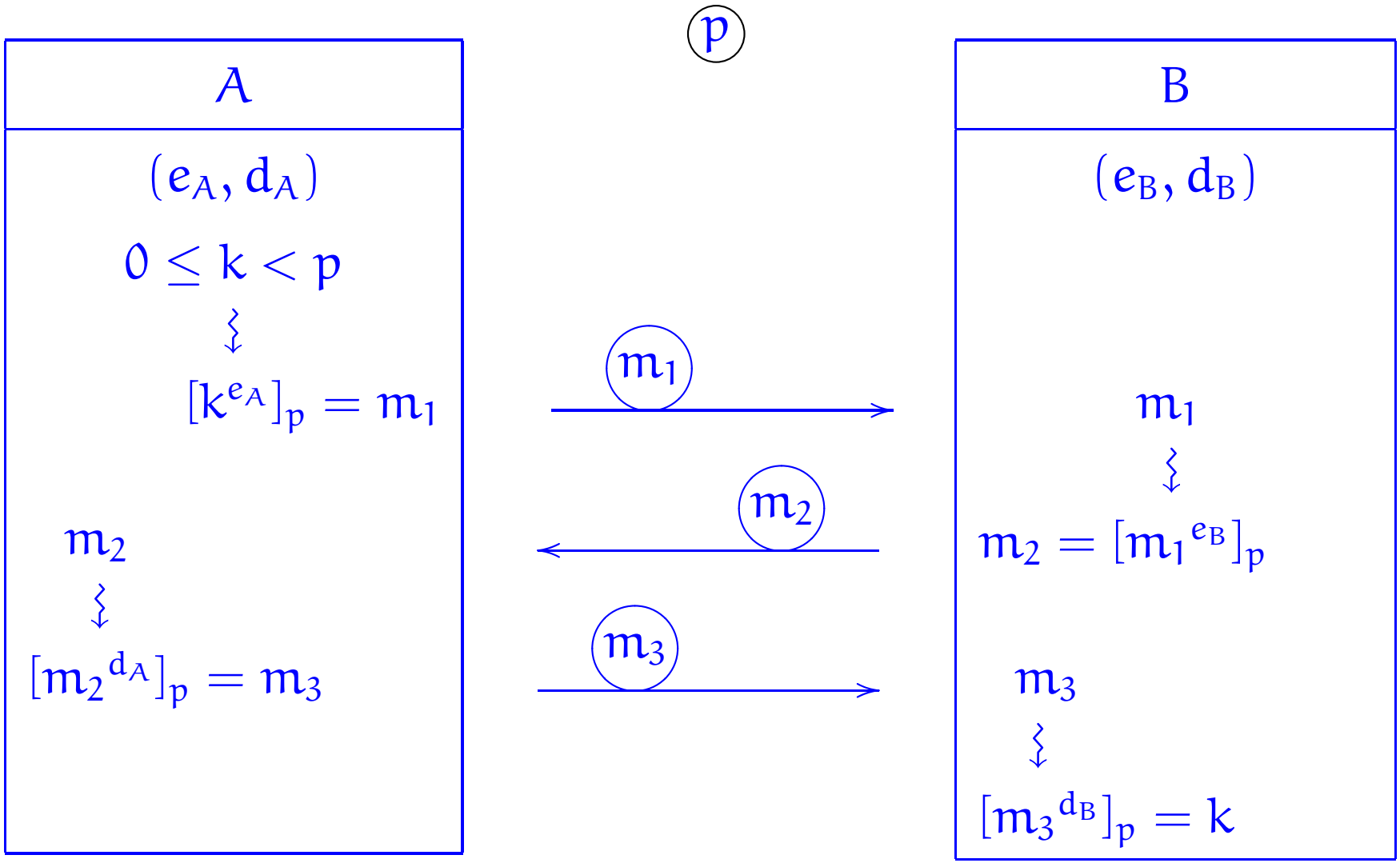

A
B


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


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


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


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



$$\left(\left(\left(k^{e_A}\right)^{e_B}\right)^{d_A}\right)^{d_B} = k^{e_A \cdot e_B \cdot d_A \cdot d_B} \equiv k$$

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.