Multiplicação de inteiros gigantescos

KT cap 5.5

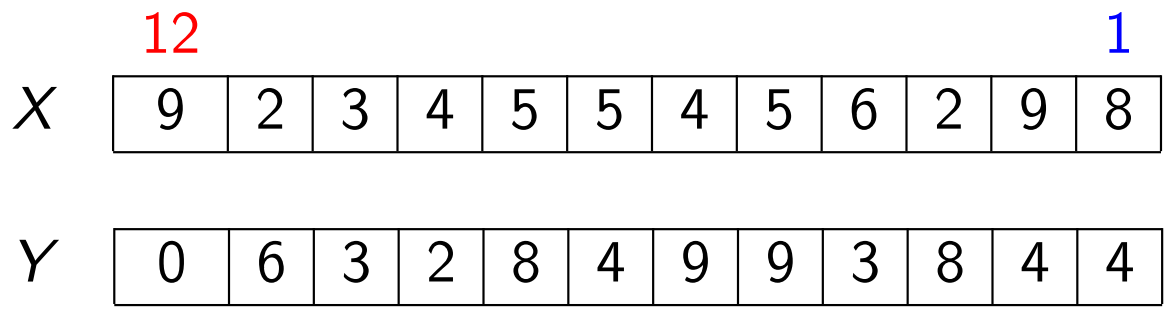
Multiplicação de inteiros gigantescos

$n :=$ número de algarismos.

Problema: Dados dois números inteiros $X[1\,..\,n]$ e $Y[1\,..\,n]$, calcular o produto $X \cdot Y$.

Exemplo com $n = 12$.

Entra:



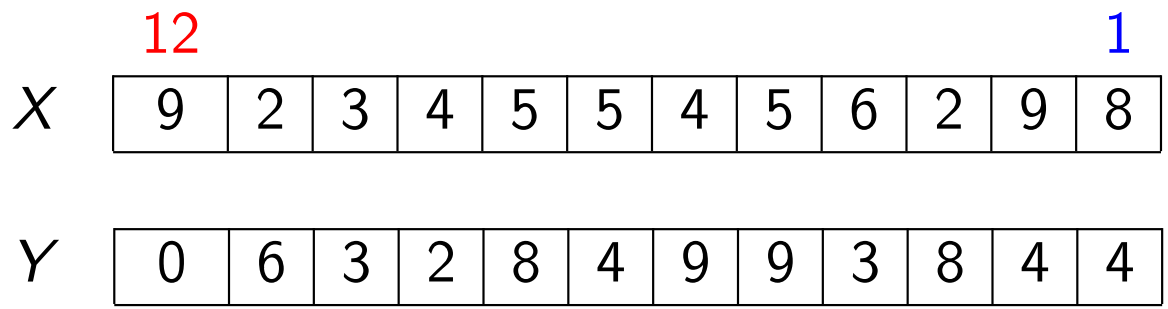
Multiplicação de inteiros gigantescos

$n :=$ número de algarismos.

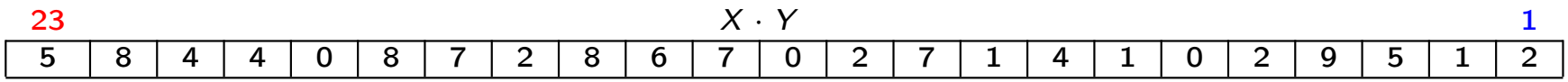
Problema: Dados dois números inteiros $X[1..n]$ e $Y[1..n]$, calcular o produto $X \cdot Y$.

Exemplo com $n = 12$.

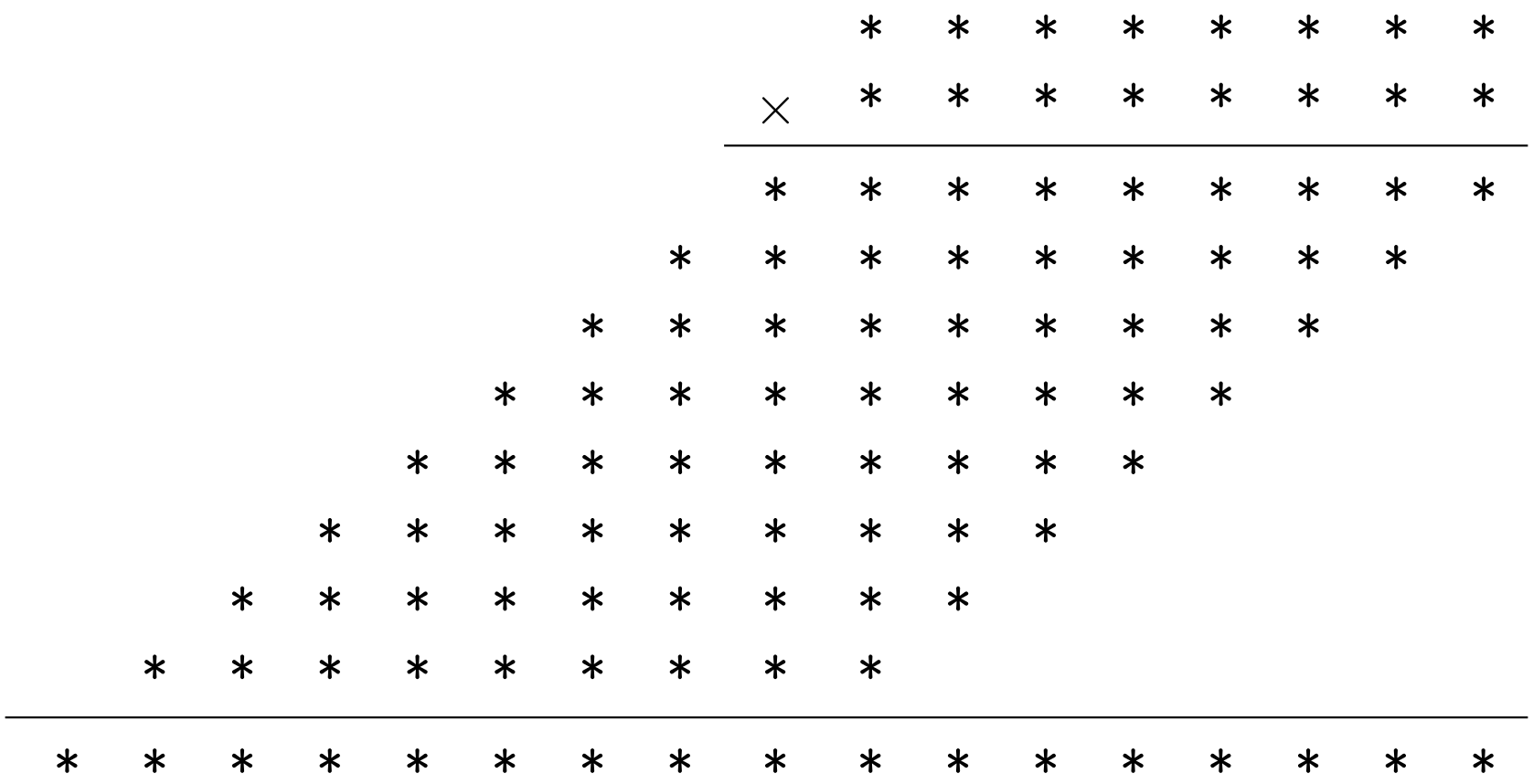
Entra:



Sai:

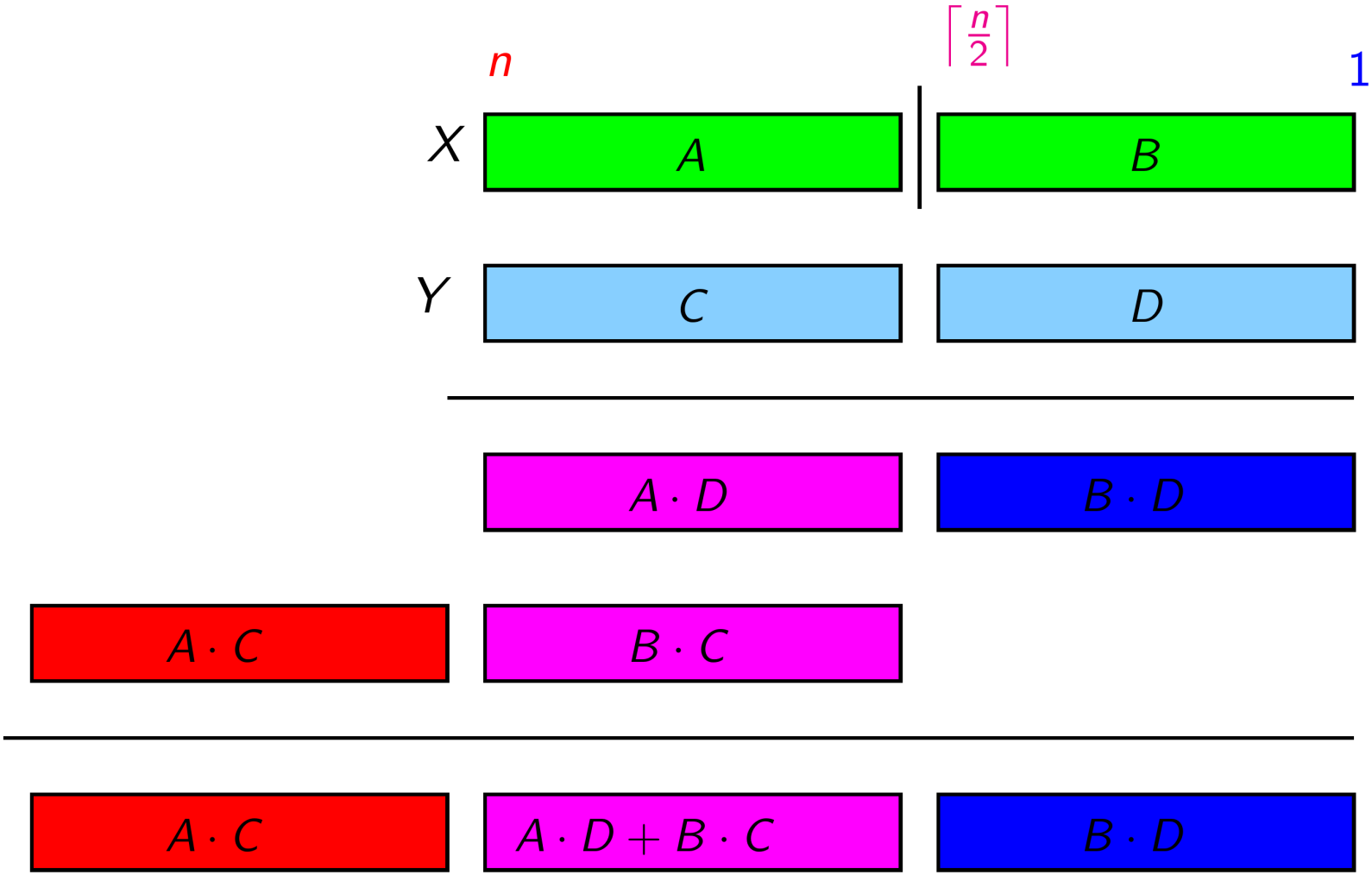


Algoritmo do ensino fundamental



O algoritmo do ensino fundamental é $\Theta(n^2)$.

Divisão e conquista

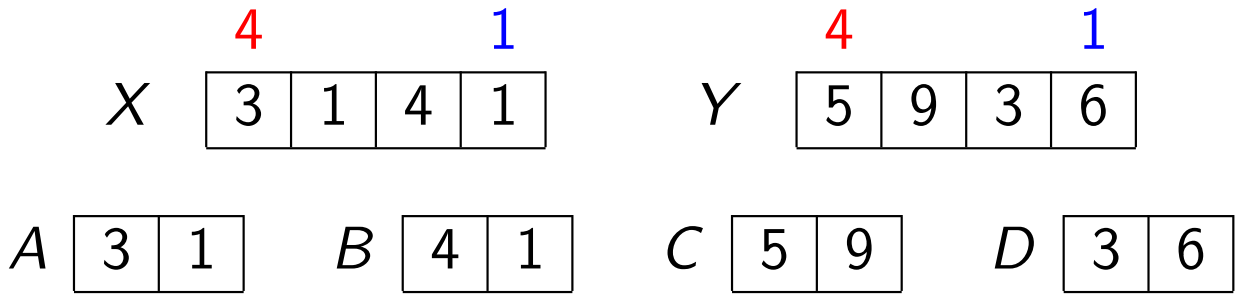


$$X \cdot Y = A \cdot C \times 10^{2\lceil n/2 \rceil} + (A \cdot D + B \cdot C) \times 10^{\lceil n/2 \rceil} + B \cdot D$$

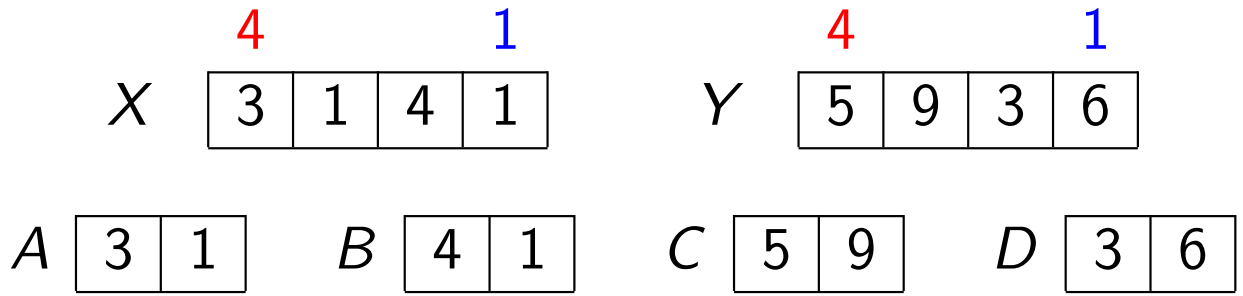
Exemplo



Exemplo



Exemplo



$$X \cdot Y = A \cdot C \times 10^4 + (A \cdot D + B \cdot C) \times 10^2 + B \cdot D$$

$A \cdot C = 1829$ $\quad (A \cdot D + B \cdot C) = 1116 + 2419 = 3535$

$B \cdot D = 1476$

$A \cdot C$	1	8	2	9	0	0	0	0
$(A \cdot D + B \cdot C)$			3	5	3	5	0	0
$B \cdot D$					1	4	7	6
$X \cdot Y =$	1	8	6	4	4	9	7	6

Algoritmo de Multi-DC

Algoritmo recebe inteiros $X[1..n]$ e $Y[1..n]$ e devolve $X \cdot Y$.

MULT (X, Y, n)

1 **se** $n = 1$ **devolva** $X \cdot Y$
2 $q \leftarrow \lceil n/2 \rceil$
3 $A \leftarrow X[q+1..n]$ $\quad$ $B \leftarrow X[1..q]$
4 $C \leftarrow Y[q+1..n]$ $\quad$ $D \leftarrow Y[1..q]$
5 $E \leftarrow \text{MULT}(A, C, \lfloor n/2 \rfloor)$
6 $F \leftarrow \text{MULT}(B, D, \lceil n/2 \rceil)$
7 $G \leftarrow \text{MULT}(A, D, \lceil n/2 \rceil)$
8 $H \leftarrow \text{MULT}(B, C, \lceil n/2 \rceil)$
9 $R \leftarrow E \times 10^{2q} + (G + H) \times 10^{\lceil n/2 \rceil} + F$
10 **devolva** R

$T(n) =$ consumo de tempo do algoritmo
para multiplicar dois inteiros com n algarismos.

Consumo de tempo

linha		todas as execuções da linha
1	=	$\Theta(1)$
2	=	$\Theta(1)$
3	=	$\Theta(n)$
4	=	$\Theta(n)$
5	=	$T(\lfloor n/2 \rfloor)$
6	=	$T(\lceil n/2 \rceil)$
7	=	$T(\lceil n/2 \rceil)$
8	=	$T(\lceil n/2 \rceil)$
9	=	$\Theta(n)$
10	=	$\Theta(1)$
total	=	$T(\lfloor n/2 \rfloor) + 3\,T(\lceil n/2 \rceil) + \Theta(n)$

Consumo de tempo

Nosso estudo de recorrências sugere que a solução da recorrência

$$\begin{aligned} T(1) &= \Theta(1) \\ T(n) &= T(\lfloor n/2 \rfloor) + 3\,T(\lceil n/2 \rceil) + \Theta(n) \quad \text{para } n = 2, 3, 4, \ldots \end{aligned}$$

está na mesma classe Θ que a solução de

$$T'(n) = 4\,T'(n/2) + n$$

n	1	2	4	8	16	32	64	128	256	512
$T'(n)$	1	6	28	120	496	2016	8128	32640	130816	523776

Conclusões

$T'(n)$ é $\Theta(n^2)$.

$T(n)$ é $\Theta(n^2)$.

O consumo de tempo do algoritmo MULT é $\Theta(n^2)$.

Tanto trabalho por nada . . .
Será?!?

Pensar pequeno

Olhar para números com 2 algarismos (n=2).

Suponha $X = a\,b$ e $Y = c\,d$.

Se cada multiplicação custa R$ 1,00 e
cada soma custa R$ 0,01, quanto custa $X \cdot Y$?

Pensar pequeno

Olhar para números com 2 algarismos (n=2).

Suponha $X = a\,b$ e $Y = c\,d$.

Se cada multiplicação custa R$ 1,00 e
cada soma custa R$ 0,01, quanto custa $X \cdot Y$?

Eis $X \cdot Y$ por R$ 4,03:

X		a	b
Y		c	d
		ad	bd
	ac	bc	
$X \cdot Y$	ac	$ad + bc$	bd

$$X \cdot Y = ac \times 10^2 + (ad + bc) \times 10^1 + bd$$

Pensar pequeno

Olhar para números com 2 algarismos (n=2).

Suponha $X = a\,b$ e $Y = c\,d$.

Se cada multiplicação custa R$ 1,00 e
cada soma custa R$ 0,01, quanto custa $X \cdot Y$?

Eis $X \cdot Y$ por R$ 4,03:

X		a	b
Y		c	d
		ad	bd
	ac	bc	
$X \cdot Y$	ac	$ad + bc$	bd

$$X \cdot Y = ac \times 10^2 + (ad + bc) \times 10^1 + bd$$

Solução mais barata?

Pensar pequeno

Olhar para números com 2 algarismos (n=2).

Suponha $X = a\,b$ e $Y = c\,d$.

Se cada multiplicação custa R$ 1,00 e
cada soma custa R$ 0,01, quanto custa $X \cdot Y$?

Eis $X \cdot Y$ por R$ 4,03:

X		a	b
Y		c	d
		ad	bd
	ac	bc	
$X \cdot Y$	ac	$ad + bc$	bd

$X \cdot Y = ac \times 10^2 + (ad + bc) \times 10^1 + bd$

Solução mais barata? Gauss faz por R$ 3,06!

$X \cdot Y$ por apenas R$ 3,06

X		a	b
Y		c	d
		ad	bd
	ac	bc	
$X \cdot Y$	ac	$ad + bc$	bd

$X \cdot Y$ por apenas R$ 3,06

X		a	b
Y		c	d
		ad	bd
	ac	bc	
$X \cdot Y$	ac	$ad + bc$	bd

$(a + b)(c + d) = ac + ad + bc + bd \Rightarrow$
$ad + bc = (a + b)(c + d) - ac - bd$

$g = (a + b)(c + d) \qquad e = ac \qquad f = bd \qquad h = g - e - f$

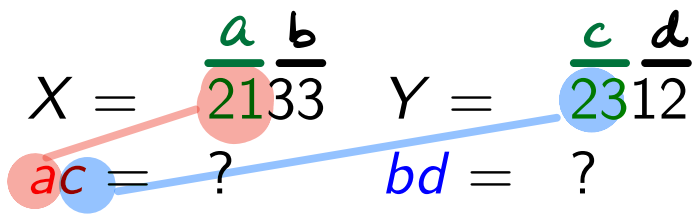
$$X \cdot Y \ \text{(por R\$ 3,06)} = e \times 10^2 + h \times 10^1 + f$$

Exemplo

$$X = \overline{21}\,\overline{33} \qquad Y = \overline{23}\,\overline{12} \qquad X \cdot Y = \; ?$$

$$ac = \; ? \qquad bd = \; ? \qquad (a+b)(c+d) = \; ?$$

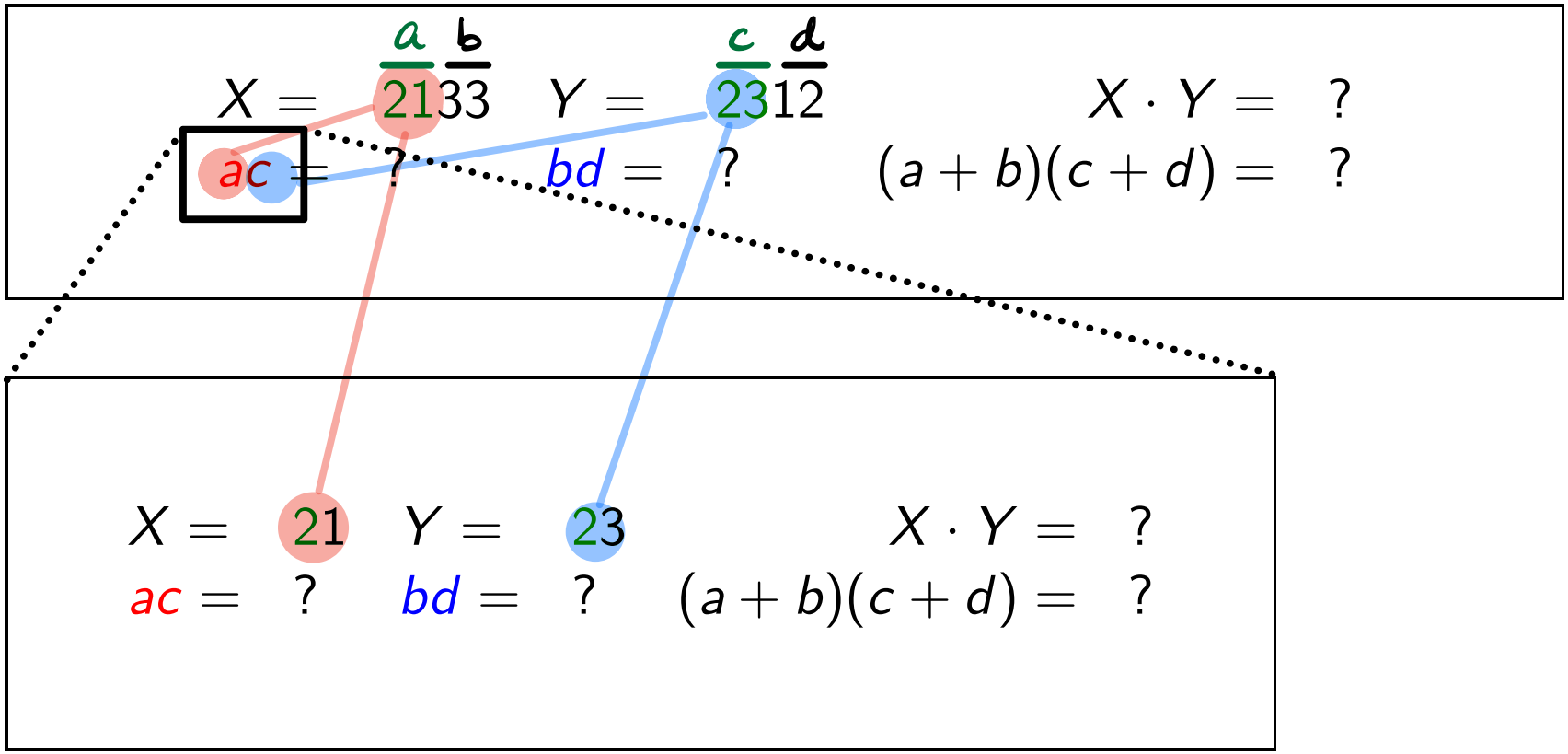
Exemplo



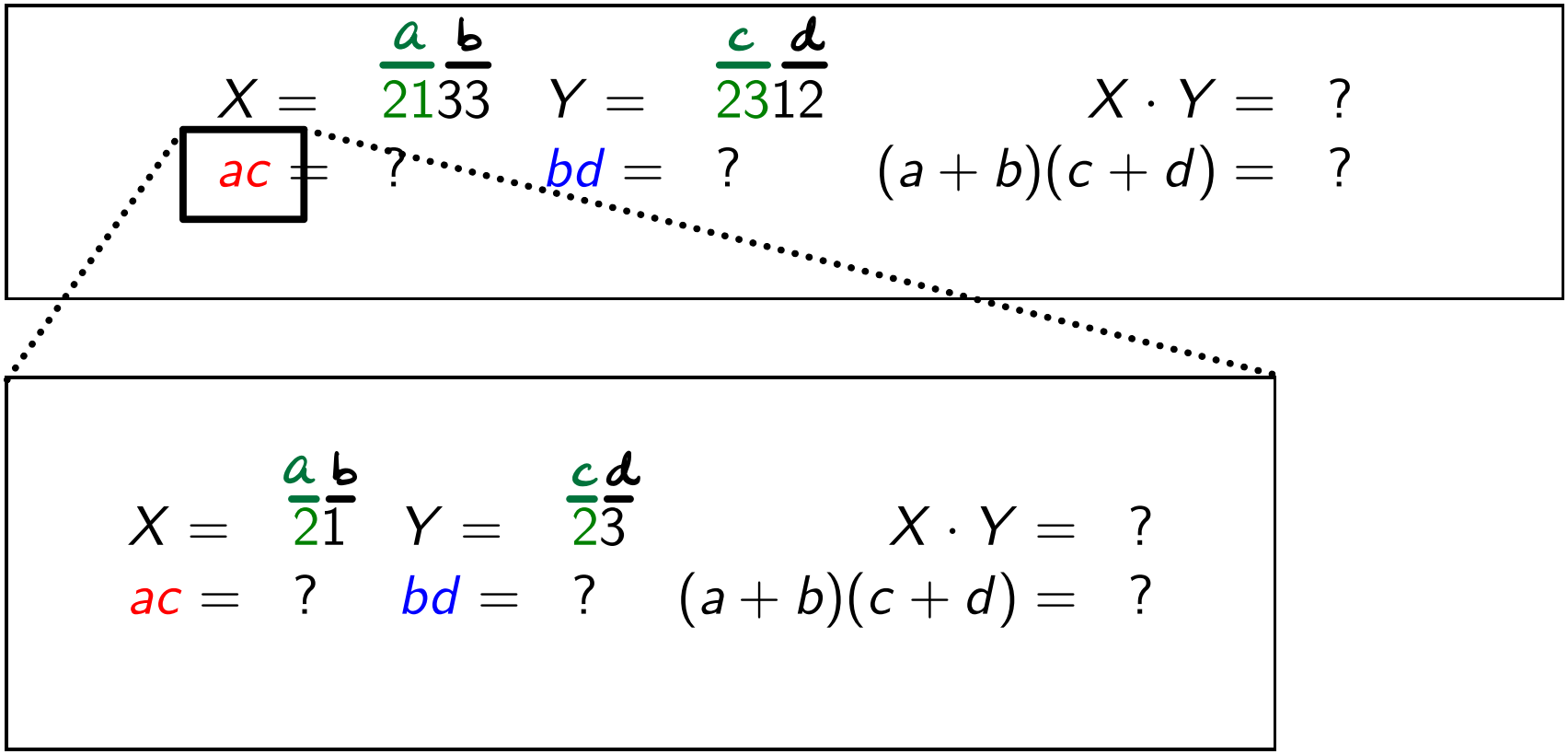
$$X \cdot Y = \quad ?$$

$$(a+b)(c+d) = \quad ?$$

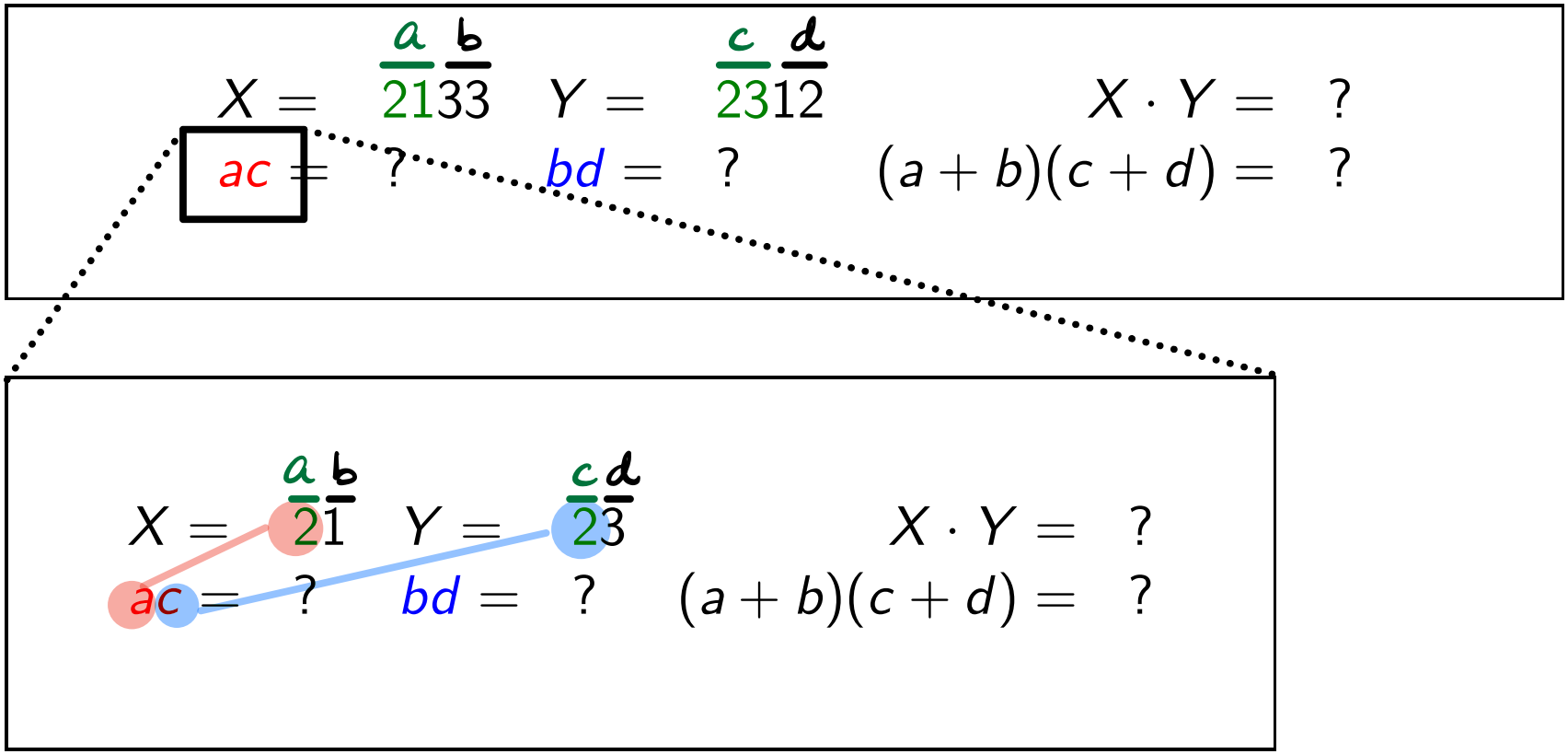
Exemplo



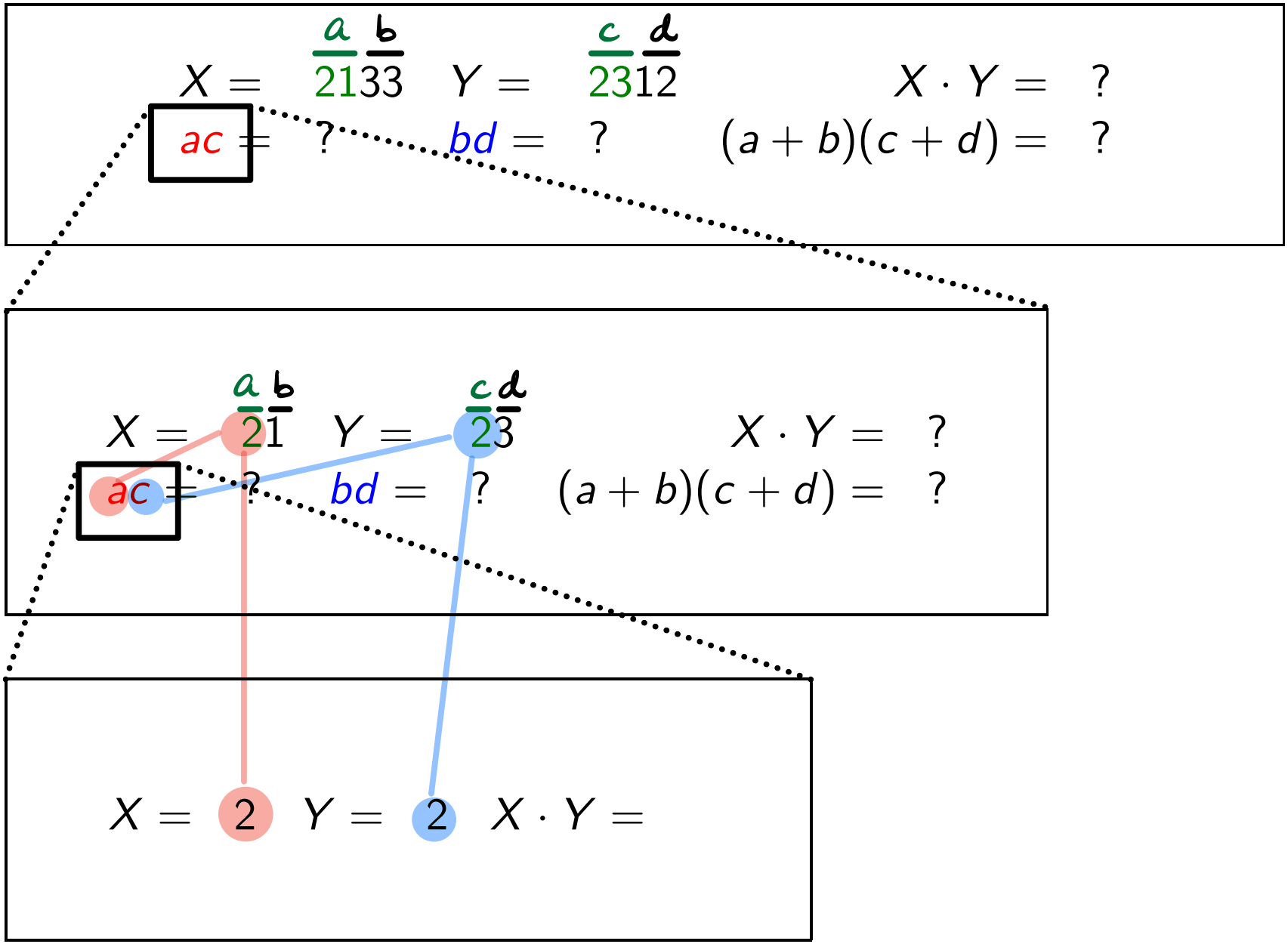
Exemplo



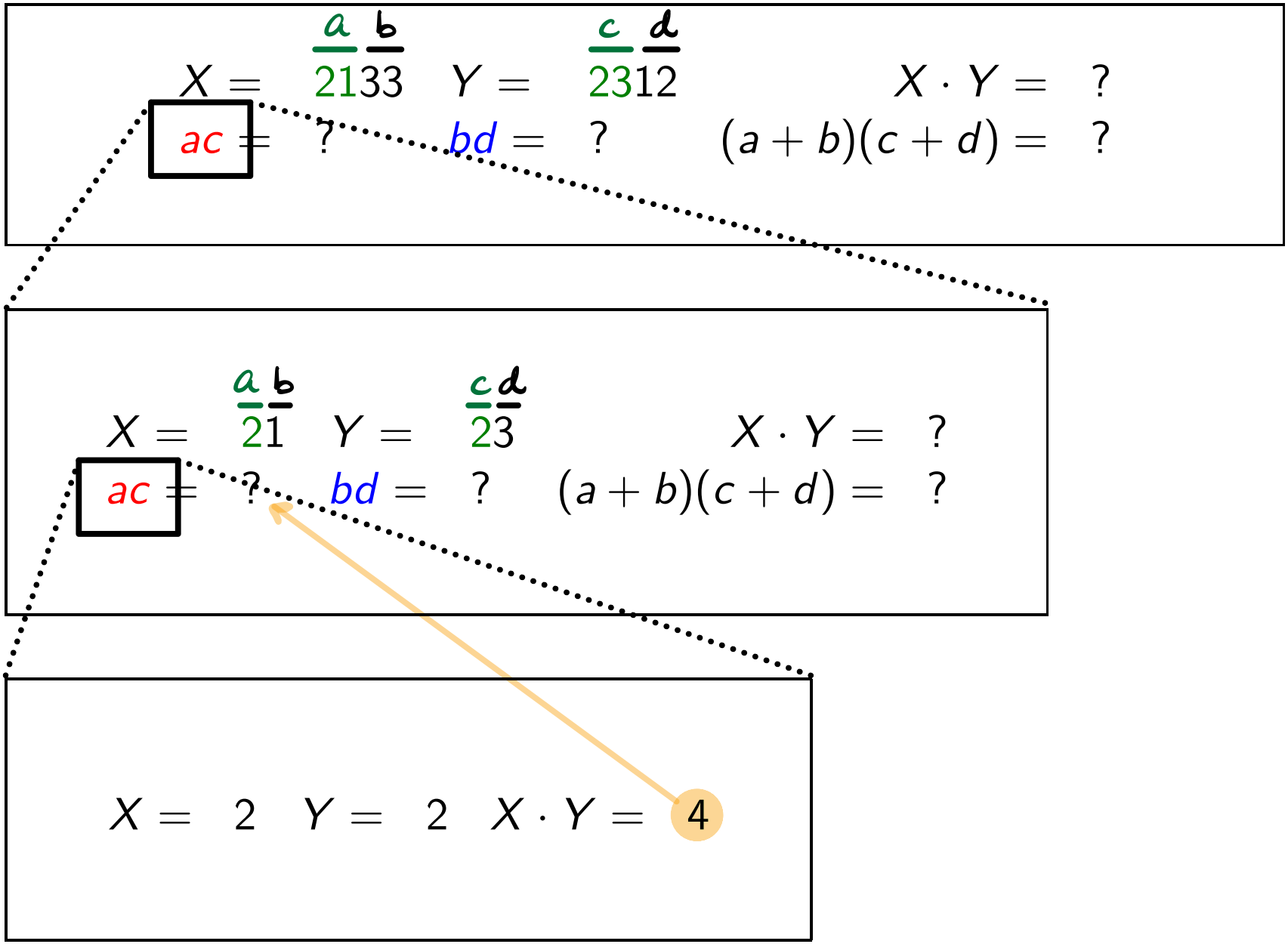
Exemplo



Exemplo



Exemplo

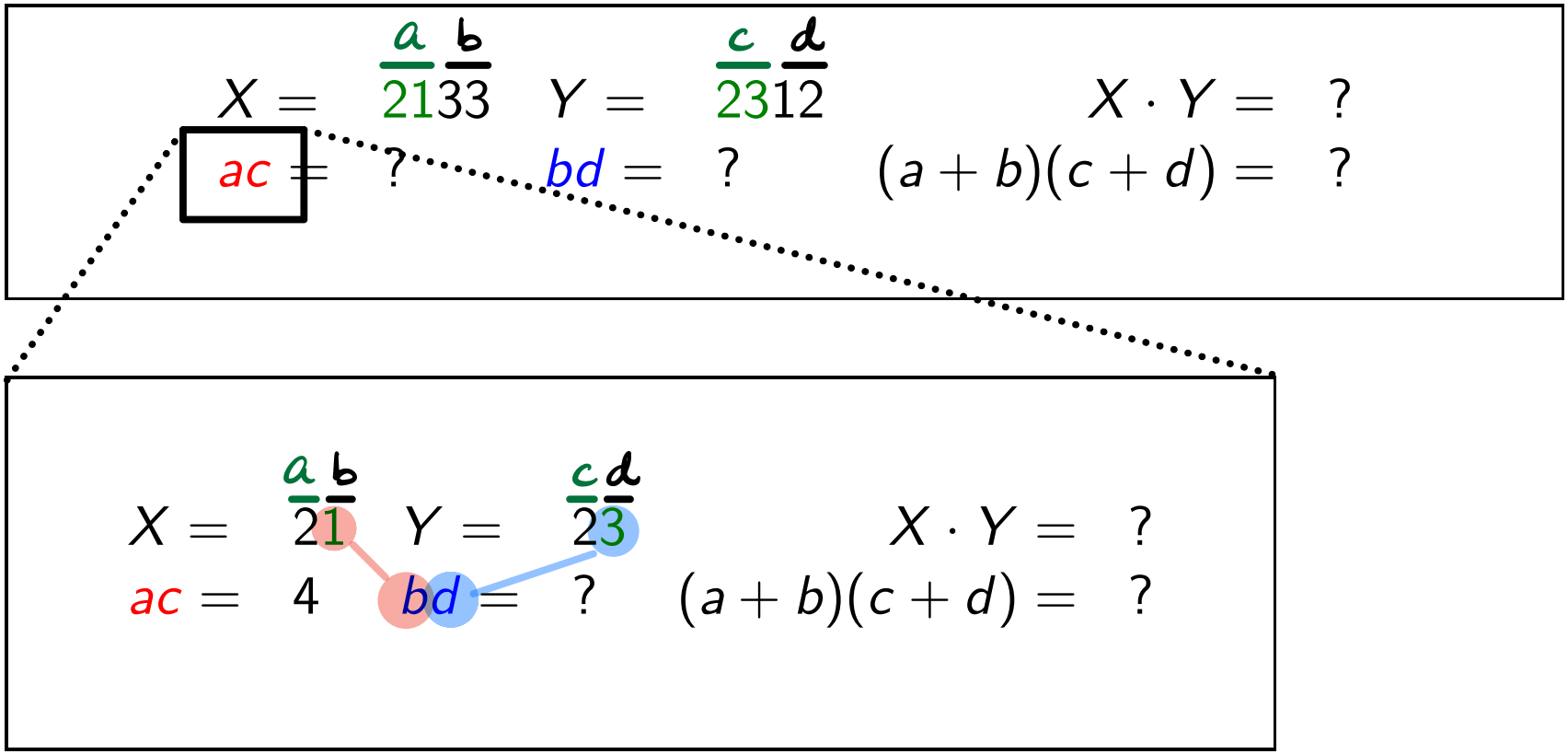

a b
c d
X = 2133
Y = 2312
X · Y = ?
ac = ?
bd = ?
(a + b)(c + d) = ?
a b
c d
X = 21
Y = 23
X · Y = ?
ac = ?
bd = ?
(a + b)(c + d) = ?
X = 2
Y = 2
X · Y = 4

Exemplo

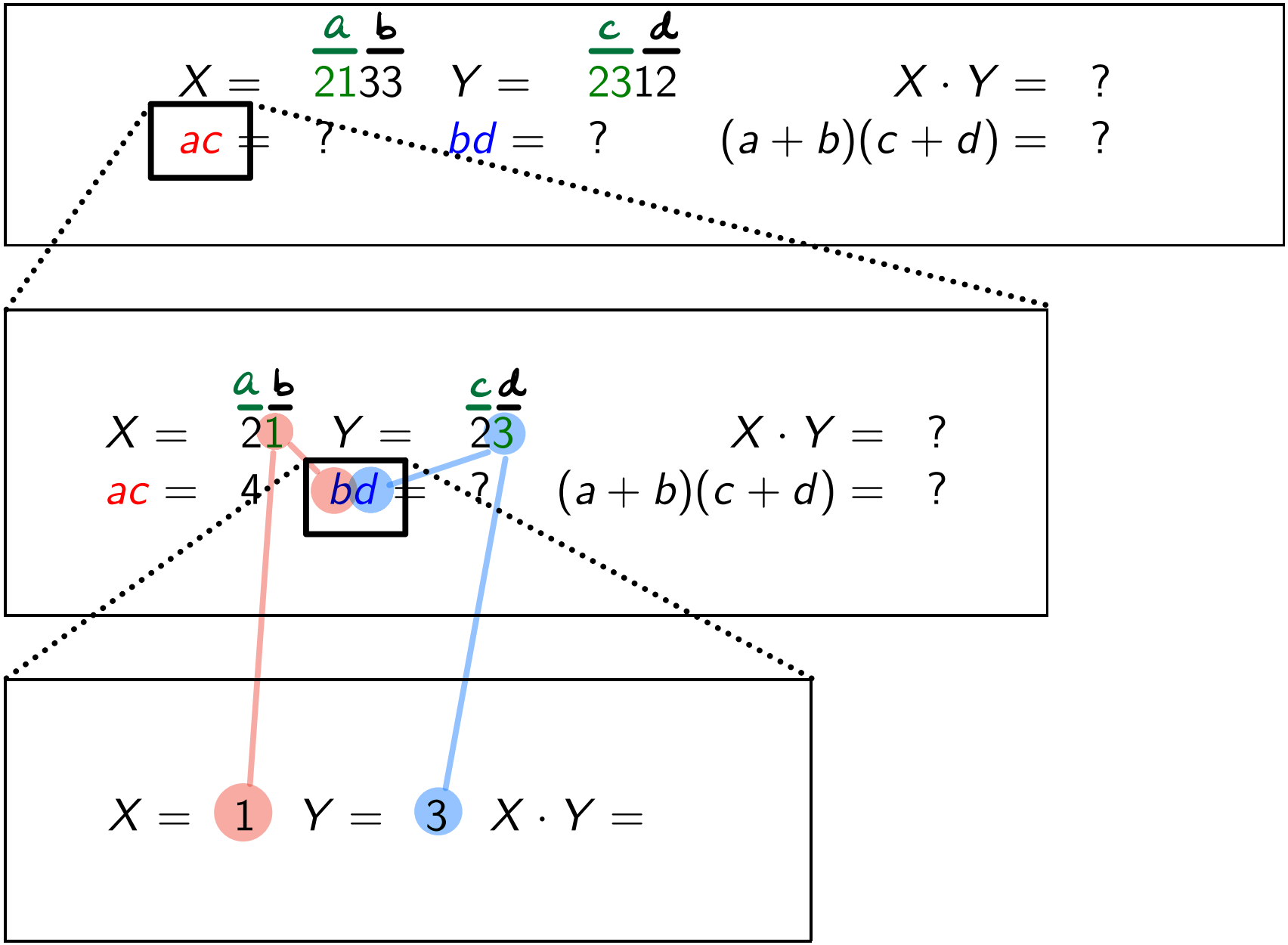
$$X = \overset{a\ b}{2133} \quad Y = \overset{c\ d}{2312} \quad X \cdot Y = \ ?$$
$$ac = \ ? \quad bd = \ ? \quad (a+b)(c+d) = \ ?$$

$$X = \overset{a\ b}{21} \quad Y = \overset{c\ d}{23} \quad X \cdot Y = \ ?$$
$$ac = 4 \quad bd = \ ? \quad (a+b)(c+d) = \ ?$$

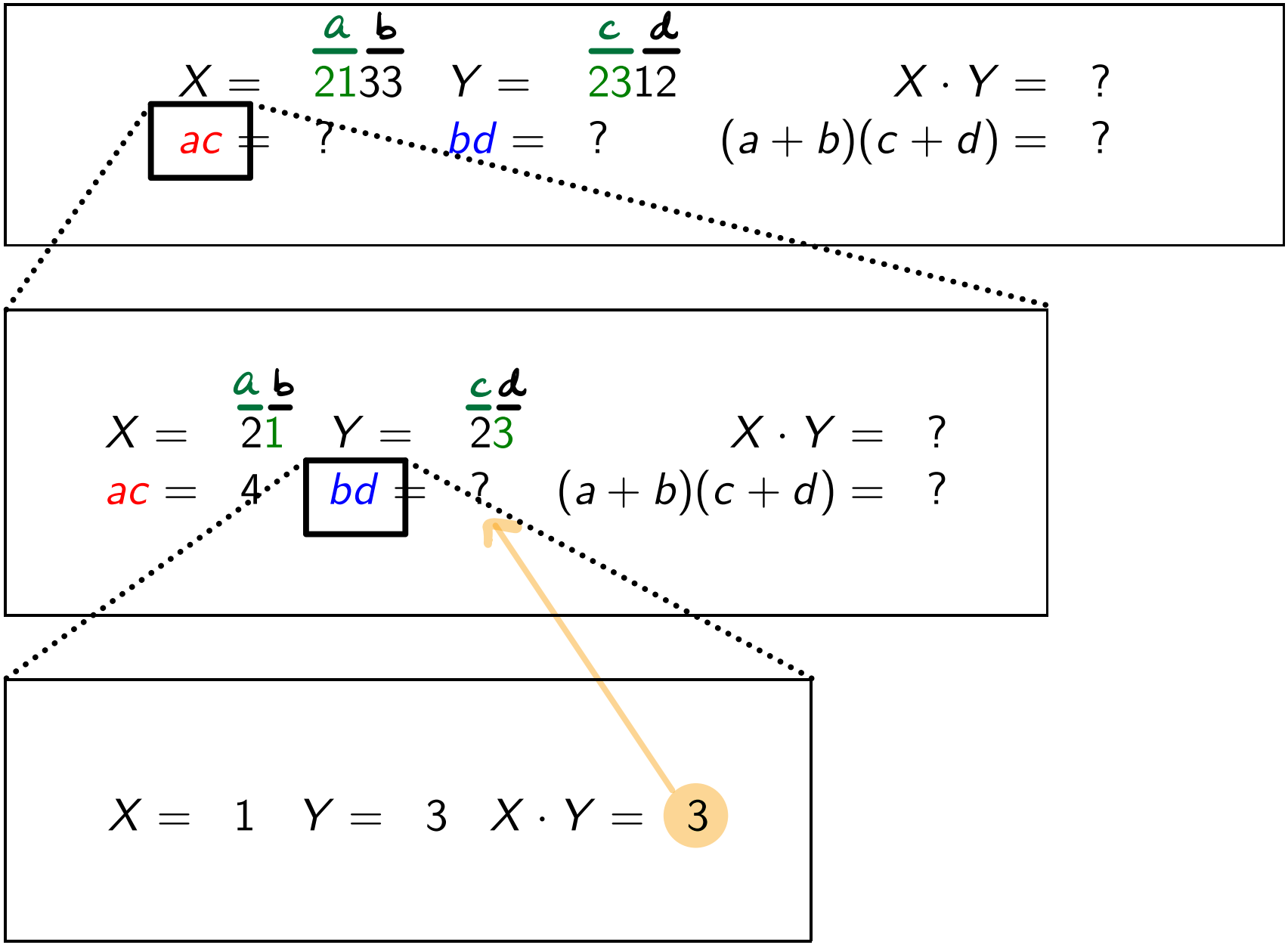
Exemplo



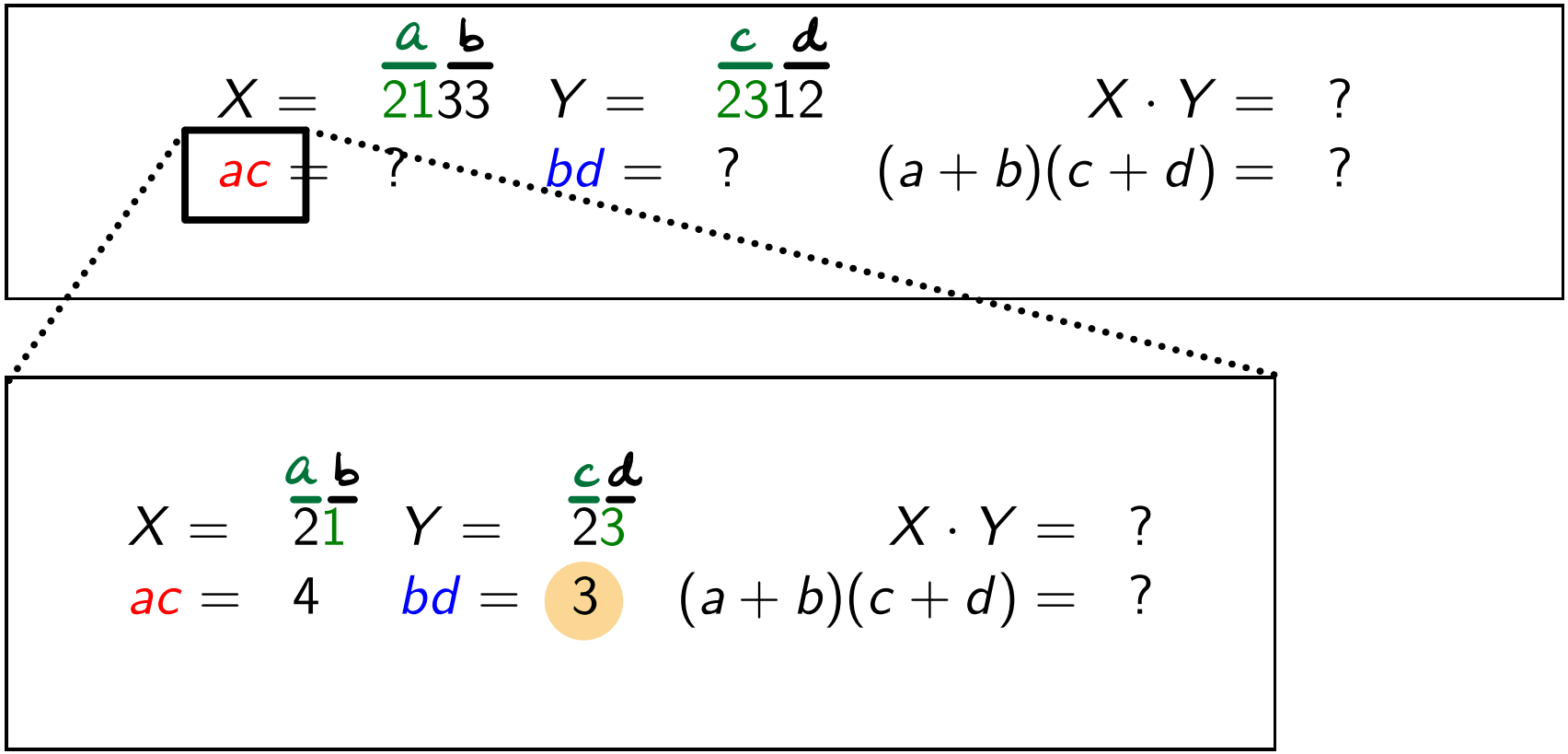
Exemplo


a b
c d
X = 2133
Y = 2312
X · Y = ?
ac = ?
bd = ?
(a + b)(c + d) = ?
a b
c d
X = 21
Y = 23
X · Y = ?
ac = 4
bd = ?
(a + b)(c + d) = ?
X = 1
Y = 3
X · Y =

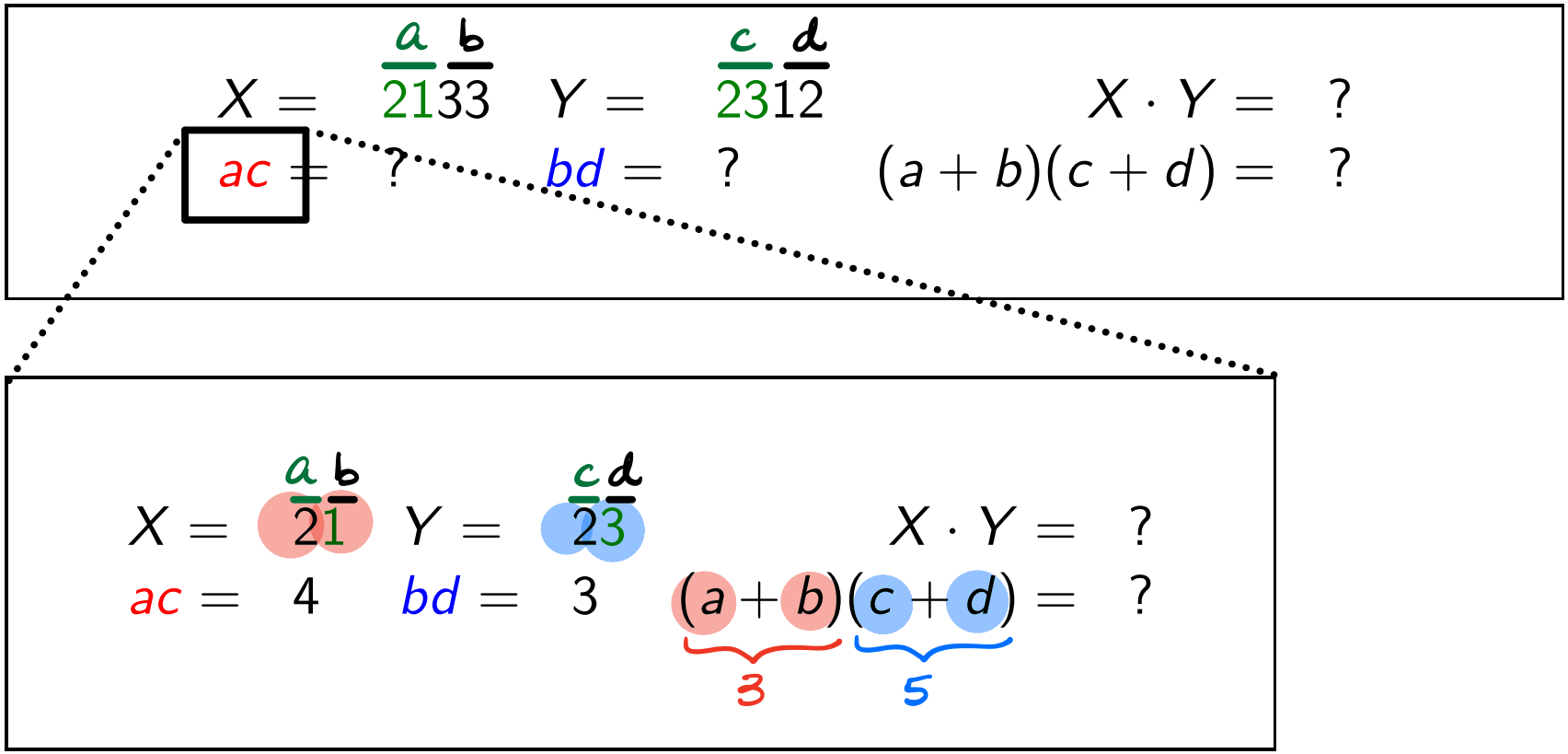
Exemplo


a b
c d
X = 2133
Y = 2312
X · Y = ?
ac = ?
bd = ?
(a + b)(c + d) = ?
a b
c d
X = 21
Y = 23
X · Y = ?
ac = 4
bd = ?
(a + b)(c + d) = ?
X = 1
Y = 3
X · Y = 3

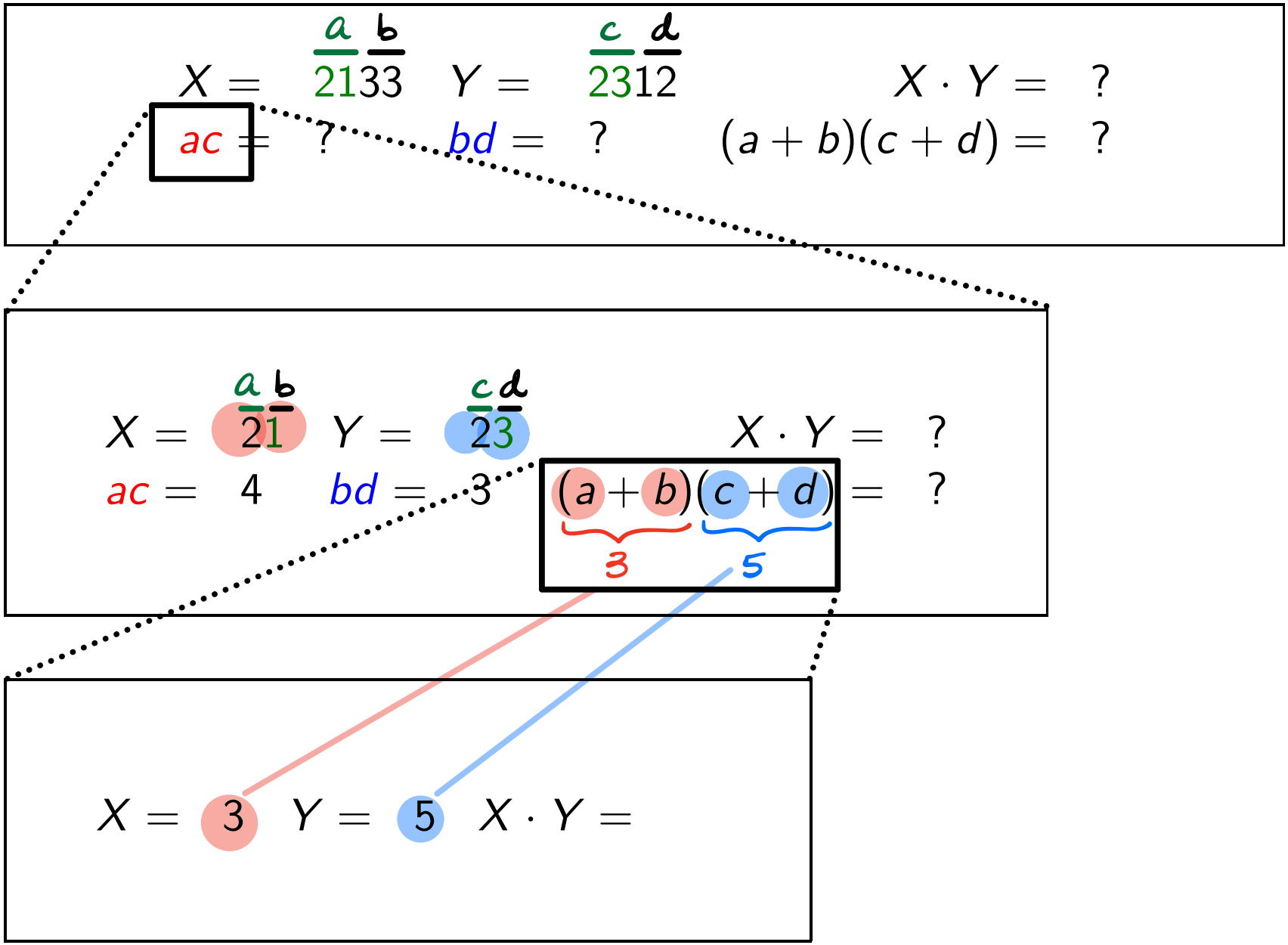
Exemplo



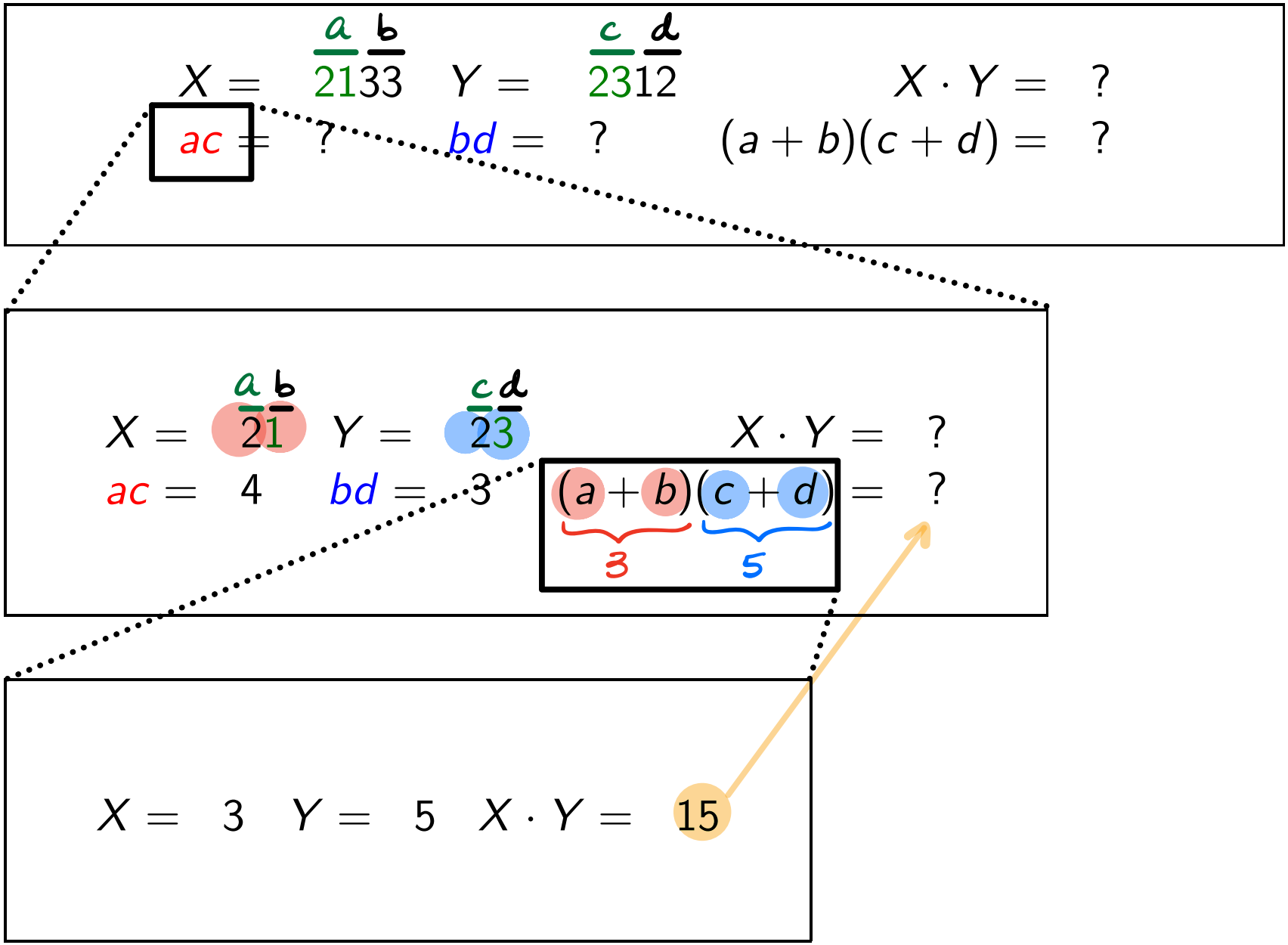
Exemplo



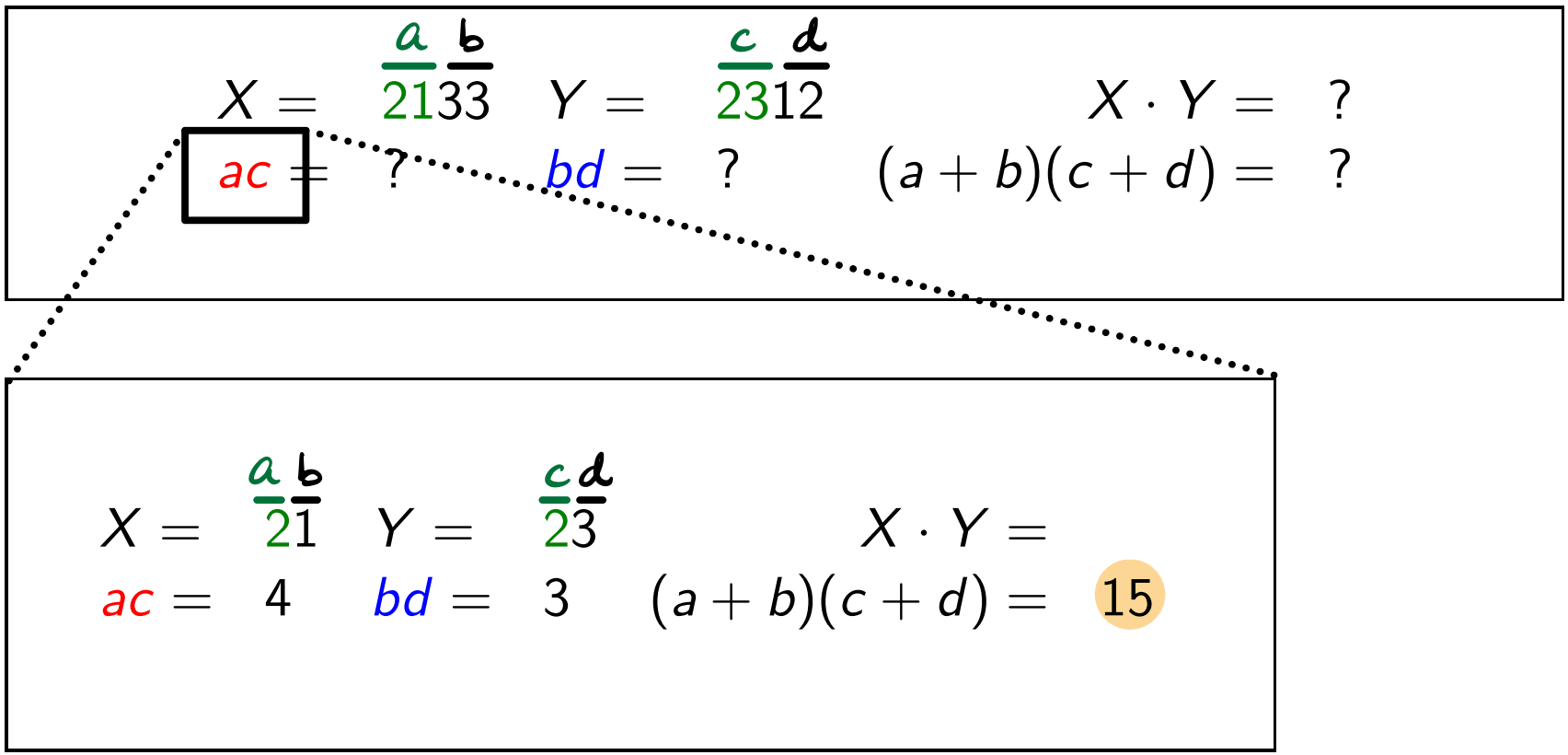
Exemplo


a b
X = 2133
Y = c d 2312
X · Y = ?
ac = ?
bd = ?
(a + b)(c + d) = ?
a b
X = 21
Y = c d 23
X · Y = ?
ac = 4
bd = 3
(a + b)(c + d) = ?
3
5
X = 3
Y = 5
X · Y =

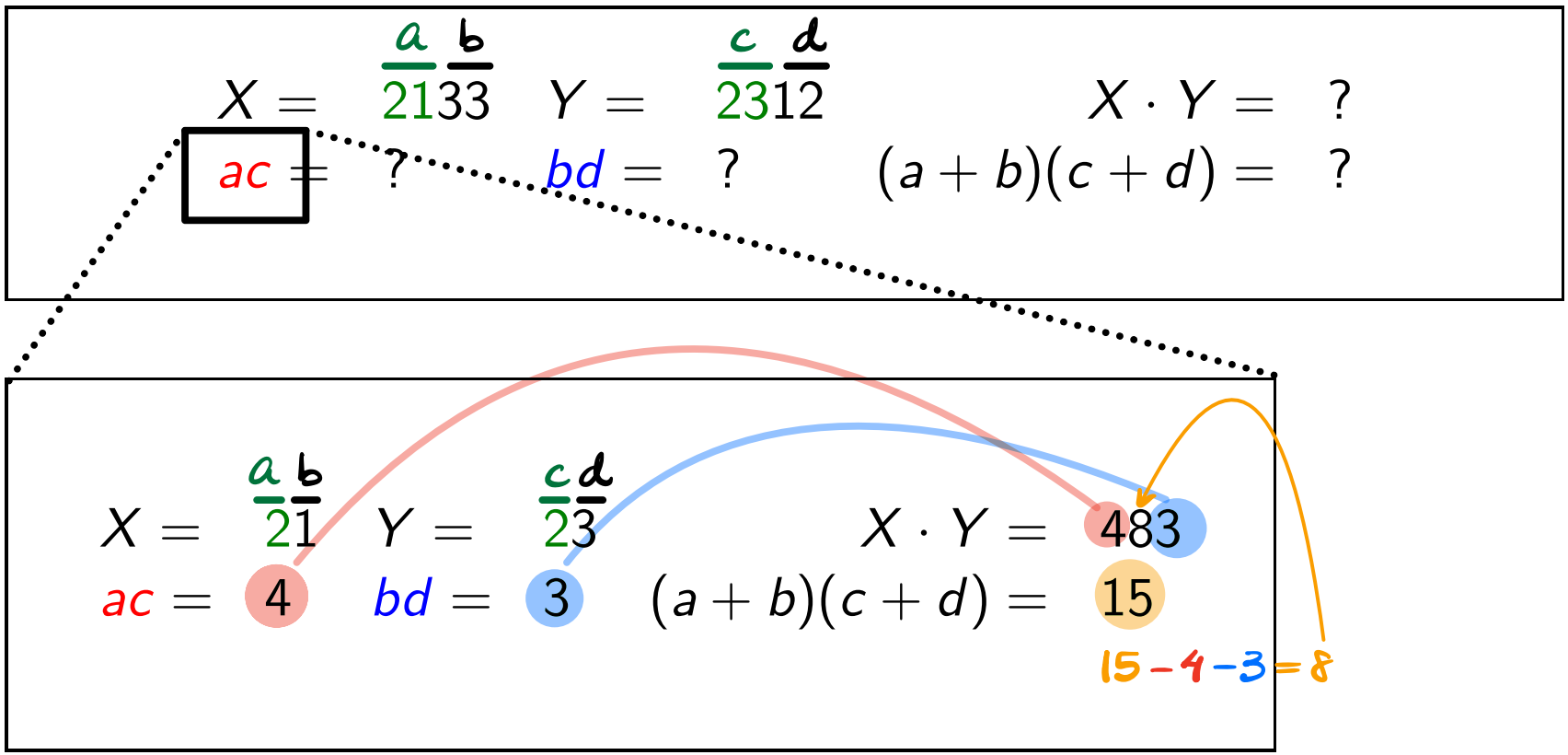
Exemplo


a b
2133
c d
2312
X = ac = ?
Y = bd = ?
X · Y = ?
(a + b)(c + d) = ?
a b
21
c d
23
X = ac = 4
Y = bd = 3
X · Y = ?
(a + b)(c + d) = ?
3
5
X = 3 Y = 5 X · Y = 15

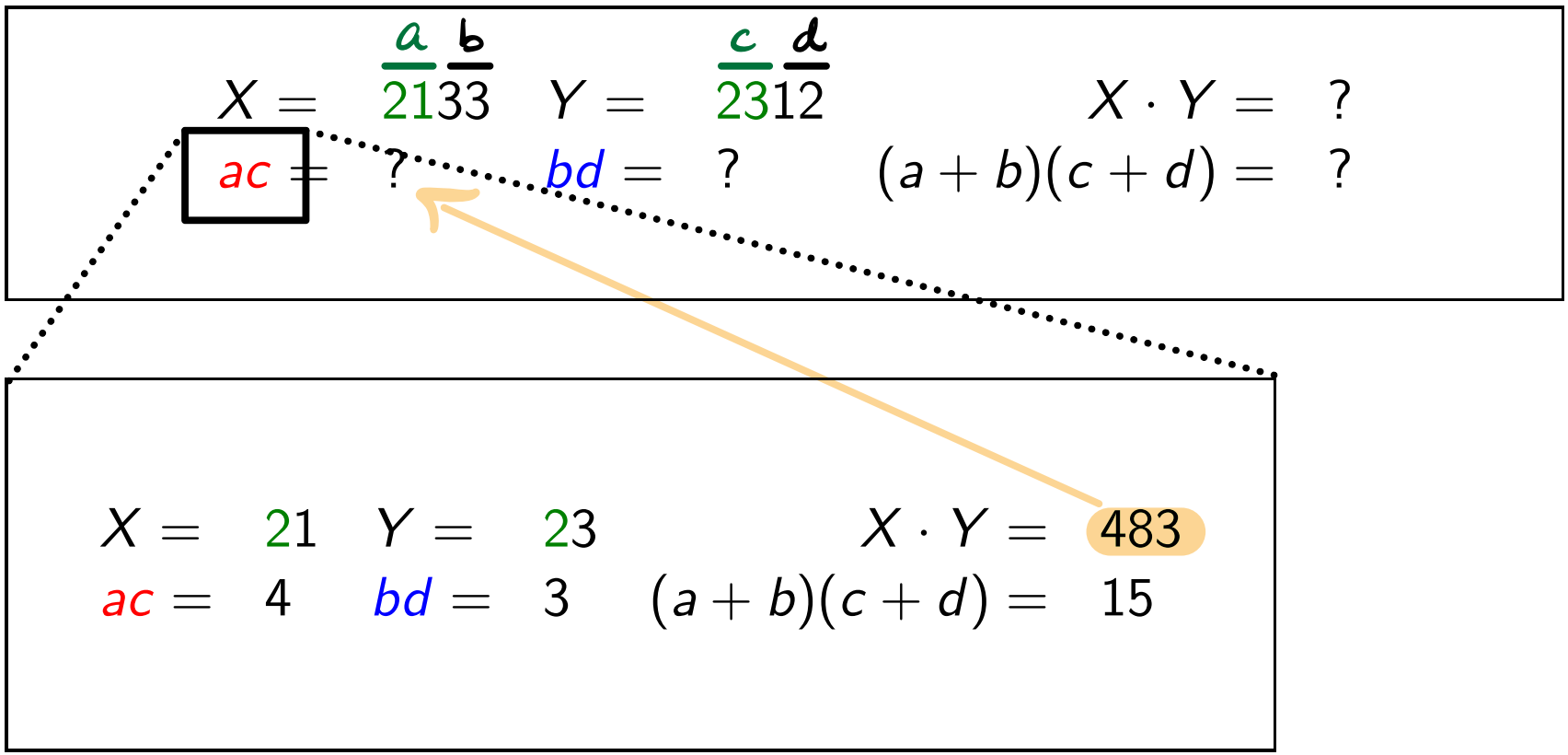
Exemplo



Exemplo


a b
c d
X = 2133
Y = 2312
X · Y = ?
ac = ?
bd = ?
(a + b)(c + d) = ?
a b
c d
X = 21
Y = 23
X · Y = 483
ac = 4
bd = 3
(a + b)(c + d) = 15
15 - 4 - 3 = 8

Exemplo



Exemplo

$$X = \overset{a}{2}\overset{b}{133} \qquad Y = \overset{c}{2}\overset{d}{312} \qquad X \cdot Y = \; ?$$

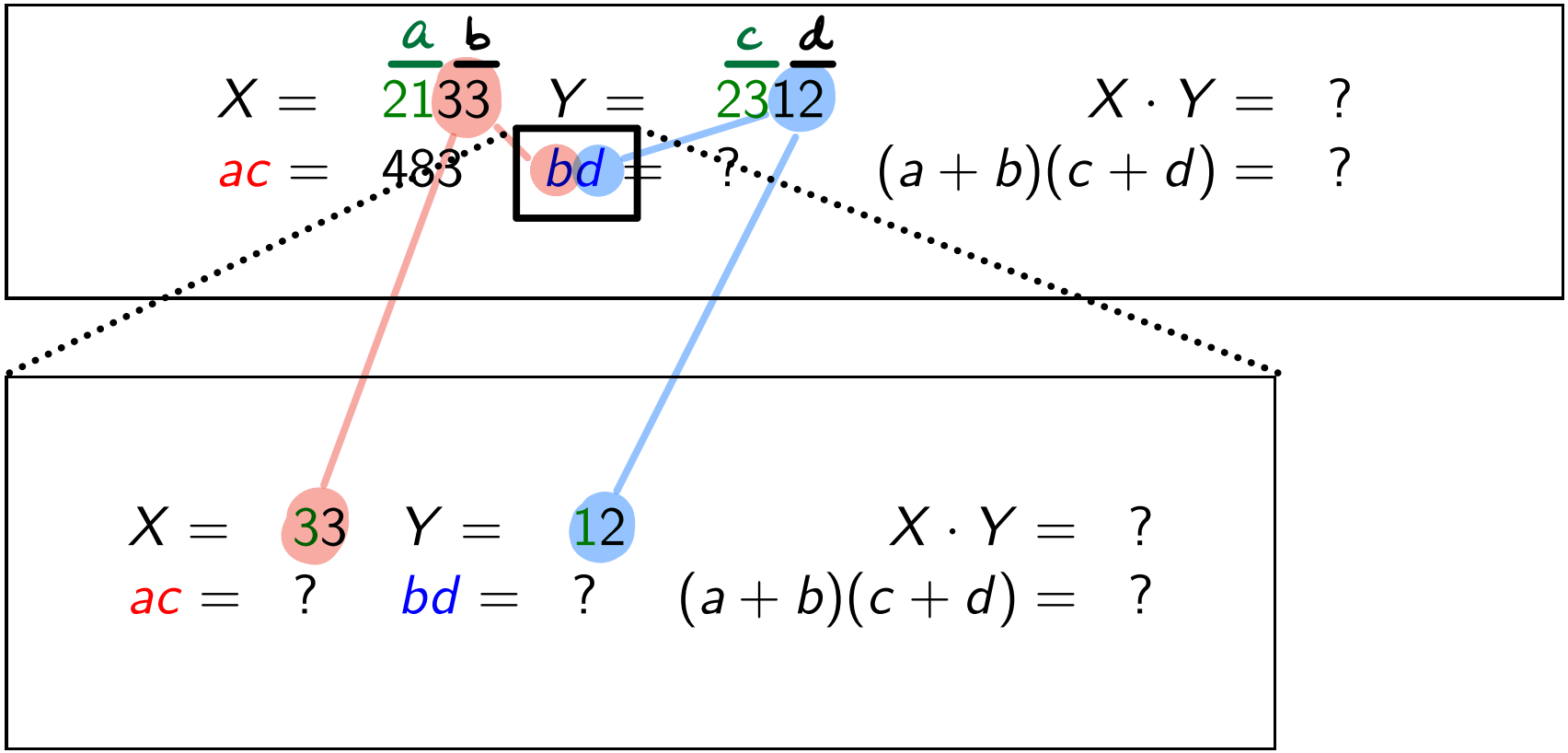
$$ac = 483 \qquad bd = \; ? \qquad (a+b)(c+d) = \; ?$$

Exemplo

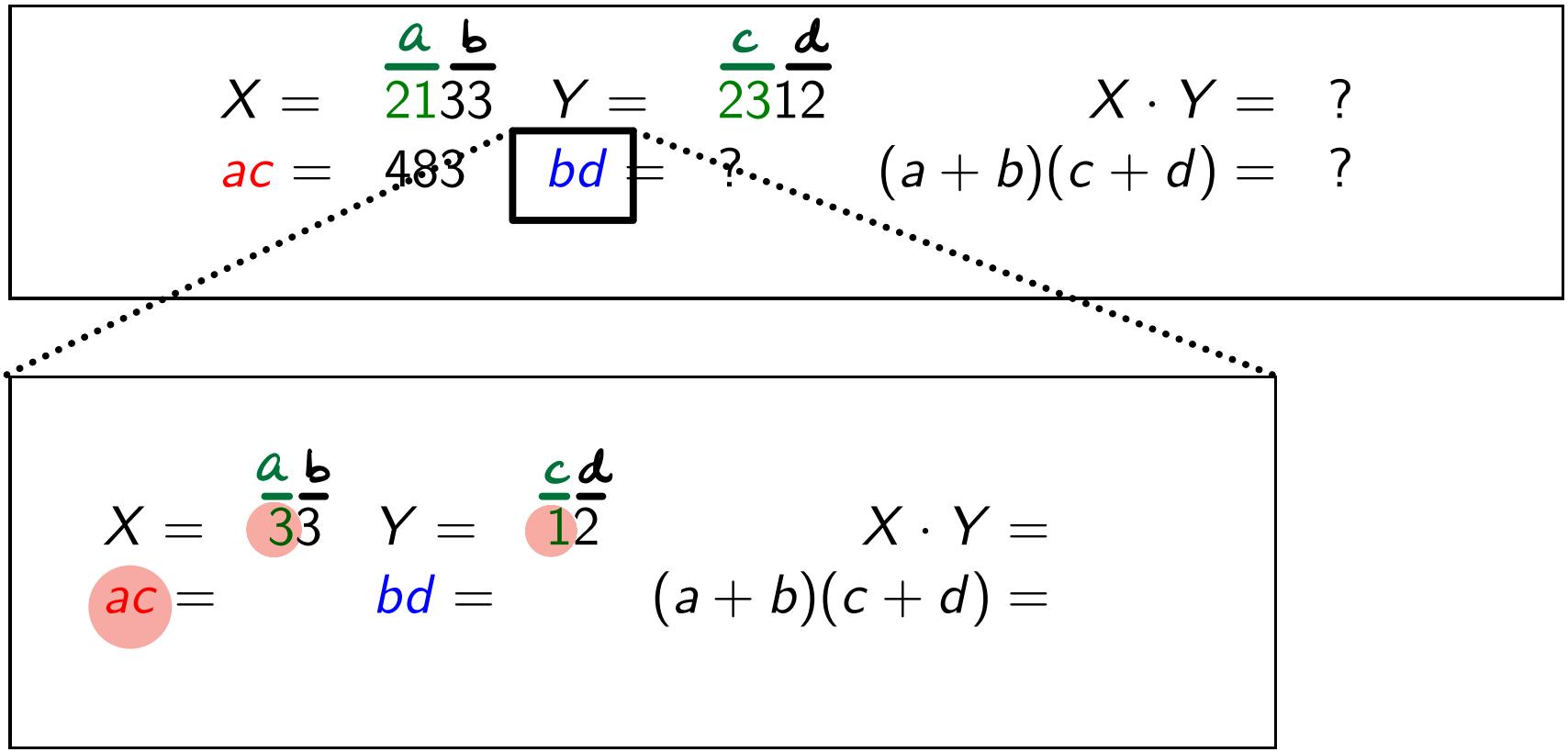
$$X = \overline{21}\,\overline{33} \qquad Y = \overline{23}\,\overline{12} \qquad X \cdot Y = \;?$$

$$ac = 483 \qquad bd = \;? \qquad (a+b)(c+d) = \;?$$

Exemplo



Exemplo



Exemplo

$$X = \overline{21}\,\overline{33} \qquad Y = \overline{23}\,\overline{12} \qquad X \cdot Y = \; ?$$

$$ac = 483 \qquad \boxed{bd = \; ?} \qquad (a+b)(c+d) = \; ?$$

$$X = \overline{3}\,\overline{3} \qquad Y = \overline{1}\,\overline{2} \qquad X \cdot Y =$$

$$ac = 3 \qquad bd = \qquad (a+b)(c+d) =$$

Exemplo

$$X = \overline{a}\,\overline{b}\,\overline{21}\,\overline{33} \qquad Y = \overline{c}\,\overline{d}\,\overline{23}\,\overline{12} \qquad X \cdot Y = \;?$$

$$ac = 483 \qquad bd = \;? \qquad (a+b)(c+d) = \;?$$

$$X = \overline{a}\,\overline{b}\,\overline{3}\,\overline{3} \qquad Y = \overline{c}\,\overline{d}\,\overline{1}\,\overline{2} \qquad X \cdot Y =$$

$$ac = 3 \qquad bd = \qquad (a+b)(c+d) =$$

Exemplo

$$X = \overset{a}{2}\overset{b}{133} \quad Y = \overset{c}{2}\overset{d}{312} \quad X \cdot Y = \; ?$$

$$ac = 483 \quad \boxed{bd = \; ?} \quad (a+b)(c+d) = \; ?$$

$$X = \overset{a}{3}\overset{b}{3} \quad Y = \overset{c}{1}\overset{d}{2} \quad X \cdot Y =$$

$$ac = 3 \quad bd = 6 \quad (a+b)(c+d) =$$

Exemplo

$$X = \overline{a}\,\overline{b}\,\overline{21}\,\overline{33} \qquad Y = \overline{c}\,\overline{d}\,\overline{23}\,\overline{12} \qquad X \cdot Y = \;?$$

$$ac = 483 \qquad \boxed{bd = \;?} \qquad (a+b)(c+d) = \;?$$

$$X = \overline{a}\,\overline{b}\,\overline{33} \qquad Y = \overline{c}\,\overline{d}\,\overline{12} \qquad X \cdot Y =$$

$$ac = 3 \qquad bd = 6 \qquad (a+b)(c+d) =$$

Exemplo

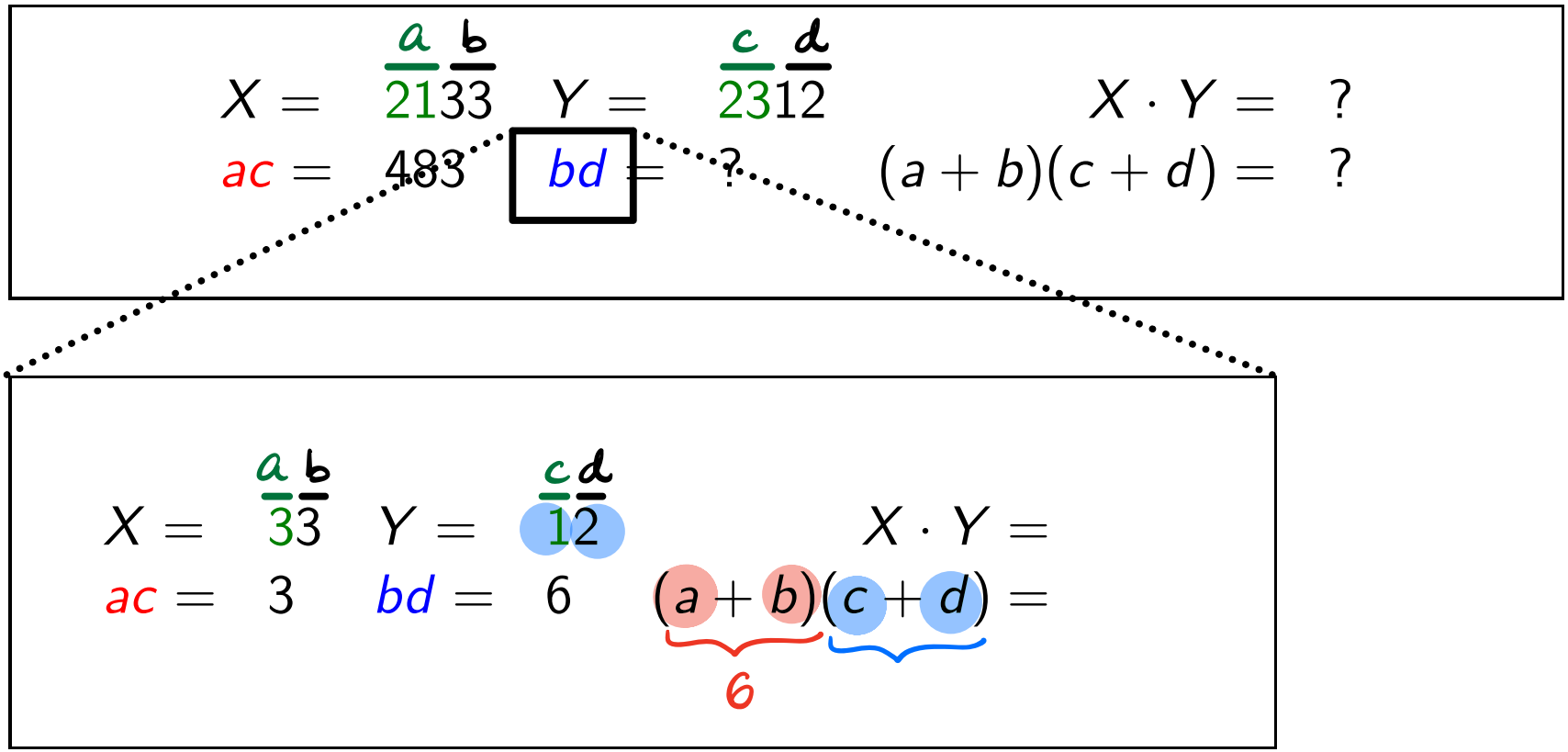
$$X = \overset{a}{2}\overset{b}{1}33 \qquad Y = \overset{c}{2}\overset{d}{3}12 \qquad X \cdot Y = \ ?$$

$$ac = 483 \qquad \boxed{bd = ?} \qquad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{3}\overset{b}{3} \qquad Y = \overset{c}{1}\overset{d}{2} \qquad X \cdot Y =$$

$$ac = 3 \qquad bd = 6 \qquad \underbrace{(a+b)}_{6}(c+d) =$$

Exemplo


a b
2133
X =
c d
2312
Y =
X · Y = ?
ac = 483
bd = ?
(a + b)(c + d) = ?
a b
33
X =
c d
12
Y =
X · Y =
ac = 3
bd = 6
(a + b)(c + d) =
6

Exemplo

$$X = \overset{a}{2}\overset{b}{1}33 \qquad Y = \overset{c}{2}\overset{d}{3}12 \qquad X \cdot Y = \ ?$$

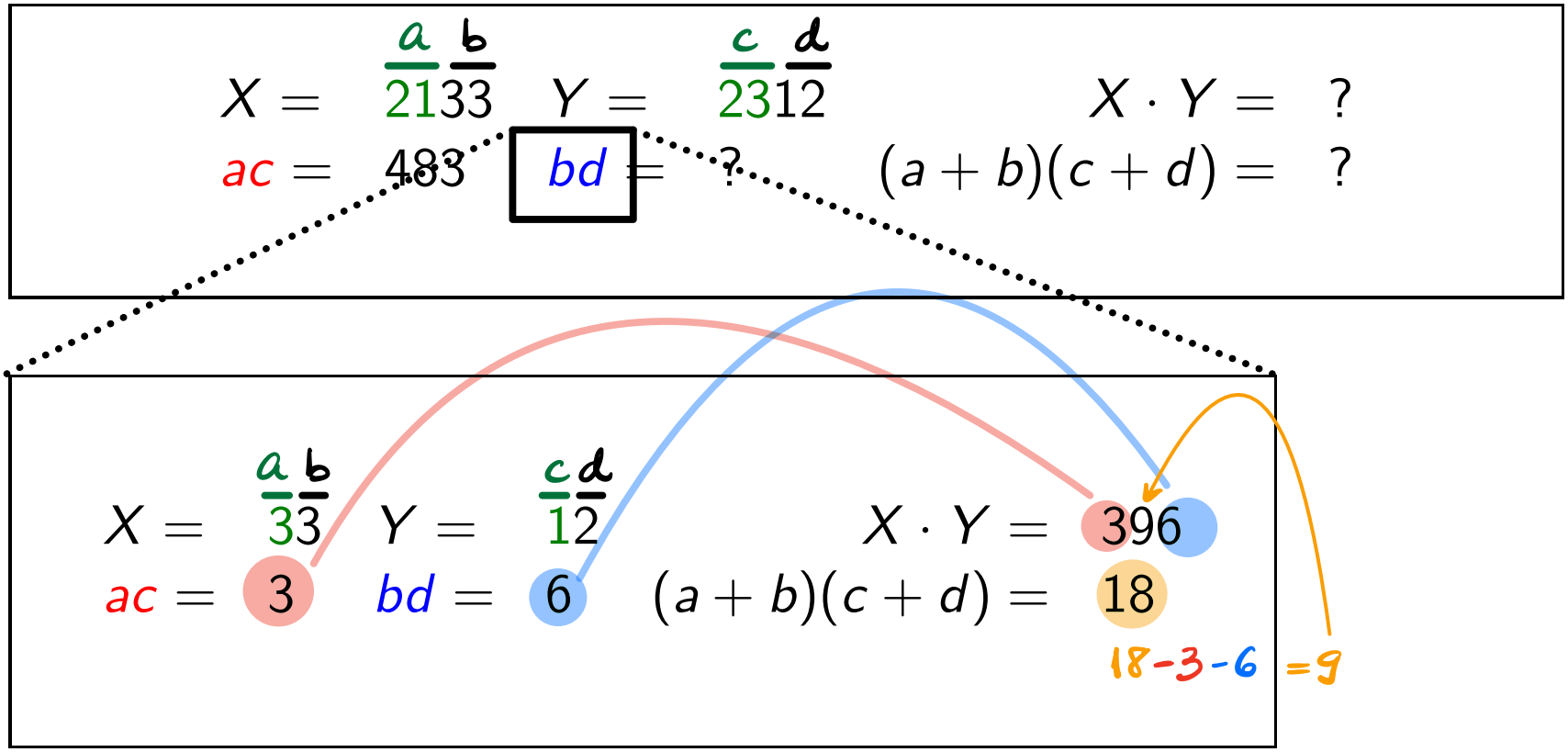
$$ac = 483 \qquad \boxed{bd = ?} \qquad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{3}\overset{b}{3} \qquad Y = \overset{c}{1}\overset{d}{2} \qquad X \cdot Y =$$

$$ac = 3 \qquad bd = 6 \qquad (a+b)(c+d) = 18$$

$a+b = 6 \qquad c+d = 3$

Exemplo


a b
c d
X = 2133
Y = 2312
X · Y = ?
ac = 483
bd = ?
(a + b)(c + d) = ?
a b
c d
X = 33
Y = 12
X · Y = 396
ac = 3
bd = 6
(a + b)(c + d) = 18
18-3-6 =9

Exemplo

$$X = \overset{a}{2}\overset{b}{133} \quad Y = \overset{c}{2}\overset{d}{312} \quad X \cdot Y = ?$$

$$ac = 483 \quad bd = ? \quad (a+b)(c+d) = ?$$

$$X = 33 \quad Y = 12 \quad X \cdot Y = 396$$

$$ac = 3 \quad bd = 6 \quad (a+b)(c+d) = 18$$

Exemplo

$$X = \underline{a}\,\underline{b} = 2133 \qquad Y = \underline{c}\,\underline{d} = 2312 \qquad X \cdot Y = \; ?$$

$$ac = 483 \qquad bd = 396 \qquad (a+b)(c+d) = \; ?$$

Exemplo

$$\underline{a}\ \underline{b} \qquad\qquad \underline{c}\ \underline{d}$$

$X = 2133 \qquad Y = 2312 \qquad X \cdot Y = \ ?$

$ac = 483 \qquad bd = 396 \qquad (a+b)(c+d) = \ ?$

Exemplo

$$\underline{a}\,\underline{b} \qquad \underline{c}\,\underline{d}$$

$X = 2133 \quad Y = 2312 \quad X \cdot Y = \ ?$

$ac = 483 \quad bd = 396 \quad (a+b)(c+d) = \ ?$

$(a+b) = 54$

Exemplo

$$\underline{a}\,\underline{b} \qquad \underline{c}\,\underline{d}$$

$X = 2133 \quad Y = 2312 \quad X \cdot Y = \ ?$

$ac = 483 \quad bd = 396 \quad (a+b)(c+d) = \ ?$

$(a+b)$: 54

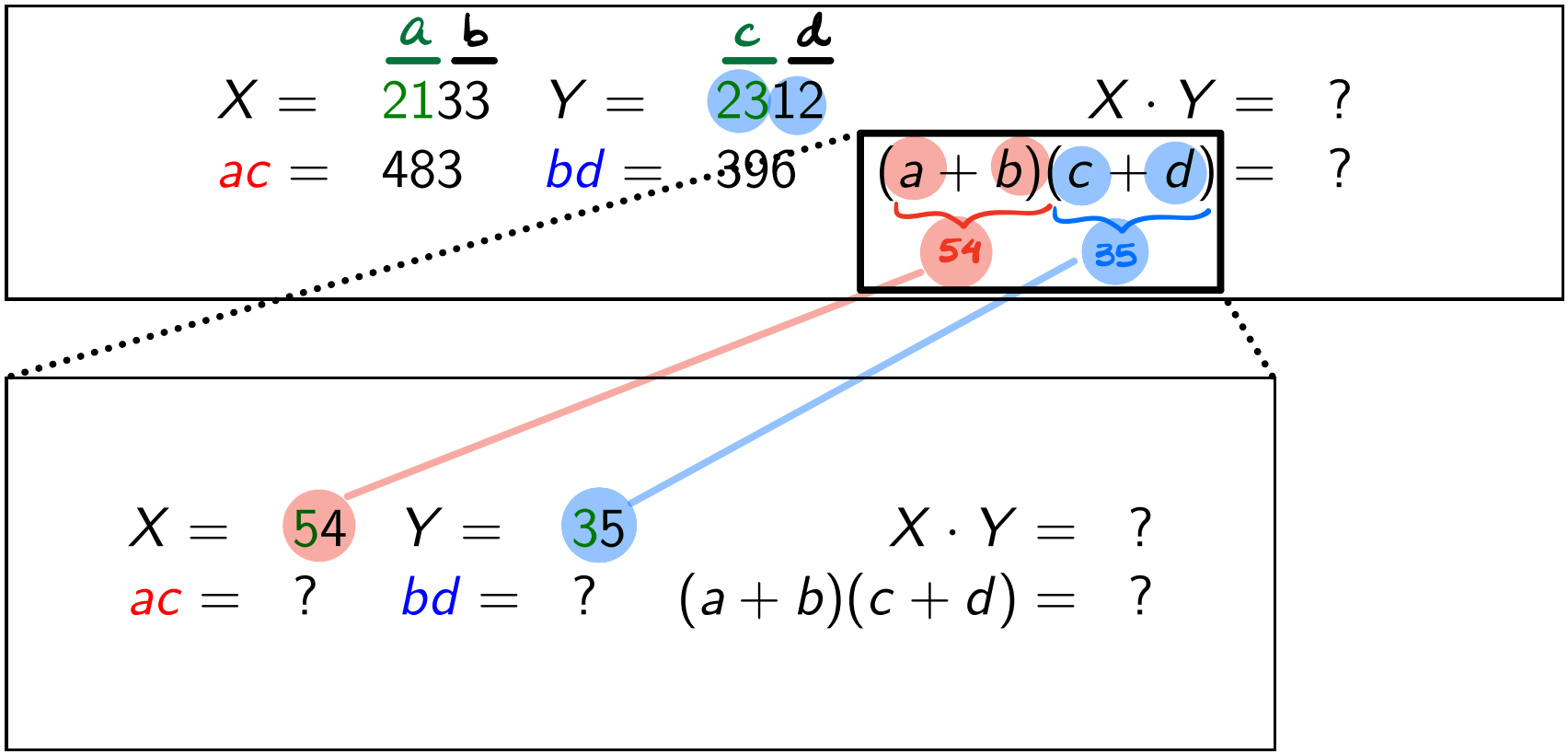
Exemplo

$$\begin{array}{llll} & \underline{a}\,\underline{b} & & \underline{c}\,\underline{d} \\ X = & 2133 & Y = & 2312 \\ ac = & 483 & bd = & 396 \end{array} \qquad X \cdot Y = \; ?$$

$$(a+b)(c+d) = \; ?$$

$a+b$: 54 — $c+d$: 35

Exemplo


a b
c d
X = 2133
Y = 2312
X · Y = ?
ac = 483
bd = 396
(a + b)(c + d) = ?
54
35
X = 54
Y = 35
X · Y = ?
ac = ?
bd = ?
(a + b)(c + d) = ?

Exemplo

$$\underline{a}\ \underline{b} \qquad \underline{c}\ \underline{d}$$

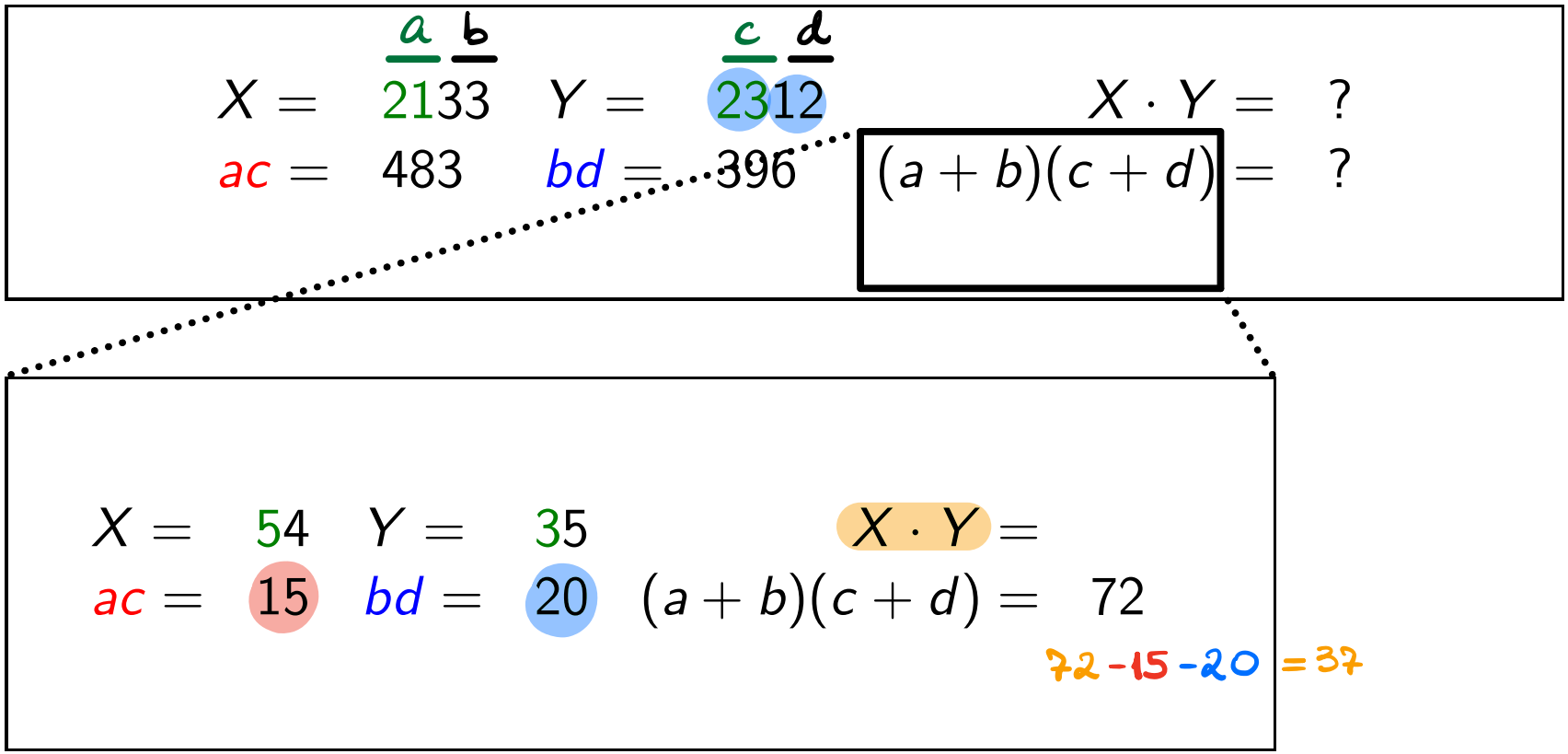
$X = 2133 \quad Y = 2312 \quad X \cdot Y = ?$

$ac = 483 \quad bd = 396 \quad (a+b)(c+d) = ?$

$X = 54 \quad Y = 35 \quad X \cdot Y =$

$ac = 15 \quad bd = 20 \quad (a+b)(c+d) = 72$

Exemplo


a b
c d
X = 2133
Y = 2312
X · Y = ?
ac = 483
bd = 396
(a + b)(c + d) = ?
X = 54
Y = 35
X · Y =
ac = 15
bd = 20
(a + b)(c + d) = 72
72 - 15 - 20 = 37

Exemplo

$a\ b$ $\quad$ $c\ d$

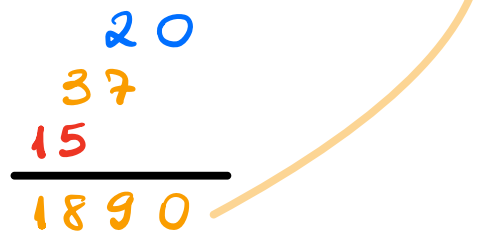
$X = 2133 \quad Y = 2312 \quad X \cdot Y = ?$

$ac = 483 \quad bd = 396 \quad (a+b)(c+d) = ?$

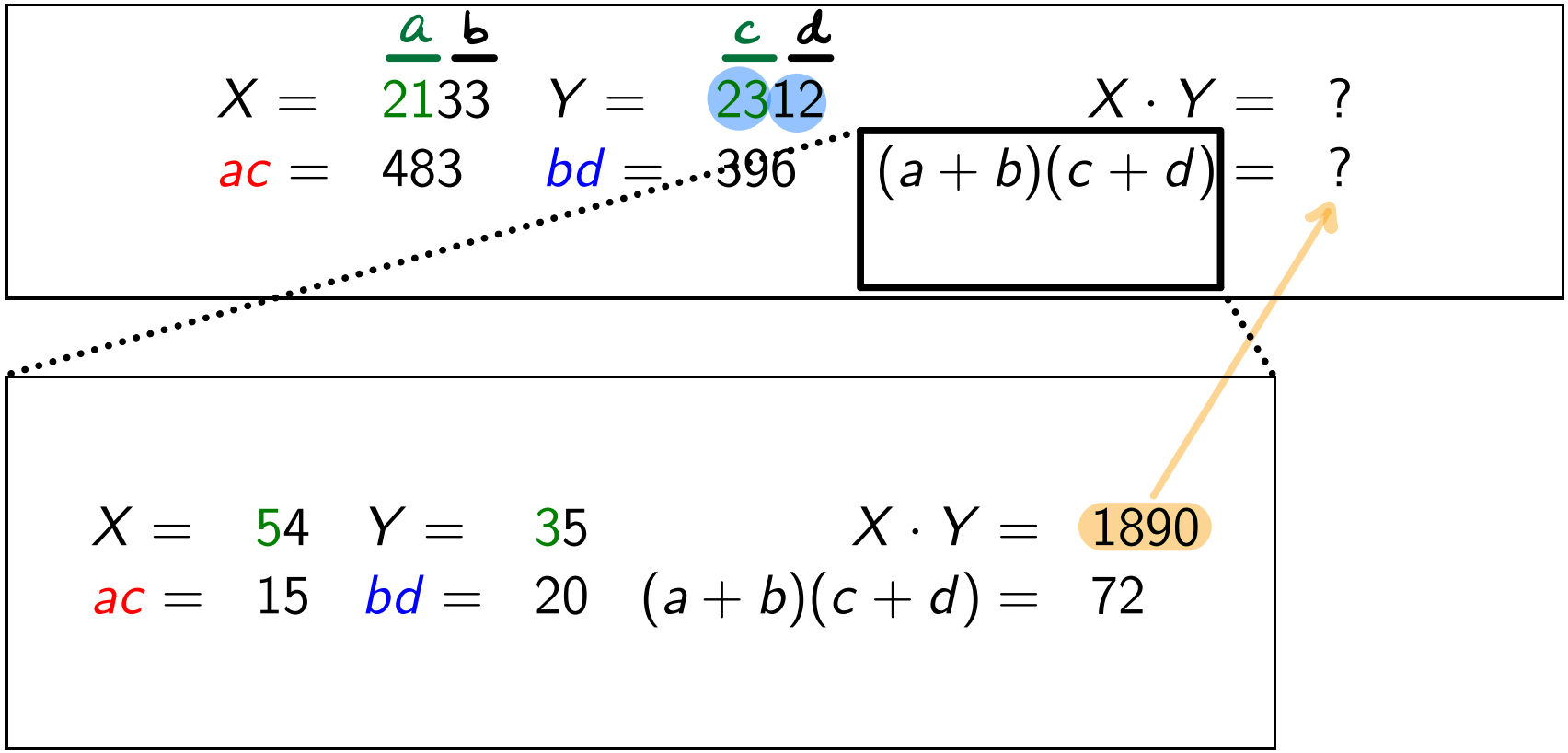
$X = 54 \quad Y = 35 \quad X \cdot Y = 1890$

$ac = 15 \quad bd = 20 \quad (a+b)(c+d) = 72$

$72 - 15 - 20 = 37$



Exemplo


a b
c d
X = 2133
Y = 2312
X · Y = ?
ac = 483
bd = 396
(a + b)(c + d) = ?
X = 54
Y = 35
X · Y = 1890
ac = 15
bd = 20
(a + b)(c + d) = 72

Exemplo

$$X = 2133 \quad Y = 2312 \quad X \cdot Y = ?$$
$$ac = 483 \quad bd = 396 \quad (a+b)(c+d) = 1890$$

Exemplo

$X = 2133$ $Y = 2312$ $X \cdot Y = ?$

$ac = 483$ $bd = 396$ $(a+b)(c+d) = 1890$

$1890 - 483 - 396 = 1011$

Exemplo

$X = 2133 \quad Y = 2312 \quad X \cdot Y = \ ?$

$ac = 483 \quad bd = 396 \quad (a+b)(c+d) = 1890$

$1890 - 483 - 396 = 1011$

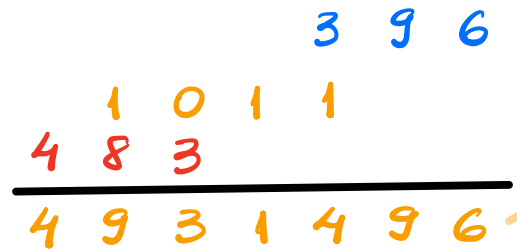
$$
\begin{array}{r}
 & & & 3 & 9 & 6 \\
 & 1 & 0 & 1 & 1 & \\
4 & 8 & 3 & & & \\
\hline
4 & 9 & 3 & 1 & 4 & 9 & 6
\end{array}
$$

Exemplo

$X = 2133 \quad Y = 2312 \quad X \cdot Y = 4931496$

$ac = 483 \quad bd = 396 \quad (a+b)(c+d) = 1890$

$1890 - 483 - 396 = 1011$



Algoritmo Multi

Algoritmo recebe inteiros $X[1\,..\,n]$ e $Y[1\,..\,n]$
e devolve $X \cdot Y$ (Karatsuba e Ofman).

KARATSUBA (X, Y, n)

1 **se** $n \leq 3$ **devolva** $X \cdot Y$
2 $q \leftarrow \lceil n/2 \rceil$
3 $A \leftarrow X[q+1\,..\,n]$ $\quad$ $B \leftarrow X[1\,..\,q]$
4 $C \leftarrow Y[q+1\,..\,n]$ $\quad$ $D \leftarrow Y[1\,..\,q]$
5 $E \leftarrow$ KARATSUBA$(A, C, \lfloor n/2 \rfloor)$
6 $F \leftarrow$ KARATSUBA$(B, D, \lceil n/2 \rceil)$
7 $G \leftarrow$ KARATSUBA$(A+B, C+D, \lceil n/2 \rceil + 1)$
8 $H \leftarrow G - F - E$
9 $R \leftarrow E \times 10^{2q} + H \times 10^{\lceil n/2 \rceil} + F$
10 **devolva** R

$T(n) =$ consumo de tempo do algoritmo
para multiplicar dois inteiros com n algarismos.

Consumo de tempo

linha		todas as execuções da linha
1	$=$	$\Theta(1)$
2	$=$	$\Theta(1)$
3	$=$	$\Theta(n)$
4	$=$	$\Theta(n)$
5	$=$	$T(\lfloor n/2 \rfloor)$
6	$=$	$T(\lceil n/2 \rceil)$
7	$=$	$T(\lceil n/2 \rceil + 1) + \Theta(n)$
8	$=$	$\Theta(n)$
9	$=$	$\Theta(n)$
10	$=$	$\Theta(1)$
total	$=$	$T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + T(\lceil n/2 \rceil + 1) + \Theta(n)$

Consumo de tempo

Nosso estudo de recorrências sugere que a solução da recorrência

$$\begin{aligned} T(n) &= \Theta(1) \quad \text{para } n = 1, 2, 3 \\ T(n) &= T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + T(\lceil n/2 \rceil + 1) + \Theta(n) \quad n \geq 4 \end{aligned}$$

está na mesma classe Θ que a solução de

$$T'(n) = 3T'(n/2) + n$$

n	1	2	4	8	16	32	64	128	256	512
$T'(n)$	1	5	19	65	211	665	2059	6305	19171	58025

Recorrência

Considere a recorrência

$$
\begin{aligned}
R(1) &= 1 \\
R(2) &= 1 \\
R(3) &= 1 \\
R(n) &= 3R(\lceil \tfrac{n}{2} \rceil + 1) + n \quad \text{para } n = 4, 5, 6 \ldots
\end{aligned}
$$

n	1	2	3	4	5	6	7	8	9	10
$T(n)$	1	1	1	7	14	15	29	36	45	53
$R(n)$	1	1	1	7	26	27	85	86	90	91

Recorrência

Considere a recorrência

$$
\begin{aligned}
R(1) &= 1 \\
R(2) &= 1 \\
R(3) &= 1 \\
R(n) &= 3R(\lceil \tfrac{n}{2} \rceil + 1) + n \quad \text{para } n = 4, 5, 6 \ldots
\end{aligned}
$$

n	1	2	3	4	5	6	7	8	9	10
$T(n)$	1	1	1	7	14	15	29	36	45	53
$R(n)$	1	1	1	7	26	27	85	86	90	91

Vamos mostra que $R(n)$ é $\mathrm{O}(n^{\lg 3})$.
Isto implica que $T(n)$ é $\mathrm{O}(n^{\lg 3})$.

Solução assintótica da recorrência

Vou mostrar que $R(n) \leq 31\,(n-3)^{\lg 3} - 6n$ para $n = 4, 5, 6, \ldots$

n	1	2	3	4	5	6	7	8	9	10
$R(n)$	1	1	1	7	26	27	85	86	90	91
$31(n-3)^{\lg 3} - 6n$	$*$	$*$	$*$	7	63	119	237	324	473	5910

Solução assintótica da recorrência

Vou mostrar que $R(n) \leq 31\,(n-3)^{\lg 3} - 6n$ para $n = 4, 5, 6, \ldots$

n	1	2	3	4	5	6	7	8	9	10
$R(n)$	1	1	1	7	26	27	85	86	90	91
$31(n-3)^{\lg 3} - 6n$	$*$	$*$	$*$	7	63	119	237	324	473	5910

Prova:

Se $n = 4$, então $R(n) = 7 = 31(n-3)^{\lg 3} - 6n$.

Solução assintótica da recorrência

Prova: (continuação) Se $n \geq 5$ vale que

$$
\begin{aligned}
R(n) &= 3R(\lceil n/2 \rceil + 1) + n \\
&\overset{\text{hi}}{\leq} 3(31(\lceil n/2 \rceil + 1 - 3)^{\lg 3} - 6(\lceil n/2 \rceil + 1)) + n \\
&\leq 3(31(\frac{(n+1)}{2} - 2)^{\lg 3} - 6(\frac{n}{2} + 1)) + n \\
&= 3(31(\frac{(n-3)}{2})^{\lg 3} - 3n - 6) + n \\
&= 3(31\frac{(n-3)^{\lg 3}}{2^{\lg 3}} - 3n - 6) + n \\
&= 3 \cdot 31\frac{(n-3)^{\lg 3}}{3} - 9n - 18 + n \\
&= 31(n-3)^{\lg 3} - 6n - 2n - 18 \\
&< 31(n-3)^{\lg 3} - 6n = \Theta(n^{\lg 3})
\end{aligned}
$$

Iiiiéééésssss!

Conclusões

$T'(n)$ é $\Theta(n^{\lg 3})$.

Logo $T(n)$ é $\Theta(n^{\lg 3})$.

O consumo de tempo do algoritmo KARATSUBA é $\Theta(n^{\lg 3})$
$(1{,}584 < \lg 3 < 1{,}585)$.

Mais conclusões

Consumo de tempo de
algoritmos para multiplicação de inteiros:

Jardim de infância	$\Theta(n\,10^n)$
Ensino fundamental	$\Theta(n^2)$
Karatsuba e Ofman'60	$\mathrm{O}(n^{1.585})$
Toom e Cook'63	$\mathrm{O}(n^{1.465})$
(divisão e conquista; generaliza o acima)	
Schönhage e Strassen'71	$\mathrm{O}(n \lg n \lg\lg n)$
(FFT em aneis de tamanho específico)	
Fürer'07	$\mathrm{O}(n \lg n\, 2^{\mathrm{O}(\log^* n)})$
Harvey e van der Hoeven'20	$\mathrm{O}(n \log n)$
(Gaussian ressampling, multidimensional DFT, Nussbaumer's fast polynomial transforms)	

Ambiente experimental

A plataforma utilizada nos experimentos é um PC rodando Linux Debian ?.? com um processador Pentium II de 233 MHz e 128MB de memória RAM .

Os códigos estão compilados com o gcc versão 2.7.2.1 e opção de compilação -O2.

As implementações comparadas neste experimento são as do algoritmo do ensino fundamental e do algoritmo KARATSUBA.

O programa foi escrito por Carl Burch:

`http://www-2.cs.cmu.edu/~cburch/251/karat/.`

Resultados experimentais

n	Ensino Fund.	KARATSUBA
4	0.005662	0.005815
8	0.010141	0.010600
16	0.020406	0.023643
32	0.051744	0.060335
64	0.155788	0.165563
128	0.532198	0.470810
256	1.941748	1.369863
512	7.352941	4.032258

Tempos em 10^3 segundos.

Multiplicação de matrizes

Problema: Dadas duas matrizes $X[1\,..\,n, 1\,..\,n]$ e $Y[1\,..\,n, 1\,..\,n]$, calcular o produto $X \cdot Y$.

O algoritmo tradicional de multiplicação de matrizes consome tempo

Multiplicação de matrizes

Problema: Dadas duas matrizes $X[1\,..\,n, 1\,..\,n]$ e $Y[1\,..\,n, 1\,..\,n]$, calcular o produto $X \cdot Y$.

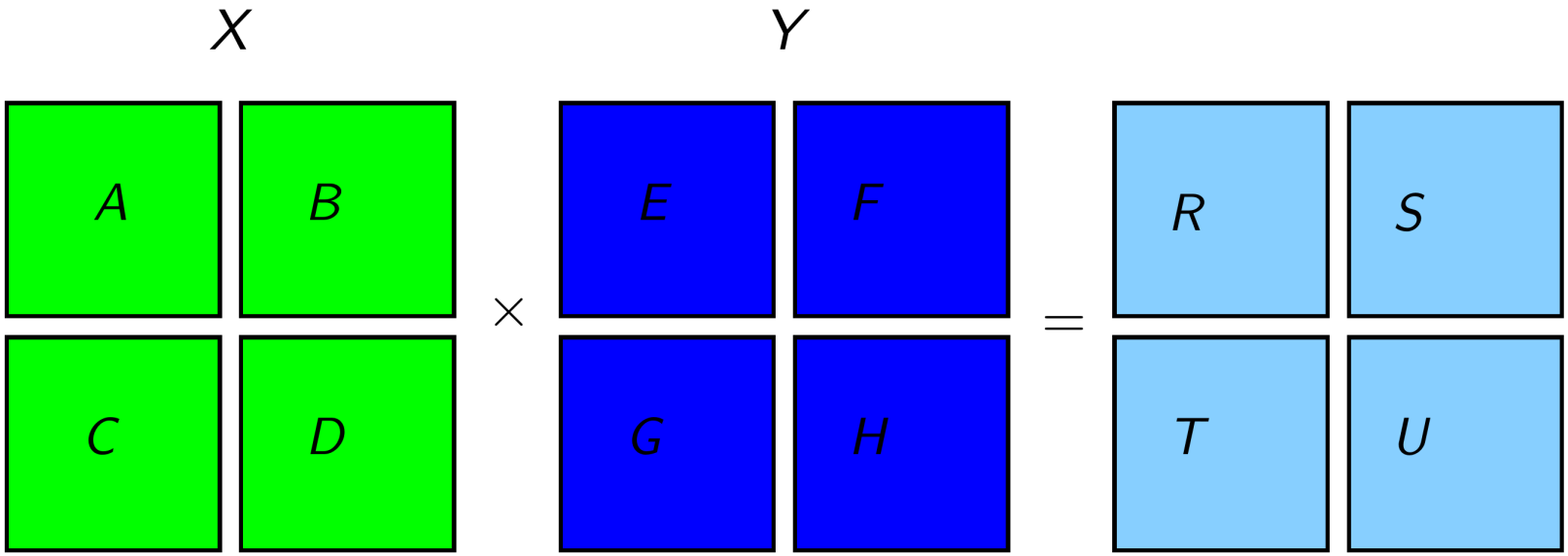
O algoritmo tradicional de multiplicação de matrizes consome tempo $\Theta(n^3)$.

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \times \begin{pmatrix} E & F \\ G & H \end{pmatrix} = \begin{pmatrix} R & S \\ T & U \end{pmatrix}$$

$$\begin{aligned} R &= AE + BG \\ S &= AF + BH \\ T &= CE + DG \\ U &= CF + DH \end{aligned} \tag{1}$$

Solução custa R$ 8,04

Divisão e conquista



$$R = AE + BG$$
$$S = AF + BH$$
$$T = CE + DG$$
$$U = CF + DH$$

Algoritmo de Multi-Mat

Algoritmo recebe matrizes $X[1\,..\,n, 1\,..\,n]$ e $Y[1\,..\,n, 1\,..\,n]$ e devolve $X \cdot Y$.

```
MULTI-M (X, Y, n)
 1  se n = 1 devolva X · Y
 2  (A, B, C, D) ← PARTICIONE(X, n)
 3  (E, F, G, H) ← PARTICIONE(Y, n)
 4  R ← MULTI-M(A, E, n/2) + MULTI-M(B, G, n/2)
 5  S ← MULTI-M(A, F, n/2) + MULTI-M(B, H, n/2)
 6  T ← MULTI-M(C, E, n/2) + MULTI-M(D, G, n/2)
 7  U ← MULTI-M(C, F, n/2) + MULTI-M(D, H, n/2)
 8  P ← CONSTRÓI-MAT(R, S, T, U)
 9  devolva P
```

$T(n) =$ consumo de tempo do algoritmo
para multiplicar duas matrizes de n linhas e n colunas.

Consumo de tempo

linha		todas as execuções da linha
1	=	$\Theta(1)$
2	=	$\Theta(n^2)$
3	=	$\Theta(n^2)$
4	=	$T(n/2) + T(n/2)$
5	=	$T(n/2) + T(n/2)$
6	=	$T(n/2) + T(n/2)$
7	=	$T(n/2) + T(n/2)$
8	=	$\Theta(n^2)$
9	=	$\Theta(1)$
total	=	$8\,T(n/2) + \Theta(n^2)$

Consumo de tempo

Nosso estudo de recorrências sugere
que a solução da recorrência

$$\begin{aligned} T(1) &= \Theta(1) \\ T(n) &= 8\,T(n/2) + \Theta(n^2) \quad \text{para } n = 2, 3, 4, \ldots \end{aligned}$$

está na mesma classe Θ que a solução de

$$T'(n) = 8\,T'(n/2) + n^2$$

n	1	2	4	8	16	32	64	128	256
$T'(n)$	1	12	112	960	7936	64512	520192	4177920	33488896

Conclusões

$T'(n)$ é $\Theta(n^3)$.

Logo $T(n)$ é $\Theta(n^3)$.

O consumo de tempo do algoritmo MULTI-M é $\Theta(n^3)$.

Strassen: $X \cdot Y$ por apenas R$ 7,18

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \times \begin{pmatrix} E & F \\ G & H \end{pmatrix} = \begin{pmatrix} R & S \\ T & U \end{pmatrix}$$

Strassen: $X \cdot Y$ por apenas R$ 7,18

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \times \begin{pmatrix} E & F \\ G & H \end{pmatrix} = \begin{pmatrix} R & S \\ T & U \end{pmatrix}$$

$$P_1 = A(F - H) = AF - AH$$
$$P_2 = (A + B)H = AH + BH$$
$$P_3 = (C + D)E = CE + DE$$
$$P_4 = D(G - E) = DG - DE$$
$$P_5 = (A + D)(E + H) = AE + AH + DE + DH$$
$$P_6 = (B - D)(G + H) = BG + BH - DG - DH$$
$$P_7 = (A - C)(E + F) = AE + AF - CE - CF$$

Strassen: $X \cdot Y$ por apenas R$ 7,18

$$P_1 = A(F - H) = AF - AH$$
$$P_2 = (A + B)H = AH + BH$$
$$P_3 = (C + D)E = CE + DE$$
$$P_4 = D(G - E) = DG - DE$$
$$P_5 = (A + D)(E + H) = AE + AH + DE + DH$$
$$P_6 = (B - D)(G + H) = BG + BH - DG - DH$$
$$P_7 = (A - C)(E + F) = AE + AF - CE - CFD$$

$$R = P_5 + P_4 - P_2 + P_6 = AE + BG$$
$$S = P_1 + P_2 = AF + BH$$
$$T = P_3 + P_4 = CE + DG$$
$$U = P_5 + P_1 - P_3 - P_7 = CF + DH$$

Algoritmo de Strassen

STRASSEN (X, Y, n)

1 **se** $n = 1$ **devolva** $X \cdot Y$
2 $(A, B, C, D) \leftarrow$ PARTICIONE(X, n)
3 $(E, F, G, H) \leftarrow$ PARTICIONE(Y, n)
4 $P_1 \leftarrow$ STRASSEN$(A, F - H, n/2)$
5 $P_2 \leftarrow$ STRASSEN$(A + B, H, n/2)$
6 $P_3 \leftarrow$ STRASSEN$(C + D, E, n/2)$
7 $P_4 \leftarrow$ STRASSEN$(D, G - E, n/2)$
8 $P_5 \leftarrow$ STRASSEN$(A + D, E + H, n/2)$
9 $P_6 \leftarrow$ STRASSEN$(B - D, G + H, n/2)$
10 $P_7 \leftarrow$ STRASSEN$(A - C, E + F, n/2)$
11 $R \leftarrow P_5 + P_4 - P_2 + P_6$
12 $S \leftarrow P_1 + P_2$
13 $T \leftarrow P_3 + P_4$
14 $U \leftarrow P_5 + P_1 - P_3 - P_7$
15 **devolva** $P \leftarrow$ CONSTRÓI-MAT(R, S, T, U)

Consumo de tempo

linha		todas as execuções da linha
1	$=$	$\Theta(1)$
2–3	$=$	$\Theta(n^2)$
4–10	$=$	$7\,T(n/2) + \Theta(n^2)$
11–14	$=$	$\Theta(n^2)$
15	$=$	$\Theta(n^2)$
total	$=$	$7\,T(n/2) + \Theta(n^2)$

Consumo de tempo

Nosso estudo de recorrências sugere que a solução da recorrência

$$\begin{aligned} T(1) &= \Theta(1) \\ T(n) &= 7\,T(n/2) + \Theta(n^2) \quad \text{para } n = 2, 3, 4, \ldots \end{aligned}$$

está na mesma classe Θ que a solução de

$$T'(n) = 7\,T'(n/2) + n^2$$

n	1	2	4	8	16	32	64	128	256
$T'(n)$	1	11	93	715	5261	37851	269053	1899755	13363821

Conclusões

$T'(n)$ é $\Theta(n^{\lg 7})$.

Logo $T(n)$ é $\Theta(n^{\lg 7})$.

O consumo de tempo do algoritmo STRASSEN é $\Theta(n^{\lg 7})$
$(2{,}80 < \lg 7 < 2{,}81)$.

Mais conclusões

Consumo de tempo de algoritmos para multiplicação de matrizes:

Ensino fundamental	$\Theta(n^3)$
Strassen (1969)	$O(n^{2.807})$
⋮	⋮
Coppersmith e Winograd (1987)	$O(n^{2.3755})$
Stothers (2010)	$O(n^{2.3736})$
Williams (2013)	$O(n^{2.3728642})$
Le Gall (2014)	$O(n^{2.3728639})$
Alman e Williams (2020)	$O(n^{2.3728596})$
Duan, Wu e Zhou (2023)	$O(n^{2.371866})$
Williams, Xu, Xu e Zhou (2024)	$O(n^{2.371552})$
Alman, Duan, Williams, Xu, Xu e Zhou (2025)	$O(n^{2.371339})$

