DMat-12

5.3: Strukturel induktion.

S: en rekursivt defineret mængde.
$P(x)$: et åbent udsagn, $x \in S$.

For at bevise at $P(x)$ er sand for alle $x \in S$ skal vi:
Basisskridt: bevise at $P(x)$ er sand for ethvert x indført i basisskridtet af definitionen af S
Rekursionsskridt: bevise at hvis x er konstrueret fra $x_1, \ldots, x_\ell$ i rekursionsskridtet af definitionen af S og hvis $P(x_1), \ldots, P(x_\ell)$ er sande så er $P(x)$ sand.

EKS S er rekursivt definert:

Basisskritt $(1,4) \in S$ og $(3,2) \in S$

Rekursjonsskritt Hvis $(a,b) \in S$ og $(c,d) \in S$ så er $(a+c, b+d) \in S$.

Antal rekursion Elementer i S

0: $(1,4)$, $(3,2)$

1: $(2,8)$, $(4,6)$, $(6,4)$

2: $(4,16), (6,14), (8,12), \cancel{(8,12)}, (10,10), (12,8)$

$(3,12), (5,10), (7,8), \cancel{(5,10)}, (7,8), (9,6)$

Påstand: Hvis $(a,b) \in S$ så går 5 op i $a+b$.

<u>Bevis</u> ved strukturel induktion

<u>Basisskridt</u> $(1,4)$, $5 \mid 1+4$

$(3,2)$. $5 \mid 3+2$ OK

<u>Rekursionsskridt</u>

Lad $(a,b) \in S$, $(c,d) \in S$

og antag at $5 \mid a+b$ og $5 \mid c+d$.

Betragt $(a+c, b+d)$

$$(a+c)+(b+d) = (a+b)+(c+d)$$

5 går op i dette, da 5 går op i hver parentes.

Påstanden er altså sand for alle $(a,b) \in S$.

5.4

$$b^n \bmod m$$

$$ac \bmod m = (a \bmod m)\cdot(c \bmod m) \bmod m$$

$$b^0 = 1$$

$$b^{2k} \bmod m = b^k \cdot b^k \bmod m = (b^k \bmod m)(b^k \bmod m) \bmod m$$

$$b^{2k+1} \bmod m = \left(\left(b^k \bmod m\right)^2 \bmod m\right)\cdot b \bmod m.$$

5.4: Rekursive algoritmer.

Algoritme 4:

Rekursiv modulær eksponentiering Side 355

---

procedure mpower (b, n, m: heltal hvor $b > 0$, $n \geq 0$, $m \geq 2$)
if $n = 0$ **then**
    return 1
else
    if n er lige **then**
        return mpower$(b, \frac{n}{2}, m)^2 \mod m$
    else
        return (mpower$(b, \frac{n-1}{2}, m)^2 \mod m) \cdot b \mod m$
$\{$ outputtet er $b^n \mod m\}$

EKS

$$4^9 \mod 7 = \left(\left(4^4 \mod 7\right)^2 \mod 7\right) \cdot 4 \mod 7 =$$

$$\left(4^2 \mod 7\right) \cdot 4 \mod 7 = \left(16 \mod 7\right) \cdot 4 \mod 7 =$$

$$2 \cdot 4 \mod 7 = 8 \mod 7 = \underline{\underline{1.}}$$

$$4^4 \mod 7 = \left(4^2 \mod 7\right)^2 \mod 7 = 2^2 \mod 7$$

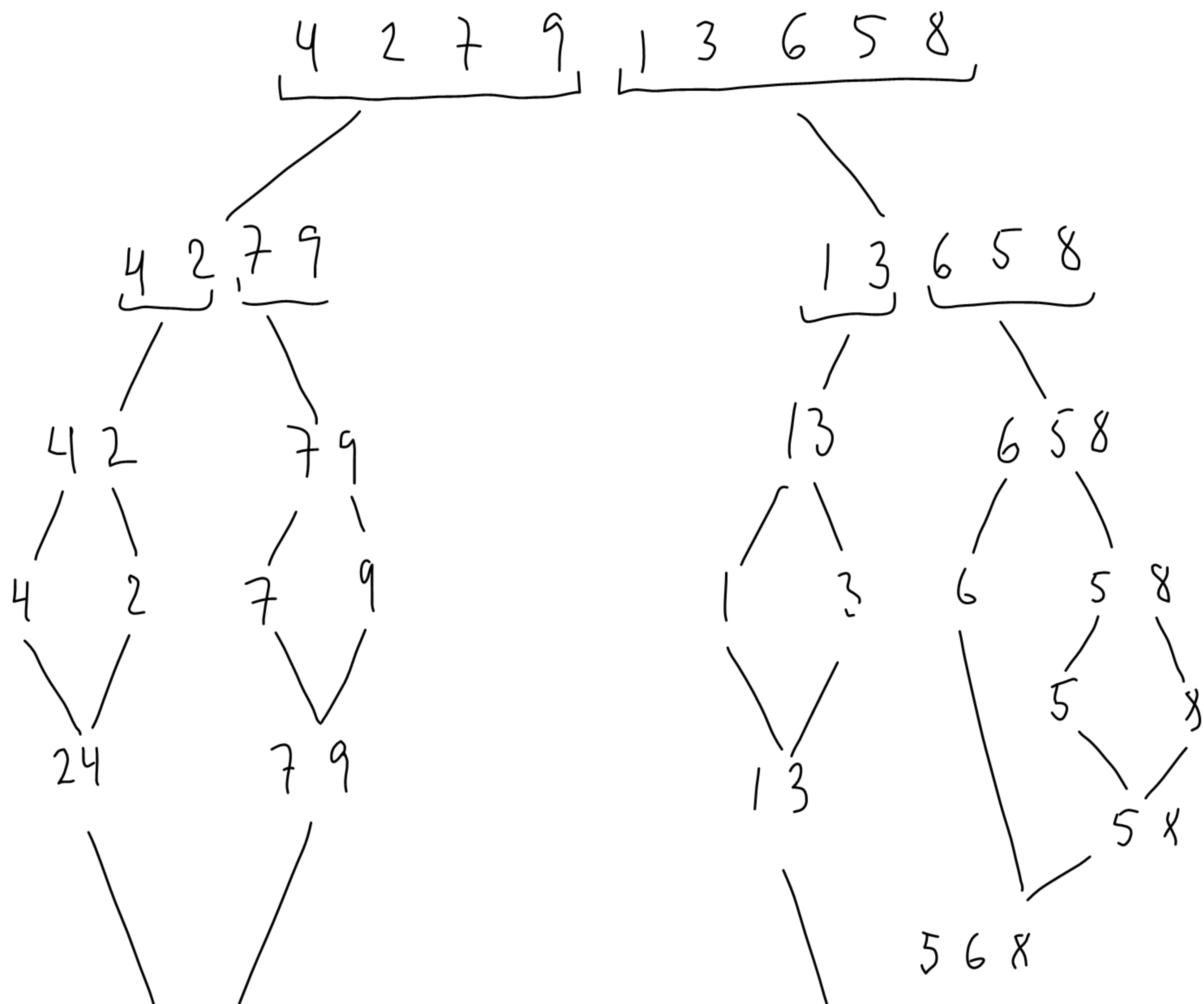
$$= 4 \mod 7 = 4$$

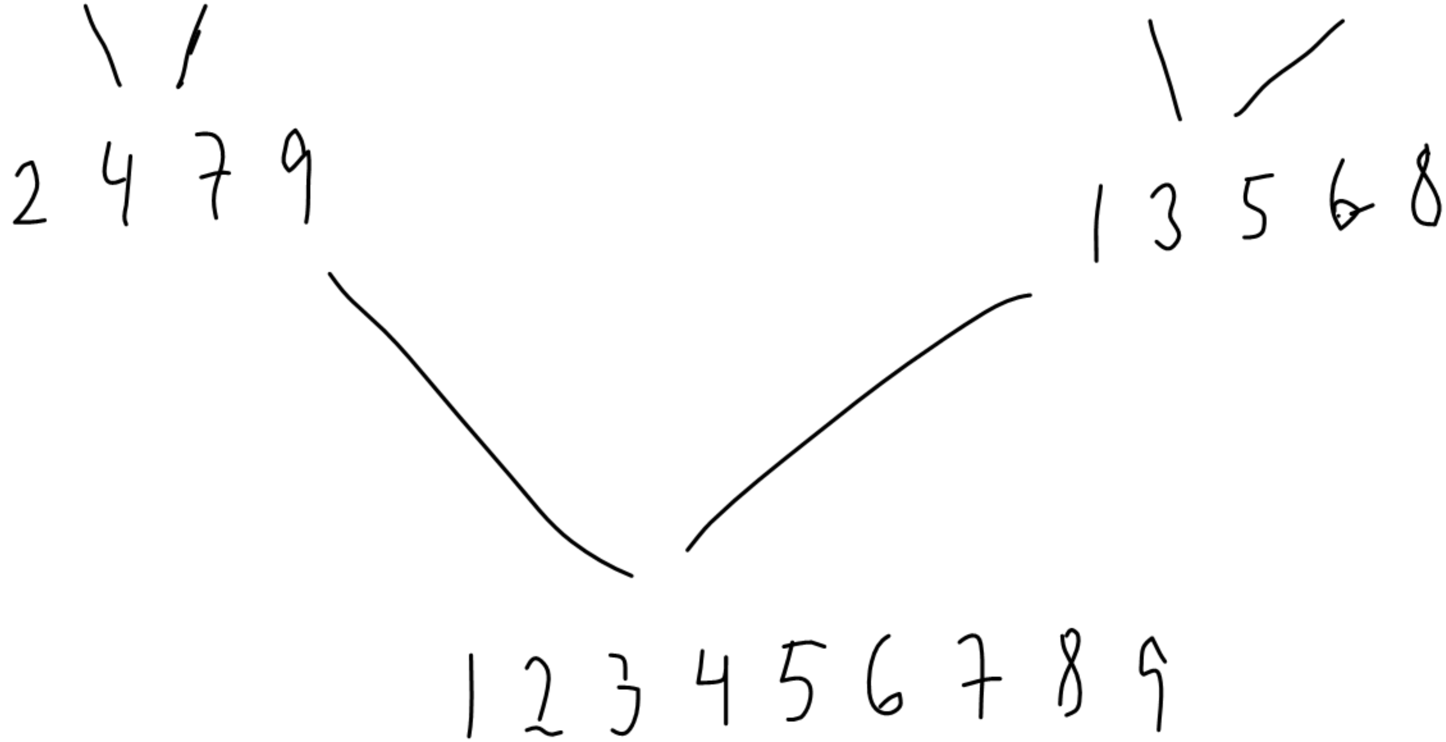
$$4^2 \mod 7 = \left(4 \mod 7\right)^2 \mod 7 = 4^2 \mod 7 =$$

$$16 \mod 7 = 2$$

procedure mergesort($L = a_1, \dots, a_n$ liste af tal)
if $n > 1$ **then**
  $m := \lfloor \frac{n}{2} \rfloor$
  $L_1 := a_1, \dots, a_m$
  $L_2 := a_{m+1}, \dots, a_n$
  $L :=$ merge(mergesort(L_1), mergesort(L_2))

Merge sort har tidskompleksitet $O(n \log n)$.
Bubble sort har tidskompleksitet $O(n^2)$.
Merge sort er altså betydeligt hurtigere end Bubble sort (når n er stor).


4 2 7 9
1 3 6 5 8
4 2 7 9
1 3
6 5 8
4 2
7 9
13
6 5 8
4
2
7
9
1
3
6
5 8
5
8
24
7 9
1 3
5 8
5 6 8



2 4 7 9
1 3 5 6 8
1 2 3 4 5 6 7 8 9