Př. 10/4: lin. kongruenční generátor náh. čísel

Ověřte, zda lineární kongruenční generátor s danými parametry má maximální možnou délku periody.

a) $x_{n+1} = (91x_n + 49)\ mod\ 600$,

b) $x_{n+1} = (8x_n + 80)\ mod\ 49$,

c) $x_{n+1} = (37x_n + 55)\ mod\ 144$,

d) $x_{n+1} = (99x_n + 81)\ mod\ 113$.

Př. 10/4: lin. kongruenční generátor náh. čísel

Ověřte, zda lineární kongruenční generátor s danými parametry má maximální možnou délku periody.

a) $x_{n+1} = (91x_n + 49)\ mod\ 600$,
b) $x_{n+1} = (8x_n + 80)\ mod\ 49$,
c) $x_{n+1} = (37x_n + 55)\ mod\ 144$,
d) $x_{n+1} = (99x_n + 81)\ mod\ 113$.

a ∤ b
2 ∤ 10
~~10k2~~

Př. 10/4: lin. kongruenční generátor náh. čísel

Ověřte, zda lineární kongruenční generátor s danými parametry má maximální možnou délku periody.

a) $x_{n+1} = (91x_n + 49) \ mod \ 600$,
b) $x_{n+1} = (8x_n + 80) \ mod \ 49$,
c) $x_{n+1} = (37x_n + 55) \ mod \ 144$,
d) $x_{n+1} = (99x_n + 81) \ mod \ 113$.

A = 91, C = 49, m = 600

1) $\gcd(C, m) = 1$
2) prime factors of m / $A-1$
3) $4 \mid m \Rightarrow 4 \mid A-1$

a) $\gcd(49, 600) = 1$
$49 = 7 \cdot 7$
$600 = 2^3 \cdot 3 \cdot 5^2$
$A-1 = 90$
$2 \mid 90, \ 3 \mid 90, \ 5 \mid 90$ ✓
$4 \nmid 600$

b) $\gcd(80, 49) = 1$
$80 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5$
$49 = 7 \cdot 7$
$A-1 = 7$
$7 \mid 7$ ✓
$4 \nmid 49$

c) $\gcd(55, 144) = 1$
$55 = 11 \cdot 5$
$144 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$
$A-1 = 36$
$2 \mid 36 \ \ 3 \mid 36$
$4 \mid 144 \Rightarrow 4 \mid 36$ ✓

d) $\gcd(81, 113) = 1$
$81 = 3 \cdot 3 \cdot 3 \cdot 3$
$113 = 113$
$A-1 = 98$
$113 \nmid 98$ ✗

Př. 10/4: lin. kongruenční generátor náh. čísel

Ověřte, zda lineární kongruenční generátor s danými parametry má maximální možnou délku periody.

a) $x_{n+1} = (91x_n + 49) \ mod \ 600$,
b) $x_{n+1} = (8x_n + 80) \ mod \ 49$,
c) $x_{n+1} = (37x_n + 55) \ mod \ 144$,
d) $x_{n+1} = (99x_n + 81) \ mod \ 113$.

1) $\gcd(c, m) = 1$
2) prime factors of m / $A-1$
3) $4 \mid m \Rightarrow 4 \mid A-1$

a) $\gcd(49, 600) = 1$
$49 = 7 \cdot 7$
$600 = 2^3 \cdot 3 \cdot 5^2$
$A-1 = 90$
$2 \mid 90$, $3 \mid 90$, $5 \mid 90$
$4 \nmid 600$ ✗

b) $\gcd(80, 49) = 1$
$80 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5$
$49 = 7 \cdot 7$
$A-1 = 7$
$7 \mid 7$
$4 \nmid 49$ ✓

c) $\gcd(55, 144) = 1$
$55 = 11 \cdot 5$
$144 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$
$A-1 = 36$
$2 \mid 36$ $3 \mid 36$
$4 \mid 144 \Rightarrow 4 \mid 36$ ✓

d) $\gcd(81, 113) = 1$
$81 = 3 \cdot 3 \cdot 3 \cdot 3$
$113 = 113$
$A-1 = 98$
$113 \nmid 98$ ✗

Př. 10/5: perioda Lehmerova generátoru náh. čísel

Určete délku periody v Lehmerově generátoru, který je dán předpisem $x_{n+1} = ((M-1) \cdot x_n)\ mod\ M$, kde M je prvočíslo.

Př. 10/5: perioda Lehmerova generátoru náh. čísel

Určete délku periody v Lehmerově generátoru, který je dán předpisem $x_{n+1} = ((M-1) \cdot x_n) \; mod \; M$, kde M je prvočíslo.

$(M-1)^2 \bmod M = M^2 - 2M + 1 \bmod M = 1$

$1 \to M-1$

M prv.

a

$a^2 = 1$

$a^3 = M-1$

$(0, \dots, M-1)$

$x_1 = b$

$x_2 = (M-1)\, b \bmod M = (Mb - b) \bmod M = -b \bmod M = b + M$

$x_3 = (M-1)(-b) \bmod M = (-Mb + b) \bmod M = b$

$|\{x_i\}| = 2$

Př. 10/6: počet prvočísel

Určete, kolik přibližně prvočísel leží v intervalu:
a) $< 0, 10^9 >$,
b) $< 10^9, 2 \cdot 10^9 >$,
c) $< 2 \cdot 10^9, 3 \cdot 10^9 >$.

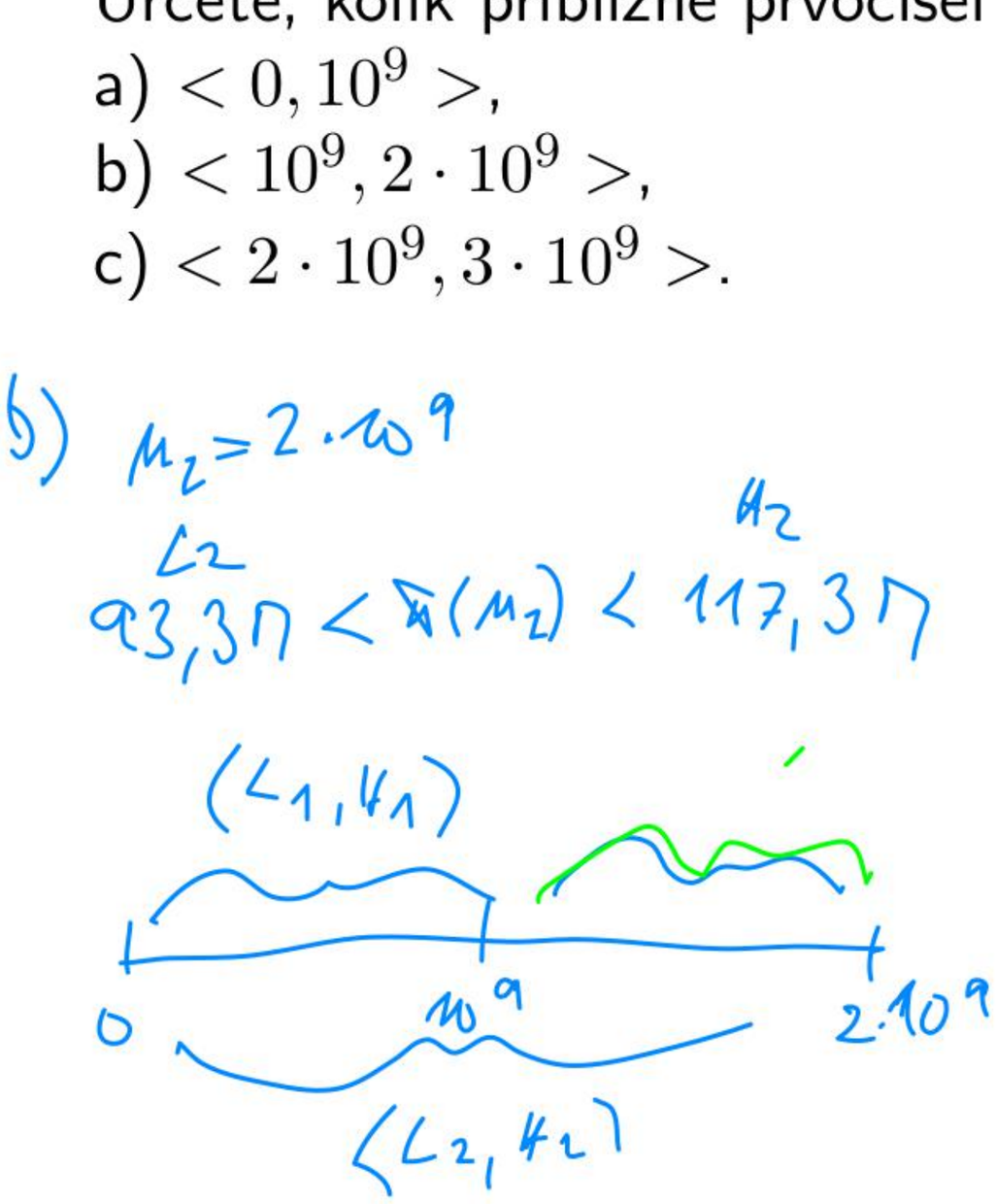
Př. 10/6: počet prvočísel

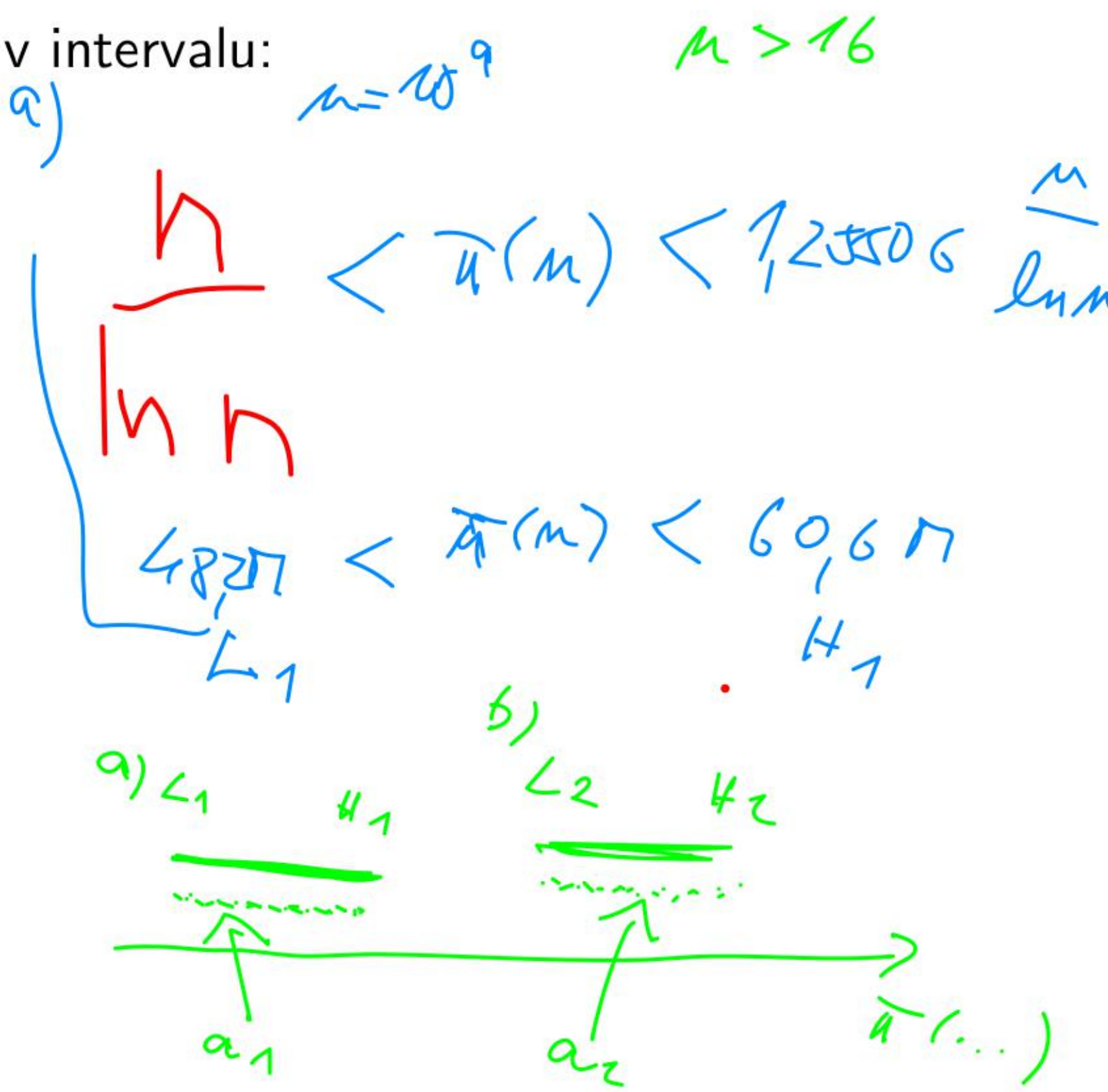
Určete, kolik přibližně prvočísel leží v intervalu:

a) $< 0, 10^9 >$,

b) $< 10^9, 2 \cdot 10^9 >$,

c) $< 2 \cdot 10^9, 3 \cdot 10^9 >$.

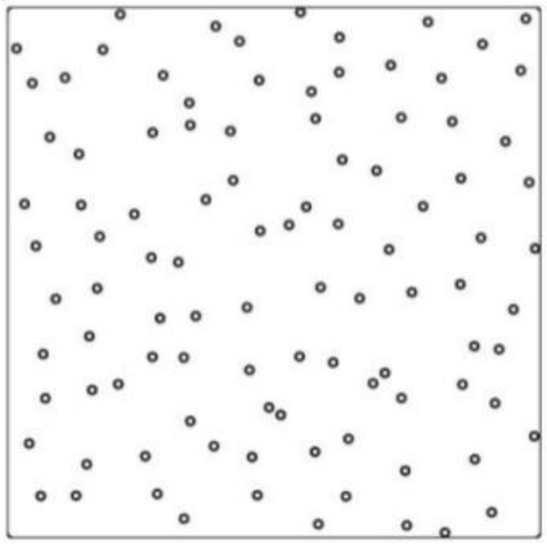


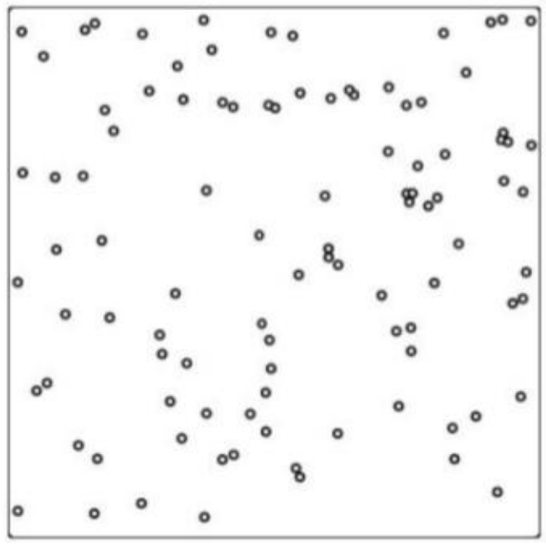


Náhodná čísla. Prvočísla. Modulární umocňování.

Př. 10/1: náhodné body

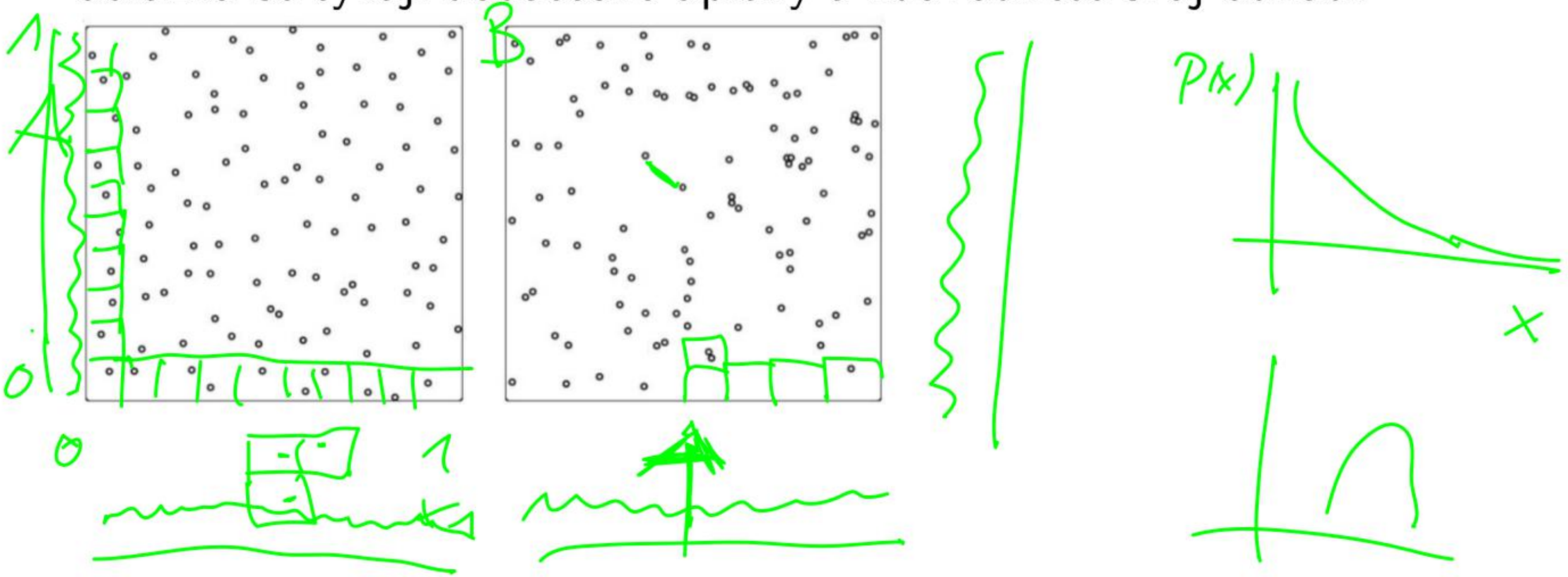
Máme dva obrázky - pokaždé jde o čtverec se 100 body uvnitř. V jednom případě byly souřadnice každého bodu generovány nezávisle a pseudonáhodně, ve druhém případě byly generovány analogicky, ale navíc byly souřadnice systematicky modifikovány (nám neznámým) způsobem. Odhadněte, kterého obrázku se týkají dodatečné úpravy a zdůvodněte svůj odhad.

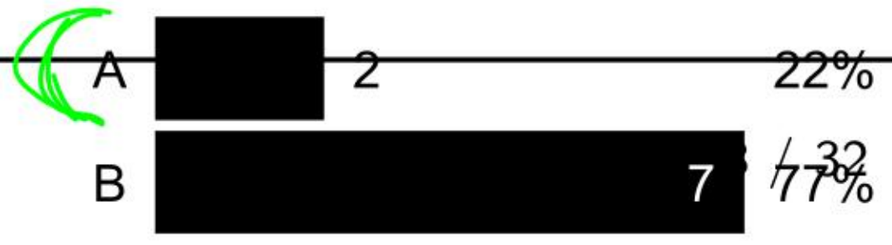




Př. 10/1: náhodné body

Máme dva obrázky - pokaždé jde o čtverec se 100 body uvnitř. V jednom případě byly souřadnice každého bodu generovány nezávisle a pseudonáhodně, ve druhém případě byly generovány analogicky, ale navíc byly souřadnice systematicky modifikovány (nám neznámým) způsobem. Odhadněte, kterého obrázku se týkají dodatečné úpravy a zdůvodněte svůj odhad.





Př. 10/2: náhodná čísla

Máte jednu hrací kostku. Popište, jak využijte házení kostkou tak, abyste měli generátor náhodných celých čísel v rozmezí $0 \ldots 10$. Všechna čísla $0, 1, 2, \ldots 10$ musí být generována se stejnou pravděpodobností.

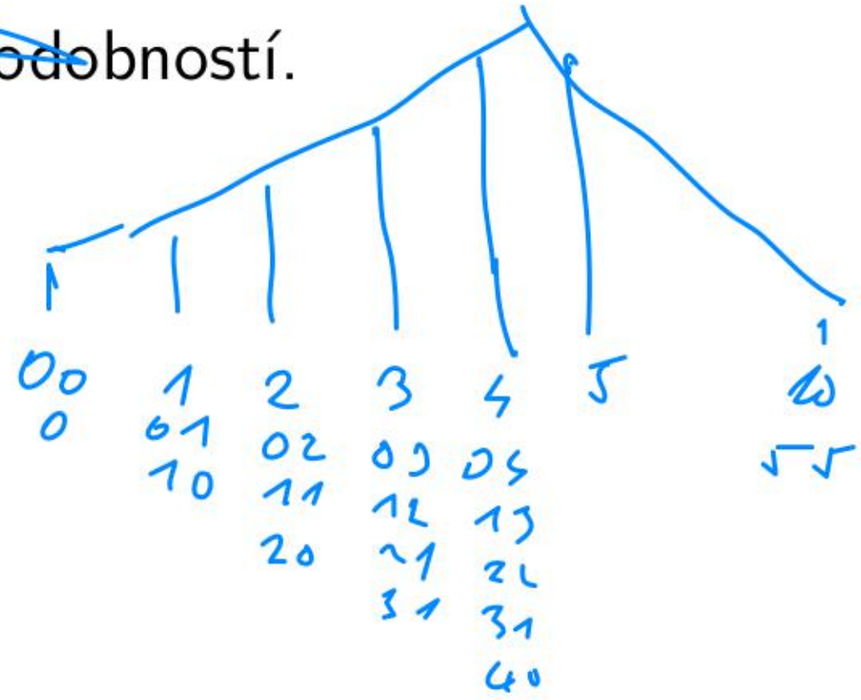
Př. 10/2: náhodná čísla

Máte jednu hrací kostku. Popište, jak využijte házení kostkou tak, abyste měli generátor náhodných celých čísel v rozmezí $0 \ldots 10$. Všechna čísla $0, 1, 2, \ldots 10$ musí být generována se stejnou pravděpodobností.

$x_1 \in \langle 0, 5)$

$x_2 \in \langle 0, 6)$

$x_3 = x_1 + x_2 \in \langle 0, 10)$

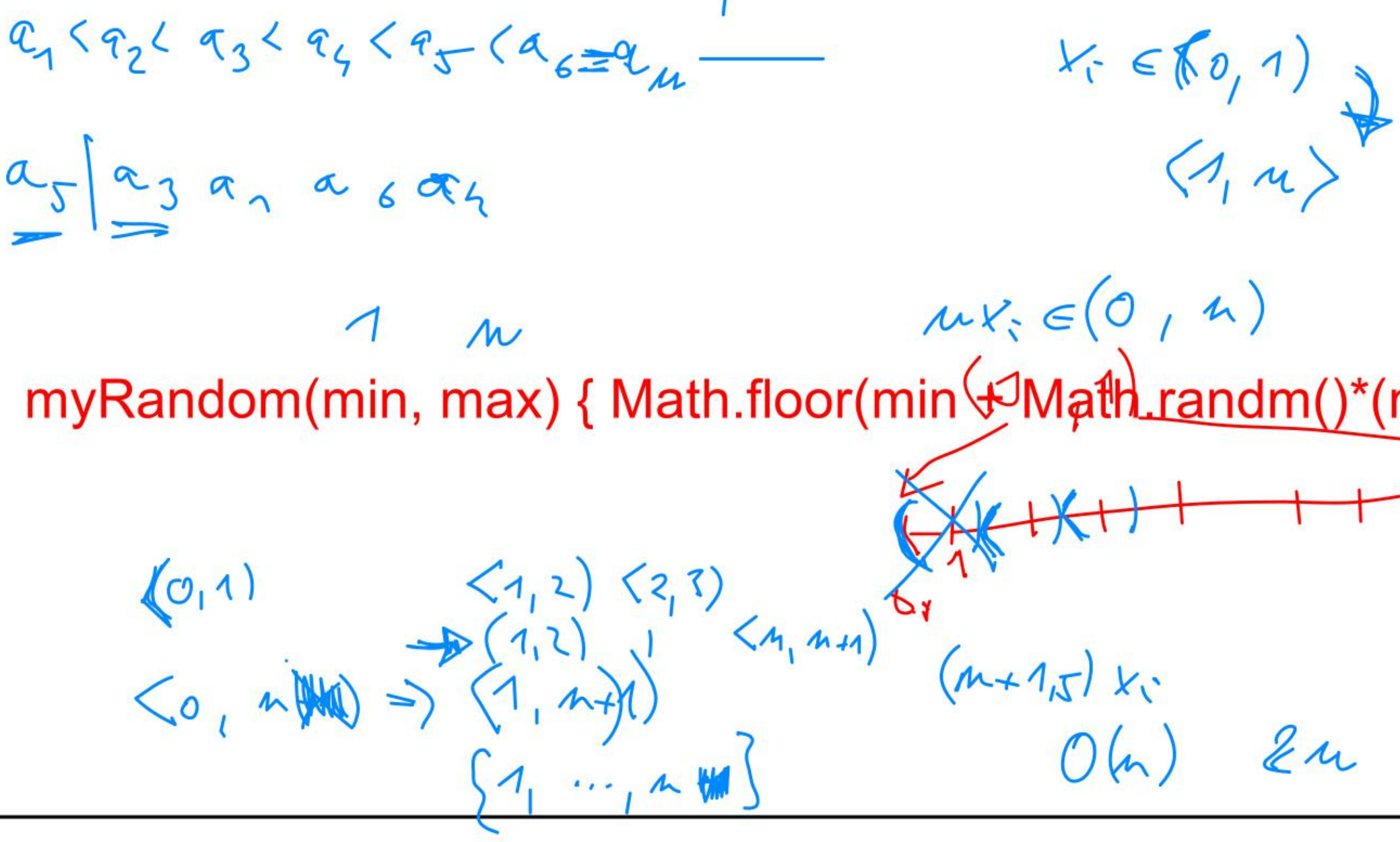


Př. 10/3: náhodné uspořádání

Vysvětlete, jak pomocí generátoru náhodných čísel zamícháte do náhodného pořadí seřazené pole čísel. Akce musí proběhnout v čase úměrném délce pole.

Př. 10/3: náhodné uspořádání

Vysvětlete, jak pomocí generátoru náhodných čísel zamícháte do náhodného pořadí seřazené pole čísel. Akce musí proběhnout v čase úměrném délce pole.

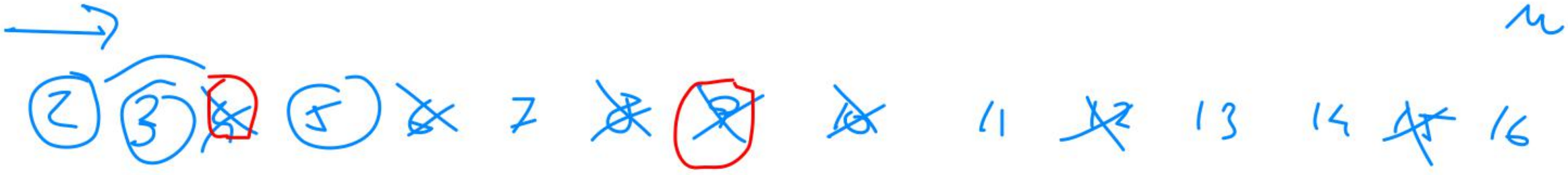


Př. 10/7: poloprvočísla

Řekneme, že přirozené číslo je poloprvočíslo, pokud je buď prvočíslem nebo celou mocninou prvočísla. Popište modifikaci Eratosthenova síta, která bude generovat právě poloprvočísla. Napište pseudokód.

Př. 10/7: poloprvočísla

Řekneme, že přirozené číslo je poloprvočíslo, pokud je buď prvočíslem nebo celou mocninou prvočísla. Popište modifikaci Eratosthenova síta, která bude generovat právě poloprvočísla. Napište pseudokód.



Př. 10/8: skoroprvočísla

Jako skoroprvočísla označíme právě ta přirozená čísla, která jsou součinem dvou různých prvočísel. Popište modifikaci Eratosthenova síta, která bude generovat skoroprvočísla. Napište pseudokód.

Př. 10/10: prvočísla v intervalu

Určete, jaký je maximální možný počet prvočísel v kterémkoli z intervalů $< 30k, 30k + 29 >, k = 1, 2, 3, 4, \ldots$

Př. 10/11a: největší společný dělitel

Vypočtěte největší společný dělitel
a) $GCD(220, 284)$,
b) $GCD(\binom{30}{10}, \binom{31}{9})$,
c) $GCD(2^{100}, 100!)$.

Př. 10/11a: největší společný dělitel

Vypočtěte největší společný dělitel

a) $GCD(220, 284)$, $= 4$

b) $GCD(\binom{30}{10}, \binom{31}{9})$,

c) $GCD(2^{100}, 100!)$.

$220 = 2 \cdot 110 = 2 \cdot 2 \cdot 55 = 2^2 \cdot 5 \cdot 11$

$284 = 2 \cdot 142 = 2^2 \cdot 71$

Př. 10/11b: největší společný dělitel

Vypočtěte největší společný dělitel
a) $GCD(220, 284)$,
b) $GCD(\binom{30}{10}, \binom{31}{9})$,
c) $GCD(2^{100}, 100!)$.

Př. 10/11c: největší společný dělitel

Vypočtěte největší společný dělitel
a) $GCD(220, 284)$,
b) $GCD(\binom{30}{10}, \binom{31}{9})$,
c) $GCD(2^{100}, 100!)$.

Př. 10/12: modulární umocňování

Vypočtěte $18^{89}\ mod\ 11$.

Př. 10/12: modulární umocňování

Vypočtěte 18^{89} *mod* 11.

$\langle 0, \ldots, 10 \rangle$

$18^{89} \% 11 = 7^{89} \% 11 = (-4)^{89} \% 11 =$

$7^{44} \cdot (-4) \not\equiv 1$

$18^{89} = 18^{8 \cdot 11 + 1} =$

$= 18^{8 \cdot 11} \cdot 18$

$= 18^{11}$

$18 = 7 \bmod 11$

$18^2 = 7^2 = 5 \bmod 11$

$18^4 = 25 = 3 \bmod 11$

$18^8 = 9 \bmod 11$

$18^{16} = 81 = 4 \bmod 11$

$18^{11} = 3$

$18^{11} = 18^{(8+2+1)} = 9 \cdot 5 \cdot 7 \bmod 11 = 7 \bmod 11$

$18^{89} = 18^{8 \cdot 11 + 1} \bmod 11$

$(18^{11})^8 \cdot 18$

$7^8 \cdot 18 \bmod 11$

$9 \cdot 7 \bmod 11$

$8 \bmod 11$

$(18^{11})^8 \cdot 18^1$

Př. 10/14: modulární umocňování - kód

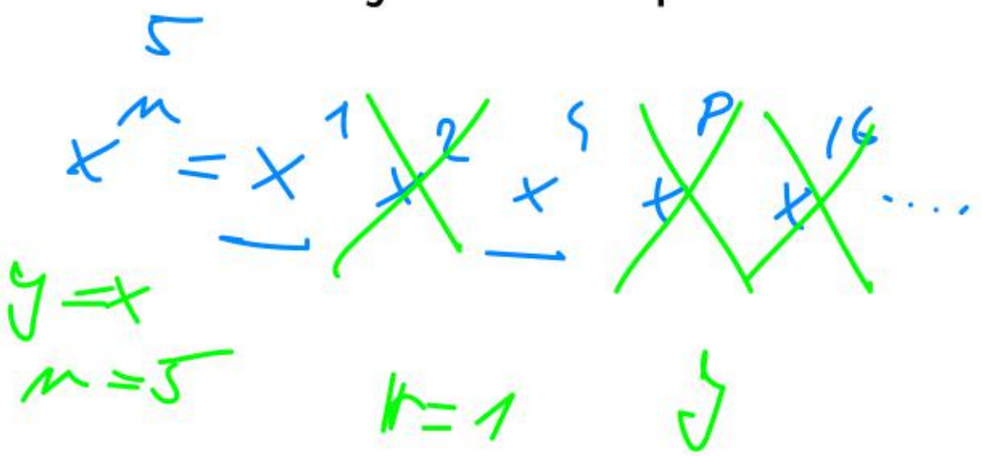
Uvedený kód počítá celočíselnou mocninu x^n. Popište, jak jej upravíte, aby počítal $x^n \; mod \; m$, pro kladné celé m. Minimalizujte riziko přetečení.

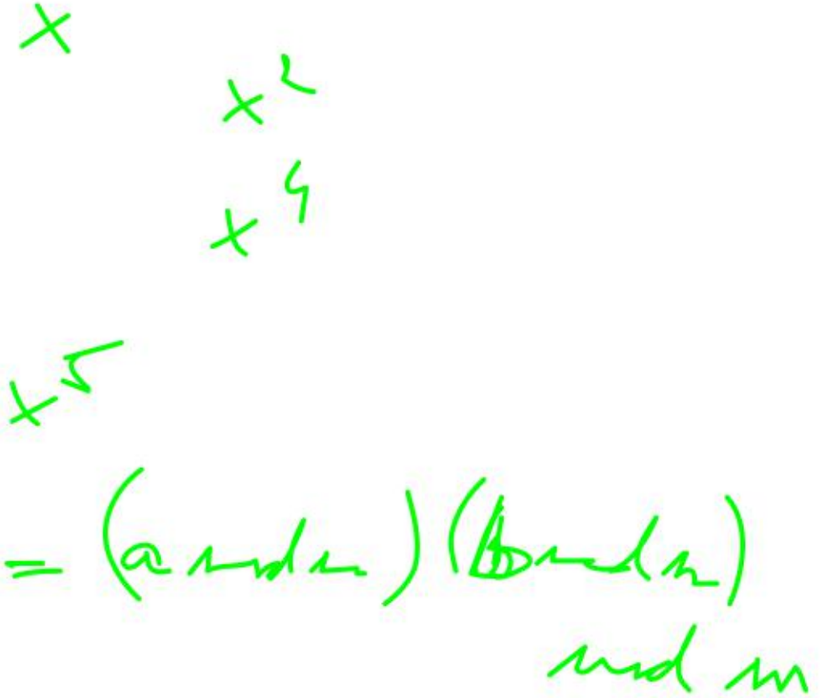
```
BinPower(int x, int n) {
 int r = 1, y = x;
 while (n > 1) {
    if (n % 2 == 1) r *= y;
    y *= y;
    n /= 2;
  }
 return r*y;
}
```

Př. 10/14: modulární umocňování - kód

Uvedený kód počítá celočíselnou mocninu x^n. Popište, jak jej upravíte, aby počítal $x^n \ mod \ m$, pro kladné celé m. Minimalizujte riziko přetečení.

```
BinPower(int x, int n) {
 int r = 1, y = x;
 while (n > 1) {
   if (n % 2 == 1) r *= y;
   y *= y;
   n /= 2;
 }
 return r*y;
}
```





Skip list. B-stromy.

Př. 11/1: skip list - konstrukce

Sestavte skip list, který je nejprve prázdný a dále do něj vkládáte dané klíče v uvedeném pořadí. Číslo za klíčem v závorce uvádí úroveň (level) klíče, tj. kolikrát byla hozena mince, než padl rub (včetně rubu): 16(3), 23(2), 18(2), 5(2), 15(1), 19(1), 33(1), 11(2), 21(2), 4(1), 22(2), 6(2), 17(4), 10(1), 9(1), 28(4).

Př. 11/1: skip list - konstrukce

Sestavte skip list, který je nejprve prázdný a dále do něj vkládáte dané klíče v uvedeném pořadí. Číslo za klíčem v závorce uvádí úroveň (level) klíče, tj. kolikrát byla hozena mince, než padl rub (včetně rubu): 16(3), 23(2), 18(2), 5(2), 15(1), 19(1), 33(1), 11(2), 21(2), 4(1), 22(2), 6(2), 17(4), 10(1), 9(1), 28(4).

Př. 11/2: skip list - sloučení

Mějme dvě datové struktury skip list délky N. Máme navrhnout efektivní algoritmus, který tyto dva seznamy spojí do seznamu jediného o délce $2N$. Jaká bude jeho asymptotická složitost?

Př. 11/3: skip list - obrácení

Je možno obrátit pořadí prvků ve struktuře skip list (z vzestupného uspořádání klíčů přejít na sestupné) v čase asymptoticky menším než $O(Nlog(N))$?

Př. 11/4: skip list - extractMin

Formulujte operaci extractMin ve struktuře skip list a popište, jak lze potom skip list použít jako prioritní frontu. Bude efektivita jednotlivých operací asymptoticky srovnatelná s binární haldou?

Př. 11/5: skip list - decreaseKey

Navrhněte efektivní operaci decreaseKey ve struktuře skip list.

Př. 11/6: skip list - jiná úroveň

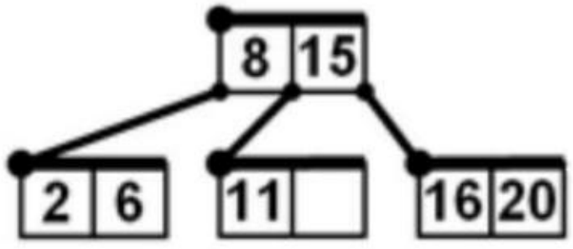
Při implementaci struktury skip list se stalo, že úroveň každého uzlu v operaci Insert je určena jako náhodné číslo z intervalu $[1, \lceil log 2N \rceil]$, přičemž se jedná o rovnoměrné rozložení a N je vždy aktuální počet prvků v seznamu. Odhadněte (pro velké N), nakolik se zhorší asymptotická složitost operací Find/Insert/Delete v této struktuře.

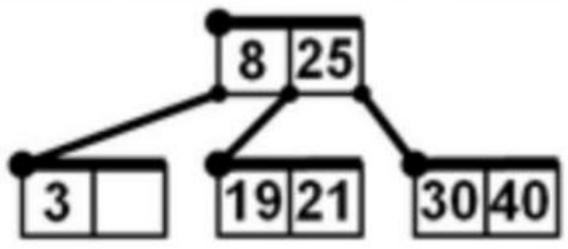
Př. 11/7: skip list - součet úrovní

Profesor Velký tvrdí, že v průměrném případě ve struktuře skip list o délce N je součet všech hodnot prvek.level úměrný hodnotě $Nlog(N)$. Profesor Malý tvrdí, že tento součet je úměrný pouze hodnotě N. Profesor Různý tvrdí, že mohou nastávat oba případy a že záleží na datech. Rozhodněte akademický spor.

Př. 11/11: B stromy

Do B-stromu znázorněného na levém resp. pravém obrázku vložíme postupně klíče 14, 10, resp. 7, 5. Jaké klíče pak bude obsahovat kořen stromu?





Př. 11/12: izomorfní B stromy

Dva prázdné B-stromy řádu 1 (max. 2 klíče v uzlu) jsou izomorfní. Neprázdný B-strom B1 řádu 1 s kořenem K1 je izomorfní s neprázdným B-stromem B2 řádu 1 s kořenem K2 právě tehdy, když zároveň platí 1. a 2.:

1. K1 obsahuje stejný počet klíčů jako K2
2. Levý podstrom K1 je izomorfní s levým podstromem K2, pravý podstrom K1 je izomorfní s pravým podstromem K2 a prostřední podstrom K1, pokud existuje, je izomorfní s prostředním podstromem K2.

Určete počet navzájem neizomorfních B-stromů řádu 1 s A) 0, B) 1, C) 3, D) 4, E) 7 uzly.

Př. 11/14: konstrukce a destrukce B stromu

B-strom je řádu k, pokud každý jeho uzel, kromě kořene, musí obsahovat alespoň k klíčů a zároveň může obsahovat nejvýše $2k$ klíčů. Vybudujte B-strom řádu 1 tak, že do prázdného stromu vložíte v uvedeném pořadí klíče $25, 13, 37, 32, 40, 20, 22$. Dále tento strom zrušte, a to tak, že jednotlivé klíče klíče odstraníte v pořadí $13, 25, 40, 22, 20, 37, 32$. Nakreslete strom po každé operaci Insert a Delete.

Př. 11/14: konstrukce a destrukce B stromu

B-strom je řádu k, pokud každý jeho uzel, kromě kořene, musí obsahovat alespoň k klíčů a zároveň může obsahovat nejvýše $2k$ klíčů. Vybudujte B-strom řádu 1 tak, že do prázdného stromu vložíte v uvedeném pořadí klíče $25, 13, 37, 32, 40, 20, 22$. Dále tento strom zrušte, a to tak, že jednotlivé klíče klíče odstraníte v pořadí $13, 25, 40, 22, 20, 37, 32$. Nakreslete strom po každé operaci Insert a Delete.