Počítačová algebra

Alexandr Kazda

Univerzita Karlova

22. května 2020

Co bylo: Algoritmus 21

Data: $f, g \in \mathbb{Z}[x]$ primitivní polynomy
Result: $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$

1 $d := \mathrm{NSD}_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$;
2 $p :=$ nejmenší prvočíslo $> 2d \cdot LM(f, g)$;
3 $h := \mathrm{NSD}_{\mathbb{Z}_p[x]}(f\%p, g\%p)$, aby $\mathrm{lc}(h) = d\%p$;
4 $h := \mathrm{pp}(h)$;
5 **if** $h | f, g$ **then**
6 | **return** h;
7 **else**
8 | zvol větší prvočíslo p, jdi na 3;
9 **end**

- Algoritmus funguje, ale není snadné ukázat časovou složitost
- Je to nepraktické, protože naše prvočíslo bude hodně velké
- Vylepšení: Místo jednoho p budeme počítat modulo několik malých p; chceme součit $> 2d \cdot LM(f, g)$

Co bylo: Algoritmus 21

Data: $f, g \in \mathbb{Z}[x]$ primitivní polynomy
Result: $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$

1 $d := \mathrm{NSD}_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$;
2 $p :=$ nejmenší prvočíslo $> 2d \cdot LM(f, g)$;
3 $h := \mathrm{NSD}_{\mathbb{Z}_p[x]}(f\%p, g\%p)$, aby $\mathrm{lc}(h) = d\%p$;
4 $h := \mathrm{pp}(h)$;
5 **if** $h | f, g$ **then**
6 | **return** h;
7 **else**
8 | zvol větší prvočíslo p, jdi na 3;
9 **end**

- Algoritmus funguje, ale není snadné ukázat časovou složitost
- Je to nepraktické, protože naše prvočíslo bude hodně velké
- Vylepšení: Místo jednoho p budeme počítat modulo několik malých p; chceme součit $> 2d \cdot LM(f, g)$

Co bylo: Algoritmus 21

Data: $f, g \in \mathbb{Z}[x]$ primitivní polynomy
Result: $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$

1 $d := \mathrm{NSD}_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$;
2 $p :=$ nejmenší prvočíslo $> 2d \cdot LM(f, g)$;
3 $h := \mathrm{NSD}_{\mathbb{Z}_p[x]}(f\%p, g\%p)$, aby $\mathrm{lc}(h) = d\%p$;
4 $h := \mathrm{pp}(h)$;
5 **if** $h | f, g$ **then**
6 | **return** h;
7 **else**
8 | zvol větší prvočíslo p, jdi na 3;
9 **end**

- Algoritmus funguje, ale není snadné ukázat časovou složitost
- Je to nepraktické, protože naše prvočíslo bude hodně velké
- Vylepšení: Místo jednoho p budeme počítat modulo několik malých p; chceme součit $> 2d \cdot LM(f, g)$

Co bylo: Algoritmus 21

Data: $f, g \in \mathbb{Z}[x]$ primitivní polynomy
Result: $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$

1 $d := \mathrm{NSD}_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$;
2 $p :=$ nejmenší prvočíslo $> 2d \cdot LM(f, g)$;
3 $h := \mathrm{NSD}_{\mathbb{Z}_p[x]}(f\%p, g\%p)$, aby $\mathrm{lc}(h) = d\%p$;
4 $h := \mathrm{pp}(h)$;
5 **if** $h | f, g$ **then**
6 | **return** h;
7 **else**
8 | zvol větší prvočíslo p, jdi na 3;
9 **end**

- Algoritmus funguje, ale není snadné ukázat časovou složitost
- Je to nepraktické, protože naše prvočíslo bude hodně velké
- Vylepšení: Místo jednoho p budeme počítat modulo několik malých p; chceme součit $> 2d \cdot LM(f, g)$

Algoritmus 22

Data: $f, g \in \mathbb{Z}[x]$ primitivní polynomy
Result: $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$

1 $d := \mathrm{NSD}_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$;
2 $p :=$ nejmenší dosud nepoužité použitelné prvočíslo;
3 $h := \mathrm{NSD}_{\mathbb{Z}_p[x]}(f\%p, g\%p)$, že $\mathrm{lc}(h) = d\%p$;
4 **if** $\deg h = 0$; // Stupeň NSD je ≤ 0
5 **then**
6 | **return** 1;
7 **end**
8 $H := h$, $P := p$; // H je odhad NSD, počítáme modulo P
9 **while** $P \leq 2d \cdot LM(f, g)$ **do**
10 | $p :=$ nejmenší dosud nepoužité použitelné prvočíslo; // Pozorování: P, p jsou nesoudělná
11 | $h := \mathrm{NSD}_{\mathbb{Z}_p[x]}(f\%p, g\%p)$, že $\mathrm{lc}(h) = d\%p$;
12 | **if** $\deg h < \deg H$; // Všechna předchozí prvočísla byla smolná
13 | **then**
14 | | jdi na 4
15 | **end**
16 | **if** $\deg h = \deg H$; // Zkombinujeme h, H do odhadu modulo $P \cdot p$
17 | **then**
18 | | Spočti H', aby $H' \equiv H \pmod{P}$ a $H' \equiv h \pmod{p}$; // Hodí se Garnerův algoritmus pro ČZV
19 | | $H := H'$, $P := P \cdot p$; // Pro nové H, P platí: H je $\mathrm{NSD}_{\mathbb{Z}_P[x]}(f\%P, g\%P)$, $\mathrm{lc}(H) = d \pmod{P}$
20 | **end**
21 **end**
22 $h := \mathrm{pp}(H)$;
23 **if** $h | f, g$ **then**
24 | **return** h;
25 **else**
26 | jdi na 2;
27 **end**

ČZV pro koeficienty polynomů

Lemma

Nechť $p, P \in \mathbb{Z}$ jsou nesoudělná. Nechť $f \in \mathbb{Z}[x]$ $h, r \in \mathbb{Z}_p[x]$, $H, R \in \mathbb{Z}_P[x]$, $H' \in \mathbb{Z}_{pP}[x]$ jsou taková, že $p, P \nmid \mathrm{lc}(H')$ a

$$H = H' \% P \qquad f \% P = HR$$
$$h = H' \% p \qquad f \% p = hr$$

Potom $H' | f \%(Pp)$.

- ČZV nám dává isomorfismus okruhů $\mathbb{Z}_P \times \mathbb{Z}_p$ a $\mathbb{Z}_{Pp}$; použijeme ji na dvojice koeficientů R_i, r_i.
- Dostaneme polynom $R' \in \mathbb{Z}_{Pp}[x]$, že $R' \% p = r$, $R' \% P = H$
- Ze vzorečku pro násobení polynomů a ismomorfismu $H'R' = f$
- Pozorování: $\deg h = \deg H' = \deg H$, proto Algoritmus 22 porovnává stupně

ČZV pro koeficienty polynomů

Lemma

Nechť $p, P \in \mathbb{Z}$ jsou nesoudělná. Nechť $f \in \mathbb{Z}[x]$ $h, r \in \mathbb{Z}_p[x]$, $H, R \in \mathbb{Z}_P[x]$, $H' \in \mathbb{Z}_{pP}[x]$ jsou taková, že $p, P \nmid \mathrm{lc}(H')$ a

$$H = H' \% P \qquad f \% P = HR$$
$$h = H' \% p \qquad f \% p = hr$$

Potom $H' | f \%(Pp)$.

- ČZV nám dává isomorfismus okruhů $\mathbb{Z}_P \times \mathbb{Z}_p$ a $\mathbb{Z}_{Pp}$; použijeme ji na dvojice koeficientů R_i, r_i.
- Dostaneme polynom $R' \in \mathbb{Z}_{Pp}[x]$, že $R' \% p = r$, $R' \% P = H$
- Ze vzorečku pro násobení polynomů a ismomorfismu $H'R' = f$
- Pozorování: $\deg h = \deg H' = \deg H$, proto Algoritmus 22 porovnává stupně

ČZV pro koeficienty polynomů

Lemma

Nechť $p, P \in \mathbb{Z}$ jsou nesoudělná. Nechť $f \in \mathbb{Z}[x]$ $h, r \in \mathbb{Z}_p[x]$, $H, R \in \mathbb{Z}_P[x]$, $H' \in \mathbb{Z}_{pP}[x]$ jsou taková, že $p, P \nmid \mathrm{lc}(H')$ a

$$H = H' \% P \qquad f \% P = HR$$
$$h = H' \% p \qquad f \% p = hr$$

Potom $H' | f \%(Pp)$.

- ČZV nám dává isomorfismus okruhů $\mathbb{Z}_P \times \mathbb{Z}_p$ a $\mathbb{Z}_{Pp}$; použijeme ji na dvojice koeficientů R_i, r_i.
- Dostaneme polynom $R' \in \mathbb{Z}_{Pp}[x]$, že $R' \% p = r$, $R' \% P = H$
- Ze vzorečku pro násobení polynomů a ismomorfismu $H'R' = f$
- Pozorování: $\deg h = \deg H' = \deg H$, proto Algoritmus 22 porovnává stupně

ČZV pro koeficienty polynomů

Lemma

Nechť $p, P \in \mathbb{Z}$ jsou nesoudělná. Nechť $f \in \mathbb{Z}[x]$ $h, r \in \mathbb{Z}_p[x]$, $H, R \in \mathbb{Z}_P[x]$, $H' \in \mathbb{Z}_{pP}[x]$ jsou taková, že $p, P \nmid \mathrm{lc}(H')$ a

$$H = H' \% P \qquad f \% P = HR$$
$$h = H' \% p \qquad f \% p = hr$$

Potom $H' | f \%(Pp)$.

- ČZV nám dává isomorfismus okruhů $\mathbb{Z}_P \times \mathbb{Z}_p$ a $\mathbb{Z}_{Pp}$; použijeme ji na dvojice koeficientů R_i, r_i.
- Dostaneme polynom $R' \in \mathbb{Z}_{Pp}[x]$, že $R' \% p = r$, $R' \% P = H$
- Ze vzorečku pro násobení polynomů a ismomorfismu $H'R' = f$
- Pozorování: $\deg h = \deg H' = \deg H$, proto Algoritmus 22 porovnává stupně

ČZV pro koeficienty polynomů

Lemma

Nechť $p, P \in \mathbb{Z}$ jsou nesoudělná. Nechť $f \in \mathbb{Z}[x]$ $h, r \in \mathbb{Z}_p[x]$, $H, R \in \mathbb{Z}_P[x]$, $H' \in \mathbb{Z}_{pP}[x]$ jsou taková, že $p, P \nmid \mathrm{lc}(H')$ a

$$H = H' \% P \qquad f \% P = HR$$
$$h = H' \% p \qquad f \% p = hr$$

Potom $H' | f \%(Pp)$.

- ČZV nám dává isomorfismus okruhů $\mathbb{Z}_P \times \mathbb{Z}_p$ a $\mathbb{Z}_{Pp}$; použijeme ji na dvojice koeficientů R_i, r_i.
- Dostaneme polynom $R' \in \mathbb{Z}_{Pp}[x]$, že $R' \% p = r$, $R' \% P = H$
- Ze vzorečku pro násobení polynomů a ismomorfismu $H'R' = f$
- Pozorování: $\deg h = \deg H' = \deg H$, proto Algoritmus 22 porovnává stupně

Správnost Algoritmu 22

- Pokud na řádku 4 vrátíme 1, bylo to proto, že $\mathrm{NSD}_{\mathbb{Z}_p[x]}(f,g)$ má stupeň 0 pro p použitelné, tedy $\mathrm{NSD}_{\mathbb{Z}}(f,g)$ je konstantní
- Pokud na řádku 8 zvolené P je větší než $2d \cdot LM(f,g)$, je to jako Algoritmus 21
- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f,g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Pozor: $\mathbb{Z}_P$ není obor integrity

Správnost Algoritmu 22

- Pokud na řádku 4 vrátíme 1, bylo to proto, že $\mathrm{NSD}_{\mathbb{Z}_p[x]}(f, g)$ má stupeň 0 pro p použitelné, tedy $\mathrm{NSD}_{\mathbb{Z}}(f, g)$ je konstantní
- Pokud na řádku 8 zvolené P je větší než $2d \cdot LM(f, g)$, je to jako Algoritmus 21
- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Pozor: $\mathbb{Z}_P$ není obor integrity

Správnost Algoritmu 22

- Pokud na řádku 4 vrátíme 1, bylo to proto, že $\mathrm{NSD}_{\mathbb{Z}_p[x]}(f, g)$ má stupeň 0 pro p použitelné, tedy $\mathrm{NSD}_{\mathbb{Z}}(f, g)$ je konstantní
- Pokud na řádku 8 zvolené P je větší než $2d \cdot LM(f, g)$, je to jako Algoritmus 21
- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Pozor: $\mathbb{Z}_P$ není obor integrity

Správnost Algoritmu 22

- Pokud na řádku 4 vrátíme 1, bylo to proto, že $\mathrm{NSD}_{\mathbb{Z}_p[x]}(f, g)$ má stupeň 0 pro p použitelné, tedy $\mathrm{NSD}_{\mathbb{Z}}(f, g)$ je konstantní
- Pokud na řádku 8 zvolené P je větší než $2d \cdot LM(f, g)$, je to jako Algoritmus 21
- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Pozor: $\mathbb{Z}_P$ není obor integrity

Správnost Algoritmu 22

- Pokud na řádku 4 vrátíme 1, bylo to proto, že $\mathrm{NSD}_{\mathbb{Z}_p[x]}(f, g)$ má stupeň 0 pro p použitelné, tedy $\mathrm{NSD}_{\mathbb{Z}}(f, g)$ je konstantní
- Pokud na řádku 8 zvolené P je větší než $2d \cdot LM(f, g)$, je to jako Algoritmus 21
- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Pozor: $\mathbb{Z}_P$ není obor integrity

Správnost Algoritmu 22

- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Důkaz indukcí: $d \pmod{Pp}$ je unikání řešení ČZV úlohy $d\%p = d\%p$ a $d\%P = d\%P$
- $H' | f, g$ podle lemmatu o slajd dřív
- Pokud $Q | f, g$ a $\mathrm{lc}(Q) = d$, tak $Q\%p | f\%p$, tedy $\deg(Q\%p) = \deg(Q) \leq \deg h$
- Až while cyklus skončí: $H | f, g$ a počítáme modulo $P > 2d \cdot ML(f, g)$, tedy se lze vrátit do $\mathbb{Z}[x]$
- Na konci opět trik s primitivní částí
- Jako v Alg 21 testujeme, zda všechna prvočísla nebyla smolná a stupeň H moc velký

Správnost Algoritmu 22

- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Důkaz indukcí: $d \pmod{Pp}$ je unikání řešení ČZV úlohy $d\%p = d\%p$ a $d\%P = d\%P$
- $H' | f, g$ podle lemmatu o slajd dřív
- Pokud $Q | f, g$ a $\mathrm{lc}(Q) = d$, tak $Q\%p | f\%p$, tedy $\deg(Q\%p) = \deg(Q) \leq \deg h$
- Až while cyklus skončí: $H | f, g$ a počítáme modulo $P > 2d \cdot ML(f, g)$, tedy se lze vrátit do $\mathbb{Z}[x]$
- Na konci opět trik s primitivní částí
- Jako v Alg 21 testujeme, zda všechna prvočísla nebyla smolná a stupeň H moc velký

Správnost Algoritmu 22

- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Důkaz indukcí: $d \pmod{Pp}$ je unikání řešení ČZV úlohy $d\%p = d\%p$ a $d\%P = d\%P$
- $H' | f, g$ podle lemmatu o slajd dřív
- Pokud $Q | f, g$ a $\mathrm{lc}(Q) = d$, tak $Q\%p | f\%p$, tedy $\deg(Q\%p) = \deg(Q) \leq \deg h$
- Až while cyklus skončí: $H | f, g$ a počítáme modulo $P > 2d \cdot ML(f, g)$, tedy se lze vrátit do $\mathbb{Z}[x]$
- Na konci opět trik s primitivní částí
- Jako v Alg 21 testujeme, zda všechna prvočísla nebyla smolná a stupeň H moc velký

Správnost Algoritmu 22

- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Důkaz indukcí: $d \pmod{Pp}$ je unikání řešení ČZV úlohy $d\%p = d\%p$ a $d\%P = d\%P$
- $H' | f, g$ podle lemmatu o slajd dřív
- Pokud $Q | f, g$ a $\mathrm{lc}(Q) = d$, tak $Q\%p | f\%p$, tedy $\deg(Q\%p) = \deg(Q) \leq \deg h$
- Až while cyklus skončí: $H | f, g$ a počítáme modulo $P > 2d \cdot ML(f, g)$, tedy se lze vrátit do $\mathbb{Z}[x]$
- Na konci opět trik s primitivní částí
- Jako v Alg 21 testujeme, zda všechna prvočísla nebyla smolná a stupeň H moc velký

Správnost Algoritmu 22

- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Důkaz indukcí: $d \pmod{Pp}$ je unikání řešení ČZV úlohy $d\%p = d\%p$ a $d\%P = d\%P$
- $H' | f, g$ podle lemmatu o slajd dřív
- Pokud $Q | f, g$ a $\mathrm{lc}(Q) = d$, tak $Q\%p | f\%p$, tedy $\deg(Q\%p) = \deg(Q) \leq \deg h$
- Až while cyklus skončí: $H | f, g$ a počítáme modulo $P > 2d \cdot ML(f, g)$, tedy se lze vrátit do $\mathbb{Z}[x]$
- Na konci opět trik s primitivní částí
- Jako v Alg 21 testujeme, zda všechna prvočísla nebyla smolná a stupeň H moc velký

Správnost Algoritmu 22

- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Důkaz indukcí: $d \pmod{Pp}$ je unikání řešení ČZV úlohy $d\%p = d\%p$ a $d\%P = d\%P$
- $H' | f, g$ podle lemmatu o slajd dřív
- Pokud $Q | f, g$ a $\mathrm{lc}(Q) = d$, tak $Q\%p | f\%p$, tedy $\deg(Q\%p) = \deg(Q) \leq \deg h$
- Až while cyklus skončí: $H | f, g$ a počítáme modulo $P > 2d \cdot ML(f, g)$, tedy se lze vrátit do $\mathbb{Z}[x]$
- Na konci opět trik s primitivní částí
- Jako v Alg 21 testujeme, zda všechna prvočísla nebyla smolná a stupeň H moc velký

Správnost Algoritmu 22

- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Důkaz indukcí: $d \pmod{Pp}$ je unikání řešení ČZV úlohy $d\%p = d\%p$ a $d\%P = d\%P$
- $H' | f, g$ podle lemmatu o slajd dřív
- Pokud $Q | f, g$ a $\mathrm{lc}(Q) = d$, tak $Q\%p | f\%p$, tedy $\deg(Q\%p) = \deg(Q) \leq \deg h$
- Až while cyklus skončí: $H | f, g$ a počítáme modulo $P > 2d \cdot ML(f, g)$, tedy se lze vrátit do $\mathbb{Z}[x]$
- Na konci opět trik s primitivní částí
- Jako v Alg 21 testujeme, zda všechna prvočísla nebyla smolná a stupeň H moc velký

Správnost Algoritmu 22

- Invariant pro while cyklus: H je polynom největšího stupně mezi děliteli f, g modulo P, že $\mathrm{lc}(H) \equiv d \pmod{P}$
- Důkaz indukcí: $d \pmod{Pp}$ je unikání řešení ČZV úlohy $d\%p = d\%p$ a $d\%P = d\%P$
- $H' | f, g$ podle lemmatu o slajd dřív
- Pokud $Q | f, g$ a $\mathrm{lc}(Q) = d$, tak $Q\%p | f\%p$, tedy $\deg(Q\%p) = \deg(Q) \leq \deg h$
- Až while cyklus skončí: $H | f, g$ a počítáme modulo $P > 2d \cdot ML(f, g)$, tedy se lze vrátit do $\mathbb{Z}[x]$
- Na konci opět trik s primitivní částí
- Jako v Alg 21 testujeme, zda všechna prvočísla nebyla smolná a stupeň H moc velký

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad

- $f = x^3 - x^2 + x - 1$, $g = x^3 + 2x^2 - x - 2$, $LM(f, g) = 16$
- $d := 1$
- $p := 2$
- $h := x^2 + 1$, $H := x^2 + 1$, $P := 2$
- $p := 3$, $h := x - 1$
- $\deg h < \deg H$, tedy 2 bylo smolné
- $H := x - 1, P := 3$
- $p := 5$, $h := x^2 + x - 2$
- $\deg h > \deg H$, volíme nové p
- $p := 7, h := x - 1$
- $H := x - 1, P = 3 \cdot 7 = 21$

Příklad dokončený

- $H := x - 1, P = 3 \cdot 7 = 21$
- $2d \cdot LM(f, g) = 32$
- $p = 11,\ h = x - 1$
- $H = x - 1, P = 11 \cdot 21 = 221 > 32$
- Všimněme si, že jsem mohli skončit dřív, kdybychom měli odvahu otestovat H pro $P = 21$
- Možná heuristika: Pokud $H = H'$, tak testuj, zda $\mathrm{pp}(H) | f, g$ a pokud ano vrať $\mathrm{pp}(H)$
- Protože $\deg H \geq \deg \mathrm{NSD}_{\mathbb{Z}}[x](f, g)$, tak to neovlivní korektnost
- Ale dělení polynomů je drahé, tak to nechcem zkoušet bezhlavě

Příklad dokončený

- $H := x - 1, P = 3 \cdot 7 = 21$
- $2d \cdot LM(f, g) = 32$
- $p = 11,\ h = x - 1$
- $H = x - 1, P = 11 \cdot 21 = 221 > 32$
- Všimněme si, že jsem mohli skončit dřív, kdybychom měli odvahu otestovat H pro $P = 21$
- Možná heuristika: Pokud $H = H'$, tak testuj, zda $\mathrm{pp}(H) | f, g$ a pokud ano vrať $\mathrm{pp}(H)$
- Protože $\deg H \geq \deg \mathrm{NSD}_{\mathbb{Z}}[x](f, g)$, tak to neovlivní korektnost
- Ale dělení polynomů je drahé, tak to nechcem zkoušet bezhlavě

Příklad dokončený

- $H := x - 1, P = 3 \cdot 7 = 21$
- $2d \cdot LM(f, g) = 32$
- $p = 11,\ h = x - 1$
- $H = x - 1, P = 11 \cdot 21 = 221 > 32$
- Všimněme si, že jsem mohli skončit dřív, kdybychom měli odvahu otestovat H pro $P = 21$
- Možná heuristika: Pokud $H = H'$, tak testuj, zda $\mathrm{pp}(H) | f, g$ a pokud ano vrať $\mathrm{pp}(H)$
- Protože $\deg H \geq \deg \mathrm{NSD}_{\mathbb{Z}}[x](f, g)$, tak to neovlivní korektnost
- Ale dělení polynomů je drahé, tak to nechcem zkoušet bezhlavě

Příklad dokončený

- $H := x - 1, P = 3 \cdot 7 = 21$
- $2d \cdot LM(f, g) = 32$
- $p = 11,\ h = x - 1$
- $H = x - 1, P = 11 \cdot 21 = 221 > 32$
- Všimněme si, že jsem mohli skončit dřív, kdybychom měli odvahu otestovat H pro $P = 21$
- Možná heuristika: Pokud $H = H'$, tak testuj, zda $\mathrm{pp}(H) | f, g$ a pokud ano vrať $\mathrm{pp}(H)$
- Protože $\deg H \geq \deg \mathrm{NSD}_{\mathbb{Z}}[x](f, g)$, tak to neovlivní korektnost
- Ale dělení polynomů je drahé, tak to nechcem zkoušet bezhlavě

Příklad dokončený

- $H := x - 1, P = 3 \cdot 7 = 21$
- $2d \cdot LM(f, g) = 32$
- $p = 11,\ h = x - 1$
- $H = x - 1, P = 11 \cdot 21 = 221 > 32$
- Všimněme si, že jsem mohli skončit dřív, kdybychom měli odvahu otestovat H pro $P = 21$
- Možná heuristika: Pokud $H = H'$, tak testuj, zda $\mathrm{pp}(H) | f, g$ a pokud ano vrať $\mathrm{pp}(H)$
- Protože $\deg H \geq \deg \mathrm{NSD}_{\mathbb{Z}}[x](f, g)$, tak to neovlivní korektnost
- Ale dělení polynomů je drahé, tak to nechcem zkoušet bezhlavě

Příklad dokončený

- $H := x - 1, P = 3 \cdot 7 = 21$
- $2d \cdot LM(f, g) = 32$
- $p = 11,\ h = x - 1$
- $H = x - 1, P = 11 \cdot 21 = 221 > 32$
- Všimněme si, že jsem mohli skončit dřív, kdybychom měli odvahu otestovat H pro $P = 21$
- Možná heuristika: Pokud $H = H'$, tak testuj, zda $\mathrm{pp}(H) | f, g$ a pokud ano vrať $\mathrm{pp}(H)$
- Protože $\deg H \geq \deg \mathrm{NSD}_{\mathbb{Z}}[x](f, g)$, tak to neovlivní korektnost
- Ale dělení polynomů je drahé, tak to nechcem zkoušet bezhlavě

Příklad dokončený

- $H := x - 1, P = 3 \cdot 7 = 21$
- $2d \cdot LM(f, g) = 32$
- $p = 11,\ h = x - 1$
- $H = x - 1, P = 11 \cdot 21 = 221 > 32$
- Všimněme si, že jsem mohli skončit dřív, kdybychom měli odvahu otestovat H pro $P = 21$
- Možná heuristika: Pokud $H = H'$, tak testuj, zda $\mathrm{pp}(H) | f, g$ a pokud ano vrať $\mathrm{pp}(H)$
- Protože $\deg H \geq \deg \mathrm{NSD}_{\mathbb{Z}}[x](f, g)$, tak to neovlivní korektnost
- Ale dělení polynomů je drahé, tak to nechcem zkoušet bezhlavě

Příklad dokončený

- $H := x - 1, P = 3 \cdot 7 = 21$
- $2d \cdot LM(f, g) = 32$
- $p = 11,\ h = x - 1$
- $H = x - 1, P = 11 \cdot 21 = 221 > 32$
- Všimněme si, že jsem mohli skončit dřív, kdybychom měli odvahu otestovat H pro $P = 21$
- Možná heuristika: Pokud $H = H'$, tak testuj, zda $\mathrm{pp}(H) | f, g$ a pokud ano vrať $\mathrm{pp}(H)$
- Protože $\deg H \geq \deg \mathrm{NSD}_{\mathbb{Z}}[x](f, g)$, tak to neovlivní korektnost
- Ale dělení polynomů je drahé, tak to nechcem zkoušet bezhlavě

Příklad dokončený

- $H := x - 1, P = 3 \cdot 7 = 21$
- $2d \cdot LM(f, g) = 32$
- $p = 11,\ h = x - 1$
- $H = x - 1, P = 11 \cdot 21 = 221 > 32$
- Všimněme si, že jsem mohli skončit dřív, kdybychom měli odvahu otestovat H pro $P = 21$
- Možná heuristika: Pokud $H = H'$, tak testuj, zda $\mathrm{pp}(H) | f, g$ a pokud ano vrať $\mathrm{pp}(H)$
- Protože $\deg H \geq \deg \mathrm{NSD}_{\mathbb{Z}}[x](f, g)$, tak to neovlivní korektnost
- Ale dělení polynomů je drahé, tak to nechcem zkoušet bezhlavě

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

Složitost Algoritmu 22 (velmi zhruba)

- Značme $n = \deg f \geq \deg g$ (búno)
- Lze dokázat složitost $O(n^3(\log n + l)^2$, kde $l = \max(\mathrm{mc}(f), \mathrm{mc}(g)$
- My naznačíme složitost $O(n^3 \log^2(n))$ pro l malé
- Pro jednoduchost předpokládáme, že smolná prvočísla jsou vzácná
- Odhadneme $LM(f, g) = O(2^n\sqrt{n})$
- P roste víc než exponenciálně, tedy while cyklus proběhne zhruba $O(\log_2(LM(f, g)) = O(n)$-krát
- n-té prvočíslo je asi $n \log n$, tedy $\ell(p) = O(\log n)$
- NSD v $\mathbb{Z}_p$ ... $O(n^2\ell(p)^2) = O(n^2 \log(n)^2)$
- ČZV přes Garnera $O(n^2 \log n)$
- While cyklus tedy stojí $O(n \cdot n^2 \log(n)^2)$
- pp(H) je asi n NSD v $\mathbb{Z}$ pro čísla délky $O(n)$, tedy $O(n^3)$ celkem
- Test $h|f, g$ je $O(n^3)$ (koeficienty h jsou délky $O(n)$)
- Celkem $O(n^3 \log(n)^2)$

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

NSD v $R[x, y]$ (orientačně)

- Reprezentujeme $R[x, y]$ jako $(R[y])[x]$
- Stupeň je stupeň v x
- Koeficienty (vč. vedoucího členu) jsou polynomy v y
- Modulární metoda tu vítězí nad pseudodělením
- Počítáme modulo polynom z $R[x]$
- Malá prvočísla $\leftrightarrow$ malé ireducibilní polynomy $y - \alpha$
- Vzpomeňme si $f(x, y)\%(y - \alpha) = f(x, \alpha)$
- Příklad: $(x + x^2y + y^2)\%(y - 7) = x + 7x^2 + 49$
- ČZV bude věta o interpolaci polynomu

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, NSD$(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, NSD$(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, NSD$(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Příklad

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Stupeň f, g v y (bacha!) je 2, tedy počítáme modulo $y - \alpha_1, y - \alpha_2, y - \alpha_3$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = 2x + 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$, kde c_0, c_1 jsou nejvýš kvadratické
- $c_0(1) = c_0(2) = c_0(3) = 1$
- $c_1(1) = 1$, $c_1(2) = 2$, $c_1(3) = 3$
- Je vidět řešení $xy + 1$
- Polynom $y - 0$ by byl nepoužitelný: Dělí vedoucí členy f i g

Šťastná to hodnota

- Hodnota $\alpha \in R$ je použitelná pro $f, g \in (R[y])[x]$, pokud $x - \alpha \not| \mathrm{NSD}_{R[y]}(\mathrm{lc}(f), \mathrm{lc}(g))$
- Opět potřebujeme dokázat (vynecháme), že pro použitelné hodnoty je

$$\mathrm{NSD}_{R[x,y]}(f, g)(x, \alpha) | \mathrm{NSD}_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je šťastná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) = \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je smolná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) < \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Smolných hodnot je jen konečně mnoho (důkaz vynecháme)

Šťastná to hodnota

- Hodnota $\alpha \in R$ je použitelná pro $f, g \in (R[y])[x]$, pokud $x - \alpha \not| \mathrm{NSD}_{R[y]}(\mathrm{lc}(f), \mathrm{lc}(g))$
- Opět potřebujeme dokázat (vynecháme), že pro použitelné hodnoty je

$$\mathrm{NSD}_{R[x,y]}(f,g)(x,\alpha) | \mathrm{NSD}_{R[x]}(f(x,\alpha), g(x,\alpha))$$

- Použitelná hodnota je šťastná, pokud

$$\deg NSD_{R[x,y]}(f,g)(x,\alpha) = \deg NSD_{R[x]}(f(x,\alpha), g(x,\alpha))$$

- Použitelná hodnota je smolná, pokud

$$\deg NSD_{R[x,y]}(f,g)(x,\alpha) < \deg NSD_{R[x]}(f(x,\alpha), g(x,\alpha))$$

- Smolných hodnot je jen konečně mnoho (důkaz vynecháme)

Šťastná to hodnota

- Hodnota $\alpha \in R$ je použitelná pro $f, g \in (R[y])[x]$, pokud $x - \alpha \not| \mathrm{NSD}_{R[y]}(\mathrm{lc}(f), \mathrm{lc}(g))$
- Opět potřebujeme dokázat (vynecháme), že pro použitelné hodnoty je

$$\mathrm{NSD}_{R[x,y]}(f, g)(x, \alpha) | \mathrm{NSD}_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je šťastná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) = \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je smolná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) < \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Smolných hodnot je jen konečně mnoho (důkaz vynecháme)

Šťastná to hodnota

- Hodnota $\alpha \in R$ je použitelná pro $f, g \in (R[y])[x]$, pokud $x - \alpha \not| \mathrm{NSD}_{R[y]}(\mathrm{lc}(f), \mathrm{lc}(g))$
- Opět potřebujeme dokázat (vynecháme), že pro použitelné hodnoty je

$$\mathrm{NSD}_{R[x,y]}(f, g)(x, \alpha) | \mathrm{NSD}_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je šťastná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) = \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je smolná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) < \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Smolných hodnot je jen konečně mnoho (důkaz vynecháme)

Šťastná to hodnota

- Hodnota $\alpha \in R$ je použitelná pro $f, g \in (R[y])[x]$, pokud $x - \alpha \not| \mathrm{NSD}_{R[y]}(\mathrm{lc}(f), \mathrm{lc}(g))$
- Opět potřebujeme dokázat (vynecháme), že pro použitelné hodnoty je

$$\mathrm{NSD}_{R[x,y]}(f, g)(x, \alpha) | \mathrm{NSD}_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je šťastná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) = \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je smolná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) < \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Smolných hodnot je jen konečně mnoho (důkaz vynecháme)

Šťastná to hodnota

- Hodnota $\alpha \in R$ je použitelná pro $f, g \in (R[y])[x]$, pokud $x - \alpha \not| \mathrm{NSD}_{R[y]}(\mathrm{lc}(f), \mathrm{lc}(g))$
- Opět potřebujeme dokázat (vynecháme), že pro použitelné hodnoty je

$$\mathrm{NSD}_{R[x,y]}(f, g)(x, \alpha) | \mathrm{NSD}_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je šťastná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) = \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Použitelná hodnota je smolná, pokud

$$\deg NSD_{R[x,y]}(f, g)(x, \alpha) < \deg NSD_{R[x]}(f(x, \alpha), g(x, \alpha))$$

- Smolných hodnot je jen konečně mnoho (důkaz vynecháme)

Kolik potřebujeme šťastných hodnot?

- Ať nejvyšší stupeň f, g v y je k
- Protože chceme interpolovat koeficienty – polynomy v $R[y]$, tak potřebujeme $k+1$ šťastných hodnot
- Toto je analogie Landau-Mignottovy meze a je snadná
- Smolné hodnoty dají vysoké stupně v x, tedy se dají snadno otestovat (obzvlášť, pokud známe aspoň jednu šťastnou hodnotu)
- Co se naopak oproti $\mathbb{Z}[x]$ zhorší je problém vedoucího koeficientu

Kolik potřebujeme šťastných hodnot?

- Ať nejvyšší stupeň f, g v y je k
- Protože chceme interpolovat koeficienty – polynomy v $R[y]$, tak potřebujeme $k+1$ šťastných hodnot
- Toto je analogie Landau-Mignottovy meze a je snadná
- Smolné hodnoty dají vysoké stupně v x, tedy se dají snadno otestovat (obzvlášť, pokud známe aspoň jednu šťastnou hodnotu)
- Co se naopak oproti $\mathbb{Z}[x]$ zhorší je problém vedoucího koeficientu

Kolik potřebujeme šťastných hodnot?

- Ať nejvyšší stupeň f, g v y je k
- Protože chceme interpolovat koeficienty – polynomy v $R[y]$, tak potřebujeme $k + 1$ šťastných hodnot
- Toto je analogie Landau-Mignottovy meze a je snadná
- Smolné hodnoty dají vysoké stupně v x, tedy se dají snadno otestovat (obzvlášť, pokud známe aspoň jednu šťastnou hodnotu)
- Co se naopak oproti $\mathbb{Z}[x]$ zhorší je problém vedoucího koeficientu

Kolik potřebujeme šťastných hodnot?

- Ať nejvyšší stupeň f, g v y je k
- Protože chceme interpolovat koeficienty – polynomy v $R[y]$, tak potřebujeme $k + 1$ šťastných hodnot
- Toto je analogie Landau-Mignottovy meze a je snadná
- Smolné hodnoty dají vysoké stupně v x, tedy se dají snadno otestovat (obzvlášť, pokud známe aspoň jednu šťastnou hodnotu)
- Co se naopak oproti $\mathbb{Z}[x]$ zhorší je problém vedoucího koeficientu

Kolik potřebujeme šťastných hodnot?

- Ať nejvyšší stupeň f, g v y je k
- Protože chceme interpolovat koeficienty – polynomy v $R[y]$, tak potřebujeme $k + 1$ šťastných hodnot
- Toto je analogie Landau-Mignottovy meze a je snadná
- Smolné hodnoty dají vysoké stupně v x, tedy se dají snadno otestovat (obzvlášť, pokud známe aspoň jednu šťastnou hodnotu)
- Co se naopak oproti $\mathbb{Z}[x]$ zhorší je problém vedoucího koeficientu

Kolik potřebujeme šťastných hodnot?

- Ať nejvyšší stupeň f, g v y je k
- Protože chceme interpolovat koeficienty – polynomy v $R[y]$, tak potřebujeme $k + 1$ šťastných hodnot
- Toto je analogie Landau-Mignottovy meze a je snadná
- Smolné hodnoty dají vysoké stupně v x, tedy se dají snadno otestovat (obzvlášť, pokud známe aspoň jednu šťastnou hodnotu)
- Co se naopak oproti $\mathbb{Z}[x]$ zhorší je problém vedoucího koeficientu

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Ted' to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Ted' to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Problém v příkladu

- $f = yx^2 + (1 - y^2)x - y = (xy + 1)(x - y)$
- $g = yx^2 + (1 + y^2)x + y = (xy + 1)(x + y)$
- Volme $\alpha_1 = 1$, $\mathrm{NSD}(x^2 - 1, x^2 + 2x + 1) = x + 1$
- Volme $\alpha_2 = 2$, $\mathrm{NSD}(2x^2 - 3x - 2, 2x^2 + 5x + 1) = -2x - 1$
- Volme $\alpha_3 = 3$, $\mathrm{NSD}(3x^2 - 8x - 3, 3x^2 + 10x + 3) = 3x + 1$
- Teď to chceme zkombinovat do polynomu $c_1(y)x + c_0(y)$
- „Řešení“ $(4y^2 - 15y + 12)x + (2y^2 - 8y + 7)$
- Uff...
- Pro správný výpočet v $\mathbb{Z}[x, y]$ musíme vědět, jak volit $\pm$; máme 2^{k+1} možností

Co lze dokázat

- Modulární algoritmus v $\mathbb{Z}[x, y]$ lze zformulovat tak, aby měl složitost $O(n^5(\log n + l)^2)$, kde l je maximální koeficient f, g
- Pro více proměnných máme stále polynomiální algoritmus, ale exponenty v odhadu složitosti rostou

Co lze dokázat

- Modulární algoritmus v $\mathbb{Z}[x, y]$ lze zformulovat tak, aby měl složitost $O(n^5(\log n + l)^2)$, kde l je maximální koeficient f, g
- Pro více proměnných máme stále polynomiální algoritmus, ale exponenty v odhadu složitosti rostou

Co lze dokázat

- Modulární algoritmus v $\mathbb{Z}[x, y]$ lze zformulovat tak, aby měl složitost $O(n^5(\log n + l)^2)$, kde l je maximální koeficient f, g
- Pro více proměnných máme stále polynomiální algoritmus, ale exponenty v odhadu složitosti rostou

Hlavní poučení

- Na detailech implementace záleží
- Přímočarý postup nemusí být ten nejrychlejší
- Fourierova transformace je skvělá
- Teoretické vhledy (např. ČZV) nám dají lepší algoritmy
- Metoda rozděl a panuj se hodí (i pro analýzu algoritmu)
- Způsob posuzování algoritmu záleží na situaci (např. dvě metody pro počítání složitosti pro polynomy)
- Pokud vám to nestačilo, je tu Počítačová algebra 2

Hlavní poučení

- Na detailech implementace záleží
- Přímočarý postup nemusí být ten nejrychlejší
- Fourierova transformace je skvělá
- Teoretické vhledy (např. ČZV) nám dají lepší algoritmy
- Metoda rozděl a panuj se hodí (i pro analýzu algoritmu)
- Způsob posuzování algoritmu záleží na situaci (např. dvě metody pro počítání složitosti pro polynomy)
- Pokud vám to nestačilo, je tu Počítačová algebra 2

Hlavní poučení

- Na detailech implementace záleží
- Přímočarý postup nemusí být ten nejrychlejší
- Fourierova transformace je skvělá
- Teoretické vhledy (např. ČZV) nám dají lepší algoritmy
- Metoda rozděl a panuj se hodí (i pro analýzu algoritmu)
- Způsob posuzování algoritmu záleží na situaci (např. dvě metody pro počítání složitosti pro polynomy)
- Pokud vám to nestačilo, je tu Počítačová algebra 2

Hlavní poučení

- Na detailech implementace záleží
- Přímočarý postup nemusí být ten nejrychlejší
- Fourierova transformace je skvělá
- Teoretické vhledy (např. ČZV) nám dají lepší algoritmy
- Metoda rozděl a panuj se hodí (i pro analýzu algoritmu)
- Způsob posuzování algoritmu záleží na situaci (např. dvě metody pro počítání složitosti pro polynomy)
- Pokud vám to nestačilo, je tu Počítačová algebra 2

Hlavní poučení

- Na detailech implementace záleží
- Přímočarý postup nemusí být ten nejrychlejší
- Fourierova transformace je skvělá
- Teoretické vhledy (např. ČZV) nám dají lepší algoritmy
- Metoda rozděl a panuj se hodí (i pro analýzu algoritmu)
- Způsob posuzování algoritmu záleží na situaci (např. dvě metody pro počítání složitosti pro polynomy)
- Pokud vám to nestačilo, je tu Počítačová algebra 2

Hlavní poučení

- Na detailech implementace záleží
- Přímočarý postup nemusí být ten nejrychlejší
- Fourierova transformace je skvělá
- Teoretické vhledy (např. ČZV) nám dají lepší algoritmy
- Metoda rozděl a panuj se hodí (i pro analýzu algoritmu)
- Způsob posuzování algoritmu záleží na situaci (např. dvě metody pro počítání složitosti pro polynomy)
- Pokud vám to nestačilo, je tu Počítačová algebra 2

Hlavní poučení

- Na detailech implementace záleží
- Přímočarý postup nemusí být ten nejrychlejší
- Fourierova transformace je skvělá
- Teoretické vhledy (např. ČZV) nám dají lepší algoritmy
- Metoda rozděl a panuj se hodí (i pro analýzu algoritmu)
- Způsob posuzování algoritmu záleží na situaci (např. dvě metody pro počítání složitosti pro polynomy)
- Pokud vám to nestačilo, je tu Počítačová algebra 2

Hlavní poučení

- Na detailech implementace záleží
- Přímočarý postup nemusí být ten nejrychlejší
- Fourierova transformace je skvělá
- Teoretické vhledy (např. ČZV) nám dají lepší algoritmy
- Metoda rozděl a panuj se hodí (i pro analýzu algoritmu)
- Způsob posuzování algoritmu záleží na situaci (např. dvě metody pro počítání složitosti pro polynomy)
- Pokud vám to nestačilo, je tu Počítačová algebra 2