Polinomfaktorizáció (egyváltozós polinomok felbontása)

F test, $F[x]$ egyváltozós polinomok gyűrűje.
Feltesszük: tudunk F-ben számolni (testműveletek, =-ség teszt). Algoritmusok költsége: F-beli alapműveletek száma

Általánosságok

analógia: $F[x] \sim \mathbb{Z}$: $\quad f = f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \sim c = c_0 + c_1 \cdot 10 + \ldots + c_{n-1}10^{n-1}$
Euklideszi gyűrű: $\quad \deg f \sim c$ számjegyei száma (kb. $\log |c|$):
van maradékos osztás $(/, \%)$, van euklideszi algoritmus
f irreducibilis $\Leftrightarrow$ f prím $\Leftrightarrow$ (f) max. ideál $\Leftrightarrow$ $F[x]/(f)$ test.
$\exists$ egyértelmű felbontás irreducibilisek szorzatára.
Megjegyzés: A felbontás egységekkel (=konstansok) való szorzás erejéig egyértelmű. Kényelmes megkövetelni, hogy a főegyütthatók 1-ek. Ekkor a felbontás egyértelmű.

Faktorizációs feladatok:	**Felbontás**	**Hasítás**
	$f = f_1^{\alpha_1} \cdots f_s^{\alpha_s}$, f_i páronként rel. prím irred.	$f = gh$, $\quad g, h$ nem konstans (ha f nem irred.)

Alapműveletek, alapvető algoritmusok költségei. $(\deg op_i \leq n)$:
$+, -, =$: $O(n)$
$*, /, \%$ standard: $O(n^2)$;
$\cdot, /, \%$ gyors: FFT-vel $O(n \log n)$; általános testekre $O(n \log n \log\log n)$ $+, -, \cdot \bmod f$: $O(1)$ osztás
(Kiterjesztett) euklideszi algoritmus: $O(n)$ osztás
inverz mod f: $\sim$ kiterjesztett Euklideszi algoritmus.
Feladat: Biz. be, hogy f/g (és $f\%g$) költsége $O(\deg g \cdot \deg(f/g))$ művelet. Biz. be, hogy az Eukl. költsége (f, g)-re $O(\deg f \cdot \deg g)$. (Segítség: Tfh. $\deg f \geq \deg g$. Mutassuk meg, hogy a futás során felmerülő osztásoknál a hányadosok fokszámösszege $\leq \deg f$.)

Maradékosztálygyűrű:. $R = F[x]/(f)$ **algebra** F fölött: vektortér és $a(uv) = (au)v = u(av)$ $(a \in F, u, v \in R)$. Dimenzió $\dim_F R = n = \deg f$: bázis $1, x, \ldots, x^{n-1}$.

Kínai maradéktétel. $f = f_1 \cdots f_s \in F[x]$, $\deg f_i > 0$, $(f_i, f_j) = 1$ $(i \neq i)$ $\Rightarrow$ $F/(f) \cong F/(f_1) \oplus \cdots \oplus F/(f_s)$

$$u \text{ mod f} \leftrightarrow (u \; mod \; f_1, \ldots, u \; mod \; f_s)$$

Megjegyzés: A megfeleltetés a kiértékelés/interpoláció általánosítása: $f_i = x - a_i$ $(a_i \neq a_j$, ha $i \neq j)$

$$u \in F[x], \deg u < s \quad \leftrightarrow \quad (u(a_1), \ldots, u(a_s)).$$

Feladat: Biz. be, hogy $f, g, h \in F[x]$, $(f, g) = 1$, $\deg h < \deg fg$, $\deg f, \deg g > 0$ esetén $\exists! u, v \in F[x] : \deg u < \deg g$, $\deg v < \deg f$ és $fu + gv = h$. Hogyan kereshető meg u és v?

Idempotensek:. $e_i \equiv \begin{cases} 0 & \text{mod } f_j \;\; (i \neq j) \\ 1 & \text{mod } f_i \end{cases}$ $\quad \deg e_i < \deg f \quad$ az $F/(f_i)$ (-nek megfelelő) részgyűrű (ideál) egységeleme.
Feladat: Tfh. adott f_i $(i = 1, \ldots, m)$. Adjunk hatékony módszert e_i kiszámítására.
Pl. $f_i = x - a_i$-re: $e_i(a_i) = \begin{cases} 0 & \text{ha } i \neq j) \\ 1 & \text{ha } i = j \end{cases}$ $\quad$ Lagrange-alappolinomok.

Négyzetmentes felbontás

Adott $f \in F[x]$. Keresendő felbontás: $f = \prod f_i^{\alpha_i}$, hogy f_i (páronként relatív prím) négyzetmentes.
($f \in F[x]$ négyzetmentes, ha $g^2 | f \;\Rightarrow\; g$ egység . Másképp: $f = f_1, \ldots, f_s$, $f_i \in F_i[x]$ páronként rel. prím (1 főegyütthatósággal: páronként kül.) irreducibilis.)

Formális deriválás:. $f(x) = \sum_{i=0}^n a_i x^i \;\mapsto f'(x) = \sum_{i=1}^n i a_i x^{i-1}$.
Tulajdonságok: F-lineáris + Leibniz-szabály: $(fg)' = fg' + f'g$.
Milyen f-ekre lesz $f' = 0$?:
(1) f konstans, vagy
(2) $\operatorname{char} F = p$, $f(x) = \sum a_{p^j} x^{pj}$ (azaz: $a_i = 0$, ha $p \not| i$).
Állítás: (1) $g^2 | f \;\Rightarrow\; g | (f, f')$; (2) g irreducibilis, $g | (f, f') \;\Rightarrow\; g^2 | f$ vagy $f' = 0$.

Perfekt testek:. F perfekt, ha $\operatorname{char} F = 0$ vagy $\operatorname{char} F = p$ és $\forall a \in F \exists \sqrt[p]{a} \in F$ ($b = \sqrt[p]{a}$, ha $b^p = a$). (Hány $\sqrt[p]{a}$ lehet?)
Állítás: F véges $\Rightarrow$ F perfekt. (Miért? Algoritmus $\sqrt[p]{\;}$ vonásra $O(\log |F|)$ szorzással?)
Állítás: $\operatorname{char} F = p$, F perfekt, $f' = 0 \Rightarrow \exists \sqrt[p]{f} \in F[x]$ $(g \in F[x] : \; f = g^p)$.
Következmény: Ha F perfekt, $g^2 | f \;\Leftrightarrow\; g | (f, f')$.

Algoritmus. (durva rekurzió, char $F=0$ vagy F véges)
(1) ha $f'=0$, akkor vagy $\deg f=0$ vagy tovább $\sqrt[p]{f}$-fel
(2) ha $f'\neq 0$, akkor $f/(f,f')$ négyzetmentes, tovább (f,f')-vel, ha az nem 1.
Leggyorsabb ismert algoritmus (Yun) költsége: $n^{1+o(1)}$, ha char $F=0$; $O(n^{1+o(1)}+n\log|F|)$, ha $|F|<\infty$.

Felbontás véges testek felett

$F=\mathbb{F}_q=GF(q)$, $q=p^d$. Izomorfia erejéig egyért.
Fermat-tétel: $a^q=a$ minden $a\in F$-re.
Reprezentáció, számolás: $\mathbb{F}_q\cong\mathbb{F}_p[x]/(h)$, $h=h(x)$ d-edfokú irred. (Alapműveletek kölsége moduláris polinomműveletek.)

$$f=f_1^{\alpha_1}\cdots f_s^{\alpha_s},\ f_i \text{ páronként rel. prím irred.}, n=\deg f.$$

Kínai maradéktétel:. $u\leftrightarrow(u_1=u \bmod f_1^{\alpha_1},\ldots,u_s=u \bmod f_s^{\alpha_s})$,

Maradékosztálygyűrű:. $R=R_f=F[x]/(f)$ n-dimenziós F-algebra (nd-dim. $\mathbb{F}_p$-alg.) Fontos hasonlóság $\mathbb{Z}$-vel: R véges.

Berlekamp algoritmusa

Frobenius-endomorfizmus:. $\Phi_0: u\mapsto u^p$ gyűrű ($\mathbb{F}_p$-algebra) endomorfizmusa R-nek (char $R=p \Rightarrow \forall u,v\in R: (u+v)^p=u^p+v^p$),

$$\Phi=\Phi_0^d: u\mapsto u^q \ F\text{-algebra endomorfizmusa } R\text{-nek.}$$

Kínai maradékokkal: $(u_1,\ldots,u_s)\mapsto\ (u_1^p,\ldots,u_s^p)$ (ill. $(u_1^p,\ldots,u_s^p)$)

Berlekamp-részalgebra:. $B_f=\{u\in R|u^q=u\}$ F-részalgebra (mert Φ fixpontjai).

Állítás:. $B_f=\{u\in R|u \bmod f_i^{\alpha_i}\in F\}$
Biz.: Kínai maradékokkal komponensenként. Azt kell látni, hogy tetsz. $u\in F[x]$-re $u^q\equiv u \bmod f_i^{\alpha_i} \Leftrightarrow u \bmod f_i^{\alpha_i}$ konstans. A $\Rightarrow$ irány következik a Fermat-tételből. $\Leftarrow$: Az $u^q\equiv u$ teljesül modulo f_i is. Mivel $F/(f_i)$ test, az x^q-x-nek legfeljebb q gyöke van $F/(f_i)$-ben. A q darab konstans mindegyike ilyen, tehát ez az összes, így $u=c+gf_i$ alakú, ahol $c\in F$. Végül $u\equiv u^{q^N}\equiv c+g^{q^N}f_i^{q^N}\equiv c \bmod f_i^{s_i}$, ha $q^N>s_i$.

Algoritmus (Berlekamp-részalgebra kiszámítása):. $B_f=\ker(\Phi-I)$ (bázisának) kiszámítása:
(1) Lin. egyenletrendszer felírása: Φ mátrixa az $1,x,\ldots,x^{n-1}$ bázisban: oszlopai az $1 \bmod f, x^q \bmod f,\ldots,x^{q(n-1)} \bmod f$ polinomok együtthatóvektorai. Gyorshatványozással $x^q \bmod f$, majd $x^{qi} \bmod f$. Költség: $O((\log q+n)n^2))$ művelet.
(2) Lin. egyeletrendszer megoldása: $O(n^3)$ művelettel.
Összköltség: $O(n^3+n^2\log q)$.

Berlekamp algoritmusa. (hasításra)
(1) B_f kiszámítása. Költség: $O(n^3+n^2\log q)$. Ha $\dim_F B_f=1$, akkor f egy irred. pol. hatványa. (Pl. a négyzetmentes faktorizáció alkalmazható.)
(2) Ha $\dim_F B_f>1$, legyen $u\in B_f$, ami nem konstans *modf* (más szóval u lin. ftlen 1 *modf*-től).
sorban $a\in F$-re, amíg nem találunk faktort, próbáljuk ki $(u-a,f)$-et.
Költség: $O(qn^3)$ (valójában $O(qn^2)$). Nem polinomiális $\log q$-ban! (f mérete: $\deg f\log q$.)

Berlekamp $\mathbb{F}_p$ fölött. (R-et $\mathbb{F}_p$-algebraként tekintjük.)
(1) $A_f=\{u\in R|u^p=u\}$ $\mathbb{F}_p$-részalgebra. (Elnevezés: **abszolút Berlekamp-részalgebra**.) Kiszámítás költsége: $O(nd)^3$ művelet $\mathbb{F}_p$-ben ($q=p^d$).
(2) Költség: $O(pn^3)$.
Összköltség: polinomiális n-ben és $\log q$-ban, ha p konstans (pl. $p=2$, $p=3$).

A Cantor-Zassenhaus algoritmus (két változata)

C-Z algorimus. ($p\neq 2$)
(1) B_f kiszámítása. Ha $\dim_F B_f=1$, akkor f egy irred. hatványa.
(2) Ha $\dim_F B_f>1$, akkor vegyünk egy u véletlen elemet B_f-ből (a báziselemek véletlen együtthatós lin. komb.), próbálkozzunk $(u^{\frac{q-1}{2}}-1,f)$-fel (gyorshatványozást használunk).
Állítás: Ha $\dim_F B_f>1$, legalább $\frac{q^2-1}{2q^2}\geq\frac{4}{9}$ valószínűséggel találunk valódi osztót.
Biz.: $u\leftrightarrow(u_1,\ldots,u_s)$, $u_i\in F$ páronként független, egyenletes eloszlású véletlen.

$$u_i^{\frac{q-1}{2}}\equiv\begin{cases}0 & \frac{1}{q}\\ 1 & \frac{q-1}{2q}\\ -1 & \frac{q-1}{2q}\end{cases}\ \text{valószínűséggel.}$$

Tehát annak valószínűsége, hogy $u_1^{\frac{q-1}{2}} \equiv 1$ de $u_2^{\frac{q-1}{2}} \not\equiv 1$: $\frac{q-1}{2q} \cdot \frac{q+1}{2q} = \frac{q^2-1}{4q^2}$. Ebben az esetben $u^{\frac{q-1}{2}} - 1$ osztható f_1-gyel, de f_2-vel nem, tehát valódi osztót kapunk. A szimmetrikus esemény ($u_1 \leftrightarrow u_2$ csere) éppilyen jó. A két esemény kizárja egymást, így legalább $\frac{q^2-1}{2q^2}$ eséllyel nyerünk.
(2') Ha $\dim_F B_f > 1$, legyen $v \in B_F \setminus F \cdot 1$ egy rögzített elem és $u = v + \alpha \cdot 1$, ahol $\alpha \in F$ véletlen skalár; próbálkozzunk $(u^{\frac{q-1}{2}} - 1, f)$-fel.
Állítás: Ha $\dim_F B_f > 1$, legalább $\frac{q-1}{2q} \geq \frac{1}{3}$ valószínűséggel találunk valódi osztót.
Biz.: $u \leftrightarrow (v_1 + \alpha, \ldots, v_s + \alpha)$. Ekkor $(v_i + \alpha)^{\frac{q-1}{2}} \in \{0, 1, -1\}$ és ha $v_i \neq v_j$ akkor a $\frac{v_i+\alpha}{v_j+\alpha}$ tört az $F \setminus \{1\} \cup \{\infty\}$ értékeket veszi föl, mindegyiket pontosan egyetlen α-ra. Ezek közül $\frac{q-1}{2}$ kvadratikus nemmaradék van, tehát $\frac{q-1}{2}$ féle α-ra $\pm 1 = (v_i + \alpha)^{\frac{q-1}{2}} = -(v_j + \alpha)^{\frac{q-1}{2}}$, azaz vagy $(v_i + \alpha)^{\frac{q-1}{2}} = 1$ és $(v_j + \alpha)^{\frac{q-1}{2}} = -1$ (ez esetben $u^{\frac{q-1}{2}} - 1$ osztható f_i-vel, de nem osztható f_j-vel), vagy fordítva.
Leggyorsabb változat (Kaltofen-Shoup, teljes felbontás) költsége: $O(n^{1.815} \log q)$ művelet.

Feladatok

1. **C-Z additív megfelelője 2 karakterisztikában:** Legyen $F = \mathbb{F}_{2^d}$, $f \in F[x]$. Egy $u \in B_f$ elem *nyoma* $\mathrm{Tr}(u) = u + u^2 + \ldots + u^{2^{d-1}} \in B_f$. Mutassuk meg, hogy ha $\dim_F B_f > 1$, akkor véletlen $u \in B_f$-re $(\mathrm{Tr}(u), f)$ egy valódi osztója f-nek. (Segítség: Kínai maradékokkal. Mutassuk meg, hogy $B_f \cong F \oplus \cdots \oplus F$ komponensein Tr lehetséges értékei 0 és 1, mindkettő $1/2$ valószínűséggel vétetik fel.)

2. **Felbontás a fokszámok szerint** (distinct degree factorization): Adjunk determinisztikus polinomidejű algoritmust, ami $f \in \mathbb{F}_q[x]$-et felbontja úgy $\prod g_i$ szorzatra úgy, hogy minden egyes g_i tényező azonos r_i fokú irreducibilis polinomok szorzata. (Segítség: feltehető, hogy f négyzetmentes. Mutassuk meg és használjuk, hogy ha $h(x)$ egy r-edfokú irreducibilis polinom, akkor $h | x^{q^r} - x$.)

3. **Gyökvonás:** Legyen r egy prím, $F = \mathbb{F}_q$, $a \in F$. Legyen $\mathrm{ord}(a)$ a (multiplikatív) rendje (F^*-ban).
(a) Ha $r \not| \mathrm{ord}(a)$, mutassuk meg, hogy $\exists! \sqrt[r]{a}$. Adjunk determiszikus polinomidejű algoritmust a meghatározására.
(b) Ha $r | \mathrm{ord}(a)$, akkor tegyük még fel, hogy adott egy $b \in F$ r-edik nem-maradék (azaz $\not\exists$ egyetlen $\sqrt[r]{b}$ sem). Adjunk $r(\log q)^{O(1)}$ idejű (vagy, ami még jobb: $\sqrt{r}(\log q)^{O(1)}$ idejű) algoritmust annak eldöntésére, van-e $\sqrt[r]{a}$, és ha igen, keressünk is egy ilyet. (Segítség: $F^* \cong G \times H$, ahol $|G|$ r-hatvány és $(|H|, r) = 1$. Oldjuk meg a feladatot külön G-ben és H-ban.)
Megjegyzés: Tegyük fel, hogy $q = p$ prím, $r | (p-1)$. Kiterjesztett Riemann Hipotézis (ERH) $\Rightarrow$ a legkisebb modulo p vett r-edik nemmaradék $O(\log^2(p))$ nagyságú. Tehát ERH $\Rightarrow$ F_p-ben gyökvonás ($x^r - 1$ egy gyökének megkeresése) polinomidőben megy.