Trükkök irreducibiltás vizsgálatára

Redukció modulo p

Jelölés.

Adott p prímszám esetén az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom modulo p redukáltján az

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x]$$

polinomot értjük, ahol $\overline{a_i}$ az a_i egész számot tartalmazó modulo p maradékosztály.

A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x]: \ \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Nyilván $\deg \overline{f} \leq \deg f$, továbbá ha $p \nmid a_n$, akkor (és csak akkor!) $\overline{a_n} \neq \overline{0}$, és így $\deg \overline{f} = \deg f = n$.

Példa.

Legyen $p = 5$ és $f = 10x^3 + 7x^2 + 25x - 2$. Ekkor

$$\overline{f} = \overline{10}x^3 + \overline{7}x^2 + \overline{25}x + \overline{-2} = \overline{0}x^3 + \overline{2}x^2 + \overline{0}x + \overline{3} = \overline{2}x^2 + \overline{3} \in \mathbb{Z}_5[x].$$

Egy trükk

Példa.

Felbontható-e az $f = x^4 + 2x^3 + 6x^2 + 7x + 5 \in \mathbb{Z}[x]$ polinom kisebb fokszámú egész együtthatós polinomok szorzatára?

Tegyük fel, hogy igen:

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \quad \text{és } 0 < \deg g, \deg h < 4.$$

Redukáljuk modulo 2: $\overline{f} = \overline{g} \cdot \overline{h}$, ahol $\overline{g} \cdot \overline{h} \in \mathbb{Z}_2[x]$ és $0 < \deg \overline{g}, \deg \overline{h} < 4$.

Node $\overline{f} = x^4 + x + 1$ irreducibilis $\mathbb{Z}_2[x]$-ben, mert nincs neki se első- se másodfokú irreducibilis osztója. 

Tehát f nem bontható fel kisebb fokú egész együtthatós polinomok szorzatára, így irreducibilis a racionális számok teste felett.

Kronecker módszere

Példa.

Irreducibilis-e az $f = x^4 - 4x^3 + 7x^2 - 6x + 3 \in \mathbb{Q}[x]$ polinom?

Tfh. $f = g \cdot h$, ahol $g, h \in \mathbb{Z}[x]$ és $0 < \deg g \overset{\text{ÁMN}}{\leq} \deg h < n$.

Ekkor $\deg g \leq 2$, és minden $k \in \mathbb{Z}$ esetén $g(k) \mid f(k)$. Például

$$a := g(0) \mid f(0) = 3, \quad b := g(1) \mid f(1) = 1, \quad c := g(2) \mid f(2) = 3.$$

Tehát az (a, b, c) számhármasra 32 lehetőség van:

$$(a, b, c) \in \{-3, -1, 1, 3\} \times \{-1, 1\} \times \{-3, -1, 1, 3\}.$$

Mind a 32 esetben egyértelműen meg tudjuk határozni a g polinomot Lagrange-interpolációval.

Ha valamelyik osztja f-et, akkor kapunk egy nemtriviális felbontást;
ha egyik se osztja f-et, akkor f irreducibilis.

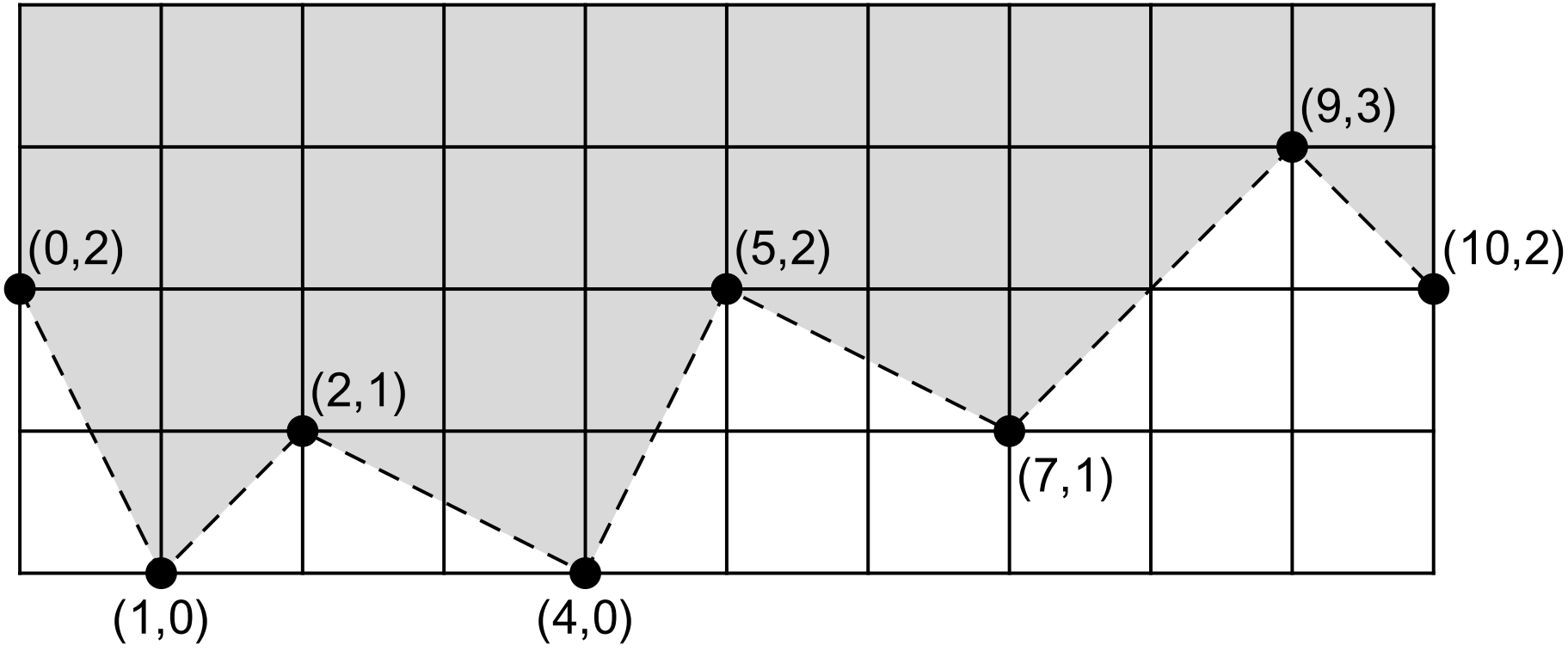
$$(a, b, c) = (1, 1, 3) \rightsquigarrow g = x^2 - x + 1 \rightsquigarrow f = (x^2 - x + 1)(x^2 - 3x + 3)$$

Newton-poligon

$f = 36 + 2x + 6x^2 + 2x^4 + 18x^5 + 3x^7 + 54x^9 + 18x^{10}$
$p = 3$

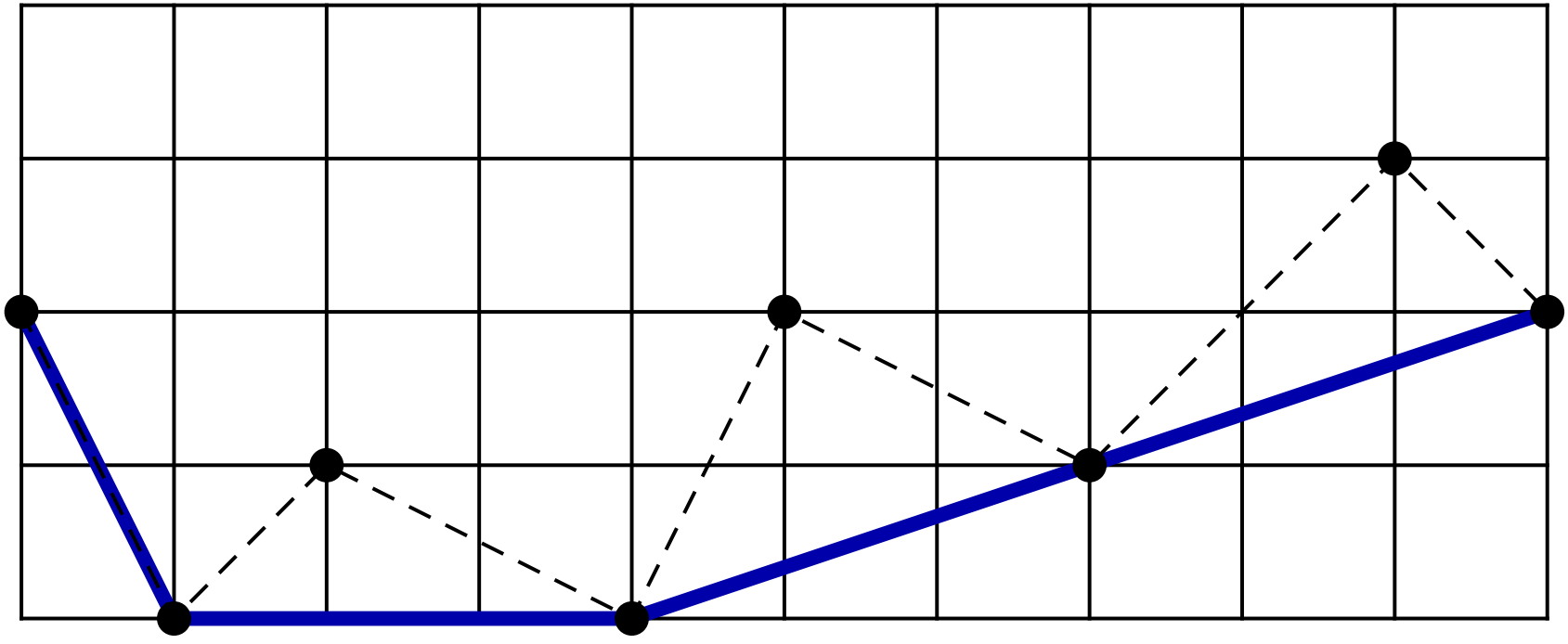
Newton-poligon

$f = 3^2 \cdot 4 + 3^0 \cdot 2x + 3^1 \cdot 2x^2 + 3^0 \cdot 2x^4 + 3^2 \cdot 2x^5 + 3^1 \cdot 1x^7 + 3^3 \cdot 2x^9 + 3^2 \cdot 2x^{10}$
$p = 3$



Newton-poligon

$f = 3^2 \cdot 4 + 3^0 \cdot 2x + 3^1 \cdot 2x^2 + 3^0 \cdot 2x^4 + 3^2 \cdot 2x^5 + 3^1 \cdot 1x^7 + 3^3 \cdot 2x^9 + 3^2 \cdot 2x^{10}$
$p = 3$



Dumas tétele

Tétel (Dumas, 1906).

Tetszőleges $f, g \in \mathbb{Z}[x]$ polinomok esetén $f \cdot g$ Newton-poligonja megkapható az f és g Newton-poligonját alkotó szakaszok összeillesztésével.

A bizonyítás elolvasható Sarró Mihály *Polinomok Newton-poligonjai* című szakdolgozatában (SZTE Bolyai Intézet, 2015).

A Schönemann–Eisenstein-tétel triviális következménye a Dumas-tételnek: az ottani oszthatósági feltételek azt jelentik, hogy a Newton-poligon egyetlen szakaszból áll, így nem rakható össze kisebb darabokból.