

(Diskret matte D, ht13: F27, må 2 dec 2013)

Föreläsningen ägnades åt exempel och utvecklingar kring det vi gjort på si-stone, bl.a. följande.

En kropp med 9 element

Vi såg explicit att två ”olika” kroppar av ordning $9 = 3^2$ var isomorfa (det finns ju precis en kropp av ordning p^r för varje primtal p och $r = 1, 2, \dots$), $\mathbb{Z}_3[x]/(x^2 + x + 2) \approx \mathbb{Z}_3[x]/(x^2 + 1)$. Både $x^2 + x + 2$ och $x^2 + 1$ är irreducibla i $\mathbb{Z}_3[x]$, men bara $x^2 + x + 2$ är primitivt irreducibelt.

Ett tärningsproblem med **genererande funktion**

Vi frågade oss, kan man finna sannolikheter $p_1, p_2, \dots, p_6$ och $q_1, \dots, q_6$ för de olika utfallen för två tärningar så att varje summa $2, 3, \dots, 12$ av deras utfall har samma sannolikhet ($\frac{1}{11}$ var)?

Med $p(x) = p_1 + p_2x + p_3x^2 + \dots + p_6x^5$ och $q(x) = q_1 + q_2x + \dots + q_6x^5$ (genererande funktioner) betyder det att man skulle ha

$$p(x)q(x) = \frac{1}{11}(1 + x + x^2 + \dots + x^{10}).$$

Men $1 + x + x^2 + \dots + x^{10} = \frac{x^{11}-1}{x-1}$ som saknar reella nollställen, medan $p(x)$ och $q(x)$ har minst ett reellt nollställe var (polynom av udda grad). Så **nej**, sådana sannolikheter finns inte.

Vi har tidigare visat att om $f(x) \in \mathbb{Z}[x]$ och $f(x)$ är reducibelt i $\mathbb{Q}[x]$, så är $f(x)$ också reducibelt i $\mathbb{Z}[x]$.

Det betyder att vi kan känna igen irreducibla polynom i $\mathbb{Q}[x]$ om vi kan känna igen dem i $\mathbb{Z}[x]$ (genom att undersöka $\alpha \cdot f(x)$ för lämpligt rationellt tal α).

Eisensteins kriterium: Om $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x]$ och p är ett primtal sådana att $p \mid a_i$ för $i = 0, 1, \dots, n-1$, $p \nmid a_n$ och $p^2 \nmid a_0$, så är $f(x)$ irreducibelt i $\mathbb{Q}[x]$.

(På föreläsningen sades felaktigt att $f(x)$ måste vara irreducibelt i $\mathbb{Z}[x]$. Av beviset följer att förutsättningarna bara ger att om $f(x) = g(x)h(x)$ med $g(x), h(x) \in \mathbb{Z}[x]$, måste en av $g(x)$ och $h(x)$ vara konstant (och därmed inverterbart i $\mathbb{Q}[x]$, men inte säkert i $\mathbb{Z}[x]$).

Bl.a. såg vi att $x^p + x^{p-1} + \dots + x + 1$, p primtal, är irreducibla i $\mathbb{Q}[x]$ (och speciellt inte har några rationella nollställen)..