(Diskret matte D, ht16: F27, ti 29 nov 2016)

Föreläsningen ägnades åt exempel och utvikningar kring det vi gjort på sistone, 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 av dem är bara x^2+x+2 primitivt irreducibelt.

Ett tärningsproblem med **genererande funktion**

Vi frågade oss, kan man finna sannolikheter p_1, p_2, …, p_6 och q_1, …, q_6 för de olika utfallen för två tärningar så att varje summa 2, 3, …, 12 av deras utfall har samma sannolikhet ($\frac{1}{11}$ var)?
Med $p(x) = p_1 + p_2x + p_3x^2 + \ldots + p_6x^5$ och $q(x) = q_1 + q_2x + \ldots + q_6x^5$ (genererande funktioner) betyder det att man skulle ha

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

Men $1 + x + x^2 + \cdots + x^{10} = \frac{x^{11}-1}{x-1}$ saknar reella nollställen, så det är en produkt av 5 (reellt) irreducibla andragradspolynom och kan inte delas upp i $p(x)$ och $q(x)$ ($p(x)$ 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 $\mathbb{Z}[x]$. Så om ett polynom är irreducibelt i $\mathbb{Z}[x]$, så är det irreducibelt i $\mathbb{Q}[x]$.
Följande ger en metod att finna irreducibla polynom av godtycklig grad i $\mathbb{Q}[x]$.

Eisensteins kriterium: Om $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Z}[x]$ och p är ett primtal sådant att $p \mid a_i$ för $i = 0,\ 1,\ \ldots, n-1,\ p \nmid a_n$ och $p^2 \nmid a_0$, så är $f(x)$ irreducibelt i $\mathbb{Q}[x]$.
(Det betyder inte 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 $x^p + x^{p-1} + \ldots + x + 1$, p primtal, är irreducibla i $\mathbb{Q}[x]$ (och speciellt inte har några rationella nollställen).

(Ett exempel med) en rolig **algoritm för att faktorisera polynom i $\mathbb{Z}_2[x]$**.
Om $f(x) \in \mathbb{Z}_2[x]$ innehåller en multipel icke-trivial faktor har ekvationen $t^2 = 0$ en lösning $t \neq 0$ i $\mathbb{Z}_2[x]/(f(x))$ med samma faktor färre gånger. $\mathrm{sgd}(t, f(x))$ ger en faktor i $f(x)$ (jfr $2 \in \mathbb{Z}_4$ med $2^2 = 0$, $4 = 2 \cdot 2$).
Om $f(x)$ kan faktoriseras i relativt prima faktorer, $f(x) = g(x)h(x)$, finns enligt kinesiska restsatsen(!) lösningar $t \in \mathbb{Z}_2[x]/(f(x))$ till $t^2 = t$ som uppfyller $t \equiv 0 \pmod{g(x)}$, $t \equiv 1 \pmod{h(x)}$ eller tvärtom. $\mathrm{sgd}(t, f(x))$ ger åter en faktor i $f(x)$ (jfr $4, 3 \in \mathbb{Z}_6$ med $4^2 = 4$, $\mathrm{sgd}(4,6) = 2$; $3^2 = 3$, $\mathrm{sgd}(3,6) = 3$).
Algoritmen är snabb eftersom $t \mapsto t^2$ är **linjär** i $\mathbb{Z}_2[x]/(f(x))$.