Polynomier med sælsomme egenskaber modulo p

Bo Vagner Hansen

Reduceres koefficienterne i et normeret heltalspolynomium modulo et primtal, opstår et nyt polynomium over restklasseringen. Både ringen af polynomier med heltalskoefficienter og ringen af polynomier med koefficienter i $\mathbb{Z}/p$ har, ligesom de hele tal, entydig primfaktorisering, og primelementerne er netop de irreducible polynomier. Det er ofte nyttigt at kunne bestemme sådanne primfaktoriseringer, eller i første omgang blot afgøre, om polynomiet er irreducibelt, eller tillader yderligere faktorisering, samt hvilke typer af faktoriseringer der i givet fald kan forekomme. Artiklen undersøger hvad vi kan sige om faktoriseringen af det reducerede polynomium ud fra egenskaber ved det oprindelige polynomium. Specifikt skal vi se, at Galoisgruppen for polynomiet kan fortælle os en del om, hvorledes det reducerede polynomium faktoriserer, og vi giver derfor en ikke-alt-for-teknisk introduktion til Galoisgrupper. Undervejs støder vi på flere spøjse og overraskende resultater, og vi bliver blandt andet i stand til at karakterisere primtallene ud fra eksistensen af polynomier med særlige egenskaber.

Reduktion modulo p

Vi betragter gennemgående i artiklen et normeret polynomium $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ med koefficienter i ringen $\mathbb{Z}$ og grad $n \geq 1$. For et primtal p haves en kanonisk homomorfi $\varphi\colon \mathbb{Z} \to \mathbb{F}_p$, der afbilder et helt tal i den tilsvarende restklasse modulo p (her og nedenfor betegner $\mathbb{F}_p$ restklasseringen $\mathbb{Z}/p$, der som bekendt udgør et legeme). Billedet af $b \in \mathbb{Z}$ under φ betegnes $\overline{b}$. Denne afbildning inducerer en homomorfi $\Phi\colon \mathbb{Z}[x] \to \mathbb{F}_p[x]$ mellem

polynomiumsringene ved at erstatte koefficienterne til $f \in \mathbb{Z}[x]$ med deres restklasser modulo p. Lad os betegne billedet af f under Φ med $\overline{f}$. Vi skal i det efterfølgende interessere os for, hvorledes polynomiet $\overline{f}$ faktoriserer i $\mathbb{F}_p[x]$.

Et normeret polynomium kaldes som bekendt irreducibelt, hvis det ikke kan skrives som et produkt af to polynomier med positiv grad. Hvis der for et polynomium f gælder, at $\overline{f}$ er irreducibelt i $\mathbb{F}_p[x]$, så følger det automatisk, at f er irreducibelt i $\mathbb{Z}[x]$. Alternativt ville vi nemlig have en ikke-triviel faktorisering $f(x) = f_1(x)f_2(x)$, hvilket under homomorfien Φ ville give en faktorisering $\Phi(f_1)\Phi(f_2)$ af $\overline{f} = \Phi(f)$, i modstrid med, at $\overline{f}$ er irreducibelt. Det er altså tilstrækkeligt at finde et primtal p, for hvilket $\overline{f}$ er irreducibelt i $\mathbb{F}_p[x]$, for at vise, at f er irreducibelt.

I almindelighed gælder ikke, at $\overline{f}$ også vil være irreducibelt, hvis blot f er det. Vi kan nemlig finde et primtal p og en rod $\overline{b} \in \mathbb{F}_p$ for $\overline{f}$ som følger: Da f er et polynomium, kan f kun antage værdierne ± 1 endeligt mange gange. Der findes altså $b \in \mathbb{Z}$, så $f(b)$ har en primdivisor p, og dermed er $f(b) \equiv 0 \pmod{p}$, eller med andre ord, $\overline{b}$ er rod i $\overline{f} \in \mathbb{F}_p[x]$. Faktisk kan vi altid finde uendeligt mange primtal p, så $\overline{f}$ har en rod i $\mathbb{F}_p$. Antag nemlig induktivt, at $\overline{f}$ har en rod modulo $p_1, \ldots, p_k$. Sæt $d = p_1 \cdots p_k$ og betragt

$$f(da_n x) = a_n(a_n^{n-1}d^n x^n + a_1 a_n^{n-2} d^{n-1} x^{n-1} + \cdots + a_{n-1}dx + 1)$$

Betegn med udtrykket i parentesen med $\hat{f}(x)$. Som før indses, at der findes $c \in \mathbb{Z}$, så $\hat{f}(c)$ har en primdivisor p. Dermed gælder

$$f(da_n c) \equiv \hat{f}(c) \equiv 0 \pmod{p} \quad \text{og} \quad \hat{f}(c) \equiv 1 \pmod{d}\ .$$

Specielt er p ikke divisor i d, så vi har fundet et primtal, som ikke allerede var på vores liste, og hvor $\overline{f}$ har en rod.

Det følger af Frobenius' Densitetssætning nedenfor, at der sågar findes uendeligt mange primtal p, så $\overline{f}$ har alle sine n rødder i $\mathbb{F}_p$.

Vi har altså set, at selvom f er irreducibelt, findes uendeligt mange primtal p, så $\overline{f}$ har en rod i $\mathbb{F}_p$, og specielt kan $\overline{f}$ ikke være irreducibelt, medmindre f er et førstegradspolynomium. Man kunne så forvente, at $\overline{f}$ i det mindste vil være irreducibelt for en delmængde af primtallene, men selv dette viser sig ikke at holde stik. Vi skal således i det følgende bl.a. vise, at polynomiet $g(x) = x^4 + 1$ er irreducibelt i $\mathbb{Z}[x]$, men reducibelt modulo ethvert primtal. Første del kan vi indse allerede nu, f.eks. ved at bruge Eisensteins kriterium på $g(x+1)$, eller ved direkte at verificere, at ingen ikke-trivielle faktoriseringer er mulige. Beviset for anden del beror på en sætning af Dedekind, samt kendskab til Galoisgruppen for polynomiet g. Herfor en kort introduktion til begrebet Galoisgrupper.

Galoisgrupper

Vi betragter fortsat et polynomium f af grad n. Som følge af Algebraens Fundamentalsætning har f nøjagtig n rødder $u_1, \ldots, u_n$ indenfor de komplekse tal, talt med multiplicitet. Vi skal i det følgende antage, at alle rødderne er simple (dvs. de er alle forskellige). Vi associerer en gruppe G til polynomiet f, bestående af de permutationer af rødderne u_i, der bevarer de indbyrdes rationale relationer mellem rødderne: Hvis rødderne opfylder en relation $\psi(u_1, \ldots, u_n) = 0$ for et polynomium $\psi \in \mathbb{Q}[x_1, \ldots, x_n]$ i n variable, da skal de permuterede rødder også opfylde relationen. For $\sigma \in G$ skal der altså gælde

$$\psi(\sigma(u_1), \ldots, \sigma(u_n)) = 0 \ .$$

Ved at identificere en rod u_i med dens indeks i, kan vi opfatte G som en undergruppe i den symmetriske gruppe S_n. Permutationen der ombytter rødderne u_1 og u_2 og fikserer de øvrige, bliver således repræsenteret ved transpositionen (12), osv.. Det ses straks, at identitetsafbildningen er i G, at kompositionen af to elementer fra G igen er i G, og hvis $\sigma \in G$ er σ^{-1} en potens af σ, eftersom S_n er en endelig gruppe, og dermed er $\sigma^{-1} \in G$. Altså er G vitterligt en gruppe. Gruppen G kaldes Galoisgruppen for polynomiet f.

Lad os bestemme Galoisgruppen for $g(x) = x^4+1$. Rødderne i g er de primitive 8. enhedsrødder: $v_1 = e^{\pi i/4}, v_2 = e^{3\pi i/4}, v_3 = e^{5\pi i/4}$ og $v_4 = e^{7\pi i/4}$. Bemærk, at der er oplagte rationale relationer mellem rødderne. Det er således muligt at udtrykke samtlige rødder ved hjælp af blot den ene. F.eks. har vi $v_2 = v_1^3$, $v_3 = v_1^5$ og $v_4 = v_1^7$. Dette sætter begrænsninger på de mulige permutationer i G. Betragter vi f.eks. en permutation σ, der sender v_1 til v_2, følger det, da σ skal bevare relationerne mellem rødderne, at $\sigma(v_2) = \sigma(v_1)^3$ og heraf $\sigma(v_2) = v_1^9 = v_1$. Tilsvarende finder vi $\sigma(v_3) = v_1^{15} = v_4$ og $\sigma(v_4) = v_1^{21} = v_3$. Læseren kan videre overbevise sig om, at hvis vi betragter permutationer τ og μ, der sender v_1 til v_3 resp. v_4, følger det, at $\tau(v_2) = v_4, \tau(v_3) = v_1, \tau(v_4) = v_2$ og $\mu(v_2) = v_3, \mu(v_3) = v_2, \mu(v_4) = v_1$. I alle tilfælde er permutationen altså fuldstændig fastlagt ved værdien i v_1. Der er således kun 3 mulige permutationer af rødderne i dette tilfælde, udover den trivielle permutation (identiteten). Samtidig er det klart, at disse permutationer bevarer enhver relation mellem rødderne: Hvis vi har en relation

$$\psi(v_1, v_2, v_3, v_4) = \psi(v_1, v_1^3, v_1^5, v_1^7) = 0 \ , \qquad (*)$$

betyder det nemlig, at v_1 er rod i et polynomium $\theta \in \mathbb{Q}[x]$. Da g er irreducibelt, er $x^4 + 1$ det normerede polynomium i $\mathbb{Q}[x]$ af

lavest positiv grad, der har $v_1 = e^{i\pi/4}$ som rod. Sætningen om division med rest giver

$$\theta(x) = (x^4 + 1)q(x) + r(x) \ ,$$

for polynomier r, q hvor $\text{grad}(r) < 4$. Da

$$0 = \theta(v_1) = (v_1^4 + 1)q(v_1) + r(v_1) = r(v_1)$$

følger det, at v_1 er rod i $r(x)$ og dermed, at r må være nulpolynomiet. Af fremstillingen $\theta(x) = (x^4 + 1)q(x)$ ses derfor, at også v_2, v_3, v_4 er rødder i θ. Dermed vil relationen $(*)$ også være opfyldt, hvis v_1 erstattes af v_2, v_3 eller v_4. Vi kan således konkludere, at Galoisgruppen G for g består af fire elementer, hvoraf de tre har orden 2, og G er således isomorf med Kleins Vierergruppe. I cykelnotation kan vi skrive

$$G = \{\text{id}, (12)(34), (13)(24), (14)(23)\} \ .$$

Klassisk benyttes Galoisgruppen for et polynomium til at afgøre, hvornår det er muligt at 'finde en formel' for rødderne i polynomiet. Det berømte resultat, at det generelle polynomium af grad større end eller lig fem ikke kan løses ved roduddragning, og som normalt tilskrives Abel og Ruffini, kan således henføres til egenskaber ved den symmetriske gruppe S_n for $n \geq 5$. Galois var den første til at relatere løsbarheden af polynomiumsligninger til egenskaber ved den tilhørende permutationsgruppe på rødderne. De dybsindige iagttagelser, som han herved gjorde, har haft vidtrækkende konsekvenser for matematikkens udvikling sidenhen.

Et vilkårligt polynomium har en naturlig tilbøjelighed til at have en stor Galoisgruppe G, dvs. indeks $[S_n : G]$ er lille (se [4] for et præcist udsagn). Statistisk set har de fleste polynomier

derfor den fulde symmetriske gruppe som Galoisgruppe. En lille Galoisgruppe er således tegn på en form for anomali eller asymmetri i polynomiet, der giver det nogle særlige egenskaber, såsom muligheden for at finde formler for rødderne i polynomiet, eller begrænsede faktoriseringsmuligheder modulo et primtal. Vi skal nu, som lovet, se nærmere på nogle af disse afvigere.

En sætning af Dedekind

Vi betragter som nævnt et heltalspolynomium f med lutter simple rødder. Sætningen vi skal formulere forudsætter endvidere, at det koefficientvist reducerede polynomium $\overline{f}$ også har lutter simple rødder. Heldigvis er det ligetil at sikre dette ud fra egenskaber ved f. Hertil har vi brug for diskriminanten. Hvis f har rødder $u_1, \ldots, u_n$ defineres diskriminanten som

$$\operatorname{disk}(f) = \prod_{1 \le i < j \le n} (u_j - u_i)^2 \ .$$

Diskriminanten for $\overline{f}$ er det tilsvarende produkt af kvadratet på differenserne mellem de n rødder i $\overline{f}$ (i et passende udvidelseslegeme). Af definitionen fremgår umiddelbart, at et polynomium har multiple rødder, hvis og kun hvis diskriminanten er nul.

Det er muligt at udtrykke diskriminanten for f alene ved summer og produkter af koefficienterne til f. Da reduktion modulo p er en ringhomomorfi, fremgår heraf formlen

$$\operatorname{disk}(\overline{f}) = \overline{\operatorname{disk}(f)} \ .$$

Heraf ses, at $\overline{f} \in \mathbb{F}_p[x]$ har multiple rødder, hvis og kun hvis diskriminanten for f er delelig med p. Ved at betragte primtal hvor $p \nmid \operatorname{disk}(f)$, sikrer vi os således, at både f og $\overline{f}$ har lutter simple rødder.

Sætning 1 (Dedekind) *Lad f være et normeret heltalspolynomium og p et primtal så $p \nmid \mathrm{disk}(f)$. Hvis det koefficientvist reducerede polynomium $\overline{f} \in \mathbb{F}_p[x]$ har (den entydige) faktorisering $\tilde{f}_1 \cdots \tilde{f}_r$, med hvert $\tilde{f}_i$ irreducibelt af grad l_i, da indeholder Galoisgruppen for f en permutation som er et produkt af disjunkte cykler $\gamma_1 \cdots \gamma_r$, hvor γ_i har længde $l_i = \mathrm{grad}(\tilde{f}_i)$ og $l_1 + \cdots + l_r = \mathrm{grad}(f)$.*

Se [2] for nærmere detaljer.

Specielt interesserer vi os for sætningen i den kontraponerede form: Hvis Galoisgruppen for f ikke indeholder nogen permutationer med en bestemt cykeltype $l_1 \ldots l_r$, da kan $\overline{f}$ ikke faktorisere som et produkt af irreducible polynomier med graderne $l_1, \ldots, l_r$.

Med ovenstående resultat i baghånden er tiden hermed kommet, hvor vi kan demonstrere vores forehavende.

Sætning 2 *Polynomiet $g(x) = x^4 + 1$ er irreducibelt i $\mathbb{Z}[x]$, men reducibelt modulo ethvert primtal.*

Bevis. Som vi har set, har polynomiet $g(x) = x^4 + 1$ Galoisgruppen

$$G = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \ .$$

Specielt indeholder G ikke nogen 4-cykel. For et primtal p så $p \nmid \mathrm{disk}(g)$, følger det af Dedekinds sætning, at fjerdegradspolynomiet $\overline{g}$ ikke kan være et produkt af en enkelt irreducibel fjerdegradsfaktor, eller med andre ord, at $\overline{g}$ er reducibelt.

Indsættes rødderne for g i definitionen på diskriminanten ovenfor, kan man beregne $\mathrm{disk}(g) = 2^8$. Vi mangler altså blot at checke primtallet $p = 2$, og modulo 2 finder vi $x^4 + 1 \equiv (x+1)^4 \pmod 2$, altså er $\overline{g}$ også reducibelt modulo 2. □

Endvidere står det klart, ud fra formen på permutationerne i G, at de eneste mulige faktoriseringer af $\overline{g}$, er som et produkt af to andengradsfaktorer eller fire førstegradsfaktorer. Da

$$\begin{aligned} x^4+1 &\equiv (x^2+2)(x^2+3) && \pmod 5\ , \\ x^4+1 &\equiv (x+2)(x+8)(x+9)(x+15) && \pmod{17} \end{aligned}$$

ses, at begge muligheder forekommer for primtal p, der ikke går op i diskriminanten. Som vi skal se nedenfor, er dette ikke nogen tilfældighed.

Lad os snuppe endnu et eksempel. Polynomiet

$$h(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$$

har rødderne $w_k = e^{2\pi ik/11} + e^{-2\pi ik/11} = 2\cos(2\pi k/11)$ for $k = 1, \ldots, 5$. Som før eksisterer der relationer mellem rødderne, idet vi har $w_{k+1} = w_k w_1 - w_{k-1}$. Læseren kan selv overbevise sig om, at en permutation σ i Galoisgruppen H for h er entydigt fastlagt ved værdien i w_1. Vælges f.eks. $\sigma(w_1) = w_2$, følger det automatisk, at $\sigma(w_2) = w_4$, $\sigma(w_4) = w_3$, $\sigma(w_3) = w_5$ og $\sigma(w_5) = w_1$. Dermed bliver $\sigma = (12435)$ en 5-cykel, og potenserne af σ vil generere hele Galoisgruppen, altså har vi $H = \langle\sigma\rangle$ og H er cyklisk af orden 5.

Vi er således i en position, hvor vi kan anvende Dedekinds sætning til at udtale os om de mulige faktoriseringer af $\overline{h}$. Hvis $p \nmid \operatorname{disk}(h)$ er der som før kun to muligheder for faktoriseringen af $\overline{h}$. Enten svarer p til den trivielle permutation i Galoisgruppen, og så spalter $\overline{h}$ til bunds som et produkt af fem førstegradsfaktorer, eller også svarer p til en 5-cykel, og da vil $\overline{h}$ være irreducibelt. Beregner man diskriminanten, finder man $\operatorname{disk}(h) = 11^4$ (det bliver en længere udregning). For $p = 11$ er det ikke svært at indse, under brug af binomialformlen, at $h(x) \equiv (x-2)^5 \pmod{11}$. Vi

kan heraf samlet konkludere, at h har den usædvanlige egenskab, at for ethvert primtal p er $\overline{h} \in \mathbb{F}_p[x]$ enten irreducibelt eller et produkt af fem førstegradsfaktorer.

Ovenstående resultat kan anvendes til let at afgøre, om $\overline{h}$ er irreducibelt. Der gælder nemlig for $p \neq 11$, at $\overline{h}$ er reducibelt hvis og kun hvis $\overline{h}$ har alle sine fem rødder i $\mathbb{F}_p$. Da $\mathbb{F}_2$ og $\mathbb{F}_3$ indeholder færre end fem elementer, kan $\overline{h}$ ikke have fem forskellige rødder modulo 2 eller 3, så i disse tilfælde bliver $\overline{h}$ automatisk irreducibelt. Videre ses med et halvt øje, at $\overline{h}$ er irreducibelt modulo 5 og 7. I første tilfælde er det nemlig nok at indse, at 0 ikke er rod, og i andet tilfælde skal det endvidere checkes, at f.eks. ± 1 ikke er rødder. Det første tilfælde hvor $\overline{h}$ har fem forskellige rødder i $\mathbb{F}_p$, indtræffer for $p = 23$.

Frobenius' Densitetssætning

Vi har set, at de irreducible faktoriseringer af $\overline{f}$, medfører eksistensen af hertil svarende permutationer i Galoisgruppen for f. Frobenius' Densitetssætning garanterer omvendt, at der til givne permutationer i Galoisgruppen, altid findes uendeligt mange primtal, så $\overline{f}$ har en faktorisering svarende til cykeltypen for permutationen. Da enhver gruppe indeholder den trivielle permutation, indebærer dette specielt, at der for et vilkårligt polynomium f, altid findes uendeligt mange primtal, så $\overline{f}$ spalter til bunds i førstegradsfaktorer.

Sætning 3 (Frobenius) *Lad f være et normeret heltalspolynomium uden multiple rødder. Antag at Galoisgruppen for f indeholder en permutation, der er et produkt af disjunkte cykler $\gamma_1 \cdots \gamma_r$, hvor γ_k er en cykel af længde l_k for $k = 1, \ldots, r$. Da findes uendeligt mange primtal p, så $\overline{f} \in \mathbb{F}_p[x]$ faktoriserer som et produkt af irre-*

ducible faktorer med graderne $l_1, \ldots, l_r$. Ydermere er tætheden af sådanne primtal givet ved kvotienten $N/|G|$, hvor N er antallet af permutationer i G med cykeltype $\gamma_1 \cdots \gamma_r$.

Med tætheden mener vi: Hvis P_n er antallet af primtal mindre end n og Q_n er antallet af primtal mindre end n der giver anledning til en faktorisering svarende til permutationen $\gamma_1 \cdots \gamma_r$, da er tætheden givet ved

$$\lim_{n\to\infty} \frac{Q_n}{P_n} = \frac{N}{|G|} \ .$$

Vi ser således, at det ikke var noget tilfælde, da vi ovenfor kunne finde primtal p, så polynomierne $g(x)$ og $h(x)$ havde en faktorisering svarende til hver type permutation i Galoisgruppen. Yderligere kan vi ud fra sætningen bestemme, hvor ofte hver type faktorisering gennemsnitligt vil forekomme. For tilfældet $g(x) = x^4 + 1$ vil således i gennemsnit hvert fjerde primtal resultere i en faktorisering af $\overline{g}$ som et produkt af fire førstegradsfaktorer, mens de øvrige tre fjerdedele af primtallene vil give en faktorisering af $\overline{g}$ som et produkt af to andengradsfaktorer. Tilsvarende gælder for $h(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$, at for fire femtedele af primtallene vil $\overline{h}$ være irreducibelt, mens $\overline{h}$ for de resterende primtal p, vil have alle sine rødder i $\mathbb{F}_p$.

Det er naturligt at spørge, for hvilke primtal de forskellige faktoriseringer indtræffer. For tilfældet $g(x) = x^4 + 1$ kan man vise, vha. basale resultater om kvadratisk reciprocitet, at $\overline{g}$ faktoriserer som et produkt af fire førstegradsfaktorer når $p \equiv 1 \pmod 8$, og som et produkt af to andengradsfaktorer når $p \not\equiv 1 \pmod 8$. Dette resultat indebærer jævnfør ovenstående, at tætheden af primtallene, der er kongruente med 1 modulo 8, er 1/4. Som tilføjelse hertil kan nævnes, at dette er i overensstemmelse med Dirichlets sætning om primtal i aritmetisk progression, der netop

angiver tætheden af primtal kongruent med 1 modulo 8 til at være $1/\varphi(8) = 1/4$ (φ er Eulerfunktionen). For nærmere detaljer om relationen mellem sætningerne af Dirichlet og Frobenius, samt et bevis for Chebotarëv's Densitetssætning, som generaliserer dem begge, se [3].

En karakterisering af primtallene

Vi har set, at polynomiet x^4+1 er irreducibelt i $\mathbb{Z}[x]$, men reducibelt modulo ethvert primtal p. Med hjælp fra Frobenius' Densitetssætning kan vi nu vise, at eksistensen af et polynomium med denne egenskab ikke er helt triviel, idet et polynomium med primtalsgrad ikke kan have selvsamme egenskab.

Sætning 4 *Lad q være et primtal og $f \in \mathbb{Z}[x]$ et normeret irreducibelt polynomium af grad q. Da findes uendeligt mange primtal p, for hvilke $\overline{f} \in \mathbb{F}_p[x]$ er irreducibelt.*

Bevis. Det er velkendt, at et irreducibelt polynomium over $\mathbb{Z}$ ikke kan have multiple rødder. Ideen er derfor at vise, at Galoisgruppen G for f indeholder en q-cykel, thi da følger eksistensen af primtallene p fra Frobenius' Densitetssætning. Det er et generelt resultat, at Galoisgruppen for et irreducibelt polynomium endvidere bliver transitiv, altså at der til to vilkårlige rødder i f, findes en permutation i G, der sender den ene rod til den anden. Betragt derfor undergruppen

$$G^1 = \{\sigma \in G \mid \sigma(1) = 1\} \ .$$

To permutationer $\sigma, \tau \in G$ er ækvivalente modulo G^1 hvis og kun hvis $\sigma^{-1}\tau$ tilhører G^1, som sker hvis og kun hvis $\sigma(1) = \tau(1)$. Da G er transitiv forekommer samtlige værdier $1, \ldots, q$ som værdi i

1 for permutationer i G. Der er altså q sideklasser modulo G^1. Lagranges Indekssætning giver derfor, at $[G : G^1] = q$ er divisor i $|G|$. Da G endvidere er en undergruppe i S_q, der har orden $q!$, må $|G| = qm$ hvor q og m er primiske. Det følger nu direkte af Sylows Første Sætning, at G har en undergruppe af orden q, og specielt altså indeholder en q-cykel. □

Specielt er fire den laveste grad, for hvilken noget irreducibelt polynomium kan være reducibelt modulo ethvert primtal. Videre kan man spørge sig selv, hvorvidt der findes et sjettegradspolynomium med samme egenskab, eller mere generelt et polynomium af grad n for et vilkårligt sammensat tal n. Det viser sig faktisk, at primtalsgraden er den eneste forhindring for, at polynomiet kan have den omtalte egenskab, og der findes således irreducible polynomier af enhver sammensat grad, der er reducible modulo ethvert primtal. Beviset herfor er dog ikke trivielt, se f.eks. [1]. Dette giver os følgende karakterisering af primtallene:

Sætning 5 *Et naturligt tal $n \neq 1$ er et primtal hvis og kun hvis der **ikke** findes et irreducibelt polynomium f af grad n, så $\overline{f}$ er reducibelt modulo ethvert primtal p.*

Selvom der altså findes irreducible polynomier af enhver sammensat grad, der er reducible modulo ethvert primtal, og selvom der altid findes uendeligt mange primtal, for hvilke et givent polynomium spalter til bunds i førstegradsfaktorer, er der alligevel en grænse for, hvor tosset et irreducibelt polynomium kan te sig modulo p. En elementær sætning af Burnside udsiger nemlig, at en transitiv undergruppe af S_n for $n \geq 2$ altid vil indeholde en permutation uden fikspunkter. Anvendt på Galoisgruppen for et irreducibelt polynomium f af grad mindst 2, følger det af Frobe-

nius' Densitetssætning, at der findes uendeligt mange primtal p, for hvilke $\overline{f}$ ikke har en rod i $\mathbb{F}_p$.

Afrunding

Læseren kan nu selv tage sin yndlingsgruppe og fundere over, hvilke sjove egenskaber et polynomium med denne gruppe som Galoisgruppe kan have. Som følge af Cayleys Sætning kan enhver endelig gruppe nemlig opfattes som en permutationsgruppe, idet en gruppe af orden n kan indlejres som en transitiv undergruppe i den symmetriske gruppe S_n. Desværre er det sjældent nogen let opgave at bestemme et polynomium med en given gruppe som Galoisgruppe, ja faktisk er det et endnu uløst problem, kendt som Galoisteoriens omvendingsproblem, at afgøre hvorvidt enhver endelig gruppe kan realiseres som Galoisgruppe for et polynomium med koefficienter i $\mathbb{Q}$ (eller ækvivalent hermed, for et normeret polynomium med heltalskoefficienter). Her 180 år efter Évariste Galois' død (i øvrigt i en alder af kun 20 år, som følge af sår tildraget i en duel!), fortsætter den eponyme matematiske disciplin således med at rejse ubesvarede spørgsmål, generere overraskende resultater og give inspiration til matematikere i alle aldre.

Galois skrev aftenen før den fatale duel: 'Der er endnu noget at eftervise. Jeg har ikke tid.' Heldigvis har mange sidenhen haft tid til at udvikle hans originale ideer, således at de tanker Galois oprindeligt satte i verden, i dag kan bibringe anvendelser langt ud over, hvad Galois selv kunne have forestillet sig.

Litteratur

[1] R. Guralnick, M. Schacher and J. Sonn, *Irreducible polynomials which are locally reducible everywhere*, Proceedings of the AMS Vol. 133 (2005), no. 11, p. 3171-3177.

[2] C. U. Jensen, *Matematik 4AL*, Matematisk Afdeling KU.

[3] P. Stevenhagen & H. W. Lenstra, *Chebotarëv and his density theorem*, The Mathematical Intelligencer Vol 18. No. 2, 1996.

[4] B. L. van der Waerden *Die Seltenheit der reduziblen Gleichungen und die Gleichungen mit Affekt*, Monatsh. Math. 43 (1936), 137-147.