Note 1

Tiden er inde til endnu en note. Denne gang handler det om irrationalitet af rødder af hele tal. Vi vil se at resultaterne fra TØ er en konsekvens af en meget generel sætning, som ofte kan være nyttig. Jeg vil derfor bede jer læse sætningen og dens bevis grundigt, og huske resultatet fra nu af og i al evighed. Efter denne sætning og udledningen af dens relation til TØ-opgaverne følger skriftlige besvarelser af de to fadølsopgaver. Jeg har i skrivende stund ikke modtaget nogen besvarelser, så det bliver formentlig en billig omgang for mig. Til sidst har jeg indsat en nogenlunde grundig besvarelse af en TØ-opgave fra 19/9-05 som vi ikke nåede.

Polynomier

Mange ting hører med til den almene dannelse; det resultat der præsenteres i dette afsnit er en af disse ting. Lad f være et polynomium, altså

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0. \tag{1}$$

Ofte er man interesseret i at finde rødder i polynomier. Hvis a_0 er 0 er $x = 0$ oplagt en rod i p.

Antag nu, at koefficienterne a_i alle er heltal. Vi taber ikke megen generalitet ved yderligere at antage, at a_n og a_0 er forskellige fra 0. Påstanden er nu følgende:

Lemma 1. *Hvis $x = \frac{p}{q}$ er en rationel rod i f, og $\frac{p}{q}$ er uforkortelig (altså* $\gcd(p,q) = 1$*), så er p divisor i a_0 og q er divisor i a_n.*

Nytten af denne påstand er følgende: *Der er kun endeligt mange potentielle rationelle rødder i et givet polynomium med heltallige koefficienter!* Med andre ord: Hvis man leder efter alle rødderne i et polynomium med heltallige koefficienter, kan man starte med at afprøve om nogen af de rationelle kandidater er rødder. Hvis man er heldig finder man en rod, og så kan man udføre polynomiers division og få et polynomium af grad en mindre.

Bevis for lemmaet. Vi antager altså at

$$a_n(\tfrac{p}{q})^n + \cdots + a_1\tfrac{p}{q} + a_0 = 0.$$

Ganger vi denne ligning igennem med q^n og flytter en smule om finder vi, at

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} = -a_0 q^n.$$

Bemærk at denne identitet kun involverer heltal. Man ser, at p er divisor i venstresiden, men det betyder at $p \mid a_0 q^n$. Da vi har antaget at p og q er indbyrdes primiske, må vi have at $p \mid a_0$.

På tilsvarende måde kan vi flytte lidt rundt på ledene og konstatere at

$$a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n = -a_n p^n.$$

Heraf aflæser man, at q er divisor i $a_n p^n$, og som før må dette betyde at q går op i a_n. $\square$

Et eksempel: Lad $f(x) = x^3 + x^2 - 13x + 3$. Det ovenstående fortæller, at de eneste mulige rationelle rødder er ± 1 og ± 3 (fordi tælleren skal være divisor i 3 og nævneren skal være divisor i 1). Ved at indsætte disse fire kandidater finder man at 3 er en rod. Ved hjælp af polynomiers division finder man så at f kan faktoriseres som $f(x) = (x-3)(x^2+4x-1)$. De øvrige rødder i f kan altså findes ved at løse andengradsligningen $x^2 + 4x - 1 = 0$, og det er en overkommelig opgave. Man finder to andre reelle rødder, nemlig $x = \frac{-4 \pm \sqrt{20}}{2} = -2 \pm \sqrt{5}$.

Prøv at overvej hvad I ville have gjort hvis I var blevet bedt om at bestemme samtlige rødder i polynomiet $x^3 + x^2 - 13x + 3$ uden at kende til ovenstående genvej. Jeg er ret sikker på, at I på et tidspunkt kommer i en eksamenssituation hvor I kan spare kostbare minutter ved at gætte en rod hurtigere end jeres nabo.

Som umiddelbar konsekvens har vi

Sætning 2. *Lad p være et primtal og $n \geq 2$ et heltal. Så er $\sqrt[n]{p}$ irrationel.*

Bevis. Betragt polynomiet $f(x) = x^n - p$. Ifølge Lemma 1 er de eneste mulige rationelle rødder i f tallene ± 1 og $\pm p$. Man indser let at ingen af udtrykkene

$$\begin{aligned} &1 - p \\ &(-1)^n - p \\ &p^n - p \\ &(-p)^n - p \end{aligned}$$

kan være lig 0, og derfor har f ingen rationelle rødder. Da $\sqrt[n]{p}$ er en rod må det betyde, at $\sqrt[n]{p}$ er irrationel. $\square$

Specielt konkluderer vi (for $n = p = 2$) at kvadratroden af 2 er et irrationelt tal. Det er heller ikke svært at vise:

Sætning 3. *Lad $m \in \mathbb{N}$ og $n \geq 2$. Hvis $\sqrt[n]{m}$ er rationel, så er det et heltal.*

Bevis. Lad $f(x) = x^n - m$. Pr. antagelse er $\sqrt[n]{m}$ et rationelt tal, så vi kan skrive det som uforkortelig brøk $\frac{p}{q}$. Men fra Lemma 1 har vi så, at $q = \pm 1$ så $\sqrt[n]{m}$ faktisk er et heltal. □

Med andre ord kan man aldrig tage et rationelt, ikke-heltal og opløfte det til en potens n og få et heltal. Løst sagt betyder Sætning 3, at langt de fleste n'te-rødder er irrationelle.

Fadøl

Skakbræt

Skakbrætsopgaven lød som følger: Betragt et sædvanligt 8×8-skakbræt, og lad der være givet en overdækning af brættet med 32 dominobrikker. Hver brik dækker altså netop to felter på skakbrættet. De vandrette brikker ligger enten som $\boxed{\text{H}|\text{S}}$ eller $\boxed{\text{S}|\text{H}}$; de dækker altså enten et hvidt felt eller et sort felt til venstre. Vis at der, uanset hvilken overdækning der er givet, vil være lige mange af de to typer brikker.

Besvarelse: Vi nummererer søjlerne i skakbrættet 1–8, og tildeler derefter hvert felt på brættet et tal som følger: Hvis feltet er hvidt får det søjlens tal, hvis det er sort får det minus søjlens tal:

1	2	3	4	5	6	7	8
1	-2	3	-4	5	-6	7	-8
-1	2	-3	4	-5	6	-7	8
1	-2	3	-4	5	-6	7	-8
-1	2	-3	4	-5	6	-7	8
1	-2	3	-4	5	-6	7	-8
-1	2	-3	4	-5	6	-7	8
1	-2	3	-4	5	-6	7	-8
-1	2	-3	4	-5	6	-7	8

Det er klart at summen af tallene på alle brættets felter er 0. Altså må dominobrikkerne tilsammen dække en sum på 0. Hver af de lodrette brikker dækker i alt 0. En vandret brik af typen $\boxed{\text{H}|\text{S}}$ dækker i alt $+1$, mens en vandret brik af typen $\boxed{\text{S}|\text{H}}$ i alt dækker -1. Da den totale sum skal være 0 må der være lige mange $+1$'er som -1'er, så der er altså lige mange af de to typer brikker.

Tværsum

Tværsumsopgaven lød i al sin enkelhed: Bestem tværsummen af tværsummen af tværsummen af 2005^{2005}, uden brug af lommeregner eller anden elektronik.

Besvarelse: Der skal bruges to ingredienser for at besvare denne opgave. Den ene er det fundamentale faktum som vi beviste til TØ, at et naturligt tal er kongruent med sin tværsum modulo 9. Den anden ingrediens vi skal bruge er, at tværsummen af et tal ikke kan være større end 9 gange antallet af cifre i tallet. Antallet af cifre i et naturligt tal N er $\lfloor \log_{10} N \rfloor + 1$, hvor $\lfloor x \rfloor$ betegner floor(x), altså det største heltal mindre end eller lig x (overvej dette!).

Vi har derfor at

$$\begin{aligned}\mathrm{ts}(2005^{2005}) &\leq 9 \cdot (\lfloor \log_{10} 2005^{2005} \rfloor + 1) \\ &= 9 \cdot (\lfloor 2005 \cdot \log_{10} 2005 \rfloor + 1) \\ &< 9 \cdot (2005 \cdot 4 + 1) \\ &= 56189.\end{aligned}$$

Men så er $\mathrm{ts}(\mathrm{ts}(2005^{2005})) \leq 9 \cdot 5 = 45$, da der jo højst er 5 cifre i $\mathrm{ts}(2005^{2005})$. Blandt tallene mindre end eller lig 45 er det 39 der har den største tværsum, nemlig 12. Vi konkluderer at $\mathrm{ts}(\mathrm{ts}(\mathrm{ts}(2005^{2005}))) \leq 12$.

Nu har vi ganske gode chancer for at bestemme tallet nøjagtigt, for hvis vi blot bestemmer kongruensklassen for tallet modulo 9 kan det jo være, at der kun er ét tal mindre end eller lig 12 som har denne kongruensklasse. Vi har at

$$\mathrm{ts}(\mathrm{ts}(\mathrm{ts}(2005^{2005}))) \equiv \mathrm{ts}(\mathrm{ts}(2005^{2005})) \equiv \mathrm{ts}(2005^{2005}) \equiv 2005^{2005} \pmod 9$$

ved gentagen anvendelse af modulo 9-factet. Samme fact fortæller endvidere at $2005 \equiv 7 \pmod 9$, så vi kan regne videre og få

$$2005^{2005} \equiv 7^{2005} \pmod 9$$

jf. regnereglerne for kongruenser. Et par hurtige udregninger viser at $7^2 = 49 \equiv 4 \pmod 9$ og $7^3 \equiv 7 \cdot 4 = 28 \equiv 1 \pmod 9$. Da $2005 \equiv 1 \pmod 3$ har vi at $2005 = 3 \cdot k + 1$, så vi får endelig at

$$7^{2005} = 7^{3k+1} = 7^{3^k} \cdot 7 \equiv 1^k \cdot 7 = 7 \pmod 9.$$

Konklusionen er, at vi leder efter et tal ≤ 12 som er kongruent med 7 modulo 9, og det eneste sådanne er naturligvis 7 selv.

Man kan bemærke, at det eneste der blev brugt om 2005 var at det er et tal som er kongruent med 7 modulo 9 (og dermed med 1 modulo 3, tænk!), og at det ikke er "for stort" således at de indledende vurderinger virker. Vi har derfor også fx at $\mathrm{ts}(\mathrm{ts}(\mathrm{ts}(4444^{4444}))) = 7$.

En lille udskrift fra en Mathematica-kørsel:

```
In[11]:= ts[n_] := Plus @@ IntegerDigits[n];
         {ts[2005^2005], ts[ts[2005^2005]], ts[ts[ts[2005^2005]]]}

Out[11]= {29779, 34, 7}

In[12]:= {ts[4444^4444], ts[ts[4444^4444]], ts[ts[ts[4444^4444]]]}

Out[12]= {72601, 16, 7}
```

En TØ-opgave

Vi nåede ikke Opgave 5 på Ugeseddel 4, men der er en del indsigt at hente i den opgave, så her er en besvarelse. Vi har givet to naturlige tal a og b sammen med deres primtalsfaktoriseringer

$$a = \prod_{i=1}^{N} p_i^{k_i} \qquad\qquad b = \prod_{i=1}^{N} p_i^{l_i}$$

hvor $\{p_1, p_2, \ldots, p_N\}$ er foreningsmængden af primdivisorerne i a og b (altså alle de primtal der skal bruges for at faktorisere a og b), og $k_i, l_i \in \mathbb{N} \cup \{0\}$. Vi har desuden navngivet p_i'erne sådan at $p_i \neq p_j$ når $i \neq j$ [hvis det samme primtal $p_i = p_j$ optrådte to steder i faktoriseringen af a, kunne vi blot erstatte $p_i^{k_i} p_j^{k_j}$ med $p_i^{k_i+k_j}$].

For hvert i mellem 1 og N lader vi nu m_i betegne den mindste af de to eksponenter k_i og l_i; altså $m_i = \min(k_i, l_i)$. Opgaven er at vise, at det tal c der fremkommer ved fastsættelsen

$$c = \prod_{i=1}^{N} p_i^{m_i}$$

er den største fælles divisor i a og b.

Bevis. Vi starter med at kontrollere, at c faktisk er en fælles divisor. Da $m_i \leq k_i$ for alle i, er $p_i^{k_i - m_i}$ et naturligt tal for alle $i = 1, \ldots, N$. Derfor er

$$\begin{aligned} a = \prod_{i=1}^{N} p_i^{k_i} &= \prod_{i=1}^{N} p_i^{m_i} p_i^{k_i - m_i} \\ &= \Big(\prod_{i=1}^{N} p_i^{m_i}\Big) \cdot \Big(\prod_{i=1}^{N} p_i^{k_i - m_i}\Big) = c \cdot \prod_{i=1}^{N} p_i^{k_i - m_i} \end{aligned}$$

så c er en divisor i a. På tilsvarende måde finder man, at c er en divisor i b.

Hvis p er et primtal som går op i $\gcd(a,b)$ må vi også have at p går op i a og b. Da alle de primtal der går op i a og b findes i mængden $\{p_1, p_2, \ldots, p_N\}$ har vi at p må være et af disse tal. Denne overvejelse viser, at de primtal der skal bruges til at faktorisere $\gcd(a,b)$ er at finde blandt $p_1, p_2, \ldots, p_N$, så vi kan skrive

$$\gcd(a,b) = \prod_{i=1}^{N} p_i^{g_i}$$

hvor $g_i \in \mathbb{N} \cup \{0\}$. Da c er en fælles divisor for a og b må c være en divisor i $\gcd(a,b)$, men det betyder at $m_i \leq g_i$ for alle i.

På den anden side: Da $\gcd(a,b)$ er en divisor i a og b, må $p_i^{g_i}$ også være en divisor i a og b for alle i. Men $p_i^{g_i}$ kan kun gå op i a hvis den i'te faktor i a, dvs. $p_i^{k_i}$ er stor nok; altså hvis $g_i \leq k_i$. På samme måde indser man at $g_i \leq l_i$. Men disse to uligheder medfører at $g_i \leq \min(k_i, l_i) = m_i$. Da således $g_i \leq m_i$ og $m_i \leq g_i$ for alle i har vi at $g_i = m_i$ for alle i, men det betyder præcis at $c = \gcd(a,b)$. □

Ekstraspørgsmålet, hvornår $\gcd(a,b)$ er lig med 1 kan man nu besvare i termer af primfaktoriseringerne af a og b: Tallet c er lig med 1 hvis og kun hvis alle eksponenterne m_i er lig 0; men dette sker hvis og kun hvis det for ethvert i gælder at mindst en af k_i og l_i er lig 0. Med andre ord, hvis og kun hvis der ikke er fælles primfaktorer i a og b.