Matematikken

bag løsningen af Enigma

Opgaver i permutationer og kombinatorik

© Erik Vestergaard
Haderslev, 2008.
Redigeret december 2015.
Redigering december 2016.

Enigma maskinens matematik

I denne note skal præsenteres lidt af den matematik, som er nødvendigt for at forstå, hvordan den polske matematiker Marian Rejewski i slutningen af 30'erne kunne bryde den tyske krypteringsmaskine *Enigma*. Frem for at præsentere det matematiske stof fiks og færdigt, er valget faldet på at udfærdige dokumentet med mange opgaver i håbet om, at det skal kunne tjene som en hjælp til for eksempel en større skriftlig opgave i gymnasiet, så eleven derved kan udvise større selvstændighed. Dokumentet er ment som en slags vejledning til at forstå følgende artikel, som kan downloades fra min hjemmeside:

Chris Christensen. *Polish Mathematicians Finding Patterns in Enigma Messages*. Mathematics Magazine (Mathematical Association of America), Vol 80, No. 4, Oct. 2007.

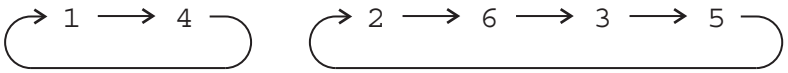
Hele idéen bag Enigma maskinen er, at den skal kunne bytte rundt på bogstaver på en indviklet måde, så det er svært at tolke, hvad der står. I den forbindelse får vi brug for begrebet en *permutation*.

Hvad er en permutation?

En permutation kan opfattes som en afbildning, hvor der byttes om på elementerne i en given mængde. Hvis mængden er $\{1,2,3,4,5,6\}$, så angiver for eksempel

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 2 & 3 \end{pmatrix}$$

den permutation, som sender $1 \to 4, 2 \to 6, 3 \to 5, 4 \to 1, 5 \to 2$ og $6 \to 3$. Man kan også se på, hvor billedelementerne afbildes hen. Herved fås en hel sekvens, hvor det altid ender med, at man på et tidspunkt kommer tilbage til udgangspunktet. Man kalder denne sekvens for en *cykel*. I dette tilfælde får vi en 2-cykel og en 4-cykel, som henviser til antallet af elementer i cyklerne.



Dette giver anledning til, at permutationen alternativt kan opskrives på *cykel-form*:

$$(14)(2635)$$

Cykelformen er ofte hurtigere at overskue: Billedelementet er blot det næste i rækken, med mindre elementet står til sidst i en cykel, i hvilket tilfælde billedelementet er det første i cyklen. Der er også den trivielle permutation, som ikke laver om på noget, og den kaldes derfor for *identiteten* og betegnes ofte med bogstavet *I*. På to-række-form og på cykelform ser identiteten således ud:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \quad \text{og} \quad (1)(2)(3)(4)(5)(6)$$

Man kan også *sammensætte* permutationer. Givet to permutationer A og B:

$$A = (124)(365)$$
$$B = (16)(235)(4)$$

Sammensætningen AB fås på følgende måde: A afbilder 1 i 2, B afbilder 2 i 3, altså afbildes 1 i 3 ved permutationen AB. Sådan fortsættes, og man får alt i alt:

$$AB = (13)(246)(5)$$

Det er vigtigt at pointere, at jeg her af overskuelighedsgrunde vælger at følge Chris Christensen og Marian Rejewski i deres valg i at lade sammensætninger af permutationer foregå fra venstre mod højre, dvs. hvis der skrives AB, så skal A anvendes først og B derefter. Der synes ikke at være fælles fodslag for, hvordan det gøres i matematik i dag: Nogle foretrækker at sammensætninger skal foretages fra højre mod venstre, ligesom man gør med sammensætninger af funktioner eller matricer.

Det anføres uden bevis, at den såkaldte *associative lov* gælder for alle permutationer, dvs. at $(AB)C = A(BC)$. Man kan altså sætte parenteser, som man vil!

Opgave 1

Man siger, at den *kommutative regel* gælder, såfremt man kan bytte rundt på rækkefølgen af elementer. Vis at den kommutative regel *ikke* gælder for sammensætning af permutationer, dvs. vis med et modeksempel, at der ikke altid gælder $AB = BA$.

Den *inverse* permutation til en permutation A er en permutation A^{-1}, som opfylder:

(1) $$A^{-1}A = I \quad \text{og} \quad AA^{-1} = I$$

Opgave 2

Bestem de inverse elementer til

a) $A = (162)(3)(45)$

b) $B = (1)(2465)(3)$

c) $C = (123456)$

Opgave 3

a) Hvad kan siges om cykellængderne for den inverse permutation i forhold til cykellængderne for den oprindelige permutation?

b) Vis, at det inverse element til AB er $B^{-1}A^{-1}$, dvs. vis, at $(AB)^{-1} = B^{-1}A^{-1}$ ved brug af definitionen (1) ovenfor.

Når man har en permutation A, og en anden permutation T, så kaldes $T^{-1}AT$ for et *konjugeret* element til A. Vi skal nu se på en vigtig egenskab for konjugerede elementer, som Marian Rejewski udnyttede kraftigt, nemlig at cykellængderne i en permutation bevares ved konjugering:

Opgave 4

Antag, at $(a_1a_2\cdots a_r)$ er en cykel i permutationen A, dvs.

(2) $$A=(\ldots)\ldots(a_1a_2\cdots a_r)\ldots(\ldots)$$

Lad T være en vilkårlig anden permutation. Vis at så er $\big(T(a_1)T(a_2)\cdots T(a_r)\big)$ en cykel i den konjugerede permutation $T^{-1}AT$, dvs.

(3) $$T^{-1}AT=(\ldots)\ldots\big(T(a_1)T(a_2)\cdots T(a_r)\big)\ldots(\ldots)$$

Hjælp: Du skal blot vise, at permutationen $T^{-1}AT$ afbilder $T(a_1)$ i $T(a_2)$, $T(a_2)$ i $T(a_3)$, … , $T(a_r)$ i $T(a_1)$. Tag hver permutation i $T^{-1}AT$ én efter én:

$$T(a_1) \xrightarrow{T^{-1}} ? \xrightarrow{A} ? \xrightarrow{T} ?$$

Tilsvarende for de øvrige elementer i cyklen. Udnyt at når $(a_1a_2\cdots a_r)$ er en cykel i A, så gælder: $A(a_1)=a_2$, $A(a_2)=a_3$, … , $A(a_r)=a_1$.

Argumenter for, at ovenstående egenskab (3) betyder, at cykellængderne i A og $T^{-1}AT$ er parvis ens – vi siger, at de har samme *cykelstruktur*.

□

Lidt senere i noten vil vi gå over til at se på en *mini-Enigma* maskine, som har 12 bogstaver: `a,b,c,d,e,f,g,h,i,j,k,l`. Derfor vil de næste opgaver ikke handle om permutationer af tal, men om permutationer af disse 12 bogstaver.

Opgave 5

Givet de to permutationer

$$A = \texttt{(akcj)(b)(dlf)(ehgi)}$$
$$T = \texttt{(ahib)(cd)(egjfkl)}$$

Bestem det konjugerede element $T^{-1}AT$ til A. Kan du bekræfte udsagnet i opgave 4, om at cykelstrukturen er bevaret under konjugering?

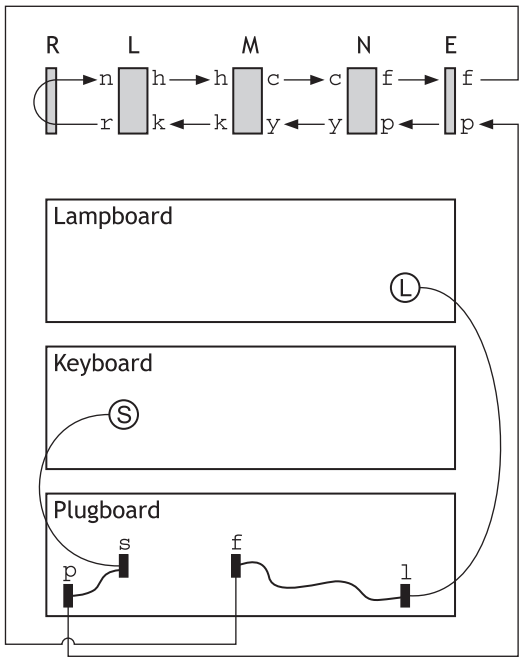
Hvis man sammensætter en permutation med sig selv et bestemt antal gange, så får man identitetspermutationen I. Det mindste positive tal n, for hvilket $A^n=I$ betegnes permutationens *orden*.

Opgave 6

Prøv at finde en matematisk regel for, hvordan man kan finde ordenen af en permutation ved at betragte permutationens cykellængder. Benyt reglen til at bestemme ordenen af følgende permutation: A = `(achbf)(di)(eklgj)`.

Hvis du ikke allerede har styr på, hvordan Enigma maskinen virker, så kan du studere figuren nedenfor, hvor dens virkning er illustreret: Der trykkes på bogstavet `s` på keyboardet. Samtidigt bevæges rotoren *N* et trin fremad. Der går en ledning til `s` i plugboardet. Da bogstaverne `s` og `p` er forbundet i plugboardet, går signalet videre til `p`. Herfra går signalet direkte videre til indgangshjulet *E* (*Entry wheel*). Der sker ikke noget i dette hjul. Det gør der derimod i de tre næste hjul, som er de tre rotorer, *N*, *M* og *L*, hvis indre indeholder en masse ledninger, som er kombineret på kryds og tværs. Bogstaverne permuteres og det samme sker i reflektoren, som sender signalet tilbage igennem de tre rotorer og tilbage til plugboardet i bogstavet `f`. Da `f` er forbundet med `l` via et kabel, kører bogstavet videre til `l`, og det ender med, at lampen `l` lyser op.

Figur 1



I det følgende skal du løse nogle af de kombinatoriske problemer i forsøget på at finde ud af, hvor mange mulige indstillinger Enigma maskinen giver anledning til. Det er omtalt på side 253-255 i artiklen.

Opgave 7

a) (*Plugboard settings*). Vis, at antallet af mulige plugboard-indstillinger ved brug af *n plugs*, altså *n* forbindelsesledninger, er givet ved følgende udtryk, hvor vi har benyttet kombinationer (Se i øvrigt artiklen nederst side 253):

$$\frac{\binom{26}{2}\cdot\binom{24}{2}\cdot\binom{22}{2}\cdot\ \cdots\ \cdot\binom{26-2(n-1)}{2}}{n!}$$

b) Prøv at udregne antal kombinationer for forskellige værdier af n mellem 1 og 13 (husk, at der er 26 bogstaver, så der kan højst være 13 par!). Hvilket antal plugs giver flest muligheder?

c) (*Rotor arrangements*). Kort før 2. verdenskrig anvendte man kun tre rotorer. De kunne sættes i den rækkefølge, man måtte ønske. Hvor mange muligheder giver det? Senere i krigen havde man 5 forskellige rotorer, hvoraf kun tre skulle benyttes. Hvor mange måder kan det gøres på, inklusiv rækkefølge?

d) (*Ring settings*). Om hver rotor sidder en ring med 26 bogstaver. Den kan drejes i forhold til rotorens indre ledningsnet og sættes på 26 forskellige måder ved hjælp af en nål. Fast på ringen og ud for et ganske bestemt bogstav sidder et hak (*notch*), som bevirker at næste hjul skubbes et trin fremad, når hakket når en pal. Kun hakkene på de to første hjul bidrager til Enigmas sikkerhed. Hvor mange ringindstillinger kan man dermed sige, at der er? (se artiklen side 254).

e) (*Rotor settings/ground settings*). Hver af de tre rotorer kan fra starten sættes på 26 forskellige måder – svarende til, at hvert af de 26 forskellige bogstaver kan være i top fra start. Hvor mange mulige rotorindstillinger fås alt i alt?

f) (*Total key number*). En nøgle (*key*) indeholder oplysning om hvilke rotorer, der er benyttet og i hvilken rækkefølge, ringindstillingerne, rotorernes grundindstillingerne samt plugboard indstillingerne. Hvor mange mulige nøgler giver det alt i alt, når vi antager, at vi var tilstede umiddelbart før krigen, hvor der kun var tre forskellige rotorer og hvor man benyttede 6 forskellige plugs i plugboardet?

Opgave 8

Husk, at Enigma-maskinen er en elektro-mekanisk realisering af et *polyalfabetisk kryptosystem*, ligesom *Vigenere cifferet* er. Hvor mange bogstaver skal man trykke ind, før Enigma maskinen begynder at gentage en permutation, den har benyttet tidligere? (Se artiklen side 251).

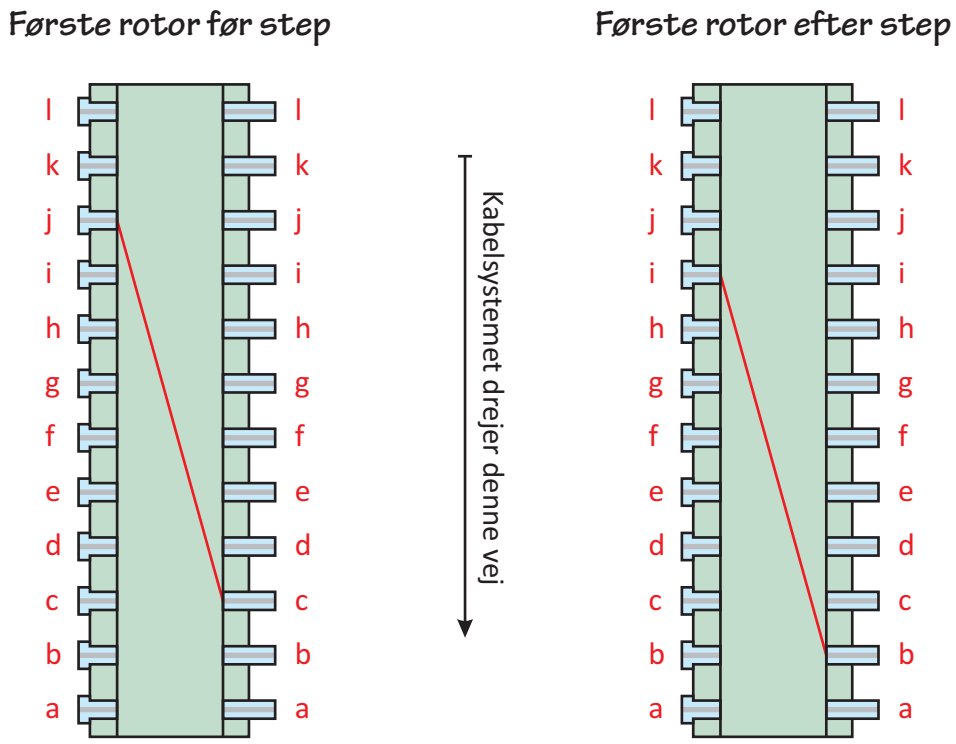
□

En vigtig pointe i Enigma maskinens virkning er, at når man trykker et bogstav ind, så kører den første rotor N (se figur 1) et trin fremad. Derved sikres det, at et nyt alfabet bliver benyttet ved krypteringen af dette bogstav. I det følgende får vi derfor brug for at repræsentere begivenheden, at rotoren N bevæger sig ét trin fremad ved en permutation P: `(abcdefghijklmnopqrstuvwxyz)`.

Lad os i det følgende antage, at vi arbejder med en mini-Enigma maskine med 12 bogstaver. Den permutation, som sender den første rotor et trin fremad, er dermed givet ved $P =$`(abcdefghijkl)`.

Opgave 9

I denne opgave skal vi kigge på, hvad der permutationsmæssigt sker, når det første hjul stepper ét trin fremad. Rent mekanisk sker det ved at indmaden i hjulet (kabelsystemet) drejer ét trin *imod* brugeren. Situationen er illustreret på figuren nedenfor. Her er det som et eksempel antaget at den permutation, der svarer til virkningen af første rotor *før* steppet, er givet ved $N = \texttt{(akcj)(b)(dlf)(ehgi)}$. Kun det ene kabel er tegnet til venstre, nemlig det, som sender $\texttt{c} \to \texttt{j}$. Husk at signalet kommer ind til højre på rotoren og kommer ud til venstre! Man ser, at efter indmaden af hjulet har flyttet, sig er kablet rykket et trin tilbage.



a) Indtegn de resterende kabler på rotoren til venstre og fuldfør også rotorens kabelnet *efter* første step. Hvilken permutation får du ud af det?

b) Udregn den konjugerede permutation PNP^{-1}. Får du den samme permutation som under spørgsmål a)? Det skulle du gerne.

c) Forklar hvorfor det er logisk, at hver gang man foretager ét step, så fås permutationen hørende til virkningen af rotoren i den nye position ved at *konjugere* permutationen hørende til virkningen af rotoren i den oprindelige position med P^{-1}, altså ved at sætte P og P^{-1} på hver sin side af den oprindelige permutation, ligesom vi gjorde under punkt b). *Hjælp*: Du kan evt. få idéer ved at starte med elementet $\texttt{b}$ og se, om det virkelig afbildes i elementet $\texttt{i}$. Hvad er det for mekanismer, der virker?

$$b = P^{-1}(c) \xrightarrow{P} ? \xrightarrow{N} ? \xrightarrow{P^{-1}} ?$$

Du kan eventuelt benytte resultatet af opgave 4 til at udføre konjugeringen i praksis. Det bemærkes, at der er konjugeret med $T = P^{-1}$ (Husk, at $(P^{-1})^{-1} = P$).

Opgave 10

Vi arbejder stadig med en mini-Enigma maskine med 12 bogstaver. I det følgende vil vi antage, at hjul nummer 2 og 3, dvs. *M* og *L*, ikke bevæger sig fremad. Kun det første hjul, *N*, bevæger sig. Antag at fire par af bogstaver er forbundet i plugboardet, beskrevet ved følgende permutation:

S: `(ai)(bc)(d)(e)(fh)(gj)(k)(l)`

Permutationen *P*, som roterer det første hjul et trin fremad, er givet ved :

P: `(abcdefghijkl)`

Kabelforbindelserne (wirings) i hjulene er vilkårlige permutationer, lad os sige:

N: `(alehbfcikj)(gd)`
M: `(a)(bikfd)(eghl)(cj)`
L: `(adgihljk)(bcef)`

Husk at reflektoren repræsenteres af en permutation, som består af seks 2-cykler, fx:

R: `(ac)(bl)(de)(fk)(gi)(hj)`

a) Udregn sammensætningen $SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$ svarende til, at man foretager den første indtastning på Enigma. Hvad bliver a afbildet i? Bestem et udtryk for hele permutationen på cykelform. *Hjælp*: Opskriv for overskuelighedens skyld alle permutationerne i rækkefølge under hinanden og løb dem alle igennem.

b) Vis, at $SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1} = \left(SPNP^{-1}ML\right)R\left(SPNP^{-1}ML\right)^{-1}$. *Hjælp*: Benyt pointen i opgave 3b).

c) Permutationen repræsenterende reflektoren *R* består af udelukkende *transpositioner*, dvs. 2-cykler. Benyt b) samt udsagnet i opgave 4 til at konkludere, at permutationen, som svarer til første indtastning, udelukkende består af 2-cykler. Det samme gælder naturligvis også for de efterfølgende indtastninger.

d) Benyt c) til at argumumentere for, at Enigma maskinen er *selv-reciprok*, dvs. at når man indtaster den krypterede tekst på Enigma – med de samme indstillinger, som meddelelsen blev krypteret med – så får man klarteksten.

e) Forklar hvorfor egenskaben i d) var vigtig for tyskerne?

f) Hvorfor kan intet bogstav krypteres til det samme bogstav? Denne egenskab var en klar svaghed, som blev benyttet til dekryptering i Bletchley Park. *Hjælp*: Antag modsætningsvist, at der var et bogstav, som blev krypteret til sig selv. Hvorfor skulle der så have været en 1-cykel i permutationen $SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$?

På side 257 i artiklen omtales problemet, der på engelsk betegnes *depth*: Hvis man krypterer alle meddelelser den samme dag med de samme grundindstillinger af rotorerne, så får modstanderen en masse statistik at arbejde med, fordi det første bogstav i meddelelsen altid vil blive krypteret med det samme alfabet den dag. Det samme med 2. bogstav osv.

Derfor gjorde tyskerne det, at de krypterede dobbelt. Udover den *daglige nøgle* fra kodebogen anvendte de en *meddelelsesnøgle*. Meddelelsesnøglen bestod af tre bogstaver, som angav de bogstaver, som skulle stå øverst på hvert af de tre hjul fra start (rotor-settings). Først blev meddelelsen krypteret med meddelelsesnøglen, dernæst anbragte man meddelelsesnøglen foran den krypterede tekst og krypterede nok en gang, nu med dagsnøglen. Når en tysk operatør dekrypterede med den daglige nøgle, kunne han se meddelelsesnøglen som de første tre bogstaver i teksten – det kunne fx være `nku`. Så satte han den første rotor i startposition `n`, den anden i startposition `k` og den tredje rotor i startposition `u`. Derefter kunne han foretage dekrypteringen af resten af dokumentet med de nye indstillinger, hvorefter han ville have klarteksten. Tyskerne begik blot en fejltagelse, som viste sig fatal: For en sikkerheds skyld skrev tyskerne meddelelsesnøglen to gange efter hinanden – de ville mindske problemet med, at kryptoteksten undertiden blev forvandsket under radiotransmissionen. Denne vane med at skrive meddelelsesnøglen dobbelt var imidlertid en svaghed, som Rejewski dygtigt udnyttede: Selvom meddelelsesnøglen `nkunku` var ukendt for ham, kunne han være sikker på, at 1. og 4. bogstav i kryptoteksten stammede fra det samme bogstav! Det samme med 2. og 5 bogstav og med 3. og 6. bogstav.

På side 257 i artiklen er det beskrevet, hvordan Rejewski indfører seks forskellige permutationer A, B, C, D, E og F. Når man trykker på en knap på keyboardet, så lyser et andet bogstav op, afhængig af, hvilket et bogstav, der blev valgt. Det giver anledning til en permutation. A er den permutation, som svarer til *første* gang man trykker, B til den permutation, som svarer til *anden* gang man trykker, etc. Lad i det følgende S være den permutation, som svarer til plugboardets virkning, og lad N, M og L være permutationerne, som repræsenterer hver af de tre hjuls virkning. Lad endvidere R være permutationen, som reflektoren giver anledning til. Det betyder, at A kan skrives på følgende måde, som også er antydet i opgave 10a):

$$A = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1} \tag{4}$$

Bemærk, at der er fejl i udtrykkene for A og D i artiklen side 259. Forfatteren Chris Christensen har gjort mig opmærksom på dette. Permutationerne er derimod korrekt skrevet op på side 265.

Opgave 11

Redegør for rigtigheden af udtrykket for A ovenfor, dvs. at det er permutationen, som svarer til første indtastning. *Hjælp*: Husk pointen i opgave 9.

På tilsvarende måde kan den permutation, som repræsenterer den 4. indtastning skrives:

$$D = SP^4NP^{-4}MLRL^{-1}M^{-1}N^{-1}P^4S^{-1}P^{-4} \tag{5}$$

Her vil P^4NP^{-4} svare til virkningen af rotoren N efter rotoren er drejet 4 trin fremad. Bemærk, at vi i udtrykkene (4) og (5) går udfra, at *kun* den første rotor N drejer! Man kan

selvfølgelig være uheldig, at første rotor er indstillet, så man indenfor de første seks indtastninger når hakket i ringen, så rotor *M* skubbes et trin fremad. I dette tilfælde kan Rejewskis analyse i det følgende ikke benyttes. Heldigvis sker det ikke så tit, da der er 26 bogstaver på ringen!

Opgave 12

a) Vis, ved at bruge teknikken fra side 259, at

(6) $$AD = SP_1P_4S^{-1} \quad \text{hvor} \quad \begin{cases} P_1 = PNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1} \\ P_4 = P^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4} \end{cases}$$

idet du korrigerer udregningerne, forårsaget af fejlene i udtrykkene for *A* og *D*. Husk at gøre rede for hvert trin i udregningerne.

b) Hvorfor er P_1 og P_4 uafhængige af plugboardets indstillinger?

c) Benyt (6) samt pointen i opgave 4 til at forklare hvorfor cykellængderne i permutationen *AD* er uafhængige af plugboardets indstillinger.

Vi mangler at argumentere for, hvorfor permutationen *AD* fra opgave 12 overhovedet er interessant. Det viser sig, at vi kan sige noget om den netop på grund af tyskernes grundighed med at skrive meddelelsesnøglen to gange efter hinanden. Vi skal tilbage til side 258 i artiklen. Først skal det dog lige nævnes, at Enigma, som nævnt i opgave 10d), er *selv-reciprok*. Hermed menes, at hvis man med de samme indstillinger taster den krypterede tekst ind, så får man klarteksten!! Det var selvfølgelig en meget nyttig egenskab, for så kunne kryptoteksten ude i felten dekrypteres lige så nemt som den blev krypteret!

Opgave 13

Antag som på side 258, at meddelelsesnøglen i klartekst er `nkunku` og at den ved dagsnøglen krypteres til `JHNQBG`.

a) Redegør for argumentet, at permutationen *AD* må afbilde det første bogstav `J` i det fjerde bogstav `Q`? *Hjælp*: Husk at Enigma er selv-reciprok, jf. opgave 10d).

b) Forklar hvordan man kan rekonstruere hele permutationen *AD*, hvis blot man opfanger tilstrækkeligt mange krypterede meddelelser den samme dag?

Når *AD* er fuldstændig kendt, kan permutationens cykellængder bestemmes. Opgave 12c) godtgjorde, at cykelstrukturen i *AD* er uafhængig af plugboardets indstillinger. Hvis man ændrer på forbindelserne i plugboardet vil det godt nok give anledning til en anden permutation, men den vil have de samme cykellængder. Dette betød i realiteten, at Rejewski kunne "adskille plugboardets virkning fra resten af maskinen". Plugboardet var netop blevet indført for at øge antallet af muligheder betragteligt, så en *brute force* strategi med at afprøve samtlige indstillinger blev uoverstigeligt på den tid. Men her havde polakken fundet en størrelse (cykellængderne), som var *invariant* overfor plugboardets indstillinger.

Opgave 14

Forklar hvordan Rejewski udnyttede cykellængderne til at finde den daglige kode (se side 259-261 i artiklen).

Den matematik, som vi indtil nu har beskæftiget os med i noten, var en vigtig bestanddel i polakkernes angreb på Enigma før krigen. Men der er mere: Rejewski var også i stand til at bestemme de indre kabelforbindelser i hvert hjul ved hjælp af matematiske overvejelser. Dermed kunne han lave en tro kopi af Enigma, uden at have en aktuel tysk Enigma maskine i hånden! Du kan læse mere herom på siderne 263-268. Læseren er velkommen til at udforske dette på egen hånd!