Excel-øvelser i tallære

av

Peer Andersen

Innhold

Innledning

Dette heftet inneholder 7 øvelser der vi ser på hvordan Excel kan anvendes på problemer i tallteori. Øvelsene forutsetter at en har grunnleggende kjennskap til Excel og at en har kjennskap til de fagområdene som øvelsene berører. Den første øvelsen tar for seg trekanttall og kvadrattall, og målet er å finne tall som både er kvadrattall og trekanttall. I den neste øvelsen studerer vi Fibonaccitalleene og vi bruker Excel til å se på noen av sammenhengene som gjelder for Fibonaccitall. I øvelse 3 bruker vi Euclids algoritme til å finne største felles faktor til to gitte tall. Det finnes en funksjon i Excel som finner største felles faktor. Målet med denne øvelsen er å ikke bare finne største felles faktor, men også vise de forskjellige stegene i Euclids algoritme. I øvelse 4 bruker vi Excel til å løse lineære kongruensligninger. Metoden som vi bruker er systematisk prøving. I den neste øvelsen studerer vi Diofantiske ligninger. Også her bruker vi systematisk prøving for å finne løsningene. Den sjette øvelsen handler om kryptografi. Vi ser her på tre forskjellige måter å kryptere meldinger på. I den siste øvelsen skal igjen se på diofantiske ligninger, men i denne øvelsen bruker vi Euclids algoritme for å løse dem.

Øvelse 1 til 5 er øvelser som ikke er spesielt krevende. Den siste delen av øvelse 6 (RSA koding) og øvelse 7 er mer krevende, men det er likevel øvelser som bør være mulig å løse hvis en jobber systematisk med dem.

Øvelse 1. Trekanttall og kvadrattall

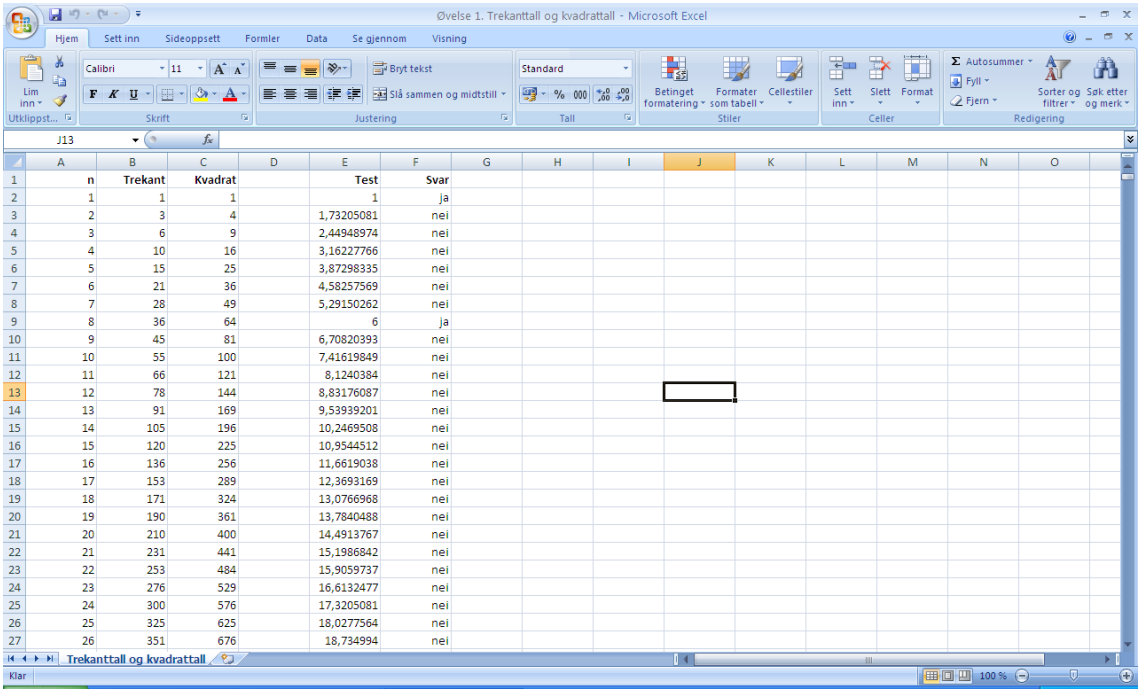
Trekanttall og kvadrattall er tall som er interessante å studere i matematikken. Trekanttall nummer n og kvadrattall nummer n kan skrives som

$$T_n = 1 + 2 + 3 + 4 + \cdots + n = \frac{n(n+1)}{2}$$

$$K_n = n^2$$

Klarer du å finne et tall som er både kvadrattall og trekanttall? Klarer du å finne flere?

Som du sikkert har oppdaget er det ikke så lett å lete frem tall som er både kvadrattall og trekanttall ved å regne for hånd. Med Excel derimot er det ganske enkelt å finne tallene som er både trekanttall og kvadrattall. Vi skal her se på hvordan er slikt regneark kan konstrueres. Vi skal lage et regneark omtrent som vist under.

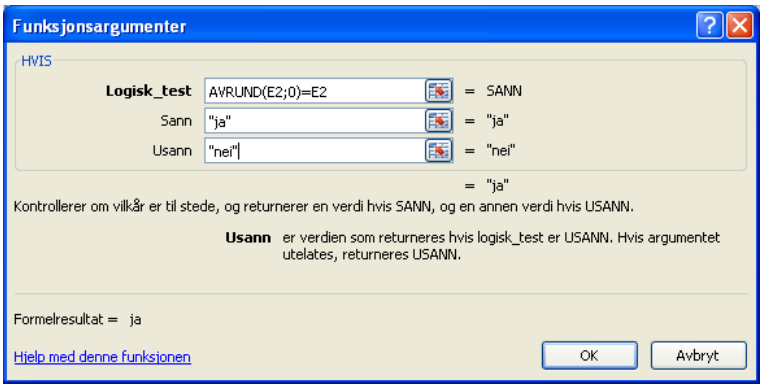


n	Trekant	Kvadrat	Test	Svar
1	1	1	1	ja
2	3	4	1,73205081	nei
3	6	9	2,44948974	nei
4	10	16	3,16227766	nei
5	15	25	3,87298335	nei
6	21	36	4,58257569	nei
7	28	49	5,29150262	nei
8	36	64	6	ja
9	45	81	6,70820393	nei
10	55	100	7,41619849	nei
11	66	121	8,1240384	nei
12	78	144	8,83176087	nei
13	91	169	9,53939201	nei
14	105	196	10,2469508	nei
15	120	225	10,9544512	nei
16	136	256	11,6619038	nei
17	153	289	12,3693169	nei
18	171	324	13,0766968	nei
19	190	361	13,7840488	nei
20	210	400	14,4913767	nei
21	231	441	15,1986842	nei
22	253	484	15,9059737	nei
23	276	529	16,6132477	nei
24	300	576	17,3205081	nei
25	325	625	18,0277564	nei
26	351	676	18,734994	nei

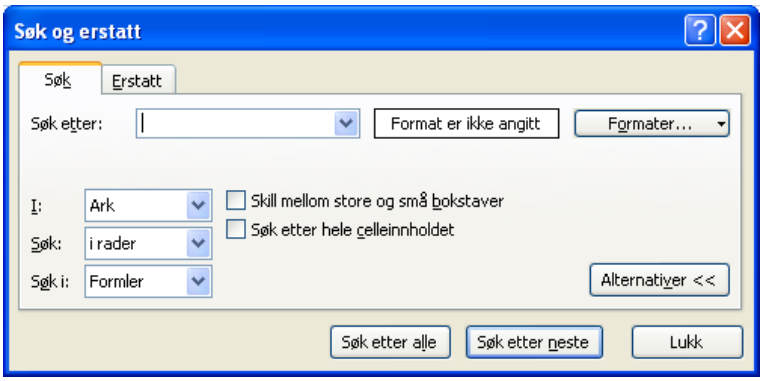
I A-kolonnen skal vi nummerere tallene fra 1 til f. eks 10 000. Skriv inn 1 i rute A2, og formelen =A2+1 i rute A3. Denne kopierer du nedover til rute A10001. I B-kolonnen skal vi beregne hva tilsvarende trekanttall blir. Vi bruker formelen fra i sted og skriver følgende formel inn i rute B2 =A2*(A2+1)/2. Denne kopierer du nedover til du kommer til rute B10001. I C-kolonnen skal vi beregne tilsvarende kvadrattall. Du skriver i rute C2 følgende formel: =A2^2. Denne kopierer du så til rute C10001. Vi har nå fått beregnet de 10 000 første kvadrattallene og trekanttallene. Vi kan gå inn i regnearket og se om vi finner tall som er begge deler. Prøv dette og se om du finner noen.

Vi kan imidlertid la Excel hjelpe oss med det. I E-kolonnen har vi laget en liten test for å avgjøre om et gitt trekanttall også er et kvadrattall. Det gjør vi ganske enkelt ved å ta kvadratroten av trekanttallet og ser på hva vi får ut. Får vi et heltall er tallet også et kvadrattall, dersom vi får ut et desimaltall ser vi at det ikke er et kvadrattall. For å gjøre dette så skriver du inn =ROT(B2) i rute E2 og kopierer den nedover til rute E10001.

I skjermbildet på forrige side ser dere at det er rubrikk med ja om det er et kvadrattall og nei om det ikke er det. Vi skal nå lage denne kolonnen. Flytt musen til rute F2 og bruk funksjonsveiviseren til å finne frem HVIS funksjonen. Du fyller den ut som vist under



Kopiere den ned til celle F10001. Det som denne formelen gjør er følgende: Uttrykket AVRUND(E2;0) runder av tallet i E2 til 0 desimaler. Vi sjekker deretter om dette tallet er lik tall et som står i celle E2. Hvis dette er tilfelle vil tallet i celle E2 være et heltall og dermed vil tallet i celle B2 være et kvadrattall. Det skrives da ja i celle F2. I motsatt fall skrives det nei i celle F2. En elegant måte å finne rutene med ja er å bruke Søk funksjonen. Du finner den først ved å gå til Hjem på menylinjen og deretter velge Søk etter og merk. Du velger der Søk. Klikk på Alternativer. Du får da opp følgende vindu



I feltet Søk etter skriver du ja. Der hvor det står Søk i og så Formler så endrer du Formler til Verdier. Klikk deretter på Søk etter neste og du får frem tallene som er både kvadrattall og trekanttall. Du vil f. eks få ja der hvor $n = 49$. Det betyr at trekanttall nummer 49 som er 1225 også er et kvadrattall, det vil si kvadrattall nummer 35. Med andre ord er

$$T_{49} = K_{35} = 1225$$

Bruk dette regnearket til å finne alle tallene som er både trekanttall og kvadrattall opp til og med kvadrat og trekanttall nummer 10000. Skriv ned tallene i kolonnen tall i tabellen under. Kolonnen faktorisert kan du vente med.

Tall	Faktorisert

Det finnes et mønster i tallene som er både trekanttall og kvadrattall, men det er ikke så lett å få se med første øyekast. For å lede dere litt på vei, skal dere skrive tallene som dere fant i sted som et produkt av to tall som begge er opphøyd i annen. La oss se på et eksempel. Tallet 2304 kan deles opp som $2304 = 6^2 \cdot 8^2$. Del opp tallene du fant i forrige spørsmål på denne måten og skriv ned resultatet i kolonnen faktorisert.

Prøv på bakgrunn av det du har gjort tidligere å finne et mønster for hvordan vi kan finne tall som både er trekanttall og kvadrattall. Hva blir det neste tallet med begge disse egenskapene?

Øvelse 2. Fibonaccitall

Fibonaccitallene er bygget opp ved at et tall er summen av de to foregående tallene. Vi definerer to de første Fibonaccitallene til begge å være 1. De første Fibonaccitallene kan skrives som

$$f_1 = 1$$

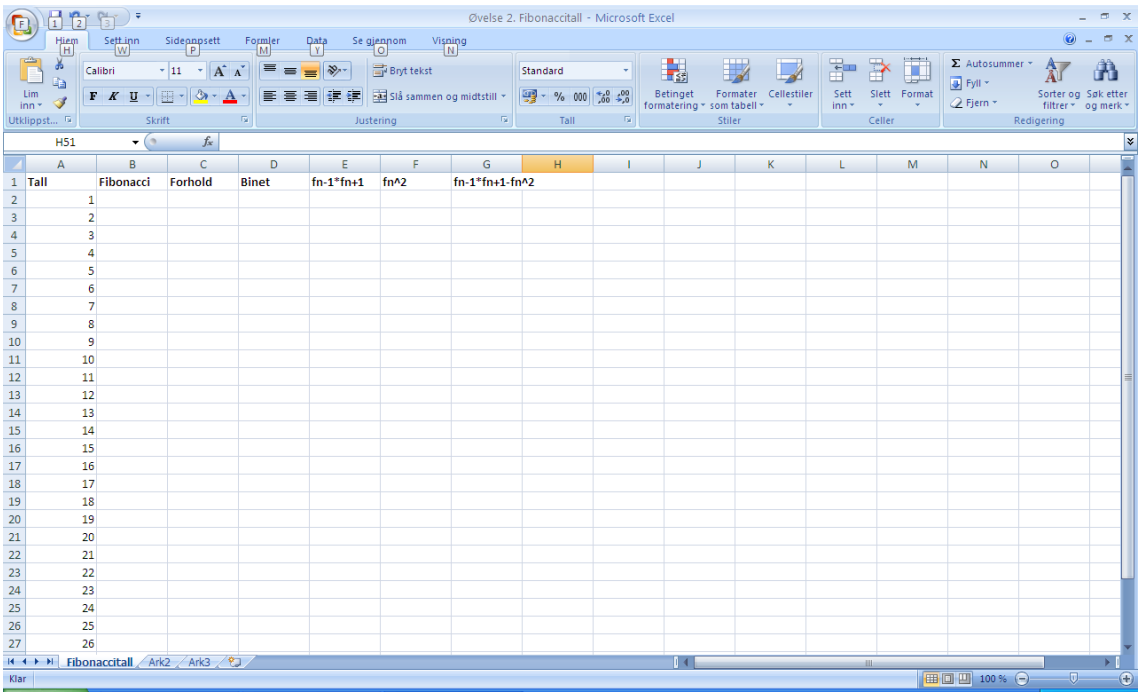
$$f_2 = 1$$

$$f_3 = f_1 + f_2 = 1 + 1 = 2$$

$$f_4 = f_2 + f_3 = 1 + 2 = 3$$

$$f_5 = f_3 + f_4 = 2 + 3 = 5$$

Fibonaccitallene har flere interessante egenskaper som kan være nyttig å studere i Excel. Vi skal se nærmere på det her. Du kan åpne et nytt regneark og fylle inn tekst som vist under.



Du kan la kolonnen tall gå ned til 30. Det neste vi skal gjøre er å regne ut Fibonaccitallene. De to første Fibonaccitallene er jo 1 så du kan starte med å skrive inn 1 i rute B2 og B3. I rute B4 skal vi beregne summen av de to foregående Fibonaccitallene. Formelen =B2+B3 gjør den jobben for oss. Du kan deretter kopiere formelen nedover til du kommer til Fibonaccitall nummer 30.

Det neste vi skal gjøre er å beregne forholdet mellom et Fibonaccitall og det foregående Fibonaccitallet. Det skal vi gjøre i C kolonnen. Vi starter med at vi i celle C3 beregner forholdet mellom f_2 og f_1. Formelen =B3/B2 gjør denne beregningen for oss. Du kan

deretter kopiere formelen ned til Fibonaccitall nummer 30. Hva observerer du? Er det noe kjent med forholdstallet som forholdet etter hvert stabiliserer seg mot?

En kan også beregne et Fibonaccitall ved å bruke Binets formel. Den sier at

$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

I D kolonnen skal vi beregne Fibonaccitallene ved hjelp av denne formelen og se om det stemmer med det vi først gjorde. Denne formelen blir ganske stygg, og en må være litt nøyaktig for å unngå parentesfeil. I rute D2 kan du skrive inn

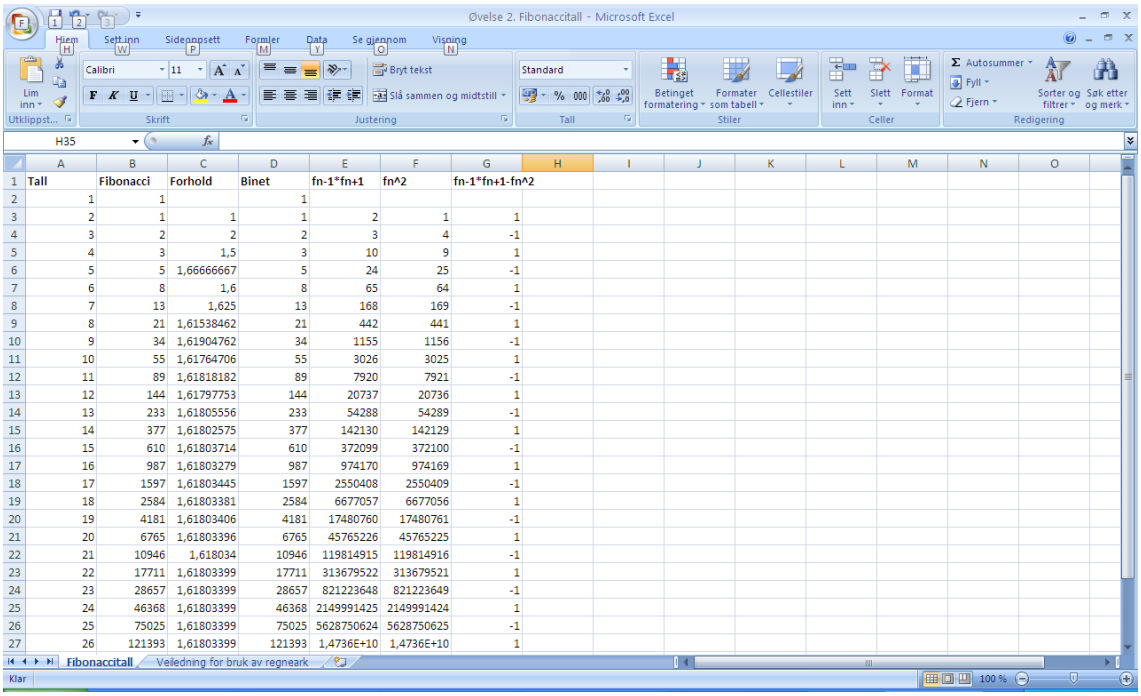
=1/ROT(5)*(((1+ROT(5))/2)^A2-((1-ROT(5))/2)^A2)

Hvordan samsvarer resultatene du får med Binets formel med det du fant i starten? Er det ikke underlig at når vi har brøk, kvadratrot og potens og likevel får vi ut et heltall som svar?

En annen interessant ting vi kan studere med Fibonaccitallene er hva følgende uttrykk blir

$$f_{n-1} \cdot f_{n+1} - {f_n}^2$$

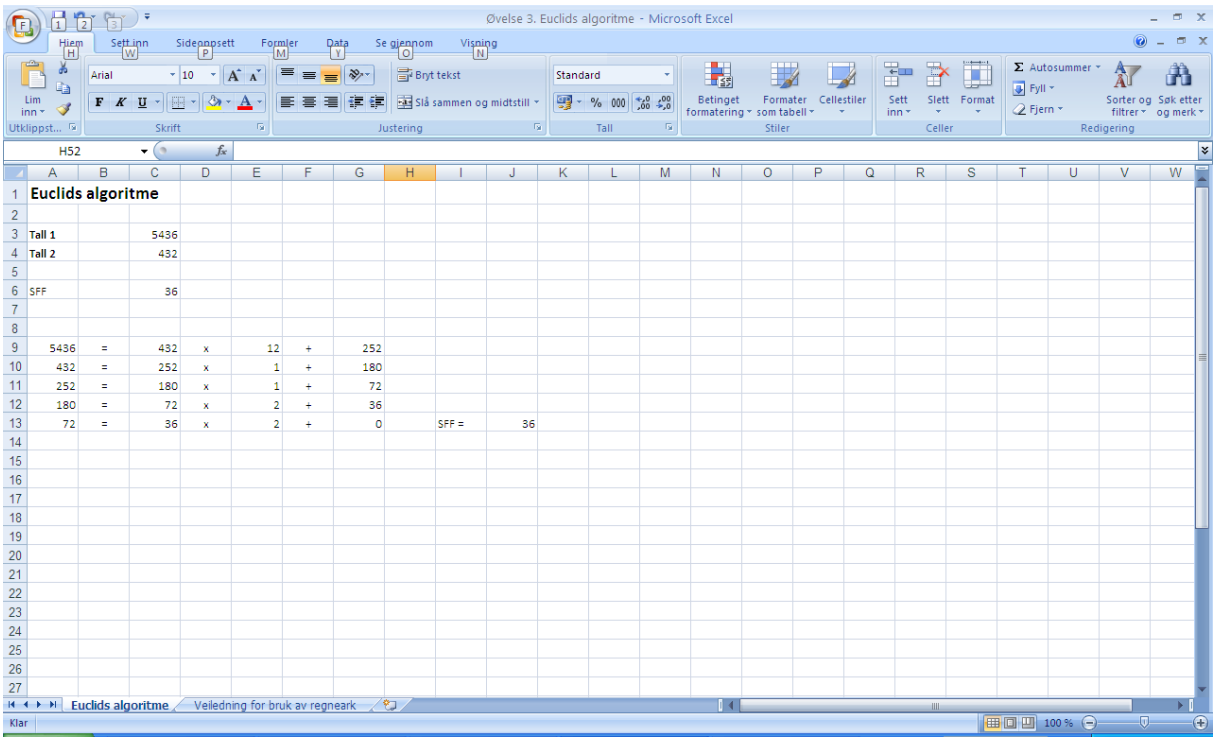
Vi skal i E kolonnen beregne $f_{n-1} \cdot f_{n+1}$ og i F kolonnen beregne ${f_n}^2$. Til slutt skal vi G kolonnen beregne differansen mellom disse to. I celle E3 kan du skrive inn =B2*B4 og i celle F3 kan du skrive inn =B3^2. I celle G3 kan du skrive inn differansen som er gitt ved =E3-F3. Hva observerer du? Denne sammenhengen var det Cassinis som fant og setningen har fått hans navn. Det ferdige regnearket skal nå se ut som vist under.



Tall	Fibonacci	Forhold	Binet	fn-1*fn+1	fn^2	fn-1*fn+1-fn^2
1	1		1			
2	1	1	1	2	1	1
3	2	2	2	3	4	-1
4	3	1,5	3	10	9	1
5	5	1,66666667	5	24	25	-1
6	8	1,6	8	65	64	1
7	13	1,625	13	168	169	-1
8	21	1,61538462	21	442	441	1
9	34	1,61904762	34	1155	1156	-1
10	55	1,61764706	55	3026	3025	1
11	89	1,61818182	89	7920	7921	-1
12	144	1,61797753	144	20737	20736	1
13	233	1,61805556	233	54288	54289	-1
14	377	1,61802575	377	142130	142129	1
15	610	1,61803714	610	372099	372100	-1
16	987	1,61803279	987	974170	974169	1
17	1597	1,61803445	1597	2550408	2550409	-1
18	2584	1,61803381	2584	6677057	6677056	1
19	4181	1,61803406	4181	17480760	17480761	-1
20	6765	1,61803396	6765	45765226	45765225	1
21	10946	1,618034	10946	119814915	119814916	-1
22	17711	1,61803399	17711	313679522	313679521	1
23	28657	1,61803399	28657	821223648	821223649	-1
24	46368	1,61803399	46368	2149991425	2149991424	1
25	75025	1,61803399	75025	5628750624	5628750625	-1
26	121393	1,61803399	121393	1,4736E+10	1,4736E+10	1

Øvelse 3. Euclids algoritme

Når vi skal finne største felles faktor til to tall kan vi bruke Euclids algoritme. Vi skal bruke Excel til å lage et regneark som finner største felles faktor ved å bruke Euclids algoritme. Målet er å konstruere et regneark omtrent som vist under.



Arket skal virke slik at når vi skriver inn de to tallene i rute C3 og C4 skal regnearket bruke Euclids algoritme for å finne største felles faktor. Regnearket skal også vise alle utregningene. Det finnes en formel i Excel som gir oss svaret direkte, men målet med denne øvelsen er i tillegg å vise utregningene og de ulike stegene på en oversiktiglig måte.

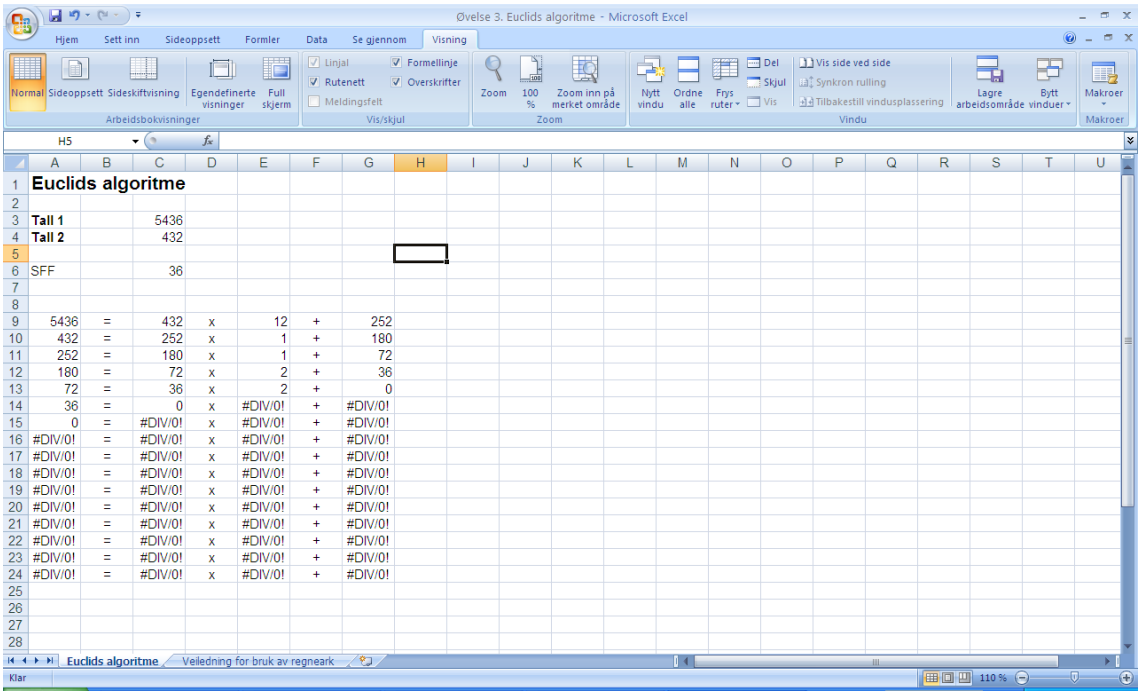
<u>Konstruksjon av regnearket</u>

Du kan først merke kolonnene og velge kolonnebredde på f. eks 7. Deretter kan du skrive inn det som står i linje 1, 3 og 4. I rute C6 kan vi beregne største felles faktor ved å bruke formelen som ligger i Excel. Hvis du i rute C6 skriver inn =SFF(C3:C4) får du beregnet største felles faktor. Fra linje 9 så skal selve utregningene foregå. Vi skal først lage linje 9. Vi skal deretter lage linje 10 og kopiere den nedover.

Rute A9 til G9 skal fylles ut slik det er vist i tabellen på neste side

Celle	Uttrykk	Forklaring
A9	=MAKSA(C3:C4)	Det største av tallene
B9	=	Tegn
C9	=MIN(C3:C4)	Det minste av tallene
D9	X	Tegn
E9	=HELTALL(A9/C9)	Det som denne funksjonen gjør er å dele A9 på C9 og runde nedover til nærmeste heltall
F9	+	Tegn
G9	=REST(A9;C9)	Beregner resten når vi deler A9 på C9

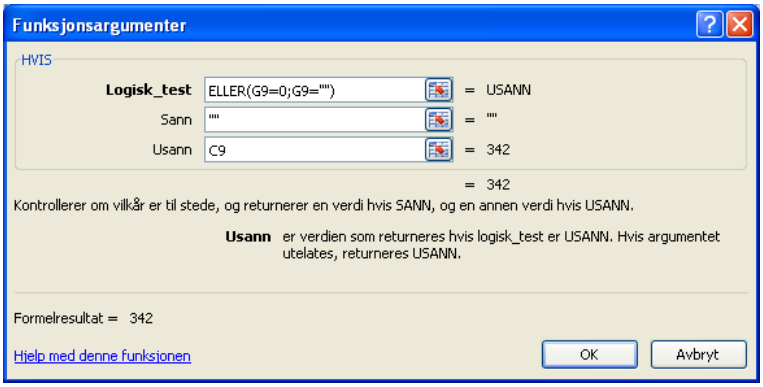
Tenk nøye gjennom at regnearket faktisk utfører første steget i Euclids algoritme før du går videre. Vi skal nå se på hvordan vi kan konstruere linje 10. I rute A10 skal tallet som stod i rute C9 stå. Skriv derfor i rute A10 inn uttrykket =C9. I rute C10 skal vi ha inn resten fra divisjonen i foregående linje. Den finner vi i rute G9. Vi skriver derfor i rute C10 uttrykket = G9. I rute E10 skal vi ha inn heltallsdelen av divisjonen mellom tallene i rute A10 og C10. Den finner vi ved å skrive formelen =HELTALL(A10/C10) inn i rute E10. I rute G10 skal resten beregnes. Den beregnes på samme måte som i rute G9. Vi skriver derfor uttrykket =REST(A10;C10) inn i rute G10. Du kan nå kopiere hele linje 10 nedover. Kopier den til linje 24. Regnearket skal nå se ut omtrent som vist på under



Vi ser at vi har fått utført Euclids algoritme og at største felles faktor til de to tallene er 36. Prøv ut med noen andre tall og se hva du får. Vi ser at presentasjonen her ikke er spesielt elegant siden vi får uttrykk som #DIV/0! i de nederste linjene. Vi skal se på hvordan vi kan justere regnearket slik at det blir litt mer elegant. Dette er ikke noe som er nødvendig å gjøre, men noe du kan gjøre hvis du har lyst.

For å gjøre regnearket mer elegant ønsker vi at når vi får 0 i rest, skal linjene som kommer etter denne være blanke. Det kan vi få til ved å bruke en HVIS setning. La oss se hvordan vi kan få dette til i rute A10.

Du kan flytte musen til rute A10 og åpne HVIS funksjonen med funksjonsveiviseren. Deretter kan du fylle ut verdiene som vist under.



Vi ønsker at feltet skal bli blankt dersom resten i foregående linje er lik 0. Feltet skal også være blankt om denne ruten er blank. På Logisk_test skriver vi derfor inn ELLER(G9=0;G9=""). Denne funksjonen tester om rute G9 er lik 0 eller om den er blank. Hvis en av disse vilkårene er oppfylt skal Excel skrive et blankt felt i rute A10. Det gjør vi ved å skrive inn "" i ruten etter Sann. I ruten Usann skriver vi inn hva som skal skje dersom G9 ikke er 0 eller blank og det er at vi i rute A10 skal ha verdien fra rute C9. De andre feltene i rad 10 modifiseres på nøyaktig samme måte. Når det er gjort kopierer du formlene nedover til og med rad 24.

I mitt regneark har jeg lagt inn en liten linje som viser hva største felles faktor er. Denne linjen kommer på samme linje som der hvor resten er lik 0. Dette er forholdsvis lett å lage til. I I kolonnen ønsker vi at det skal skrives SFF etter linjen hvor resten er lik 0. Ellers skal de øvrige feltene i være blanke. Flytt musen til rute I9 og skriv inn formelen

=HVIS(G9=0;"SFF = ";"")

Alternativt kan du selvsagt bruke funksjonsveiviseren. Kopier deretter formelen ned til linje 24. I J kolonnen skal vi skrive hva største felles faktor er i samme linje som SFF= står. De øvrige feltene skal være blanke. I rute J9 kan du skrive inn

=HVIS(G9=0;C9;"")

Siden første linjen er litt spesiell må vi også fylle ut rute J10. Der kan vi skrive inn

=HVIS(G10=0;G9;"")

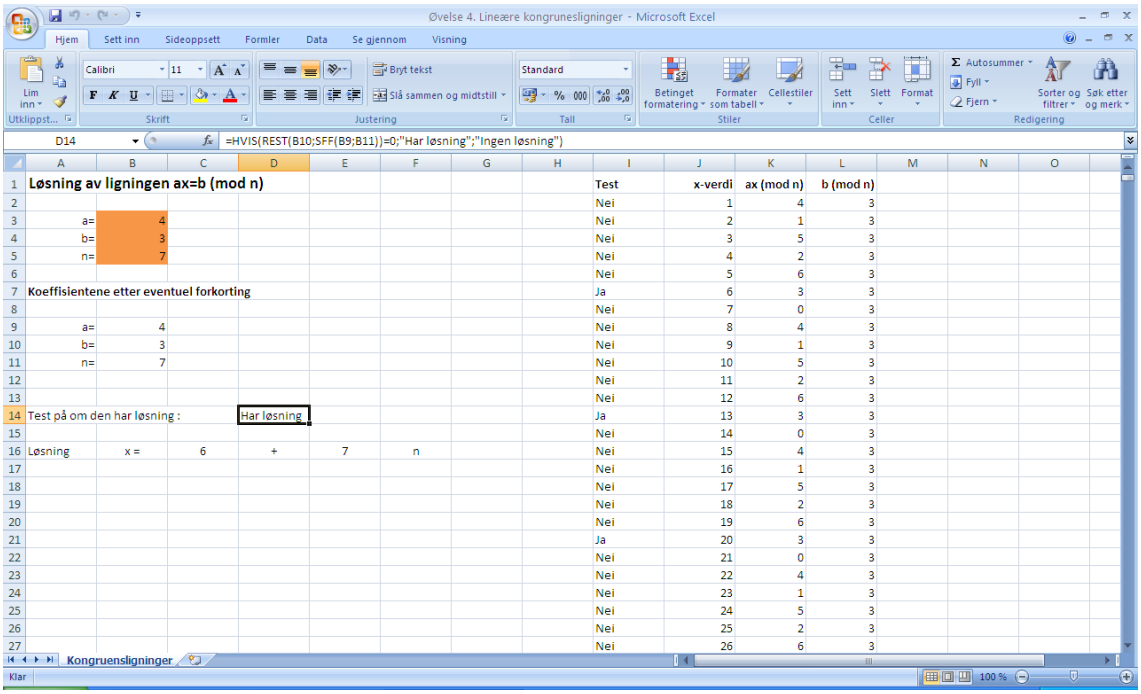
Denne formelen kan du kopiere ned til linje 24. Regnearket er nå ferdig og klar til bruk. Test det ut på noen kjente tall og se at det virker som det skal.

Øvelse 4. Lineære kongruensligninger

I denne øvelsen skal vi se på hvordan vi kan bruke Excel til å løse lineære kongruensligninger som

$$ax \equiv b \pmod{n}$$

Metoden vi skal bruke for å løse denne i Excel er systematisk prøving. Vi skal lage et regneark som prøver x verdier fra 1 og opp til og med 10000 for å se om noen av disse passer i ligningen. Regnearket vi skal konstruere kan se ut som vist under.

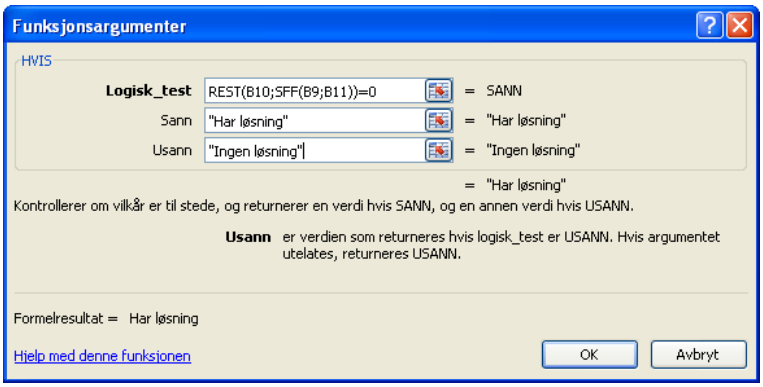


Du kan starte med å skrive inn teksten i feltet fra celle A1 til celle B7. De oransje rutene indikerer at det er her koeffisientene a, b og n skal stå. Det neste vi skal gjøre er å gjøre eventuelle forkortelser på ligningen. Vi sjekker hva største felles faktor er til koeffisientene a, b og n. Vi deler deretter koeffisientene på største felles faktor. Dersom største felles faktor er 1, blir det ingen forandring, men hvis den er noe annet blir ligningen forkortet. I rute B9 kan du skrive inn formelen

=B3/SFF(B3;B4;B5)

Tilsvarende formel kan du skrive inn i rute B10 og B11.

For at en kongruensligning skal ha løsning må b være et multiplum av største felles faktor til a og n. Vi ønsker derfor først å teste dette. Denne testen skal vi gjennomføre i rute D14. Vi skal bruke HVIS funksjonen til dette. Du kan bruke funksjonsveiviseren til å åpne HVIS funksjonen og fylle den ut som vist på neste side.



Det vi i tester her er om resten av divisjonen $\frac{b}{\mathrm{sff}(a,n)}$ er lik 0 eller ikke. Dersom den er lik 0 vil ligningen ha løsning og dersom den er forskjellig fra 0 vil den ikke ha løsning. I celle A14 kan du skrive inn en liten tekst med f. eks Test på om den har løsning.

Vi er nå klare til å gå videre for å finne løsningen. Vi lager oss først en tellekolonne i J kolonnen. Vi starter med tallet 1 i rute J2. I rute J3 kan du skrive inn =J2+1 og kopiere denne ned til celle J10001. Vi vil på den måten ta høyde for at vi kan løsning for x verdier på inntil 10000. I K kolonnen skal vi beregne hva resten blir når vi ganger a med valgte x verdi og deretter deler på n. Funksjonen REST hjelper oss med dette. Finn REST funksjonen ved hjelp av funksjonsveiviseren og fyll den ut som vist under.

Vi bruker dollartegn på cellene B9 og B11 slik at de ikke skal forandre seg når vi kopierer cellen nedover. Når du har fylt ut funksjonen kan du kopiere den ned til rute K10001. I L kolonnen skal vi beregne resten når vi deler b på n. Funksjonen

=REST($B$10;$B$11)

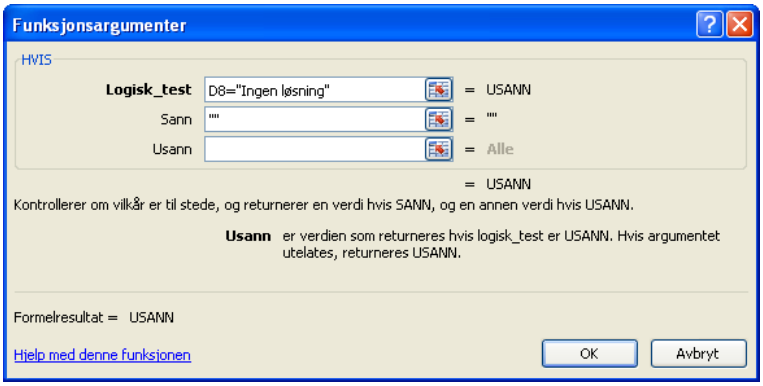
kan du skrive inn i celle L2. Du kan eventuelt bruke funksjonsveiviseren. Kopier deretter cellen ned til rute L10001. Det er egentlig ikke nødvendig å ha med denne kolonnen, men jeg har valgt å ta den med for oversiktens skyld. Løsningen av ligningen vil være den x verdien der verdiene i samme rad er lik i K og L kolonnen. Vi kan nå lete oss nedover i tabellen og se hvor disse verdiene er like. Det går greit om koeffisientene i ligningen ikke er for store, men det kan bli et møysommelig arbeid dersom koeffisientene er store. Vi ønsker derfor å gjøre en liten test i I kolonnen. Vi vil her sjekke om verdien i samme rad i K og L kolonnen er like

eller ikke. Hvis de er like skriver vi inn Ja, i motsatt fall skriver vi inn Nei. For å få dette til bruker vi HVIS funksjonen som vist under. Du fyller ut celle I2 som vist på neste side. Deretter kan du kopiere den ned til celle I10001.

Vi ser at der vi har fått Ja har vi en løsning. I vårt eksempel ser vi at vi har løsning for $x = 6, x = 13, x = 20$ osv. Generelt kan løsningen i vårt eksempel skrives som

$$x = 6 + 7n$$

Vi ønsker nå at regnearket skal skrive løsningen på denne formen. Dersom det ikke er løsning skal vi la rutene være blanke. For å få dette til bruker vi HVIS funksjonen på rutene fra B16 til F16. De to første linjene i HVIS funksjonen er felles for alle rutene. (Se under)



Vi tester her om ligningen har løsning eller ikke. Dersom den ikke har løsning skal feltet være blankt. Hva som skal skje dersom den har løsning fyller vi ut i feltet etter Usann. I rute B16 skal vi skrive inn ”x =” i feltet etter Usann. I rute C16 skal den første av løsningene våre stå. For å finne den kan vi benytte oss av en funksjon som heter FINN.RAD. I feltet etter USANN i rute C16 kan du fylle inn

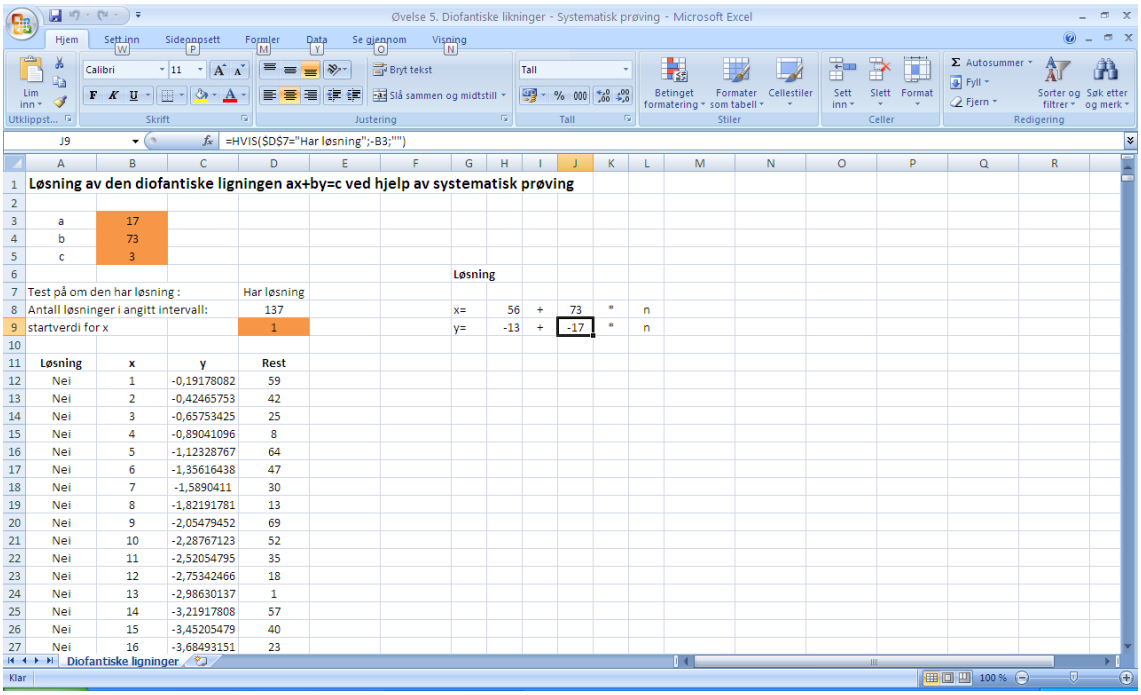
FINN.RAD("Ja";I2:J10001;2;USANN)

Det som denne funksjonen gjør er at den søker etter ordet Ja i første kolonnen i feltet I2 til J10001. Når den har funnet Ja første gang, gir den ut den tilsvarende verdien i J kolonnen. USANN må vi ta med for å indikere at det eksakte ordet ja vi søker etter. I vårt eksempel skal funksjonen returnere verdien 6. I rute D16, E16 og F16 fyller du inn henholdsvis +, B11 og n i

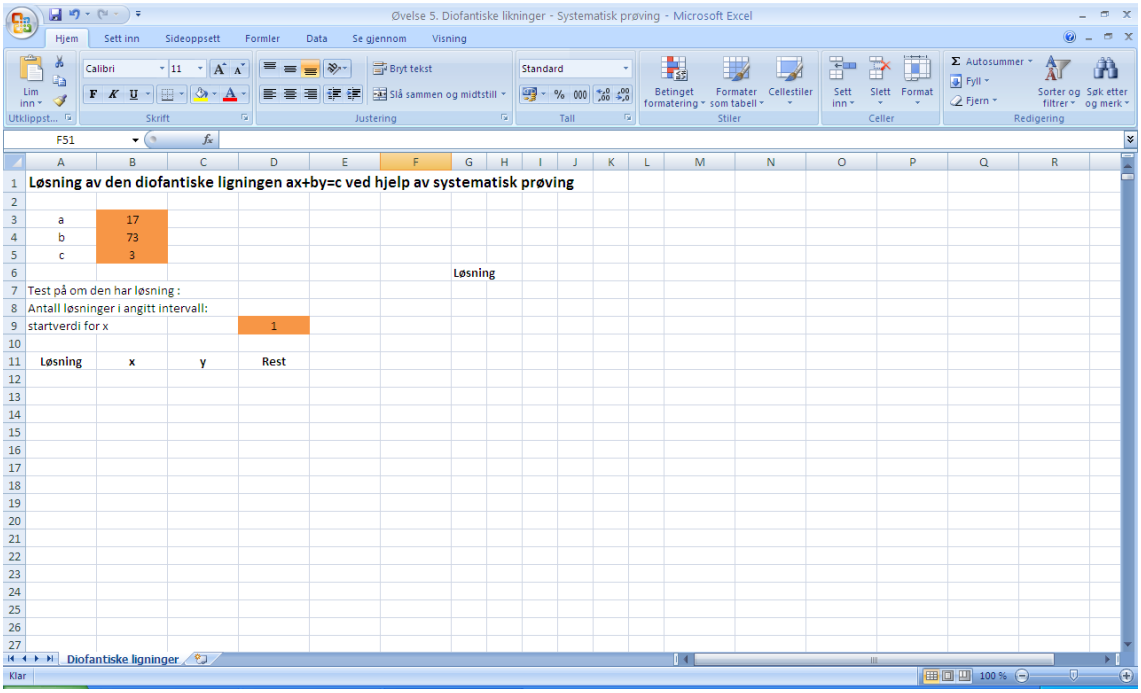
feltet etter USANN. Vi har dermed funnet en generell løsning for kongruensligningen. Prøv ut regnearket på noen kjente ligninger og se om det fungerer som det skal.

Øvelse 5. Diofantiske ligninger – systematisk prøving

Ligninger av typen $ax + by = c$ der en er på jakt etter heltallsløsninger kalles for diofantiske likninger. Diofantiske ligninger kan løses på flere måter, blant annet ved å bruke Euclids algoritme. Det skal vi gjøre i øvelse 7. I denne øvelsen skal vi se hvordan vi kan bruke Excel til å finne løsninger ved systematisk prøving. Regnearket vi skal konstruere skal se ut omtrent som vist under



Regnearket er bygget opp ved at vi skriver inn koeffisientene a, b og c i de oransje feltene. Vi velger oss også en passende startverdi for x for eksempel 1. Regnearket vil beregne den tilhørende y verdien og også de 10000 neste x og y verdiene. Regnearket vil også avgjøre hvilken av disse tallparene som er løsning av den diofantiske ligningen. Dette regnearket er ikke spesielt komplisert å lage til. Vi skal her se hvordan dette gjøres. Du kan starte med å skrive inn teksten som skal være med på regnearket. Regnearket på neste side viser hva du skal starte med å skrive inn.



Vi skal nå se på hva som skal stå i A, B, C og D kolonnen. I A kolonnen skal vi ha en test for å avgjøre om verdiene vi har funnet er en løsning eller ikke. Vi er nødt til å plassere denne testen i A kolonnen siden FINN.RAD funksjonen som vi skal bruke krever at denne kolonnen står først. Vi venter litt med å fylle ut A kolonnen. I B kolonnen skal vi skrive inn x verdiene. I rute B12 skriver vi inn =D9 slik at vi starter med angitte startverdi. I rute B13 skriver du inn =B12+1 og kopierer denne ned til celle B10011. Det neste vi skal gjøre er å regne ut tilhørende y verdier. Vi beregner y ved å løse ligningen med hensyn på y. Det gir oss at

$$y = \frac{c - ax}{b}$$

I rute C12 skal vi beregne dette uttrykket og det gjør vi ved å bruke formelen

=($B$5-$B$3*B12)/$B$4

Vi bruker dollartegn rundt cellene hvor koeffisientene a, b og c står, slik at disse ikke forandrer seg når vi kopierer cellen nedover. Når du har fått skrevet inn denne funksjonen kopierer du den ned til og celle C10011.

Når vi skal løse en diofantisk ligning er vi kun interessert i heltallsløsninger for x og y. Vi skal i D kolonnen regne ut hva resten blir når vi beregner y. Dersom resten er lik 0 vil x og y verdiene være løsning av ligningen. Vi beregner resten ved hjelp av funksjonen REST. Du kan flytte musen til celle D12 og åpne funksjonsveiviseren. Finn funksjonen REST og fyll den ut som vist på neste side

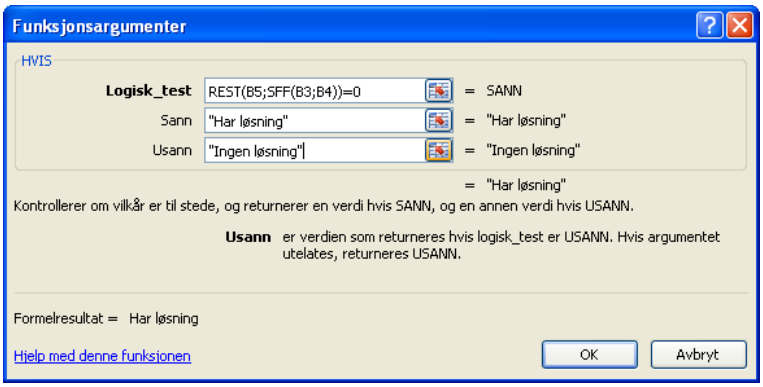
I feltet etter Tall har vi beregnet $c - ax$ og i feltet etter divisor har vi skrevet inn verdien til b. Kopier deretter formelen ned til og med rute D10011.

Vi er nå klare til å fylle ut A kolonnen der vi skal skrive inn Ja dersom tilhørende x og y verdier er løsning og Nei dersom de ikke er løsning. Vi benytter oss av HVIS funksjonen til dette. Flytt musen til rute A12 og fyll ut HVIS funksjonen som vist under.

Vi tester da på om resten i rute D12 er lik 0 eller ikke. Dersom den er 0 har vi en løsning, i motsatt fall har vi ikke løsning. Kopier cellen ned til og med celle A10011.

Vi kan nå lete opp løsningene ved å bla oss nedover regnearket til vi finner Ja. Vi kan også benytte oss av søkeverktøyet. Hvis du vil benytte deg av dette, klikker du på Søk og Merk og velger deretter Søk. Skriv inn Ja i feltet Søk etter. Klikk så på alternativer og velg verdier der hvor det står Søk i formler. Klikk til slutt på Søk etter neste. Regnearket vil nå lete opp linjene med Ja.

Regnearket kan fint brukes slik det er nå til å finne løsningene av ligningen $ax + by = c$. Imidlertid kan vi gjøre regnearket litt mer elegant. Det ene er å legge inn en test på ligningen har løsning eller ikke. Det andre er å skrive løsningen på generell form. La oss først se på hvordan vi kan avgjøre om ligningen har løsninger eller ikke. En diofantisk ligning har løsning bare dersom c kan skrivers som et multiplum av største felles faktor til a og b. Det vil være tilfelle om divisjonen $\frac{c}{\text{sff}(a,b)}$ går opp, hvilket vil si at resten er lik 0. I rute D7 skal vi teste dette ved hjelp av HVIS funksjonen. Du kan fylle ut HVIS funksjonen som vist på neste side.

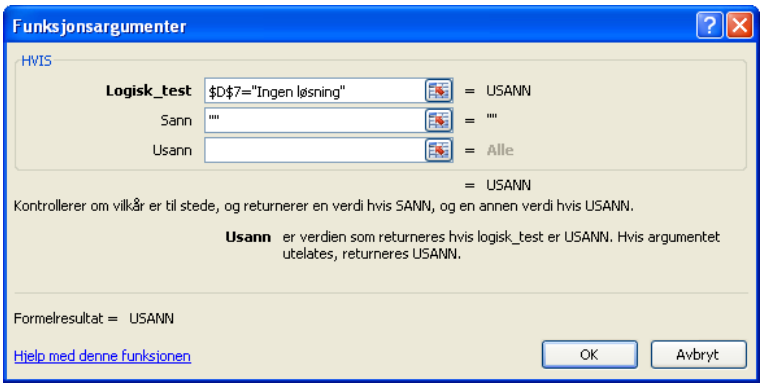


Funksjonen SFF beregner største felles faktor til to tall. I vårt tilfelle beregner den største felles faktor til a og b. Funksjonen REST beregner resten når vi deler ett tall på et annet. I vårt tilfelle deler vi c på $\text{sff}(a,b)$. Dersom resultatet er 0 skal regnearket skrive Har løsning, i motsatt fall skriver det Ingen løsning. I rute D8 har vi tatt en celle som forteller hvor mange løsninger vi har i det angitte intervallet. Funksjonen

=ANTALL.HVIS(A12:A10011;"ja")

teller opp hvor mange ganger ordet ja inntreffer i A kolonnen og dermed hvor mange løsninger vi har.

I rute G8 til L8 skal vi skrive inn den generelle løsningen til x. I raden under skal vi skrive inn løsningen til y. Vi ønsker at celle skal være blank hvis ligningen ikke har løsning. For alle cellene fra G8 til L8 benytter vi oss av en HVIS setning der de to øverste feltene er fylt ut som vist under.



Vi tester her på om det står Ingen løsning i rute D7. Dersom det er tilfelle skal ruten være blank noe vi indikerer med "" i feltet etter SANN. Feltet etter USANN blir litt forskjellig for de ulike cellene. I Celle G8 kan du skrive inn "x=". I celle I8 til L8 skal det stå henholdsvis +, B4, * og n. Til slutt skal vi se på celle H8. Her skal vi hente ut x verdien fra første raden der vi har Ja. Funksjonen FINN.RAD hjelper oss med det. Etter USANN kan du fylle ut

FINN.RAD("Ja";A11:C10010;2;USANN)

Denne funksjonen tar utgangspunkt i A, B og C kolonnen og leter etter første gang den finner Ja i A kolonnen. Den gir deretter ut verdien som er i kolonne nummer to, hvilket i vårt tilfelle er kolonnen der x verdiene står. Vi må ham med USANN for at regnearket skal lete etter eksakt Ja, og ikke noe som ligner. Den generelle løsningen for y finnes på tilsvarende måte. Husk bare på at du må ha –B3 i rute J9.

Regnearket skal nå være ferdig. Test det ut på noen kjente ligninger og se at det fungerer som det skal.

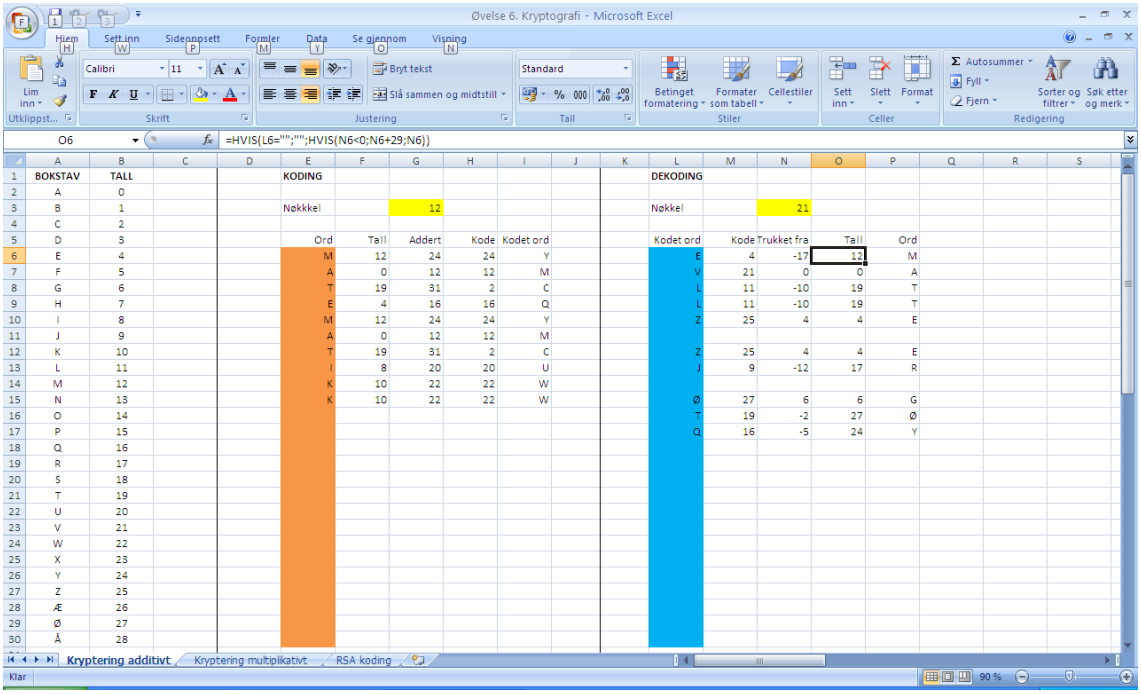
Øvelse 6. Kryptografi

I denne øvelsen skal vi se på hvordan Excel kan brukes til å kryptere meldinger. Vi skal først se på en situasjon der vi bruker en additiv kode, også kalt Cesær kode. Vi skal deretter se på en situasjon der vi bruker en multiplikativ kode og til slutt skal vi ta for oss RSA systemet som er et krypteringssystem som er mye brukt.

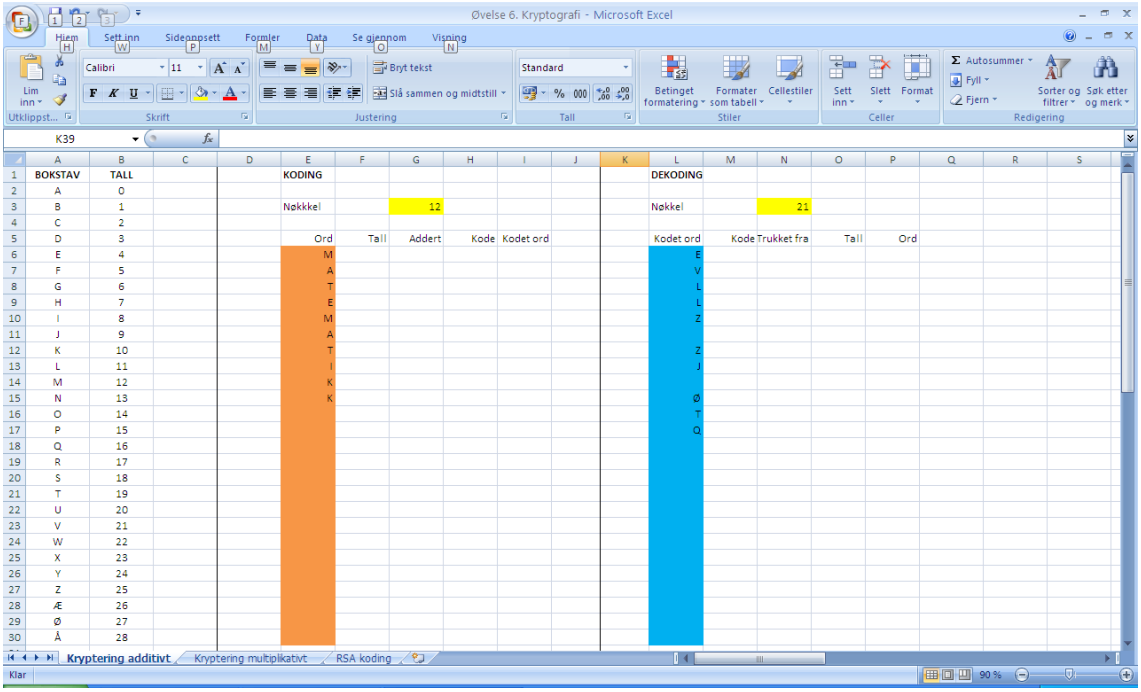
Additiv kode

Dette er et svært enkelt kodesystem. Det går ut på at vi tilordner tallet 0 til bokstaven A, 1 til B osv. Deretter plusser vi på et fast tall. Dersom summen blir større eller lik 29 trekker vi fra 29. La oss se på et eksempel. Vi skal kode ordet BRA der vi bruker 20 som addend. B tilsvarer tallet 1. Når vi plusser på 20 får vi 21, som tilsvarer bokstaven V. Bokstaven R tilsvarer tallet 17. Etter vi har plusset på 20 får vi 37. Siden dette tallet er større enn 29 trekker vi fra 29 og får 8. Dette tilsvarer bokstaven I. Tilslutt koder vi bokstaven A. Ved å addere 20 til 0 får vi 20 som tilsvarer U. Ordet 'BRA' er nå blitt kodet til ordet 'VIU'. Når vi skal dekode meldingen bruker vi samme prinsipp, bare at vi trekker fra det faste tallet. Får vi et negativt tall må vi plusse på 29. La oss dekode ordet 'VIU' og se om vi kommer tilbake til utgangspunket. Bokstaven V tilsvarer 21. Trekker vi fra 20 får vi 1 som gir bokstaven B. Bokstaven I tilsvarer 8. Når vi trekker fra 20 får vi -12. Vi må da plusse på 29 som gir oss 17. Tallet 17 tilsvarer R. Vi kan på samme måte forvisse oss om at U tilsvarer A. Vi ser da at når vi dekoder 'VIU' får vi 'BRA'.

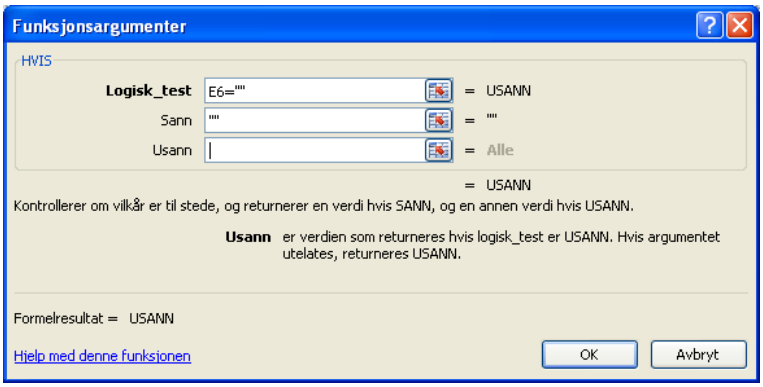
Vi skal nå se hvordan vi kan lage et regneark som utfører denne type koding og dekoding. Det er ganske enkelt å lage et slikt regneark. Regnearket vi skal konstruere skal se ut som vist på neste side.



Vi må lage en et felt der vi tilordner et tall til hver bokstav. Det gjør vi i A og B kolonnen. Meldinger som skal kodes skal vi skrive inn i det oransje feltet, mens meldinger som skal dekodes skrives i det blå feltet. Nøkkelen vi skal bruke skal stå i det gule feltet. Du kan starte med å fylle ut tekst og tall som vist under.



Vi ser først på hvordan vi kan kode en melding. I regnearket vårt skal vi kunne kode ord eller setninger på inntil 24 tegn. Det er ingenting i veien for å forlenge kolonnene slik at vi kan lage større meldinger. Vi fyller først ut rad 6 og deretter kopierer vi den nedover. Cellene F6 til I6 skal være blanke dersom celle E6 er blank. Vi må derfor lage en test ved hjelp av en HVIS setning for å avgjøre om celle E6 er blank eller ikke. Vi bruker følgende setning for rutene F6 til I6.



Den logiske testen og det som står i feltet etter Sann er det samme for alle rutene. Feltet etter Usann vil være forskjellig fra celle til celle og vi skal nå se på hva dette feltet blir for de ulike cellene. I celle F6 skal vi først tilordne et tall til bokstaven ut i fra tabellen i A og B kolonnen. Vi må bruke en funksjon som heter SLÅ.OPP til dette. Den kan brukes på flere måter, men i vårt tilfelle kan vi skrive inn

SLÅ.OPP(E6;$A$2:$B$30)

i feltet etter Usann. Det denne funksjoner gjør er at den leter etter verdien som står i rute E6 (M i vårt tilfelle) i A kolonnen. Når den har funnet verdien i A kolonnen gir den oss verdien som den finner i samme rad i B kolonnen. I vårt tilfelle vil den finne M i rute A14. Den gir oss da verdien som står i rute B14 som er 12. Vi bruker dollartegn slik at vi kan kopiere funksjonen nedover etterpå. Det neste skrittet er å plusse på nøkkelen som står i rute G3. Det betyr at i feltet etter Usann skal det for celle G6 stå F6+$G$3. Vi skal nå se på celle H6. Dersom verdien i celle G6 er mindre enn 29 skal det samme tallet også stå i rute H6, men dersom verdien er større eller lik 29 må vi trekke fra 29 fra verdien i rute G6. Vi må med andre ord inn med en HVIS setning i feltet etter USANN. I feltet etter USANN kan du skrive inn følgende setning

HVIS(G6>=29;G6-29;G6)

Vi tester da på om G6 er større eller lik 29. Dersom det er tilfelle trekker vi fra 29 fra G6, hvis ikke lar vi bare verdien være den samme som i G6. Det siste som gjenstår er å tilordne en bokstav til det kodede tallet. I vårt tilfelle har vi fått tallet 24 i rute H6. Vi ser at dette tilsvarer bokstaven Y. Vi ønsker at Excel skal slå dette opp for oss. Funksjonen INDEKS hjelper oss med dette. I feltet etter USANN kan du skrive inn

INDEKS($A$2:$A$30;H6+1)

Det som funksjonen gjør er at den tar for seg område A2 til A30. Deretter blar den seg nedover til den kommer til raden som er gitt i celle H6+1. I vårt tilfelle er det 25. Den henter da ut verdien som står i den 25 raden i området A2 til A30. I denne raden finner den bokstaven Y. (Grunnen til at vi bruker H6+1 er at A tilsvarer tallet 0 og at tallet 24 finnes i den 25 raden) Du kan nå kopiere cellene F6 til I6 ned til rad 30.

Hvis du har gjort det riktig skal ordet ’MATEMATIKK’ være kodet til ’YMCQYMCUWW’.

Vi skal nå ta for oss dekodingen. Dette er svært enkelt når vi først har laget kodedelen. Vi kan kopiere det vi nettopp gjorde over i feltet for dekoding og bare modifisere formlene litt. Du kan starte med å merke cellene F6 til I6 og kopiere de ved å trykke Crtl C. Flytt musen til M6 og lim inn formlene der ved å trykke Ctrl V. Cellene M6 og P6 trenger vi ikke å gjøre noe med da disse er lik det vi gjorde i sted når vi kodet meldingen. Cellene N6 og O6 må vi derimot modifisere litt. I celle N6 skal vi ta verdien fra M6 og trekke fra N3. Vi må derfor erstatte M6+$G$3 med M6-$N$3. Rute Q3 må vi også modifisere litt. Her skal vi legge til 29 dersom verdien i rute N3 er mindre enn 0. Vi erstatter derfor N6>=29;N6-29 med N6<0;N6+29 i funksjonen som står i celle O6. Du kan nå kopiere formlene ned til rad 30. Hvis du har gjort det riktig skal setningen ’EVLLZ ZJ ØTQ’ bli kodet til ’MATTE ER GØY’.

Multiplikativ kode

Additiv kode som vi nettopp så på er dessverre svært enkel å knekke, og koding på denne formen har liten praktisk nytteverdi. En bedre kode får en ved først å multiplisere et fast tall med det tallet som hver bokstav er assosiert med og deretter legge vi til et annet fast tall. Tallet vi multipliserer med kalles ofte for multiplikator. Ofte vil vi få et tall som er større en 29. Vi deler da tallet på 29 og bruker resten. Hvis vi skal kode tall x til y kan vi skrive det som kongruensen

$$y \equiv ax + b \pmod{29}$$

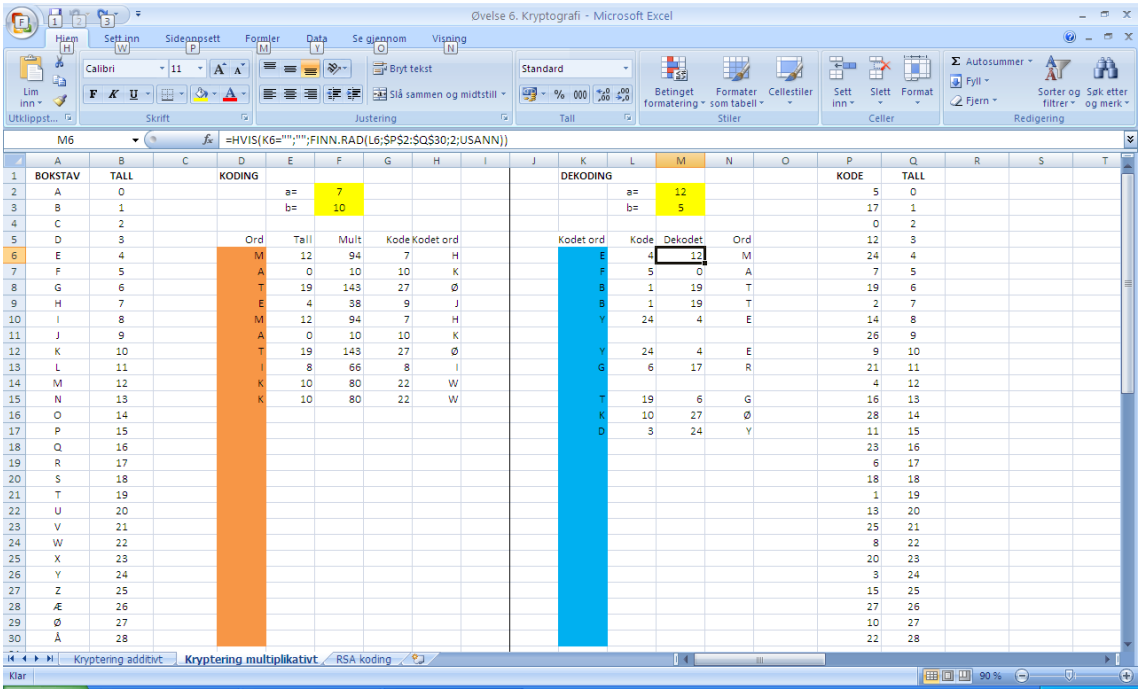
der a er multiplikatoren og b er tallet vi adderer med. La oss kode ordet 'GOD' når vi bruker vi setter $a = 20$ og $b = 7$. Bokstaven G tilsvarer tallet 6. Når vi multipliserer 6 med 20 får vi 120. Etter å ha lagt til 7 får vi 127. Resten vi står igjen med etter vi har delt på 29 blir 11 som tilsvarer bokstaven L. Vi kan sette det opp på følgende måte.

$$\text{G} \rightarrow 6 \rightarrow 2 \cdot 20 + 7 \equiv 127 \equiv 11 \pmod{29} \rightarrow L$$

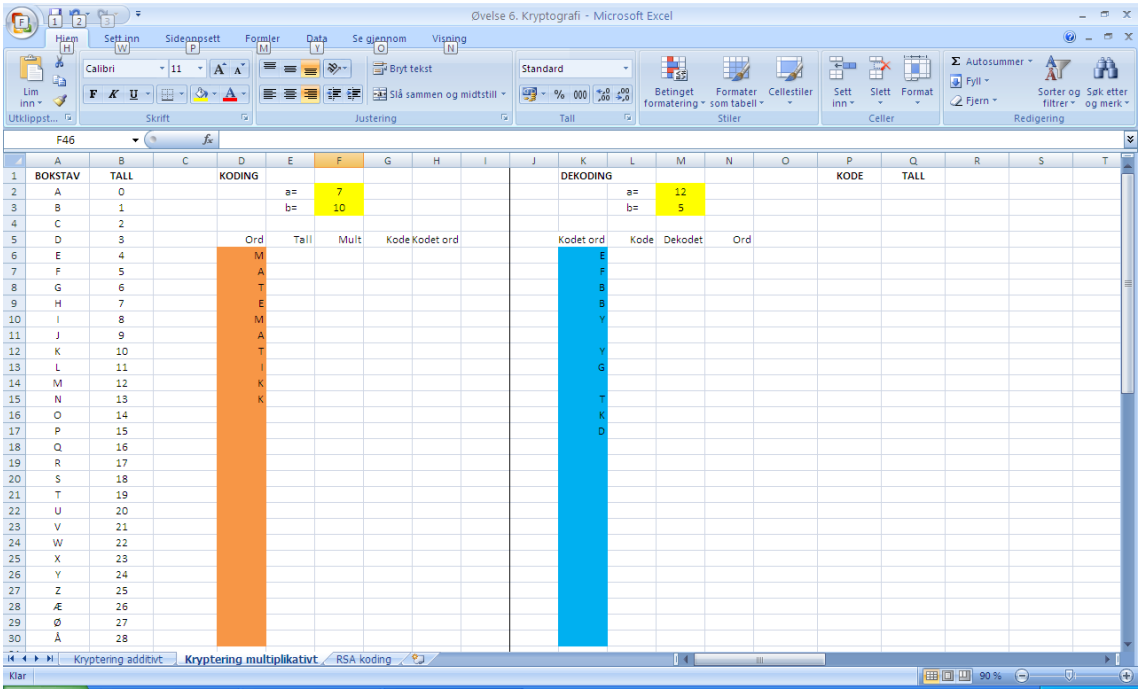
$$O \rightarrow 14 \rightarrow 14 \cdot 20 + 7 \equiv 287 \equiv 26 \pmod{29} \rightarrow Æ$$

$$D \rightarrow 3 \rightarrow 3 \cdot 20 + 7 \equiv 67 \equiv 9 \pmod{29} \rightarrow J$$

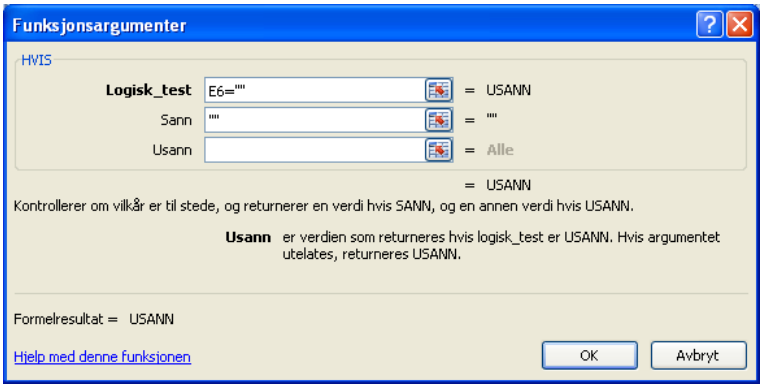
Vi skal nå se på hvordan vi kan bruke Excel til å kode og etter hvert dekode etter dette systemet. Regnearket vi skal lage skal se ut som vist under.



Også her starter vi må å fylle ut tekst og tall som skal ligge fast. Du kan åpne et nytt ark og fylle ut som vist på neste side.



Selve kodingen er forholdsvis enkel å lage og vi ser først på den. Vi skal fylle ut feltene E6 til H6 og deretter kopiere de nedover. Også her ønsker vi at feltene skal være blanke dersom det oransje feltet er blankt. Vi bruker derfor HVIS setningen på samme måte som i forrige eksempelet, slik at det som blir forskjellig er det som skal stå etter feltet USANN.



Formlene som det refereres til under skal altså stå i feltet etter USANN. I rute E6 skal vi tilordne bokstaven et tall. Det gjøres på samme måte som i sted med formelen

SLÅ.OPP(D6;$A$2:$B$30)

I rute F6 skal vi multiplisere verdien fra rute E6 med multiplikatoren som vi finner i celle F2. Vi skal deretter plusse på verdien fra rute F3. Uttrykket som skal stå i celle F6 blir derfor

E6*$F$2+$F$3

I rute G6 skal vi beregne resten vi får når vi deler tallet fra rute F6 på 29. Funksjonen

REST(F6;29)

vil utføre den beregningen for oss. Til slutt skal vi i rute H6 finne hvilken bokstav det kodede tallet tilsvarer. På tilsvarende måte som vi gjorde med den additive koden, bruker vi INDKES funksjonen til det. I vårt tilfelle blir funksjonen

INDEKS($A$2:$A$30;G6+1)

Hvis f. eks verdien i G6 er lik 7, så tilsvarer det bokstaven H. Den finner vi i rad 8 i A kolonnen. Vi må derfor bruke G6 +1 i INDEKS funksjonen. Du kan nå kopiere formlene du har laget ned til rad 30. Prøv å kode ordet 'MATEMATIKK' og se om du får ordet 'HKØJHKØIWW'

Å dekode en melding i et multiplikativt system er mye mer krevende enn i det additive systemet. La oss prøve å dekode bokstaven L når vi $a = 12$ og $b = 5$. La oss kalle den dekodede bokstaven for x. For å finne x må vi løse følgende kongruensligning

$$12x + 5 \equiv 11 \pmod{29}$$

siden bokstaven L tilsvarer tallet 11. Det finnes flere måter å løse slike ligninger på og en kan vise at $x = 15$ er en løsning av ligningen. Det tilsvarer bokstaven P. Ingen av de vanlige løsningsmetodene egner seg for å bruke i Excel. Vi skal derfor se på en metode der vi bruker systematisk prøving.

I rute L6 skal vi tilordne et tall til bokstaven. Vi kan kopiere formelen fra E6 til rute L6. I rute N6 skal vi gå motsatt vei. Du kan kopiere funksjonen fra celle H6 til N6. Her må vi gjøre en liten modifikasjon og det er at vi endrer J6 til K6. Det som gjenstår da er å beregne det dekodede tallet som jo vil være løsningen av kongruensligningen over. Det skal vi gjøre i rute M6. Vi skal som sagt bruke systematisk prøving på for å løse denne ligningen. I Q kolonnen skriver vi inn tallene fra 0 til 28 i feltene Q2 til Q30. I P kolonnen skal vi beregne $12 \cdot 0 + 5 \pmod{29}$ i rute P2, $12 \cdot 1 + 5 \pmod{29}$ i rute P3, $12 \cdot 2 + 5 \pmod{29}$ i rute P4 osv. Vi bruker funksjonen REST til dette. Du kan flytte musen til celle P2, åpne REST funksjonen med funksjonsveiviseren og fylle den ut som vist under.

I celle P2 regner vi ut resten når vi deler $a \cdot 1 + b$ på 29. Når vi kopierer formelen nedover vil vi i celle P3 få beregnet resten når vi deler $a \cdot 2 + b$ på 29. I celle P3 beregnes resten når vi deler $a \cdot 3 + b$ på 29 osv. I vårt tilfelle der vi starter med bokstaven L som tilsvarer tallet 11,

så er det cellen der resten er 11 vi er interessert i. Ved å lete i tabellen vil vi se x verdi på 15 gir oss en rest på 11. Vi ønsker imidlertid at Excel skal finne denne verdien for oss uten av trenger å lete den opp manuelt. Funksjonen FINN.RAD hjelper oss med dette. Du kan i celle M6 fylle inn

FINN.RAD(L6;$P$2:$Q$30;2;USANN)

i feltet etter USANN i HVIS funksjonen. Det funksjonen gjør er at den søker etter verdien som står i L6 i P kolonnen. Når den har funnet hvilken rad denne verdien står, henter den ut verdien fra samme rad i Q kolonnen. Som vi ser så vil det i vårt tilfelle være 15. Du kan nå kopiere formlene ned til rad 30. Prøv å skrive inn setningen 'EFBBY YG TKD' og se om du får ut meldingen 'MATTE ER GØY'

RSA systemet

Begge de to krypteringssystemene vi til nå har beskrevet har sine svakheter. For det første er det med dagens teknologi enkelt å knekke koden. For det andre er systemene basert på at både sender og mottaker må kjenne nøkkelen. Dette er risikabelt og upraktisk. Vi skal nå se på et system som kalles RSA systemet, der koden er vesentlig vanskeligere å knekke. En annen styrke med RSA systemet er at det er det vi kaller et "public key" system. Det betyr at både kodesystem og nøkkel for koding er kjent. Nøkkel for dekoding er derimot hemmelig. Vi skal her gi en kortfattet beskrivelse av hvordan RSA systemet fungerer. For en mer fullstendig beskrivelse se f. eks Tallære av Kjartan Tvete.

Vi tar først for oss hvordan vi kan kode et tall i RSA systemet. Først må vi velge oss to primtall som vi kaller for p og q. I virkeligheten brukes det gjerne primtall som inneholder flere hundre siffer. Vi nøyer oss med litt færre siffer og velger oss f. eks $p = 5$ og $q = 7$. Produktet av disse tallene kaller vi n og vil i vårt tilfelle bli $n = 35$. Vi skal i tillegg velge oss et tredje tall som vi kaller for r som skal være relativt primisk med $\varphi(n)$. I vårt tilfelle vil $\varphi(35) = 24$. La oss velge $r = 11$. Den offentlige nøkkelen vil være $n = 35$ og $r = 11$.

Hvis vi har et tall x som skal kodes beregnes det kodede tallet k ved hjelp av kongruensen

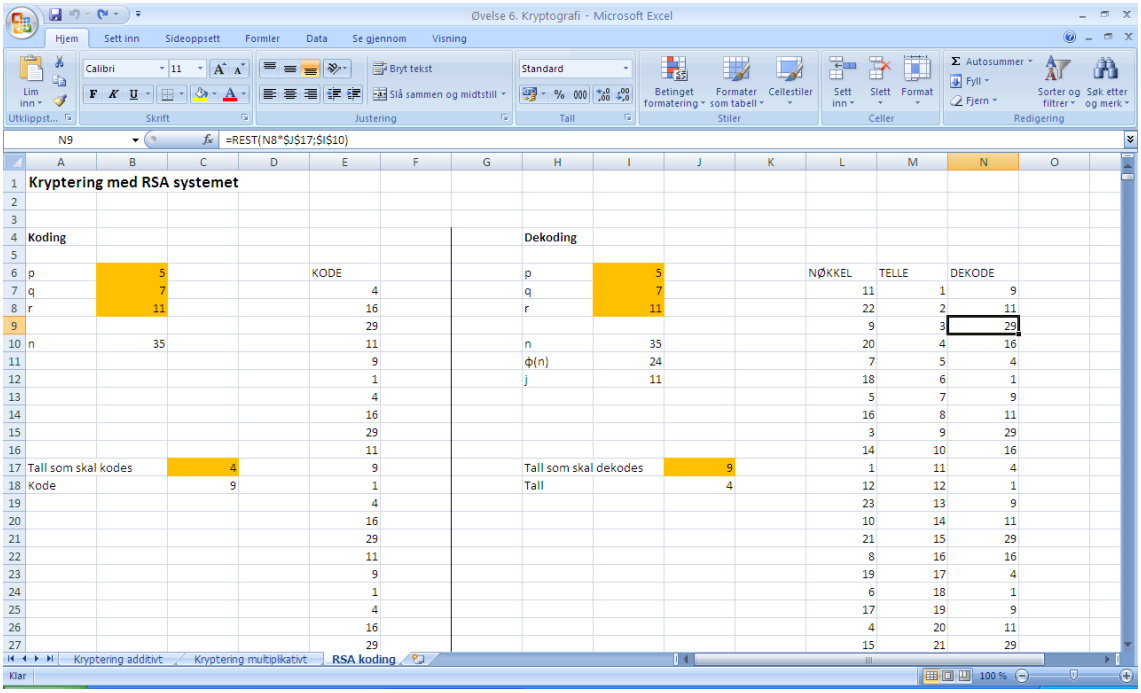
$$x^r \equiv k \pmod{n}$$

Hvis vi skal kode tallet 4 i vårt eksempel må vi finne k ut i fra kongruensen

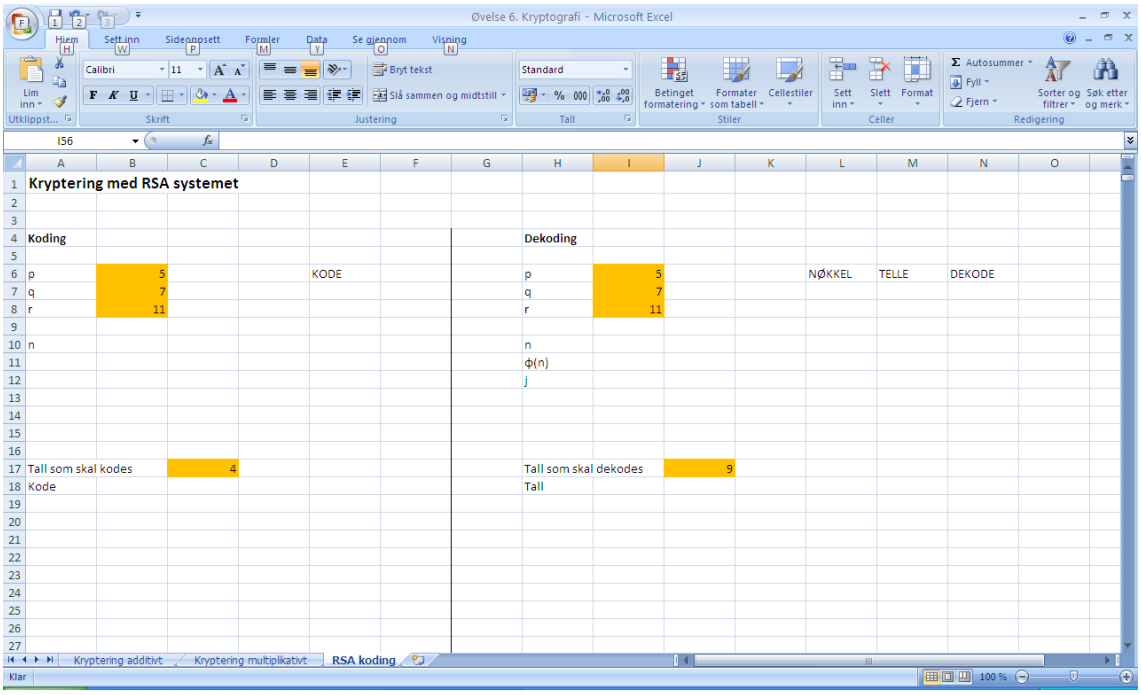
$$4^{11} \equiv k \pmod{35}$$

Ved hjelp av potensregelen eller andre metoder kan en vise at $k = 9$ i dette tilfelle. Med andre ord vil tallet 4 kodes til tallet 9 i dette kodesystemet.

Vi er nå klare til å lage et regneark som koder et tall i RSA systemet. Regnearket vi skal lage skal se ut som vist under.



Vi starter med å skrive inn teksten og nøkkelverdiene som vist under



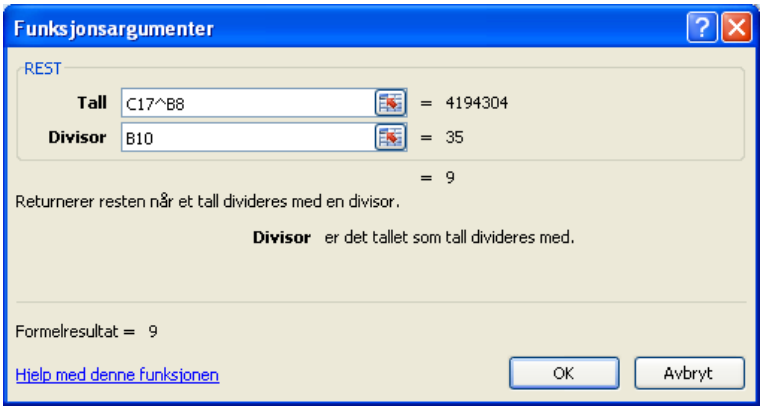
Feltene vi skal fylle ut har jeg valgt å merke med gult. De øvrige cellene beregner Excel for oss. La oss først se på hvordan vi kan kode et tall i Excel. Vi har skrevet inn p, q og r. Det første vi skal gjøre er å beregne n. (I virkeligheten vil vi kjenne n men ikke p og q.) Den finner vi ved å gange p med q. I celle B10 kan du derfor skrive inn

=B6*B7

Den kodede meldingen beregnes (vårt talleksempel) ved hjelp av kongruensen

$$4^{11} \equiv k \pmod{35}$$

I Excel kan vi finne k ved hjelp av REST funksjonen. Ved å skrive inn funksjonen



skulle vi ha fått beregnet resten og dermed koden. I dette talleksempelet går det fint, men med litt større tall så klarer dessverre ikke Excel lenger å regne ut resten med REST funksjonen. Om vi endrer r til 17 får vi f. eks problemer. Vi må derfor finne en annen måte å beregne resten på. Det finnes ikke en enkel måte å gjøre dette på, men ved å lage en tabell kan en beregne resten for ganske store verdier. Vi skal lage denne tabellen i E kolonnen. I første rad skal vi beregne resten når vi dividerer 4^1 på 35. I neste rad skal vi beregne resten når vi dividerer 4^2 på 35, i tredje rad skal vi beregne resten når vi dividerer 4^3 på 35 osv. I første raden som er celle E7 skriver du inn formelen

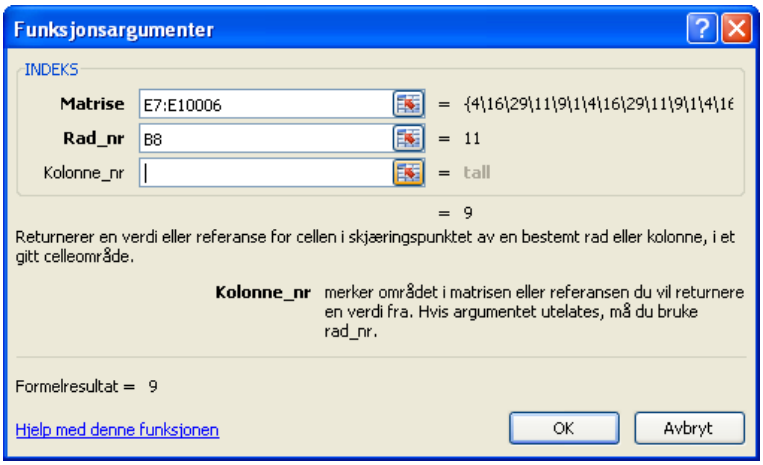
=REST(C17;B10)

Du kan eventuelt bruke funksjonsveiviseren. I de neste radene skal vi utnytte setningen at hvis $a \equiv b \ (mod\ n)$ gjelder vil også $a \cdot c \equiv b \cdot c \ (mod\ n)$. I celle E8 skal vi utnytte resultatet fra celle E7 ved at vi skriver inn formelen

Vi tar da svaret vi fant i celle E7 og multipliserer med tallet vi skal kode. Det finner vi i rute C17 og er 4 i vårt tilfelle. Denne formelen kan du nå kopiere nedover. I celle E9 vil den da ta utgangspunkt i resultatet fra E8 og beregne resten etter at resultatet er multiplisere dette med 4. Jeg har kopiert den slik at jeg har 10000 rader i tabellen. Vi kan da ta hånd om situasjoner helt opp til r verdier på 10000. Vi har valgt $r = 11$. Løsningen på kongruensen

$$4^{11} \equiv k \pmod{35}$$

finner vi i rad 11 i tabellen vår. Vi ser at det er tallet 9. Det stemmer med det vi fant ut tidligere. Vi skal la Excel lete opp verdien for oss. Du kan flytte musen til rute C18 og fylle ut INDEKS funksjonen som vist under



Vi søker gjennom tabellen vår og plukker ut verdien i raden som er angitt i celle B8. I vårt tilfelle blir det rad 11 og der finner vi verdien 9.

Prøv å kode tallene 8 og 13 med de nøklene vi har valgt. Se om du får ut verdiene 22 og 27. Velg en annen nøkkel, f. eks $p = 5, q = 11$ og $r = 23$. Prøv å kode tallene 2, 9 og 12 og se om du får 8, 14 og 23 som svar.

Som nevnt innledningsvis i avsnittet om RSA systemet må r være relativt primisk med φ. Det kan være greit å lage en liten test på om dette er tilfelle. Funksjonen

tester dette og gir beskjed om å velge en annen r dersom dette ikke er tilfelle. Du kan f. eks sette inn formelen i celle C8.

Vi skal nå se på hvordan vi bruke Excel til å dekode en melding i RSA systemet. Hvis vi har et tall k som skal dekodes til x gjøres det ved å løse kongruensen

$$k^j \equiv x \pmod{n}$$

Problemet her er at j er ukjent, det er dette som er den hemmelige nøkkelen. Den hemmelige nøkkelen j kan vi beregne ved å løse kongruensen

$$r \cdot j \equiv 1 \pmod{\varphi(n)}$$

Når vi kjenner p og q kan vi beregne $\varphi(n)$ og dermed løse kongruensen. Selv om n er kjent vil vi i praksis bruke så store tall at selv kraftige datamaskiner ikke vil klare å beregne hva p og q er i løpet av rimelig tid. En må altså kjenne p og q for å kunne knekke koden.

Vi er nå klar til å ta fatt på å lage den delen av regnearket der vi dekoder en melding. Det første vi skal gjøre er å beregne $n, \varphi(n))$ og j. Det skal vi gjøre i cellene I10 til I12. I celle I10 beregner vi n som vil være gitt ved formelen

=I6*I7

Når vi velger p og q til å være primtall vil $\varphi(n) = (p-1)(q-1)$. Formelen i rute C11 blir da

=(I6-1)*(I7-1)

Til slutt skal vi se på hvordan j kan beregnes. Dessverre er det ikke noe enkel måte å gjøre dette på og vi må benytte oss av en tabell. Vi lager oss en tabell i L og M kolonnen. M kolonnen skal være en tellekolonne som starter på 1 og går ned til f. eks 10000. Du kan la 1 stå i celle M7. I L kolonnen skal vi i celle L7 regne ut $r \cdot 1 \pmod{\varphi}$, i celle L8 skal vi regne ut $r \cdot 2 \pmod{\varphi}$, i celle L9 skal vi regne ut $r \cdot 3 \pmod{\varphi}$. Dette gjør vi til vi har fått 10000 rader i tabellen. Uttrykket du kan skrive inn i L7 blir

Verdien for r finner vi i celle I8, og verdien for φ finner vi i celle I11. Vi bruker dollartegn slik at vi kan kopiere formelen. Denne formelen kan du nå kopiere ned slik at du får 10000 rader. Det som nå gjenstår er å finne ut hvilken rad vi finner en rest på 1. I vårt tilfelle kan vi se at det er i rad 11 og at $j = 11$ gir en rest på 1. Vi skal imidlertid la Excel lete frem raden som gir rest på 1 for oss. Funksjonen FINN.RAD kan brukes til dette. Du kan fylle den ut som vist på neste side og plassere den i celle I12.

Vi har først merket at det er L og M kolonnen vi skal søke i. Det har vi gjort i feltet Matrise. Søkeverdien som er 1 i vårt tilfelle er det vi skal søke etter. Funksjonen FINN.RAD vil alltid søke etter denne verdien i første kolonnen som er L kolonnen i vårt tilfelle. Når vi angir Kolonneindeks til å være 2 betyr det at den skal hente ut verdien fra tilsvarende rad i kolonne 2, altså M kolonnen. Vi tar i siste feltet med USANN for å indikere at det er eksakt 1 vi leter etter.

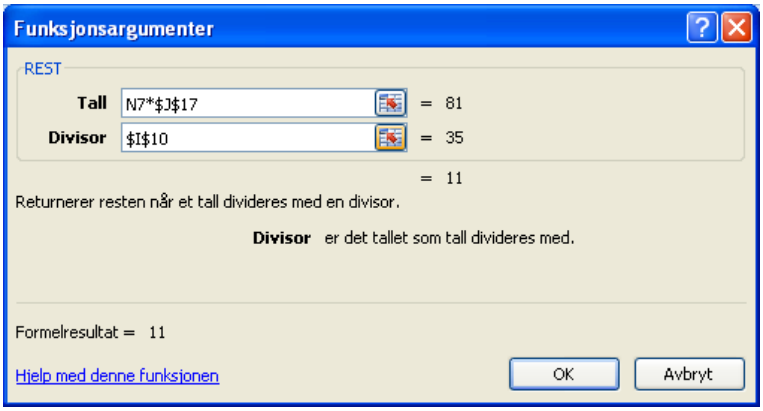
Nå som vi har funnet j kan vi løse kongruensen

$$k^j \equiv x \pmod{n}$$

for å finne ut hva x blir når vi dekoder k. I prinsippet kunne vi nå brukt REST funksjonen for å beregne hva resten blir når vi deler k^j på n men dessverre skal ikke tallene bli særlig store før REST funksjonen ikke klarer å håndtere det. Vi lager oss derfor en tabell etter samme mønster som når vi kodet melding i sted. Vi bruker nøyaktig samme prinsippet her og vi utnytter at vi allerede har en tellekolonnen i M kolonnen. I N kolonnen beregner vi derfor resten vi får når vi lar j løpe fra 1 til 10000. I celle N7 kan du skrive inn formelen

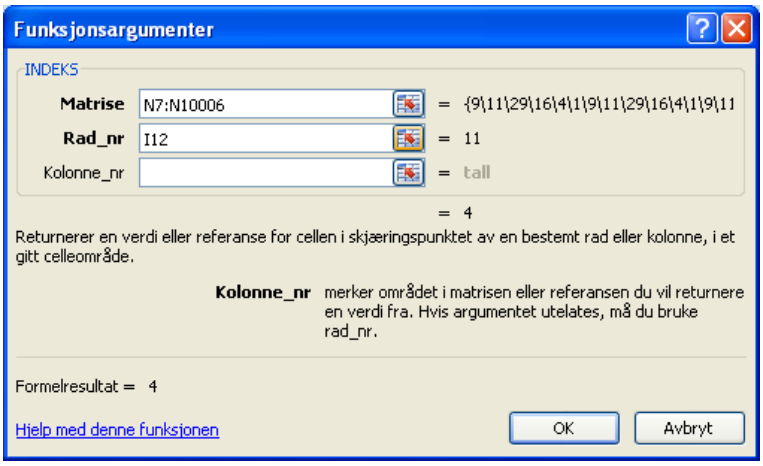
=REST(J17;I10)

I rute N8 kan du skrive inn



som du kopierer ned til rad 10000. Det som siste som gjenstår før regnearket vårt er ferdig er å fiske ut den riktige x verdien. Den finnes i vårt tilfelle i rad nummer 11 i N kolonnen. Vi

ser at når vi dekoder 9 får vi 4. Vi kan la Excel lete frem verdien for oss ved å bruke INDEKS funksjonen. Den kan du fylle ut som vist under.



Vi søker her i N kolonnen og vi søker etter raden som tilsvarer *j* verdien vår. Prøv å dekode tallene 8, 14 og 23 og se om du får 2, 9 og 12 som svar

Øvelse 7. Diofantiske ligninger - med Euclids algoritme

Ligninger av typen $ax + by = c$ der en er på jakt etter heltallsløsninger kalles gjerne for diofantiske likninger. Diofantiske ligninger kan løses på flere måter, blant annet ved å bruke Euclids algoritme. Boken Tallteori av Reinert Rinvold gir en grei beskrivelse av hvordan denne metoden fungerer. La oss se på hvordan metoden fungerer ved å studere likningen

$$17x + 73y = 3$$

Linkningen $ax + by = c$ har løsning hvis c er et multiplum av største felles faktor til a og b. I vårt eksempel er største felles faktor til 17 og 33 lik 1 så ligningen har løsning. Vi bruker nå Euclids algoritme på tallene 17 og 73. Dette gir oss

$$73 = 4 \cdot 17 + 5 \qquad (1)$$

$$17 = 3 \cdot 5 + 2 \qquad (2)$$

$$5 = 2 \cdot 2 + 1 \qquad (3)$$

Det neste vi skal gjøre er å finne et utrykk for høyre kolonne i uttrykkene over.

$$5 = 1 \cdot 73 - 4 \cdot 17 \qquad (4)$$

$$2 = 1 \cdot 17 - 3 \cdot 5 \qquad (5)$$

$$1 = 1 \cdot 5 - 2 \cdot 2 \qquad (6)$$

Vi setter nå inn utrykket for 2 fra linje 5 inn i linje 6. Dette gir oss

$$1 = 1 \cdot 5 - 2 \cdot (1 \cdot 17 - 3 \cdot 5)$$

Dette kan vi skrive som

$$1 = -2 \cdot 17 + 7 \cdot 5 \qquad (7)$$

Vi setter nå inn utrykket for 5 fra linje 4 inn i linje 7. Dette gir oss

$$1 = -2 \cdot 17 + 7 \cdot (1 \cdot 73 - 4 \cdot 17) \qquad (8)$$

Dette kan vi skrive som

$$1 = 7 \cdot 73 - 30 \cdot 17 \qquad (9)$$

Vi ser nå at $x = -30$ og $y = 7$ vil være en løsning av ligningen

$$17x + 73y = 1$$

og at $x = -90$ og $y = 21$ vil da være en løsning av ligningen

$$17x + 73y = 3$$

Den generelle løsningen kan vi skrive som

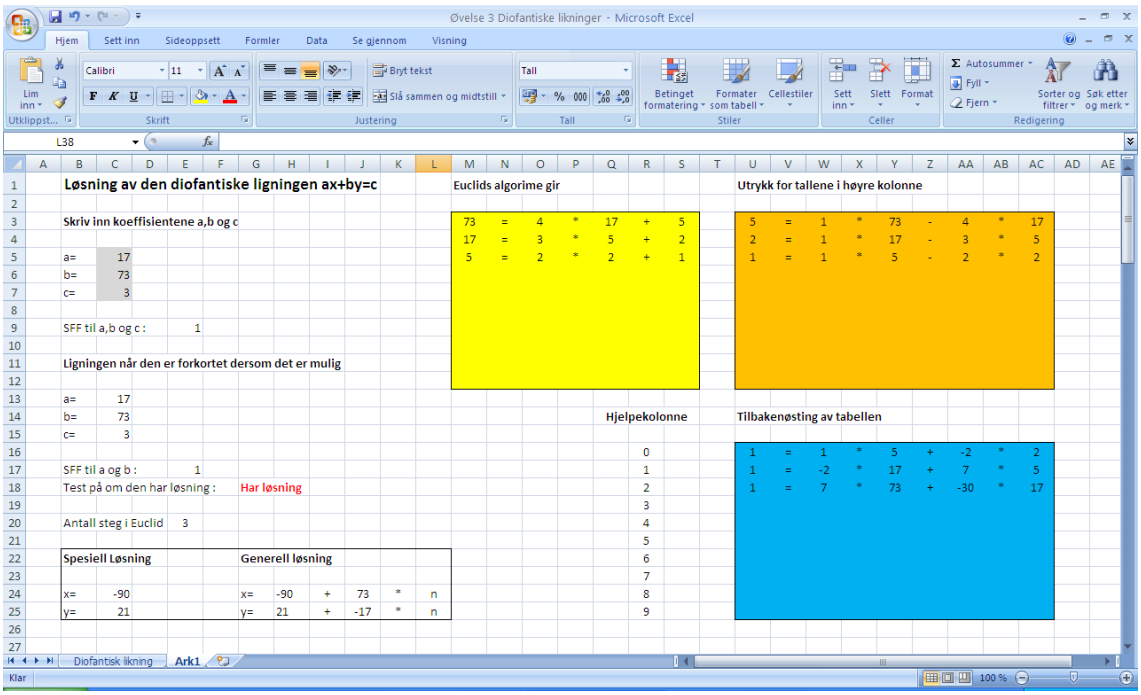
$$x = -90 + 73n$$

$$y = 21 - 17n$$

Det kan fort bli en del arbeid med å løse diofantiske ligninger på denne måten, spesielt hvis en må bruke mange steg i Euclids algoritme. Vi skal nå se på hvordan vi bruke Excel til å løse diofantiske ligninger ved bruk av Euclids algoritme.

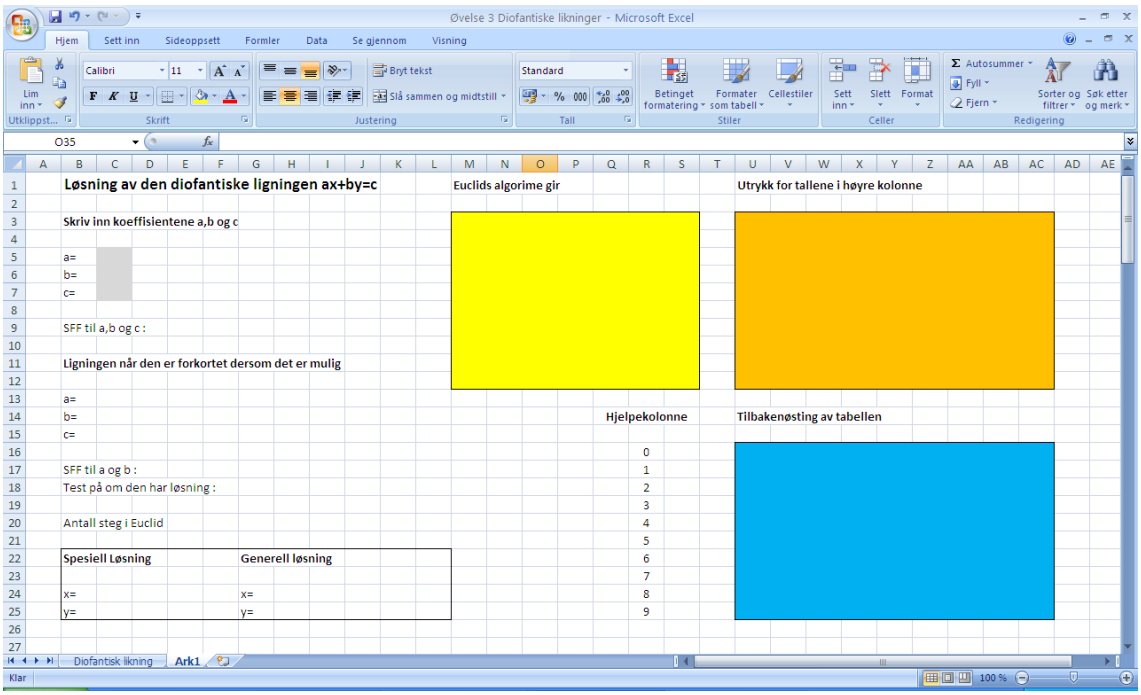
<u>Konstruksjon av regnearket</u>

Vi skal konstruere et regneark omtrent som vist på under.



Vi skal ta høyde for at vi må bruke inntil 10 steg i Euclids algoritme. Ved å ta høyde for 10 steg vil en kunne løse de fleste ligninger der tallene a og b består av inntil 6 siffer. Det vil også takle en del tilfeller med enda større tall. Det er selvsagt ikke noe i veien for å lage et regneark som tar høyde for enda flere steg, men jeg har valgt å begrense det til 10, siden jeg da får all informasjonen på en side, uten at det er behov for å scrolle. Dette regnearket vil foruten å gi løsningen på ligningen også vise stegene i Euclids algoritme og hvordan vi regner oss tilbake til løsningen av ligningen.

Det første vi skal gjøre er å skrive inn nødvendig tekst i regnearket. Du kan fylle ut regnearket som vist på neste side.



I de grå feltene skal vi skrive inn koeffisientene a, b og c. I fargede feltene skal selve utregningene gjennomføres. Vi kan bruke samme ligning som i sted ved konstruksjon av regnearket. Det vil si at du fyller inn tallene, 17, 73 og 3 i rute C5 til C7. Det neste vi skal gjøre er å finne største felles faktor til a, b og c slik at vi kan forkorte ligningen dersom det er mulig. Funksjonen SFF finner største felles faktor mellom de angitte tallene. Du kan derfor skrive inn =SFF(C5:C7) i rute E9. Det neste vi skal gjøre er å dele a, b og c på største felles faktoren. Dette skal vi gjøre i rute C13 til C15. Vi skal samtidig også gjøre en annen ting, og det er å eventuelt bytte om koeffisientene a og b slik at a blir minst og b blir størst. I rute C13 kan du skrive inn

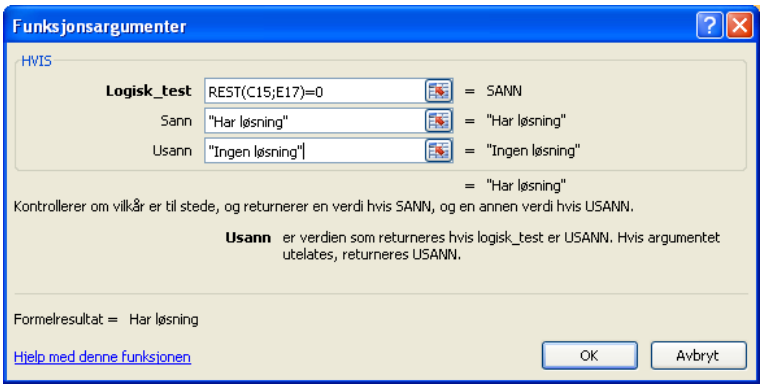
=MIN(C5/E9;C6/E9)

Regnearket vil da ta den minste verdien av a og b og dele den på største felles faktor. Tilsvarende kan du i rute C14 skrive inn

=MAKSA(C5/E9;C6/E9)

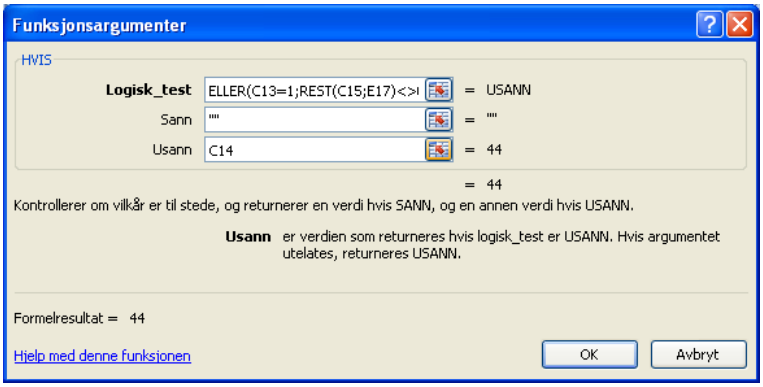
Regnearket vil da plassere den største av verdiene i rute C14. Tilslutt i rute C15 skriver du inn =C7/E9. Vi har nå fått gjort eventuelle forkortelser på ligningen og vi har også sørget for at den minste koeffisienten er plassert først.

Det neste vi skal sjekke er om ligningen har løsning. Ikke alle diofantiske ligninger har det og en enkel sjekk på om det finnes løsninger er å se om c er delelig på største felles faktor til a og b. I rute C17 beregner vi største felles faktor til a og b ved hjelp av funksjonen SFF som vi brukte i sted. I rute G19 skal vi teste om ligningen har løsning. For å gjøre det skal vi bruke HVIS funksjonen. Du kan åpne HVIS funksjonen ved hjelp av funksjonsveiviseren og fylle den ut som vist på neste side.



Det vi tester her er om c delt på største felles faktor har rest eller ikke. Dersom resten er 0 har ligningen løsning, men i motsatt fall har den ikke løsning.

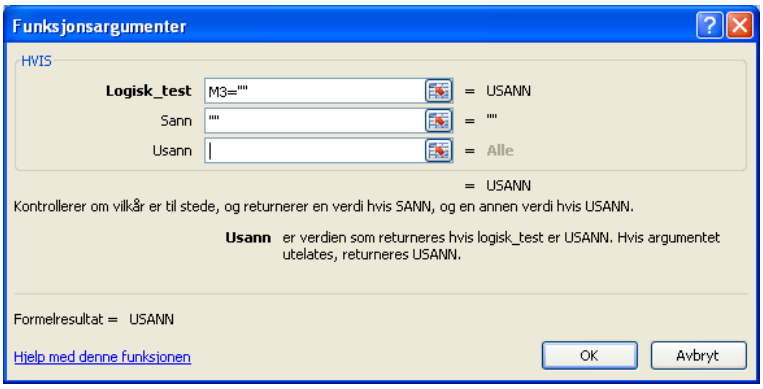
Vi er nå klar til å bruke Euclids algoritme på koeffisientene a og b. Dersom ligningen ikke har løsning ønsker vi at det gule feltet skal være blankt. Det er også et spesialtilfelle dersom $a = 1$ etter forkorting som vi må se spesielt på. Også i dette tilfelle skal det gule feltet være blankt. Vi skal i første linjen i gule feltet skrive inn uttrykk tilsvarende linje 1 i eksempelet i starten av øvelsen. For alle cellene i den første linjen må vi ta høyde for de to spesialtilfellene som vi nettopp har skissert. HVIS funksjonen hjelper oss med dette. Vi skal først se på rute M3. Du kan åpne HVIS funksjonen og fylle den ut som vist under.



I feltet etter Logisk_test står det:

ELLER(C13=1;REST(C15;E17)<>0)

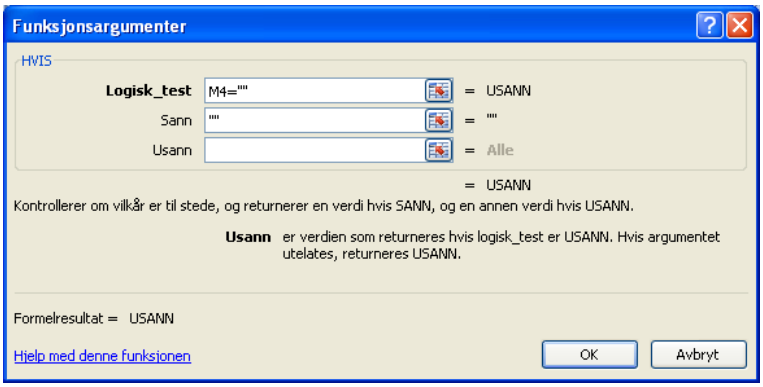
Det vi gjør her er at vi først tester om $a = 1$ det vil si om rute C13 er lik 1, eller om ligningen har løsning ved hjelp av REST funksjonen. Dersom resten er forskjellig fra 0 slik at ligningen ikke har løsning eller dersom $a = 1$ skrives bare en tom rute i celle M3. Når vi skal ha en tom rute skriver vi inn "". I de neste rutene i denne linjen skal vi benytte oss av en litt enklere variant av HVIS funksjonen. Vi skal sjekke om celle M3 er blank, og dersom den er det skal cellen vi står i være blank. I motsatt fall skriver vi inn den ønskede verdien. For cellene fra N4 til S4 skal vi bruke en HVIS funksjon der de to øverste linjene er som vist på neste side



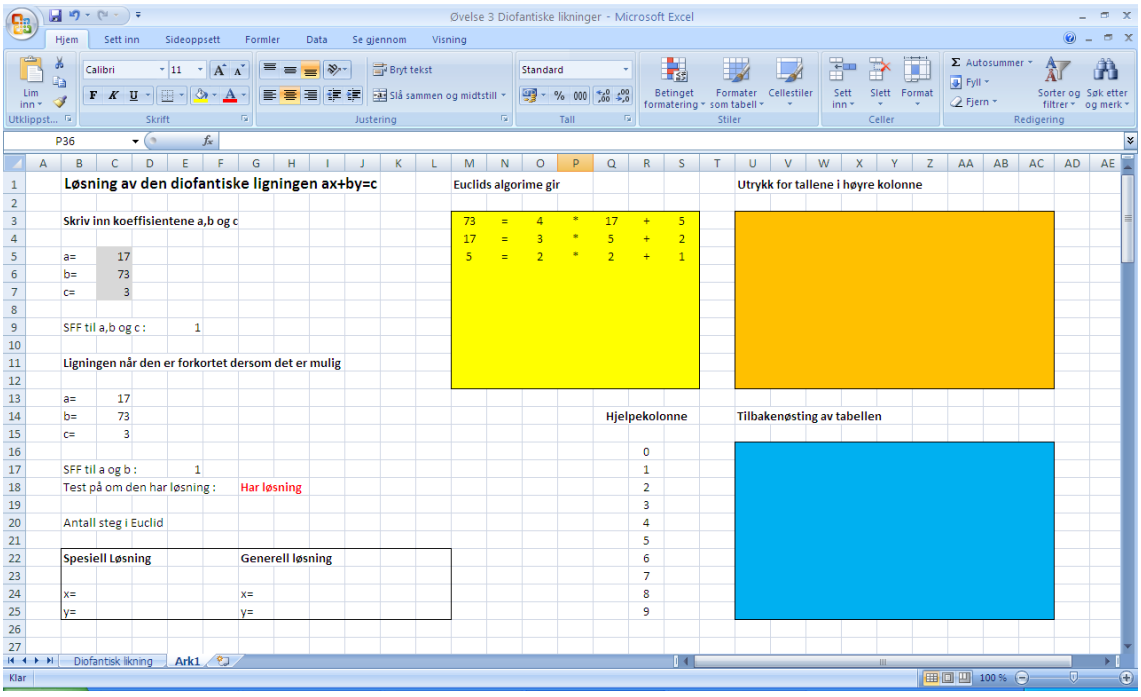
Hvis vi ser på celle N3, P3 og R3 skal det i feltet etter USANN stå = i celle N3, * i celle P3 og + i celle R3. Den neste cellen vi skal fylle ut er celle O3. Det vi skal beregne her er heltallsdelen av divisjonen $\frac{b}{a}$. I vårt eksempel vil det si heltallsdelen av $\frac{73}{17}$. I ruten etter USANN skriver du inn HELTALL(M3/C13). Vi går videre til rute Q3. Her skal verdien til b stå. I feltet etter USANN skriver du derfor inn C13. I rute S3 skal vi beregne resten av divisjonen $\frac{b}{a}$. I feltet etter USANN skriver du derfor inn REST(M3;C13). Den første linjen i Euclids algoritme skulle med det være ferdig.

Vi skal nå ta for oss linje 2 i det gule feltet. I denne linjen ønsker vi at linjen skal være blank hvis resten i foregående linje er lik 1. Vi ønsker også at linjen skal være blank dersom cellen med resten i foregående linje er 1. Vi starter med rute M4 og bruker HVIS funksjonen som vist under. Dersom resten i forrige linje er lik 1 eller dersom feltet er blankt vil celle M4 bli blank. I motsatt fall vil regnearket skrive inn verdien vi finner i celle Q3.

Også her skal vi bruke en litt enklere HVIS setning for rutene N4 til S4 der vi tester om rute N4 er blank eller ikke. For cellene N4 til S4 vil de første linjene i HVIS funksjonen se ut som vist på neste side.



I celle N4, P4 og R4 skriver dere i feltet etter USANN på tilsvarende måte som i sted inn tegnene =, * og +. I rute O4 skal vi beregne heltallsdelen av divisjonen $\frac{17}{5}$. Du kan derfor skrive inn HELTALL(Q3/S3) i feltet etter USANN. I rute Q4 skal resten vi fikk i forrige linje stå, det vil si at du kan skrive inn S3 i feltet etter USANN. Til slutt skal vi i rute S4 beregne resten av divisjonen $\frac{17}{5}$. Dette gjør vi ved at du skriver inn REST(Q3;S3)etter USANN. Vi har dermed fått fylt ut hele andre linjen. Du kan nå kopiere hele linjen ned til og med den siste linjen i det gule feltet. Regnearket ditt skal nå se omtrent slik ut:



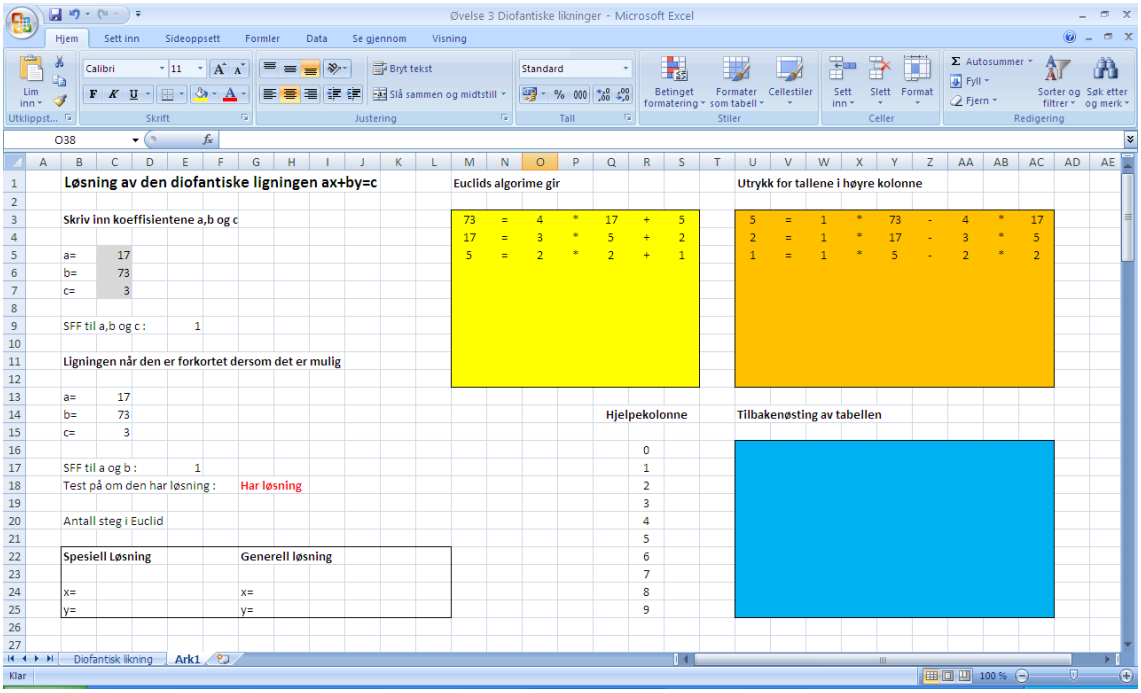
Test ut regnearkene med noen andre verdier for a, b og c og se at Excel utfører Euclids algoritme slik det skal.

I det oransje feltet skal vi finne et utrykk for resten for uttrykkene i det gule feltet. Dette er egentlig en ganske enkel operasjon. La oss ta feltene systematisk. I celle U3 skal resten stå, det vil si du kan skrive inn =S3 i denne cellen. I rute V3 skal det stå et likhetstegn dersom vi ikke har noen av spesialtilfellene. Da skal imidlertid ruten være blank. Dette løser vi at vi i celle V3 skriver =N3. Vi henter da det som står i celle N3. Dette vil vanligvis være

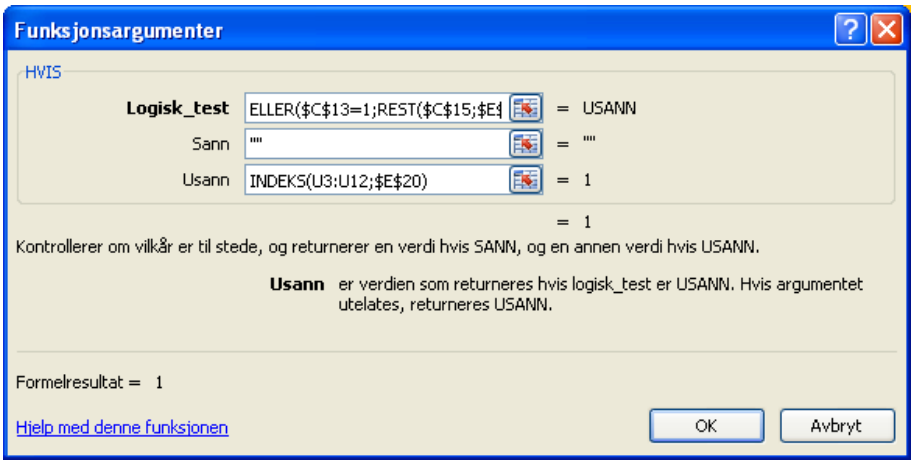
likhetstegnet, men dersom vi har et av spesialtilfellene vil ruten bli blank. Tilsvarende kan du i celle X3 og AB3 skrive inn =P3. I celle W3 skal vi ha inn et 1 tall om vi ser bort fra spesialtilfellene. Vi bruker en HVIS setning som vist under.

Vi sjekker om innholdet i rute O3 er blankt eller ikke. Dersom det er blankt skal også W3 være blank. I motsatt fall skal vi skrive inn et 1 tall. Egentlig kunne denne kolonnen vært utelatt, men vi har valgt å ta den med for fullstendighetens skyld. I rute Y3 skal vi ha inn verdien fra rute M3. Vi skriver derfor inn =M3. I rute Z3 skal vi ha inn et minustegn bortsett fra i spesialtilfellene. Vi bruker igjen en HVIS setning

I rute AA3 skal verdien fra rute O3 stå. Vi skriver derfor inn =03 i denne ruten. På tilsvarende måte skriver vi inn =Q3 i rute AC3. Når hele denne linjen er ferdig kan du kopiere den til linje 10 i det oransje feltet. Det gule og det oransje feltet skal med det være ferdig og regnearket ditt skal nå se ut som vist på neste side.



Det neste vi skal gjøre er at vi i det blå feltet skal la Excel nøste tilbake tabellen fra det oransje feltet. Dette vil tilsvare utregningene i linje 7, 8 og 9 i eksempelet som er beskrevet innledningsvis. Dette er den klart mest krevende delen av regnearket, og noen av formlene er litt kompliserte. I den øverste linjen i det blå feltet skal vi skrive inn den siste linjen i det oransje feltet. Det vil si den siste linjen med tall. Problemet vårt er at det kan variere fra ligning til ligning. Men det finnes en måte å løse dette på i Excel og det er ved å bruke INDEKS funksjonen. Vi har i den forbindelse behov for å vite hvor mange steg vi har i Euclids algoritme, og det skal vi beregne i celle E20. Du kan flytte musen til E20 og skrive inn følgende formel =ANTALL(U3:U12). Vi får da talt opp hvor mange steg vi har brukt i Euclids algoritme. La oss nå se på hvordan vi kan bruke den. I celle U16 skal vi skrive inn det som står i siste linjen i det oransje feltet, det vi si U5. Funksjonen INDEKS(U3:U12;3) ordner dette for oss. Funksjonen virker slik at den tar utgangspunkt i kolonnen fra U3 til U12. Den plukker deretter ut cellen som står i linjen som angitt etter semikolonet, det vil si linje 3 i det merkede område. Vi tar nå for oss celle U16 mer generelt. Vi skal la den ruten være blank hvis likningen ikke har løsning eller dersom vi har situasjonen der $a = 1$. Vi må derfor først bruke HVIS funksjonen. Den kan du fylle ut som vist på neste side.

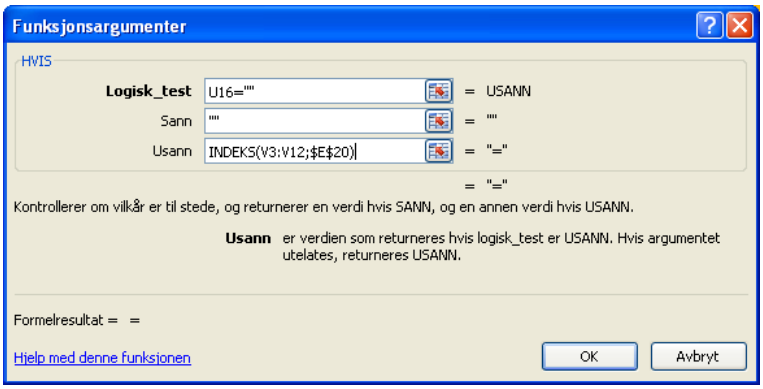


I skjermbilde over får vi ikke frem alt som står i feltet etter Logisk_test. Det som skal stå der er imidlertid

ELLER($C$13=1;REST($C$15;$E$17)<>0)

Det vi gjør her er å teste om $a = 1$ eller om vi har en situasjon der likningen ikke har løsning. Skulle en av disse to tilfellene inntreffe skal ruten være blank. Dersom det ikke er tilfelle skal verdien fra siste linjen i U kolonnen i det oransje feltet skrives inn. For å finne denne bruker vi INDEKS funksjonen som vist over. Vi lar område være U3:U12. Vi søker etter linjen som tilsvarer antall ledd i Euclids algoritme. Antall ledd i Euclids algoritme finner vi i rute E20. Siden vi etterpå skal kopiere formelen velger vi å bruke dollartegn og skrive $E$20 i indeks funksjonen.

Den neste ruten vi skal se på er V16. Vi må bruke HVIS funksjonen og INDEKS funksjonen også her, men vi kan forenkle den litt i forhold til i sted ved at vi tester om rute U16 er blank eller ikke. Funksjonen som skal stå i rute V16 blir derfor



Denne funksjonen kan du kopiere til rute W16, X16, Y16, AB16 og AC16. Excel vil hente verdiene fra tilsvarende kolonne i siste linjen i det oransje feltet. Rute Z16 og AA16 må vi se litt nærmere på siden de ikke er helt lik tilsvarende celle i det oransje område. I rute Z16 skal vi ha et pluss tegn nå, og ikke et minustegn som i det oransje feltet. Funksjonen

=HVIS(U16="";"";"+")

hjelper oss med dette. I rute AA16 skal vi ha motsatt fortegn av hva vi finner i tilsvarende celle i det oransje feltet. Vi må derfor modifisere denne cellen med et minustegn foran INDEKS funksjonen. Celle AA3 skal etter det se slik ut

=HVIS(U16="";"";-INDEKS(AA3:AA12;$E$20))

Vi skal nå se på linje 2 i det blå feltet. Dette er nok den mest kompliserte delen av regnearket. Vi skal lage linje 2 slik at den kan kopieres ned til og med linje 10 etterpå. Linje 2 i det blå feltet skal tilsvare linje 8 i eksempelet som er beskrevet innledningsvis. La oss først se på celle U17. Vi ønsker å stoppe utregningene og ha et blankt felt i ruten dersom verdien i celle Y16 er lik koeffisienten b eller dersom celle Y16 er blank. I motsatt fall skal vi skrive inn 1, som vi henter fra celle U16. Funksjonen vi skal bruke i celle U17 blir da

For de øvrige cellene i denne linjen skal vi sjekke om celle U17 er blank eller ikke. Dersom den er blank skal de andre cellene også være blank. Det betyr at for de øvrige rutene i denne linjen skal vi bruke en HVIS setning der de to første feltene er lik for cellene fra V17 til AC17.

Feltet etter USANN vil imidlertid være forskjellig for de ulike cellene. De enkleste cellene er de cellene med bare tegn. I feltet etter USANN kan du for cellene V17, X17, Z17 og AB 17 skrive inn de respektive tegnene. (=, *, + og *) Som nevnt tidligere tilsvarer linje 2 i det blå feltet linje 8 i eksempelet tidligere, det vil si uttrykket

$$1 = -2 \cdot 17 + 7 \cdot 5$$

I vårt eksempel skal det i rute Y17 stå 17. Denne verdien henter vi fra rute Y4. Generelt vil verdien i rute Y17 hentes fra den nest nederste raden med tall i Y kolonnen i det oransje feltet. Ved å bruke INDEKS funksjonen kan vi få dette til. Du kan i feltet etter USANN skrive inn

INDEKS($Y$3:$Y$12;$E$20-R17)

Den ønskede verdi blir da hentet. Vi velger å bruke dollartegn på området vi søker i, slik at funksjonen kan kopieres nedover. Rute AC17 kan fylles ut tilsvarende som Y17. Der skal vi hente verdien fra nest nederste rad i AC kolonnen. Etter USANN kan du derfor skrive inn

INDEKS($AC$3:$AC$12;$E$20-R17)

Det som gjenstår å beregne er koeffisientene som skal stå foran takkene i rute Y17 og AC17. I vårt eksempel vil det si koeffisientene foran 17 og 5. Koeffisienten som står i rute W17 er den samme som står i celle AA16. I feltet etter USANN kan du derfor skrive inn AA16. Vi ser nå på siste cellen i denne linjen, det vil si celle AA17. Vi går først tilbake til uttrykket

$$1 = 1 \cdot 5 - 2 \cdot (1 \cdot 17 - 3 \cdot 5)$$

som er beskrevet i det innledende eksempelet. Dette kan vi omfore til

$$1 = -2 \cdot 17 + 1 \cdot 5 - 2 \cdot (-3) \cdot 5$$

Dette kan vi igjen skrive som

$$1 = -2 \cdot 17 + (1 + 2 \cdot 3) \cdot 5$$

Det er uttrykket tilsvarende

$$1 + 2 \cdot 3$$

vi skal sette inn i celle AA17. Det betyr at i feltet etter USANN kan du skrive

W16-AA16*INDEKS($AA$3:$AA$12;$E$20-R17)

Fra rute W16 henter vi 1 tallet. Fra rute AA16 henter vi -2 men siden vi skal ha motsatt fortegn setter vi – foran AA16 i formelen. Til slutt bruker vi INDEKS formelen for å hente 3 tallet fra nest nederste rad i AA kolonnen i det oransje feltet. Linje 2 skal da være ferdig og den kan kopieres ned til siste linje i det blå feltet.

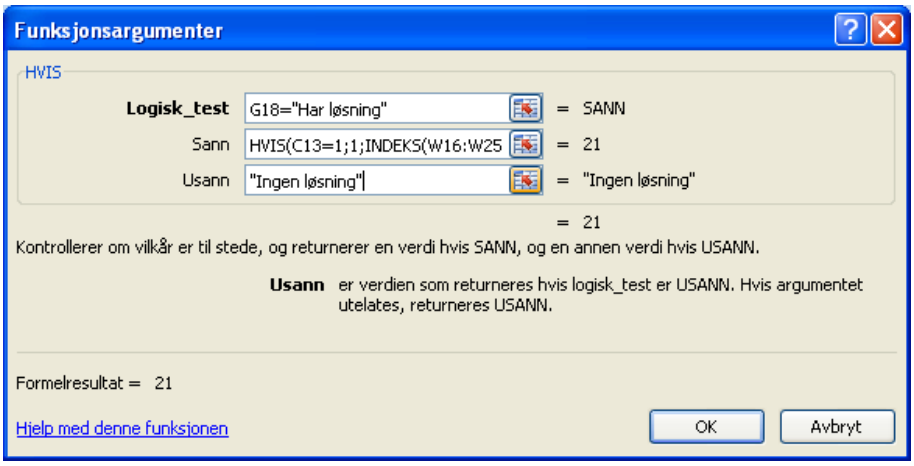
Nå som vi har tilbakenøstet tabellen i det blå feltet gjenstår det bare å finne løsningen. Hvis vi ser på det blå feltet vil $x = -30$ og $y = 7$ være en løsning av den diofantiske ligningen

$$17x + 73y = 1$$

I forhold til vår ligning som er

$$17x + 73y = 3$$

vil en løsningen være $x = -90$ og $y = 21$. Med andre ord vil x være lik AA18*C15 mens y vil være lik W18*C15. Når vi skal lage formelen som gir oss en spesiell løsning i celle C24 og C25 må vi ta hensyn til både om ligningen har løsning eller ikke og i tillegg ta høyde for hva løsningen blir dersom $a = 1$. For å få dette til må vi bruke en nøstet HVIS setning. Vi ser først på celle C25. Den skal se ut som vist under



Vi tester først om ligningen har løsning eller ikke. Hvis den ikke har løsning skal det i rute C25 stå Ingen løsning. Vi skriver derfor i feltet etter USANN ”Ingen løsning”. Hvis ligningen har løsning skal vi i feltet etter SANN skrive inn hva løsningen blir. Problemet er bare det at det blir forskjellig løsning om $a = 1$ eller ikke. For å ta høyde for det må vi bruke en HVIS setning i feltet etter SANN. Hele setningen er ikke kommet med i skjermbilde over, men den er gjengitt under.

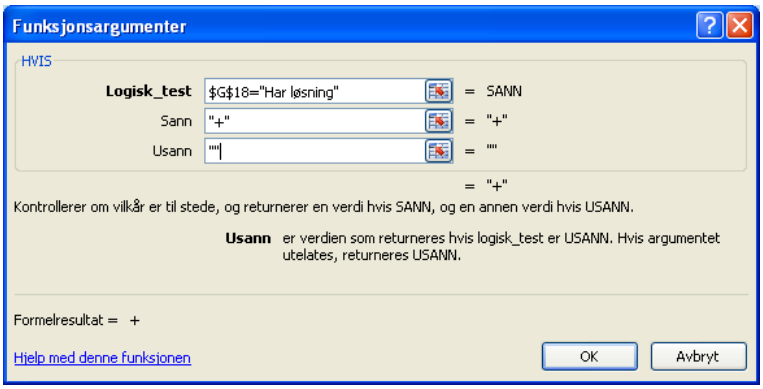
HVIS(C13=1;1;INDEKS(W16:W25;E20)*C15)

Vi tester først på C13 er lik 1. Dersom den er det, vil vi kunne sette $y = 1$. Dersom C13 ikke er lik 1 må vi hente løsningen fra W kolonnen i det blå feltet. Vi bruker INDEKS funksjonen til det. Til slutt må vi multiplisere resultatet fra INDEKS funksjonen med c som vi finner i C15.

Løsningen for x blir ganske lik den til y. Forskjellen er det som skal stå i HVIS setningen i feltet etter SANN. Setningen blir i dette tilfelle

HVIS(C13=1;C15-C14*C25;INDEKS(AA16:AA25;E20)*C15)

Vi har nå funnet en spesiell løsning til ligningen. Det siste som gjenstår er å finne en generell løsning. Vi ser først på den generelle løsningen for x. I rute H24 skal vi skrive inn den spesielle løsningen som vi finner i rute C24. Skriv derfor inn =C24 i celle H24. I rute I24 skal vi ha inn et plusstegn dersom det finnes løsning. Funksjonen



løser den jobben for oss. Tilsvarende funksjon kan brukes for gange tegnet i rute K24 og n i rute L24. I rute J24 skal vi ha inn verdien av b dersom ligningen har løsning. Du kan bruke samme HVIS setning som over, bare at du skriver inn C14 istedenfor + tegnet. Den generelle løsningen for y finnes på tilsvarende måte. Husk bare på at du må ha et minustegn foran koeffisienten a. Merk at løsningen som vi har angitt er løsningen av ligningen der vi har brukt koeffisientene i cellene B13 til B15.

Regnearket skal nå være klar til bruk. Test det ut på noen likninger og se hvordan det fungerer.