Kapittel 27

Litt mer tallteori

I dette kapitlet fortsetter vi med mer tallteori. Vi ser blant annet på det kinesiske restteoremet, Fermats lille teorem, og Eulers φ-funksjon.

Det kinesiske restteoremet

Vi skal nå se på hvordan vi kan løse et likningssystem bestående av flere kongruenser med ulik modulus:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

Vi begynner med å se på systemer av to kongruenslikninger, for å få tak i noen av ideene vi trenger uten at det blir altfor mye å holde styr på. Etterpå tar vi for oss det generelle tilfellet med r likninger, og beviser *det kinesiske restteoremet*, som beskriver nøyaktig hva løsningene av et slikt system er.

Bakgrunnen for det litt underlige navnet «det kinesiske restteoremet» er at den eldste kjente beskrivelsen av et problem som tilsvarer et system av kongruenslikninger ble gitt i den omtrent 1500 år gamle kinesiske teksten 孙子算经 (*Sunzi Suanjing*).

La oss først se på et enkelt eksempel.

Eksempel Vi vil løse systemet

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{4} \end{cases}$$

Vi kan observere at hvis to tall er kongruente modulo $12 = 3 \cdot 4$, så er de også kongruente modulo både 3 og 4. For å sjekke om et gitt tall x er en løsning av systemet, er det altså tilstrekkelig å sjekke om x mod 12 er en løsning.

Vi lager en tabell der vi skriver opp både $x \bmod 3$ og $x \bmod 4$ for forskjellige verdier av $x \bmod 12$:

$x \bmod 12$:	0	1	2	3	4	5	6	7	8	9	10	11
$x \bmod 3$:	0	1	2	0	1	2	0	1	2	0	1	2
$x \bmod 4$:	0	1	2	3	0	1	2	3	0	1	2	3

Vi ser i tabellen at det er ett tilfelle der vi får både $x \equiv 1 \pmod 3$ og $x \equiv 3 \pmod 4$ samtidig, og det er når x er kongruent med 7 modulo 12. Alle løsninger av systemet vårt er altså gitt ved:

$$x \equiv 7 \pmod{12}.$$

Nå har vi løst systemet, men la oss se litt mer på tabellen vi lagde. Vi kan stokke om på den slik:

$x \bmod 12$:	0	9	6	3	4	1	10	7	8	5	2	11
$x \bmod 3$:	0	0	0	0	1	1	1	1	2	2	2	2
$x \bmod 4$:	0	1	2	3	0	1	2	3	0	1	2	3

Da er det lett å se at ethvert system på formen

$$\begin{cases} x \equiv a \pmod 3 \\ x \equiv b \pmod 4 \end{cases}$$

har en løsning, og løsningen er entydig modulo 12. Hvis vi for eksempel har $a = 0$ og $b = 1$, så gir tabellen at løsningen er $x \equiv 9 \pmod{12}$. Hvis vi har $a = 2$ og $b = 3$, så er løsningen $x \equiv 11 \pmod{12}$. ♦

Med relativt primiske moduluser

La oss nå se på et vilkårlig system

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

av to likninger. Vi antar at de to modulusene m og n er relativt primiske, for det viser seg at det gjør ting mye greiere (mer om dette etterpå).

Kan vi klare å finne løsningen på et slikt system på en enklere måte enn ved å lage en tabell slik som i eksemplet? Siden vi antar at $m \perp n$, vet vi fra tidligere at det finnes heltall u og v slik at $mu + nv = 1$. Da har vi følgende:

$$mu \equiv 0 \pmod m \qquad nv \equiv 1 \pmod m$$
$$mu \equiv 1 \pmod n \qquad nv \equiv 0 \pmod n$$

La c være følgende tall:

$$c = anv + bmu$$

Da er c en løsning av systemet, siden vi har

$$c = anv + bmu \equiv a \cdot 1 + b \cdot 0 = a \pmod{m}$$
$$c = anv + bmu \equiv a \cdot 0 + b \cdot 1 = b \pmod{n}$$

Vi kan dessuten observere at løsningen er entydig modulo mn: Hvis x er en løsning av systemet, så må x være kongruent med c modulo både m og n. Det vil si at $m|(x-c)$ og $n|(x-c)$, og det følger at $mn|(x-c)$. Da har vi $x \equiv c \pmod{mn}$. Alle løsninger av systemet er altså kongruente med c modulo mn.

Vi oppsummerer det vi har vist nå i et resultat for følgende likningssystem:

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Anta at m og n er relativt primiske, og la u og v være heltall slik at $mu + nv = 1$. Da er alle løsninger av systemet gitt ved

$$x \equiv anv + bmu \pmod{mn}.$$

(Når vi skal velge tallene u og v er det egentlig ikke nødvendig at vi har $mu + nv = 1$; det viktige er at u er en invers til m modulo n og at v er en invers til n modulo m.)

Eksempel Vi løser systemet

$$\begin{cases} x \equiv 4 \pmod{10} \\ x \equiv 9 \pmod{17} \end{cases}$$

ved å bruke resultatet ovenfor. Modulusene 10 og 17 er relativt primiske, og ved å bruke Euclids algoritme får vi:

$$10 \cdot (-5) + 17 \cdot 3 = 1.$$

Det betyr at vi kan velge $u = -5$ og $v = 3$. Løsningen av systemet er:

$$\begin{aligned} x &\equiv a \cdot n \cdot v + b \cdot m \cdot u \\ &= 4 \cdot 17 \cdot 3 + 9 \cdot 10 \cdot (-5) \\ &= -246 \equiv 94 \pmod{170}. \end{aligned}$$

♦

Ikke relativt primiske moduluser. Hvorfor antok vi at de to modulusene i systemet vårt skulle være relativt primiske? La oss se på et par eksempler som viser hva som kan skje hvis de ikke er det.

Eksempel Vi ser på systemet

$$\begin{cases} x \equiv 4 \pmod{8} \\ x \equiv 9 \pmod{26} \end{cases}$$

der de to modulusene 8 og 26 har en felles faktor 2. Her medfører den første kongruensen at x må være et partall, mens den andre medfører at x må være et oddetall. Dermed finnes det ingen x som oppfyller begge kongruensene. ♦

Eksempel Vi ser på systemet

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 9 \end{cases}$$

der de to modulusene 6 og 9 har en felles faktor 3. Ved å prøve oss frem med alle tallene mellom 0 og $6 \cdot 9 = 54$ finner vi ut at både 14, 32 og 50 er løsninger av systemet. ♦

Hvis modulusene m og n ikke er relativt primiske, kan det altså hende at systemet ikke har noen løsning, eller at det har flere forskjellige løsninger modulo mn. Men hvis m og n *er* relativt primiske, har vi vist både at det finnes en løsning, og at den er entydig modulo mn. La oss generalisere dette resultatet til systemer med vilkårlig mange likninger.

Med vilkårlig mange likninger

Nå tar vi for oss det generelle tilfellet, altså et system med vilkårlig mange likninger. Da vi skulle løse systemer av to likninger antok vi at modulusene var relativt primiske. Nå vil vi anta at hver modulus er relativt primisk til alle de andre. Vi definerer et navn på denne egenskapen:

Definisjon 27.1 Parvis primske likinger

La $n_1, n_2, \ldots, n_r$ være en liste med tall. Vi sier at disse tallene er *parvis relativt primiske* dersom n_i er relativt primisk til n_j for alle $i \neq j$.

Eksempel Tallene 4, 7 og 15 er parvis relativt primiske, siden vi har $4 \perp 7$ og $4 \perp 15$ og $7 \perp 15$. ♦

Eksempel Tallene 5, 17, 12 og 32 er ikke parvis relativt primiske, fordi 12 og 32 ikke er relativt primiske. ♦

Vi viser først at hvis vi har en liste med tall som er relativt primiske, så er det å være kongruent modulo alle disse tallene det samme som å være kongruent modulo produktet deres:

La $m_1, m_2, \ldots, m_r$ være naturlige tall som er parvis relativt primiske, og la

$$M = m_1 \cdot m_2 \cdots m_r$$

være produktet av disse tallene. Da er to tall kongruente modulo M hvis og bare hvis de er kongruente modulo alle tallene $m_1, m_2, \ldots, m_r$. Med andre ord: For alle heltall a og b har vi at

$$a \equiv b \pmod{M} \iff \begin{cases} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \\ \quad \vdots \\ a \equiv b \pmod{m_r} \end{cases}$$

Det er lett å se at dersom a og b er kongruente modulo M, så er de også kongruente modulo hver m_i: Siden $m_i | M$ og $M | (a - b)$, gir det at $m_i | (a - b)$.

Anta nå at a og b er kongruente modulo alle tallene $m_1, m_2, \ldots, m_r$, altså at alle disse tallene deler $(a - b)$. Da får vi at $M | (a - b)$, altså at $a \equiv b \pmod{M}$.

Nå er vi klare for å vise det kinesiske restteoremet. Dette er helt tilsvarende som resultatet som vi beviste over, men med et system bestående av vilkårlig mange likninger istedenfor bare to.

Vi ser på det følgende systemet av kongruenslikninger:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

Anta at modulusene $m_1, m_2, \ldots, m_r$ er parvis relativt primiske, og la $M = m_1 \cdot m_2 \cdots m_r$ være produktet av modulusene. Da har systemet en entydig løsning modulo M.

Vi kan finne løsningen av systemet på følgende måte. For hver $i \in \{1, 2, \ldots, r\}$: La $M_i = M/m_i$, og la k_i være en invers til M_i modulo m_i. Løsningen av systemet er da gitt ved:

$$x \equiv \sum_{i=1}^{r} a_i M_i k_i \pmod{M}.$$

La oss først sjekke at det går an å gjøre det vi sier i resultatet. Vi sa at hver k_i skal være en invers til M_i modulo m_i. Kan vi være sikre på at det finnes en slik invers? Vel, vi har antatt at modulusene er parvis relativt primiske, og vi har definert M_i til å være produktet av alle modulusene unntatt m_i. Det medfører at M_i og m_i er relativt primiske, og dermed har M_i en invers modulo m_i.

Så vil vi sjekke at vi virkelig får en løsning ved å gjøre det resultatet sier. La

$$c = \sum_{i=1}^{r} a_i M_i k_i.$$

Vi vil vise at dette tallet er en løsning av alle kongruensene i systemet. Hvis vi lar l være et vilkårlig tall i mengden $\{1, 2, \ldots, r\}$, vil vi altså vise at vi har $c \equiv a_l \pmod{m_l}$. Vi kan først se at enhver M_j med $j \neq l$ inneholder m_l som en faktor, så alle disse blir bare 0 modulo m_l. Dermed har vi:

$$c = \sum_{i=1}^{r} a_i M_i k_i \equiv a_l M_l k_l \pmod{m_l}.$$

Men siden k_l er en invers til M_l modulo m_l har vi $M_l k_l \equiv 1 \pmod{m_l}$, og vi får

$$c \equiv a_l M_l k_l \equiv a_l \cdot 1 \equiv a_l \pmod{m_l}.$$

Siden dette holder for hver $l \in \{1, 2, \ldots, r\}$, har vi:

$$\begin{aligned} a_1 &\equiv c \pmod{m_1} \\ a_2 &\equiv c \pmod{m_2} \\ &\vdots \\ a_r &\equiv c \pmod{m_r} \end{aligned}$$

Dermed kan vi bruke resultatet ovenfor og få følgende ekvivalenser:

$$\begin{aligned} x \equiv c \pmod{M} &\iff \left\{ \begin{aligned} x &\equiv c \pmod{m_1} \\ x &\equiv c \pmod{m_2} \\ &\vdots \\ x &\equiv c \pmod{m_r} \end{aligned} \right\} \\ &\iff \left\{ \begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned} \right\} \end{aligned}$$

Vi har dermed vist at løsningene av systemet er nøyaktig de tallene som er kongruente med c modulo M.

Eksempel Vi løser systemet

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{5} \end{cases}$$

Siden modulusene er parvis relativt primiske, sier det kinesiske restresultatet at systemet har en løsning, som er entydig modulo $M = 3 \cdot 4 \cdot 5 = 60$. La oss nå konstruere løsningen etter oppskriften i resultatet. Vi får

$$M_1 = 20, \qquad M_2 = 15, \qquad M_3 = 12.$$

Vi vet at k_1 skal være en invers til $M_1 = 20$ modulo $m_1 = 3$. Men siden $20 \equiv 2 \pmod 3$ er dette det samme som en invers til 2 modulo 3. Det er lett å se at 2 er sin egen invers modulo 3, siden $2 \cdot 2 = 4 \equiv 1 \pmod 3$. Vi regner ut de andre inversene vi trenger, og får

$$k_1 = 2, \qquad k_2 = 3, \qquad k_3 = 3.$$

Dermed har vi løsningen

$$\begin{aligned} x &\equiv a_1 \cdot M_1 \cdot k_1 + a_2 \cdot M_2 \cdot k_2 + a_3 \cdot M_3 \cdot k_3 \\ &= 1 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 2 \cdot 12 \cdot 3 \\ &= 247 \equiv 7 \pmod{60}. \end{aligned}$$

♦

Med vilkårlige moduluser

Ved hjelp av det kinesiske restteoremet vet vi alt vi trenger å vite om systemer

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

der modulusene $m_1, m_2, \ldots, m_r$ er parvis relativt primiske: Vi vet at det finnes en løsning, at den er entydig modulo $M = m_1 \cdot m_2 \cdots m_r$, og vi vet hvordan vi kan finne løsningen.

Men hva om vi vil løse et system der modulusene *ikke* er parvis relativt primiske? Hva kan vi gjøre da?

Da kan vi ikke være sikre på at det finnes en løsning. På den annen side kan vi heller ikke være sikre på at det *ikke* finnes en løsning.

Det vi må gjøre med et slikt system er for det første å finne ut om det har noen løsning eller ikke. Da kan vi se på alle par av likninger i systemet som ikke har relativt primiske moduluser, og sjekke om de er i konflikt med hverandre. For eksempel er kongruensene

$$\begin{cases} x \equiv 12 \pmod{20} \\ x \equiv 29 \pmod{35} \end{cases}$$

i konflikt med hverandre, fordi den første av dem medfører at $x \equiv 2 \pmod 5$, mens den andre medfører at $x \equiv 4 \pmod 5$. Da er det ikke mulig at begge er oppfylt samtidig.

Hvis ingen av kongruensene i systemet har slike konflikter, kan vi skrive om systemet til et nytt system der modulusene er parvis relativt primiske. Det følgende eksemplet viser hvordan dette kan gjøres.

Eksempel Vi vil løse dette systemet:

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 0 \pmod 7 \\ x \equiv 5 \pmod 9 \\ x \equiv 11 \pmod{12} \end{cases}$$

Modulusene er ikke parvis relativt primiske, siden $\gcd(4,12) = 4$ og $\gcd(9,12) = 3$. Men vi kan se at kongruensen

$$x \equiv 11 \pmod{12}$$

er ekvivalent med de to kongruensene

$$\begin{cases} x \equiv 11 \pmod 3 \\ x \equiv 11 \pmod 4 \end{cases}$$

(siden $12 = 3 \cdot 4$ og $3 \perp 4$). Disse kan vi forenkle til:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \end{cases}$$

Vi kan altså sette inn disse to likningene istedenfor $x \equiv 11 \pmod{12}$ i systemet vårt, og få et ekvivalent system:

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 0 \pmod 7 \\ x \equiv 5 \pmod 9 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \end{cases}$$

Her kan vi for det første legge merke til at den samme likningen, $x \equiv 3 \pmod 4$, står to ganger, så vi kan sløyfe den ene av dem. Videre kan vi observere at hvis $x \equiv 5 \pmod 9$ er oppfylt, så må også $x \equiv 2 \pmod 3$ være oppfylt, slik at den sistnevnte er overflødig.

Systemet kan dermed forenkles til:

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 0 \pmod 7 \\ x \equiv 5 \pmod 9 \end{cases}$$

Nå har vi endelig fått et system der modulusene er parvis relativt primiske, og dermed kan vi løse det med det kinesiske restteoremet. Da finner vi løsningen

$$x \equiv 203 \pmod{252}.$$

♦

Det kan være fristende å prøve å splitte opp kongruensen med 9 som modulus på samme måte: Siden $9 = 3 \cdot 3$, kan vi vel splitte den opp i to kongruenser som begge har 3 som modulus? Men nei, det kan vi ikke gjøre, siden 3 ikke er relativt primisk til seg selv. Når vi vil splitte en kongruens i flere på denne måten, må vi alltid passe på at de nye modulusene er parvis relativt primiske.

Det vi gjorde isteden, var å sammenligne de to kongruensene

$$\begin{cases} x \equiv 5 \pmod 9 \\ x \equiv 2 \pmod 3 \end{cases}$$

og se at den første av dem medfører den andre. Her er det viktig å legge merke til at disse to kongruensene ikke sier nøyaktig det samme, for den første stiller sterkere krav til x enn den andre gjør (for eksempel er 8 en løsning av den andre kongruensen, men ikke av den første). Dermed kan vi beholde den første og sløyfe den andre uten at det påvirker hvilke løsninger vi får, men vi kan ikke sløyfe den første og beholde den andre.

Med det kinesiske restteoremet og ideene fra dette eksemplet er vi i stand til å håndtere et hvilket som helst system av kongruenslikninger. (Hurra!)

Fermats lille teorem og Eulers φ-funksjon

I forrige kapittel så vi at $3^4 \bmod 5 = 1$. Ved å regne litt, kan vi også se at vi for eksempel har $6^{16} \bmod 17 = 1$, og $4^{28} \bmod 29 = 1$. Faktisk er det slik at hvis vi tar et hvilket som helst tall a, og regner ut $a^{p-1} \bmod p$, der p er et primtall, så får vi 1 som svar. (Det eneste unntaket er hvis vi starter med et tall a som er kongruent med 0 modulo p, da får vi selvfølgelig 0.)

Dette resultatet ble oppdaget av Pierre de Fermat, og det er derfor oppkalt etter ham. For å skille det fra det kjente *Fermats siste resultat*, kalles dette resultatet vanligvis *Fermats lille resultat*:

La p være et primtall, og a et heltall slik at $p \nmid a$. Da er

$$a^{p-1} \equiv 1 \pmod p.$$

Hvorfor stemmer dette? Se på tallene

$$0 \cdot a, \quad 1 \cdot a, \quad 2 \cdot a, \quad \ldots, \quad (p-1) \cdot a.$$

Vi begynner med å observere at ingen av disse er kongruente med hverandre modulo p. Dersom vi har at $i \cdot a \equiv j \cdot a \pmod p$, så får vi også $i \equiv j \pmod p$ fordi p er et primtall. Og når både i og j er hentet fra mengden $\{0, 1, \ldots, (p-1)\}$, betyr det at $i = j$.

Så vi har altså listen $0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a$ med p ulike tall, og vi vet at ingen av dem er kongruente med hverandre modulo p. Men hvert av dem må jo være

kongruent modulo p med et av tallene

$$0, \quad 1, \quad 2, \quad \ldots, \quad (p-1).$$

Det at ingen av de p tallene våre er kongruente med hverandre, gjør at nøyaktig ett av dem må være kongruent med 0, ett med 1, ett med 2, og så videre. Når vi ser på alle tallene $0 \cdot a$, $1 \cdot a$, $\ldots$, $(p-1) \cdot a$, er de altså kongruente med tallene 0, 1, $\ldots$, $(p-1)$, i en eller annen rekkefølge.

Ved å ta produktet av alle tallene i hver av disse listene (unntatt 0), får vi dermed kongruensen

$$(1 \cdot a) \cdot (2 \cdot a) \cdots ((p-1) \cdot a) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Uttrykket på høyre side av kongruensen er lik $(p-1)!$, og det på venstre side er lik $(p-1)! \cdot a^{p-1}$, og vi har altså:

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}.$$

Siden $p \nmid (p-1)!$ kan vi forkorte bort $(p-1)!$ fra begge sider av kongruensen. Da får vi

$$a^{p-1} \equiv 1 \pmod{p},$$

som var det vi ville vise.

Modulær potensiering à la Fermat. Ved hjelp av Fermats lille teorem kan vi lett regne ut potenser modulo primtall.

Eksempel Vi regner ut 6^{195} mod 17. Fra Fermats lille teorem vet vi at $6^{16} \equiv 1 \pmod{17}$, siden 17 er et primtall. Da får vi:

$$\begin{aligned} 6^{195} &= 6^{12 \cdot 16 + 3} = (6^{16})^{12} \cdot 6^3 \\ &\equiv 1^{12} \cdot 6^3 = 216 \equiv 12 \pmod{17} \end{aligned}$$

Dermed har vi $6^{195} \bmod 17 = 12$. ♦

Eulers teorem

Vårt neste steg nå er å utvide Fermats lille teorem til den generelle situasjonen hvor modulusen vår ikke nødvendigvis er et primtall. Til det trenger vi et nytt verktøy:

Definisjon 27.2 Eulers φ-funksjon

For et naturlig tall n definerer vi $\varphi(n)$ til å være antallet naturlige tall som er relativt primiske til n og ikke større enn n. φ uttales *phi*.

Eksempel La $n = 10$. De naturlige tallene som ikke er større enn 10 er 1, 2, 3, 4, 5, 6, 7, 8, 9 og 10. Av disse er det fire tall som er relativt primiske til 10, nemlig 1, 3, 7 og 9. Dermed er $\varphi(10) = 4$. ♦

Tallet 1 er litt spesielt, siden det er det eneste naturlige tallet som er relativt primisk til seg selv. Vi har altså $\varphi(1) = 1$. For alle $n > 1$ har vi $\varphi(n) < n$, siden n ikke er relativt primisk til seg selv.

Denne funksjonen er essensiell i *Eulers teorem*, som er en generalisering av Fermats lille teorem. Resultatet er oppkalt etter Leonhard Euler, og sier at

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

for alle naturlige tall n og alle tall a som er relativt primiske til n.

En formel for φ

For å ha nytte av Eulers teorem, må vi være i stand til å beregne $\varphi(n)$. Vi begynner derfor med å se litt nøyere på φ-funksjonen. Vi viser at den er *multiplikativ*, og bruker det til å finne en formel for å regne ut $\varphi(n)$ basert på primtallsfaktoriseringen til n.

Husk definisjonen av φ-funksjonen: $\varphi(n)$ er antall naturlige tall som er relativt primiske til n og ikke større enn n. Hvis p er et primtall, så er alle tallene

$$1,\ 2,\ \ldots,\ p-1$$

relativt primiske til p, og dermed er $\varphi(p) = p - 1$. På den annen side, hvis n er et sammensatt tall, så har det en divisor d med $1 < d < n$. Da er d ikke relativt primisk til n, og dermed er $\varphi(n) < n - 1$. Vi har dermed vist:

For et naturlig tall n er $\varphi(n) = n - 1$ hvis og bare hvis n er et primtall.

Nå som vi vet hva φ anvendt på et primtall blir, går vi videre til å regne ut φ anvendt på en primtallspotens. La p være et primtall og k et naturlig tall. Da er $\varphi(p^k) = p^k - p^{k-1}$. Bevis:

Et tall er relativt primisk til p^k hvis og bare hvis det ikke er delelig med p. Av tallene $1, 2, \ldots, p^k$ er det disse som er delelige med p:

$$1p,\ 2p,\ 3p,\ \ldots,\ (p^{k-1})p$$

Det er p^{k-1} tall i denne listen. Dermed står vi igjen med $p^k - p^{k-1}$ tall som er relativt primiske til p^k.

Eksempel $\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54$. ♦

Funksjonen φ er multiplikativ. Dersom m og n er to naturlige tall som er relativt primiske til hverandre, så er $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. Det gir følgende formel for å regne ut $\varphi(n)$ gitt primtallsfaktoriseringen av n:

La $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$, der $p_1, p_2, \ldots, p_r$ er forskjellige primtall. Da er $\varphi(n)$ gitt ved:

$$\varphi(n) = \prod_{i=1}^{r} \left(p_i^{k_i} - p_i^{k_i - 1} \right).$$

Eksempel Vi kan se at $\varphi(24) = 8$ fordi det finnes 8 naturlige tall $(1, 5, 7, 11, 13, 17, 19, 23)$ som er relativt primiske til 24 og ikke større enn 24. Men nå som vi har vist resultatet ovenfor trenger vi ikke finne alle disse tallene for å regne ut $\varphi(24)$. Det er nok å se at primtallsfaktoriseringen er $24 = 2^3 \cdot 3$; da får vi:

$$\varphi(24) = (2^3 - 2^2)(3^1 - 3^0) = 4 \cdot 2 = 8. \qquad \blacklozenge$$

Eksempel Vi regner ut $\varphi(54208)$. Primtallsfaktoriseringen er $54208 = 2^6 \cdot 7 \cdot 11^2$, så vi får at:

$$\varphi(54208) = (2^6 - 2^5)(7^1 - 7^0)(11^2 - 11^1) = 21120.$$

Blant tallene $1, 2, 3, \ldots, 54208$ er det altså nøyaktig 21120 tall som er relativt primiske til 54208. $\blacklozenge$

Modulær potensiering à la Euler. Vi har tidligere brukt Fermats lille teorem til å gjøre store forenklinger av potensuttrykk a^i modulo et primtall p. Ved hjelp av Eulers teorem kan vi gjøre tilsvarende forenklinger modulo alle naturlige tall. Det krever imidlertid litt mer regning, siden vi må beregne φ av modulusen. Hvis vi skal forenkle uttrykket a^i modulo n, må vi dessuten passe på at a er relativt primisk til n før vi forsøker å bruke Eulers teorem.

Eksempel Vi regner ut 5^{196} mod 72. Tallet 72 har primtallsfaktoriseringen $2^3 \cdot 3^2$, og dermed har vi

$$\varphi(72) = (2^3 - 2^2)(3^2 - 3^1) = 24.$$

Vi ser at 5 og 72 er relativt primiske, så vi kan bruke Eulers resultat og få

$$5^{24} \equiv 1 \pmod{72}.$$

Siden $196 = 8 \cdot 24 + 4$, får vi:

$$\begin{aligned} 5^{196} &= 5^{8 \cdot 24 + 4} = (5^{24})^8 \cdot 5^4 \\ &\equiv 1^8 \cdot 5^4 = 5^4 = 625 \\ &\equiv 49 \pmod{72} \end{aligned}$$

Vi har altså at $5^{196} \bmod 72 = 49$. $\blacklozenge$