Forelesning 23 — torsdag den 6. november

6.1 Totienten

Merknad 6.1.1. La p være et primtall. Fermats lille teorem, altså Korollar 4.10.8, fastslår at, dersom det ikke er sant at

$$x \equiv 0 \pmod{p},$$

er

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

Vi har sett at dette resultatet er svært nyttig.

Hva om vi erstatter p med et hvilket som helst naturlig tall? Er et lignende utsagn sant? Det er visselig ikke nødvendigvis sant at

$$x^{n-1} \equiv 1 \pmod{n}$$

når n ikke er et primtall. For eksempel er

$$27 \equiv 3 \pmod{4},$$

altså

$$3^{4-1} \equiv 3 \pmod{4},$$

og det er ikke sant at

$$3 \equiv 1 \pmod{4}.$$

Likevel kan Fermats lille teorem generalises, ved å ertsatte potensen $p-1$ med noe som kalles totienten til n. Nå kommer vi til å se på dette resultatet, som kalles Eulers teorem, og etterpå til å utforske hvordan det benyttes i kryptografi.

Definisjon 6.1.2. La n være et naturlig tall. Da er *totienten* til n antall naturlige tall x slik at $x \leq n$ og $\mathsf{sfd}(x, n) = 1$.

Notasjon 6.1.3. La n være et naturlig tall. Vi betegner totienten til n som $\phi(n)$.

Eksempel 6.1.4. Det eneste naturlige tallet x slik at $x \leq 1$ er 1. Det er sant at $\mathsf{sfd}(1, 1) = 1$. Dermed er $\phi(1) = 1$.

Eksempel 6.1.5. De eneste naturlige tallene x slik at $x \leq 2$ er 1 og 2. Det er sant at $\mathsf{sfd}(1, 2) = 1$, men $\mathsf{sfd}(2, 2) = 2$. Dermed er 1 det eneste naturlige tallet x slik at $x \leq 2$ og $\mathsf{sfd}(x, 2) = 1$. Således er $\phi(2) = 1$.

Eksempel 6.1.6. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(3)$.

x	$\mathsf{sfd}(x, 3)$	Bidrar til $\phi(3)$?
1	1	✓
2	1	✓
3	3	✗

Dermed finnes det to naturlige tall x slik at $x \leq 3$ og $\mathsf{sfd}(x, 3) = 1$. Således er $\phi(3) = 2$.

Eksempel 6.1.7. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(4)$.

x	$\mathsf{sfd}(x, 4)$	Bidrar til $\phi(4)$?
1	1	✓
2	2	✗
3	1	✓
4	4	✗

Dermed finnes det to naturlige tall x slik at $x \leq 4$ og $\mathsf{sfd}(x, 4) = 1$. Således er $\phi(4) = 2$.

Eksempel 6.1.8. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(5)$.

x	$\mathsf{sfd}(x, 5)$	Bidrar til $\phi(5)$?
1	1	✓
2	1	✓
3	1	✓
4	1	✓
5	5	✗

Dermed finnes det fire naturlige tall x slik at $x \leq 5$ og $\mathsf{sfd}(x, 5) = 1$. Således er $\phi(5) = 4$.

Eksempel 6.1.9. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(6)$.

x	$\mathsf{sfd}(x, 6)$	Bidrar til $\phi(6)$?
1	1	✓
2	2	✗
3	3	✗
4	2	✗
5	1	✓
6	6	✗

Dermed finnes det to naturlige tall x slik at $x \leq 6$ og $\mathsf{sfd}(x, 6) = 1$. Således er $\phi(6) = 2$.

Eksempel 6.1.10. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(10)$.

x	$\mathsf{sfd}(x, 10)$	Bidrar til $\phi(10)$?
1	1	✓
2	2	✗
3	1	✓
4	2	✗
5	5	✗
6	2	✗
7	1	✓
8	2	✗
9	1	✓
10	10	✗

Dermed finnes det fire naturlige tall x slik at $x \leq 10$ og $\mathsf{sfd}(x, 10) = 1$. Således er $\phi(10) = 4$.

Eksempel 6.1.11. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(12)$.

x	$\mathsf{sfd}(x, 12)$	Bidrar til $\phi(12)$?
1	1	✓
2	2	✗
3	3	✗
4	4	✗
5	1	✓
6	3	✗
7	1	✓
8	4	✗
9	3	✗
10	2	✗
11	1	✓
12	12	✗

Dermed finnes det fire naturlige tall x slik at $x \leq 12$ og $\mathsf{sfd}(x, 12) = 1$. Således er $\phi(12) = 4$.

Proposisjon 6.1.12. La n være et naturlig tall. Da er $\phi(n) = n - 1$ om og bare om n er et primtall.

Bevis. Anta først at n er et primtall. Vi gjør følgende observasjoner.

(1) Ut ifra Korollar 4.2.5, er da $\mathsf{sfd}(x, n) = 1$ for et hvilket som helst naturlig tall x slik at $x \leq n - 1$.

(2) Vi har: $\mathsf{sfd}(n, n) = n$. Siden n er et primtall, er $n > 1$. Dermed er $\mathsf{sfd}(n, n) \neq 1$.

Vi konkluderer at $\phi(n) = n - 1$.

Anta istedenfor at $\phi(n) = n - 1$. Vi gjør følgende observasjoner.

(1) Vi har: $\mathsf{sfd}(n, n) = n$. Siden $\phi(1) = 1$, er det ikke sant at $n = 1$. Derfor er $n \geq 2$. Dermed er $\mathsf{sfd}(n, n) \neq 1$.

(2) Det følger fra (1) at $\phi(n)$ antall naturlige tall x slik at $x \leq n - 1$ og $\mathsf{sfd}(x, n) = 1$. Siden $\phi(n) = n - 1$, følger det at $\mathsf{sfd}(x, n) = 1$ for alle de naturlige tallene x slik at $x \leq n - 1$.

(3) La x være et naturlig tall slik at $x \mid n$. Da er $\mathsf{sfd}(x, n) = x$.

Det følger fra (2) og (3) at, dersom x er et naturlig tall slik at $x \mid n$ og $x \neq n$, er $x = 1$. Derfor er n et primtall.

□

Eksempel 6.1.13. Proposisjon 6.1.12 fastslår at $\phi(3) = 2$. Ut ifra Eksempel 6.1.6 er dette riktignok sant.

Eksempel 6.1.14. Ut ifra Eksempel 6.1.8 er $\phi(5) = 4$. Da fastslår Proposisjon 6.1.12 at 5 er et primtall. Dette er riktignok sant.

Lemma 6.1.15. La p være et primtall. La n være et naturlig tall. La y være et naturlig tall slik at $y \mid p^n$ og $y > 1$. Da har vi: $p \mid y$.

Bevis. Ut ifra Korollar 4.3.19 finnes det et primtall q slik at $q \mid y$. Ut ifra Proposisjon **??** har vi da: $q \mid p^n$. Det følger fra Korollar 4.2.23 at $q = p$. Siden $q \mid y$, konkluderer vi at $p \mid y$. □

Eksempel 6.1.16. Vi har: $9 \mid 27$, altså $9 \mid 3^3$. Siden 3 er et primtall, fastlår Lemma 6.1.15 at $3 \mid 9$. Dette er rikignok sant.

Eksempel 6.1.17. Vi har: $16 \mid 64$, altså $16 \mid 2^6$. Siden 2 er et primtall, fastlår Lemma 6.1.15 at $2 \mid 16$. Dette er riktignok sant.

Proposisjon 6.1.18. La p være et primtall. La n være et naturlig tall. Da er $\phi(p^n) = p^n - p^{n-1}$.

Bevis. La x være et naturlig tall slik at $x \leq p^n$ og $\mathsf{sfd}(x, p^n) \neq 1$. Vi gjør følgende observasjoner.

(1) Da finnes det et naturlig tall y slik at $y \mid x$ og $y \mid p^n$, og slik at $y > 1$. Siden $y \mid p^n$, følger det fra Lemma 6.1.15 at $p \mid y$. Dermed er $y = kp$, hvor k er et naturlig tall.

(2) Siden $y \mid x$, finnes det et naturlig tall l slik at $x = ly$. Dermed er $x = l(kp)$, altså $x = (kl)p$. La oss betegne det naturlige tallet kl som m.

(3) Siden $x \leq p^n$, altså $mp \leq p^n$, er $m \leq p^{n-1}$.

La nå m være et hvilket som helst naturlig tall slik at $m \leq p^{n-1}$. Da har vi: $p \mid mp$ og $p \mid p^{n-1}$. Derfor er $\mathsf{sfd}(mp, p^n) \geq p$, altså $\mathsf{sfd}(mp, p^n) > 1$.
Således har vi bevist:

(A) dersom $x \leq p^n$ og $\mathsf{sfd}(x, p^n) \neq 1$, finnes det et naturlig tall m slik at $m \leq p^{n-1}$ og $x = mp$;

(B) dersom m er et naturlig tall slik at $m \leq p^{n-1}$, er $\mathsf{sfd}(mp, p^n) \neq 1$.

Det følger at de naturlige tallene x slik at $x \leq p^n$ og $\mathsf{sfd}(x, p^n) \neq 1$ er akkurat de naturlige tallene p, $2p$, $3p$, $\ldots$, $\left(p^{n-1}\right) p$. Denne lista består av akkurat p^{n-1} ulike naturlige tall. Siden antall naturlige tall x slik at $x \leq p^n$ er p^n, konkluderer vi at antall naturlige tall slik at $x \leq p^n$ og $\mathsf{sfd}(x, p^n) = 1$ er $p^n - p^{n-1}$, altså at $\phi\left(p^n\right) = p^n - p^{n-1}$.

□

Eksempel 6.1.19. Proposisjon 6.1.18 fastslår at $\phi(2^2) = 2^2 - 2^1$, altså at $\phi(4) = 2$. Ut ifra Eksempel 6.1.7 er dette riktignok sant.

Eksempel 6.1.20. Proposisjon 6.1.18 fastslår at $\phi(3^2) = 3^2 - 3^1$, altså at $\phi(9) = 6$. Følgende tabell viser at dette riktignok er sant.

x	$\mathsf{sfd}(x, 9)$	Bidrar til $\phi(9)$?
1	1	✓
2	1	✓
3	3	✗
4	1	✓
5	1	✓
6	3	✗
7	1	✓
8	1	✓
9	9	✗

Som fastslått av beviset for Proposisjon 6.1.18, er det de naturlige tallene 3, 6, og 9, altså 3, $2 \cdot 3$, og $3 \cdot 3$, som ikke bidrar til $\phi(9)$.

Eksempel 6.1.21. Proposisjon 6.1.18 fastslår at $\phi(2^3) = 2^3 - 2^2$, altså at $\phi(8) = 4$. Følgende tabell viser at dette riktignok er sant.

x	$\mathsf{sfd}(x, 8)$	Bidrar til $\phi(8)$?
1	1	✓
2	2	✗
3	1	✓
4	4	✗
5	1	✓
6	2	✗
7	1	✓
8	8	✗

Som fastslått av beviset for Proposisjon 6.1.18, er det de naturlige tallene 2, 4, 6, og 8, altså 2, $2 \cdot 2$, $3 \cdot 2$, og $4 \cdot 2$, som ikke bidrar til $\phi(8)$.

6.2 Eulers teorem

Merknad 6.2.1. Vi kommer til å bygge på følgende proposisjon, som er viktig i seg selv, for å gi et bevis for Eulers teorem.

Proposisjon 6.2.2. La m og n være naturlige tall slik at $\mathsf{sfd}(m, n) = 1$. Da er $\phi(mn) = \phi(m) \cdot \phi(n)$.

Bevis. Ut ifra Eksempel 6.1.4 er $\phi(1) = 1$. Det følger umiddelbart at utsagnet er sant når $m = 1$ eller når $n = 1$.

Anta at $m > 1$ og at $n > 1$. Ut ifra definisjonen til $\phi(m)$, finnes det $\phi(m)$ naturlige tall x slik at $\mathsf{sfd}(x, m) = 1$. La oss betegne disse naturlige tallene som x_1, x_2, …, $x_{\phi(m)}$.

Ut ifra definisjonen til $\phi(n)$, finnes det $\phi(n)$ naturlige tall y slik at $\mathsf{sfd}(y, n) = 1$. La oss betegne disse naturlige tallene som y_1, y_2, …, $y_{\phi(n)}$.

Ut ifra Proposisjon 3.2.1 finnes det, for hvert naturlig tall i slik at $i \leq \phi(m)$ og hvert naturlig tall j slik at $j \leq \phi(n)$, et naturlig tall $r_{i,j}$ slik at

$$nx_i + my_j \equiv r_{i,j} \pmod{mn}$$

og $0 \leq r_{i,j} < mn$.

Anta at følgende utsagn har blitt bevist.

(A) For hvert naturlig tall i slik at $i \leq \phi(m)$, og hvert naturlig tall j slik at $j \leq \phi(n)$, er $\mathsf{sfd}(r_{i,j}, mn) = 1$.

(B) La nå i og i' være naturlige tall slik at $i \leq \phi(m)$ og $i' \leq \phi(m)$. La j og j' være naturlige tall slik at $j \leq \phi(n)$ og $j' \leq \phi(n)$. Da er $r_{i,j} = r_{i',j'}$ om og bare om $x_i = x_{i'}$ og $y_j = y_{j'}$.

(C) Dersom z er et naturlig tall slik at $z < mn$ og $\mathsf{sfd}(z, mn) = 1$, finnes det et naturlig tall i og et naturlig tall j slik at $z = r_{i,j}$.

Det følger fra (A) og (C) at $\phi(mn)$ er antall ulike naturlige tall blant de naturlige tallene $r_{i,j}$, hvor i er et naturlig tall slik at $i \leq \phi(m)$, og j er et naturlig tall slik at $j \leq \phi(n)$. Siden alle de naturlige tallene $x_1, x_2, \ldots, x_{\phi(m)}$ er ulike, og siden alle de naturlige tallene $y_1, y_2, \ldots, y_{\phi(n)}$ er ulike, følger det fra (B) at alle de naturlige tallene $r_{i,j}$ er ulike, hvor $i \leq \phi(m)$ og $j \leq \phi(n)$, altså at det er akkurat $\phi(m) \cdot \phi(n)$ av dem. Vi konkluderer at

$$\phi(mn) = \phi(m) \cdot \phi(n).$$

La oss nå bevise at (A) – (C) er sanne. La i være et naturlig tall slik at $i \leq \phi(m)$. La j være et naturlig tall slik at $j \leq \phi(n)$. La z være et naturlig tall slik at $z \mid r_{i,j}$ og $z \mid mn$. Vi gjør følgende observasjoner.

(1) Siden

$$nx_i + my_j \equiv r_{i,j} \pmod{mn},$$

følger det da fra Proposisjon **??** og antakelsen $z \mid r_{i,j}$ at

$$nx_i + my_j \equiv 0 \pmod{z},$$

altså at

$$z \mid nx_i + my_j.$$

(2) Dersom $z > 1$, følger det fra Korollar 4.3.19 at det finnes et primtall p slik at $p \mid z$. Da følger det fra (1) og Proposisjon 2.5.27 at $p \mid nx_i + my_j$.

(3) Siden $p \mid z$ og $z \mid mn$, følger det fra Proposisjon 2.5.27 at $p \mid mn$. Siden p er et primtall, følger det da fra Proposisjon 4.2.12 at enten $p \mid m$ eller $p \mid n$.

(4) Anta først at $p \mid m$. Siden $\mathsf{sfd}(m, n) = 1$, er det da ikke sant at $p \mid n$.

(5) Siden $p \mid m$, følger det fra Korollar 2.5.18 at $p \mid -my_j$.

(6) Det følger fra (3), (5), og Proposisjon 2.5.24 at

$$p \mid (nx_i + my_j) - my_j,$$

altså at $p \mid nx_i$.

(7) Siden det ikke er sant, ut ifra (4), at $p \mid n$, følger det fra (6) og Proposisjon 4.2.12 at $p \mid x_i$. Siden vi har antatt at $p \mid m$, er da $\mathsf{sfd}(x_i, m) \geq p$.

(8) Ut ifra definisjonen til x_i, er imidlertid $\mathsf{sfd}(x_i, m) = 1$. Siden antakelsen at $p \mid m$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $p \mid m$.

(9) Anta istedenfor at $p \mid n$. Et lignende argument som i (4) – (7) fastslår at det da finnes et primtall q slik at $\mathsf{sfd}(y_j, n) \geq q$. Ut ifra definisjonen til y_j, er imidlertid $\mathsf{sfd}(y_j, n) = 1$. Siden antakelsen at $p \mid n$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $p \mid n$.

(10) Dermed har vi en motsigelse: (2) fastslår at enten $p \mid m$ eller $p \mid n$, mens (8) og (9) fastslår at verken $p \mid m$ eller $p \mid n$. Siden antakelsen at $z > 1$ fører til denne motsigelsen, konkluderer vi at $z = 1$.

Således har vi bevist at, dersom $z \mid r_{i,j}$ og $z \mid mn$, er $z = 1$. Vi konkluderer at $\mathsf{sfd}(r_{i,j}, mn) = 1$, altså at (A) er sant.

La nå i og i' være naturlige tall slik at $i \leq \phi(m)$ og $i' \leq \phi(m)$. La j og j' være naturlige tall slik at $j \leq \phi(n)$ og $j' \leq \phi(n')$. Anta at $r_{i,j} = r_{i',j'}$. Da er

$$ns_i + my_j \equiv nx_{i'} + my_{j'} \pmod{mn}.$$

Vi gjør følgende observasjoner.

(1) Det følger at

$$n(x_i - x_{i'}) + m(y_j - y_{j'}) \equiv 0 \pmod{mn}.$$

Derfor har vi:

$$mn \mid n(x_i - x_{i'}) + m(y_j - y_{j'}).$$

(2) Dermed finnes det et heltall k slik at

$$n(x_i - x_{i'}) + m(y_j - y_{j'}) = k(mn),$$

altså slik at

$$n(x_i - x_{i'}) = \big(y_{j'} - y_j + kn\big)m.$$

Således har vi: $m \mid n(x_i - x_{i'})$.

(3) Ut ifra Proposisjon 2.8.22 har vi da: enten $m \mid n$ eller $m \mid x_i - x_{i'}$.

(4) Dersom $m \mid n$, følger det fra Proposisjon 2.6.21 at $\mathsf{sfd}(m, n) = m$. Imidlertid har vi antatt at $\mathsf{sfd}(m, n) = 1$. Siden $m > 1$, har vi da en motsigelse. Siden antakelsen at $m \mid n$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $m \mid n$.

(5) Dersom $m \mid x_i - x_{i'}$, er

$$x_i \equiv x_{i'} \pmod{m}.$$

Siden $x_i < m$ og $x_{i'} < m$, følger det fra Proposisjon 3.2.11 at $x_i = x_{i'}$.

(6) Et lignende argument som i (1) – (5) fastslår at $n \mid m(y_{j'} - y_j)$, og deretter at $y_{j'} = y_j$.

Således har vi bevist at, dersom $r_{i,j} = r_{i',j'}$, er $x_i = x_{i'}$ og $y_j = y_{j'}$. Dermed er (B) sant.

La nå z være et naturlig tall slik at $z < mn$ og $\mathsf{sfd}(z, mn) = 1$. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 2.8.30 er da $\mathsf{sfd}(m, z) = 1$.

(2) Ut ifra Proposisjon 1.2.6, finnes et naturlig tall k og et naturlig tall r slik at $0 \leq r < m - 1$ og

$$z = km + r.$$

(3) Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(m, r) = \mathsf{sfd}(z, m)$.

(4) Det følger fra (1) og (3) at $\mathsf{sfd}(m, r) = 1$. Ut ifra definisjonen til de naturlige tallene x_1, x_2, ..., $x_{\phi(m)}$, finnes det derfor et naturlig tall i slik at $i \leq \phi(m)$ og $r = x_i$. Dermed er

$$km + r \equiv 0 + x_i \pmod{m},$$

altså er

$$z \equiv x_i \pmod{m}.$$

(5) Ut ifra Proposisjon 2.8.30 er $\mathsf{sfd}(n, z) = 1$. Et lignende argument som i (2) – (4) fastslår da at det finnes et naturlig tall j slik at $j \leq \phi(n)$ og

$$z \equiv y_j \pmod{n}.$$

(6) Ut ifra (4) og (5) er $x = z$ en løsning både til kongruensen

$$x \equiv x_i \pmod{m}$$

og til kongruensen

$$x \equiv y_j \pmod{n}.$$

Siden $\mathsf{sfd}(m, n) = 1$, følger det fra Proposisjon 5.7.2 (I) at $x = nx_i + my_j$ også er en løsning til begge kongruensene.

(7) Det følger fra (6) og Proposisjon 5.7.2 (II) at

$$z \equiv nx_i + my_j \pmod{mn},$$

altså at

$$z \equiv r_{i,j} \pmod{mn}.$$

Siden $z < mn$ og $r_{i,j} < mn$, følger det fra Proposisjon 3.2.11 at $z = r_{i,j}$.

Således har vi bevist at, dersom $z < mn$ og $\mathsf{sfd}(z, mn) = 1$, finnes det et naturlig tall i og et naturlig tall j slik at $z = r_{i,j}$, hvor $i \leq \phi(m)$ og $j \leq \phi(n)$. Dermed er (C) sant. □

Eksempel 6.2.3. Ut ifra Eksempel 6.1.6 er $\phi(3) = 2$. Ut ifra Eksempel 6.1.7 er $\phi(4) = 2$. Da fastslår Proposisjon 6.2.2 at $\phi(3 \cdot 4) = \phi(3) \cdot \phi(4)$, altså at $\phi(12) = 2 \cdot 2 = 4$. Ut ifra Eksempel 6.1.11 er dette riktignok sant.

Ut ifra Eksempel 6.1.6 er 1 og 2 de to naturlige tallene x slik at $x \leq 3$ og $\mathsf{sfd}(x, 3) = 1$. Ut ifra Eksempel 6.1.7 er 1 og 3 de to naturlige tallene x slik at $x \leq 4$ og $\mathsf{sfd}(x, 4) = 1$. Da fastslår beviset for Proposisjon 6.2.2 at de naturlige tallene x slik at $x \leq 12$ og $\mathsf{sfd}(x, 12) = 1$ er kongruent modulo 12 til $4 \cdot 1 + 3 \cdot 1$, $4 \cdot 1 + 3 \cdot 3$, $4 \cdot 2 + 3 \cdot 1$, og $4 \cdot 2 + 3 \cdot 3$, altså til 7, 13, 11, og 17. De naturlige tallene x slik at $x \leq 12$ som er kongruent modulo 12 til disse er: 7, 1, 11, og 5. Ut ifra Eksempel 6.1.11 er det riktignok disse fire naturlige tallene som bidrar til $\phi(12)$.

Eksempel 6.2.4. Ut ifra Eksempel 6.1.8 er $\phi(5) = 4$. Ut ifra Eksempel **??** er $\phi(6) = 2$. Da fastslår Proposisjon 6.2.2 at $\phi(5 \cdot 6) = \phi(5) \cdot \phi(6)$, altså at $\phi(30) = 4 \cdot 2 = 8$.

Ut ifra Eksempel 6.1.8 er 1, 2, 3, og 4 de fire naturlige tallene x slik at $x \leq 5$ og $\mathsf{sfd}(x, 5) = 1$. Ut ifra Eksempel **??** er 1 og 5 de to naturlige tallene x slik at $x \leq 6$ og $\mathsf{sfd}(x, 6) = 1$. Da fastslår beviset for Proposisjon 6.2.2 at de naturlige tallene x slik at $x \leq 30$ og $\mathsf{sfd}(x, 30) = 1$ er kongruent modulo 30 til $6 \cdot 1 + 5 \cdot 1$, $6 \cdot 1 + 5 \cdot 5$, $6 \cdot 2 + 5 \cdot 1$, $6 \cdot 2 + 5 \cdot 5$, $6 \cdot 3 + 5 \cdot 1$, $6 \cdot 3 + 5 \cdot 5$, $6 \cdot 4 + 5 \cdot 1$, og $6 \cdot 4 + 5 \cdot 5$, altså til 11, 31, 17, 37, 23, 43, 29, og 49. De naturlige tallene x slik at $x \leq 30$ som er kongruent modulo 30 til disse er: 11, 1, 17, 7, 23, 13, 29, og 19.

Merknad 6.2.5. Proposisjon 6.2.2 er ikke nødvendigvis sant om vi ikke antar at $\mathsf{sfd}(m, n) = 1$. Ut ifra Eksempel 6.1.5 er $\phi(2) = 1$. Derfor er $\phi(2) \cdot \phi(2) = 1 \cdot 1 = 1$. Ut ifra Eksempel 6.1.7 er imidlertid $\phi(2 \cdot 2) = \phi(4) = 2$.

For et annet eksempel, er, ut ifra Eksempel 6.1.7, $\phi(4) = 2$. Ut ifra Eksempel 6.1.7, er $\phi(6) = 2$. Imidlertid viser følgende tabell at $\phi(24) = 8$.

x	$\mathsf{sfd}(x, 24)$	Bidrar til $\phi(24)$?
1	1	✓
2	2	✗
3	3	✗
4	4	✗
5	1	✓
6	6	✗
7	1	✓
8	8	✗
9	1	✓
10	2	✗
11	1	✓
12	12	✗
13	1	✓
14	2	✗
15	3	✗
16	8	✗
17	1	✓
18	6	✗
19	1	✓
20	4	✗
21	3	✗
22	2	✗
23	1	✓
24	24	✗

Merknad 6.2.6. At Proposisjon 6.2.2 er sann gir oss muligheten til å benytte oss av en kraftig og begrepsmessig tilnærmingsmetode for å bevise en proposisjon om totienten til et hvilket som helst naturlig tall n:

(1) Observer at, ut ifra Korollar 4.3.16, finnes det en primtallsfaktorisering

$$n = p_1^{k^1} p_2^{k_2} \cdots p_t^{k_t}$$

til n slik at $p_i \neq p_j$ dersom $i \neq j$.

(2) Siden $p_i \neq p_j$ dersom $i \neq j$, følger det fra Korollar 4.2.9 at $\mathsf{sfd}(p_i^{k_i}, p_j^{k_j}) = 1$ dersom $i \neq j$. Observer at, ut ifra Proposisjon 6.2.2, er da

$$\phi(n) = \phi\left(p_1^{k_1}\right) \phi\left(p_2^{k_2}\right) \cdots \phi\left(p_t^{k_t}\right).$$

(3) Bevis at proposisjonen er sann når $n = q$, hvor q er et primtall.

(4) Benytt (2) og (3) for å gi et bevis for proposisjonen når n er et hvilket som helst naturlig tall.

Vi kommer nå til å benytte oss av denne tilnærmingsmetoden for å gi et bevis for Eulers teorem.

Proposisjon 6.2.7. La p være et primtall. La n være et naturlig tall. La x være et heltall slik at det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

Da er

$$x^{\phi(p^n)} \equiv 1 \pmod{p^n}.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at

$$x^{\phi(p)} \equiv 1 \pmod{p}.$$

Ut ifra Proposisjon 6.1.12 er $\phi(p) = p - 1$. Derfor er utsagnet at

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

Ut ifra Korollar 4.10.8 er dette sant.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m et et gitt naturlig tall. Således har det blitt bevist at

$$x^{\phi(p^m)} \equiv 1 \pmod{p^m}.$$

Vi gjør følgende observasjoner.

(1) Da har vi: $p^m \mid x^{\phi(p^m)} - 1$. Dermed finnes det et naturlig tall k slik at

$$x^{\phi(p^m)} - 1 = kp^m,$$

altså slik at

$$x^{\phi(p^m)} = 1 + kp^m.$$

(2) Ut ifra Proposisjon 6.1.18 er

$$\phi\left(p^{m+1}\right) = p^{m+1} - p^m = p\left(p^m - p^{m-1}\right).$$

Det følger også fra Proposisjon 6.1.18 at

$$\phi\left(p^m\right) = p^m - p^{m-1}.$$

Dermed er

$$\phi\left(p^{m+1}\right) = p\phi\left(p^m\right).$$

(3) Det følger fra (1) og (2) at

$$\begin{aligned} x^{\phi\left(p^{m+1}\right)} &= x^{p\phi(p^m)} \\ &= \left(x^{\phi(p^m)}\right)^p \\ &= (1 + kp^m)^p \end{aligned}$$

(4) Ut ifra Proposisjon 1.9.30 er

$$\begin{aligned} (1 + kp^m)^p &= \sum_{i=0}^{p} \binom{p}{i} 1^{p-i} \left(kp^m\right)^i \\ &= 1 + \binom{p}{1} \cdot \left(kp^m\right)^1 + \cdots + \binom{p}{p-1} \left(kp^m\right)^{p-1} + \left(kp^m\right)^p. \end{aligned}$$

(5) For hvert naturlig tall i slik at $i \geq 2$, er

$$im \geq 2m \geq m + 1.$$

Derfor er

$$im - (m + 1) \geq 0.$$

Siden

$$p^{im} = p^{im-(m+1)} p^{m+1},$$

har vi da: $p^{m+1} \mid p^{im}$. Det følger fra Korollar 2.5.18 at $p^{m+1} \mid kp^{im}$, altså at $p^{m+1} \mid (kp)^i$. Således er

$$(kp)^i \equiv 0 \pmod{p^{m+1}}.$$

(6) Siden $\binom{p}{1} = p$, er

$$\binom{p}{1} kp^m = kpm + 1.$$

Siden $p^{m+1} \mid kp^{m+1}$, har vi da:

$$p^{m+1} \mid \binom{p}{1} kp^m.$$

Derfor er

$$\binom{p}{1} kp^m \equiv 0 \pmod{p^{m+1}}.$$

(7) Ut ifra (5) og (6) er

$$\begin{aligned} &1 + \binom{p}{1} \cdot (kp^m)^1 + \cdots + \binom{p}{p-1} (kp^m)^{p-1} + (kp^m)^p \\ &\equiv 1 + 0 + \cdots + 0 + 0 \pmod{p^{m+1}}, \end{aligned}$$

altså

$$1 + \binom{p}{1} \cdot (kp^m)^1 + \cdots + \binom{p}{p-1} (kp^m)^{p-1} + (kp^m)^p \equiv 1 \pmod{p^{m+1}}.$$

Det følger fra (3), (4), og (7) at

$$x^{\phi\left(p^{m+1}\right)} \equiv 1 \pmod{p^{m+1}}.$$

Således er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall.

□

Eksempel 6.2.8. Ut ifra Eksempel 6.1.21 er $\phi(8) = 4$, altså $\phi\left(2^3\right) = 4$. Da fastslår Proposisjon 6.2.7 at

$$x^4 \equiv 1 \pmod{8}$$

for et hvilket som helst heltall x slik at det ikke er sant at

$$x \equiv 0 \pmod{2}.$$

For eksempel:

$$5^4 \equiv 1 \pmod{8}.$$

Riktignok har vi:

$$5^4 = \left(5^2\right)^2 = 25^2 \equiv 1^2 = 1 \pmod{8}.$$

Eksempel 6.2.9. Ut ifra Eksempel 6.1.20 er $\phi(9) = 6$, altså $\phi\left(3^2\right) = 6$. Da fastslår Proposisjon 6.2.7 at

$$x^6 \equiv 1 \pmod{9}$$

for et hvilket som helst heltall x slik at det ikke er sant at

$$x \equiv 0 \pmod{3}.$$

For eksempel:

$$4^6 \equiv 1 \pmod{9}.$$

Riktignok har vi:

$$4^6 = \left(4^3\right)^2 = 64^2 \equiv 1^2 = 1 \pmod{9}.$$

Proposisjon 6.2.10. La n være et naturlig tall. La x være et heltall slik at $\mathsf{sfd}(x, n) = 1$. Da er

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Korollar 4.3.16, finnes det et naturlig tall t og primtall p_1, p_2, ..., p_t slik at

$$n = p_1^{k^1} p_2^{k_2} \cdots p_t^{k_t},$$

og $p_i \neq p_j$ dersom $i \neq j$.

(2) Siden $p_i \neq p_j$ dersom $i \neq j$, følger det fra Korollar 4.2.9 at $\mathsf{sfd}(p_i^{k_i}, p_j^{k_j}) = 1$ dersom $i \neq j$. Ved å benytte Korollar **??** gjentatte ganger, følger det at

$$\mathsf{sfd}(p_1^{k_1} \cdots p_{i-1}^{k_{t-1}}, p_i^{k_i}) = 1$$

for et hvilket som helst naturlig tall i slik at $2 \leq i \leq t$.

(3) Ut ifra Proposisjon 6.2.2, er da

$$\phi(n) = \phi\left(p_1^{k_1}\right) \phi\left(p_2^{k_2}\right) \cdots \phi\left(p_t^{k_t}\right).$$

(4) La i være et naturlig tall slik at $i \leq t$. La m_i være

$$\phi\left(p_1^{k_1}\right) \cdots \phi\left(p_{i-1}^{k_{i-1}}\right) \phi\left(p_{i+1}^{k_{i+1}}\right) \cdots \phi\left(p_t^{k_t}\right).$$

Ut ifra (3), er $\phi(n) = m_i \phi\left(p_i^{k_i}\right)$.

(5) Dermed er

$$x^{\phi(n)} = x^{m_i \phi\left(p_i^{k_i}\right)} = \left(x^{\phi\left(p_i^{k_i}\right)}\right)^{m_i}.$$

(6) Siden $\mathsf{sfd}(x, n) = 1$, og siden $p_i \mid n$, er det ikke sant at $p_i \mid x$. Ut ifra Proposisjon 6.2.7 er da, for hvert naturlig tall i slik at $i \leq t$,

$$x^{\phi\left(p_i^{k_i}\right)} \equiv 1 \pmod{p_i^{k_i}}.$$

(7) Det følger fra (5) og (6) at

$$x^{\phi(n)} \equiv 1^{m_i} = 1 \pmod{p_i^{k_i}}.$$

Således har vi bevist at, for hvert naturlig tall i slik at $i \leq t$, er

$$x^{\phi(n)} \equiv 1 \pmod{p_i^{k_i}}.$$

Siden

$$\mathsf{sfd}(p_1^{k_1} \cdots p_{i-1}^{k_{t-1}}, p_i^{k_i}) = 1$$

for et hvilket som helst naturlig tall i slik at $2 \leq i \leq t$, følger det fra Korollar 5.7.30 at

$$x^{\phi(n)} \equiv 1 \pmod{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}},$$

altså at

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

□

Terminologi 6.2.11. Proposisjon 6.2.10 kalles *Eulers teorem.*

Eksempel 6.2.12. Ut ifra Eksempel 6.1.21 er $\phi(8) = 4$. Da fastslår Proposisjon 6.2.10 at, for et hvilket som helst heltall x slik at $\mathsf{sfd}(x, 8) = 1$, er

$$x^4 \equiv 1 \pmod{8}.$$

For eksempel:

$$3^4 \equiv 1 \pmod{8}.$$

Riktignok har vi:

$$3^4 = \left(3^2\right)^2 \equiv 1^2 = 1 \pmod{8}.$$

Eksempel 6.2.13. Ut ifra Merknad 6.2.5 er $\phi(24) = 8$. Da fastslår Proposisjon 6.2.10 at, for et hvilket som helst heltall x slik at $\mathsf{sfd}(x, 24) = 1$, er

$$x^8 \equiv 1 \pmod{24}.$$

For eksempel:

$$7^8 \equiv 1 \pmod{24}.$$

Riktignok har vi:

$$7^8 = \left(7^2\right)^4 \equiv 1^4 = 1 \pmod{24}.$$

Merknad 6.2.14. Følgende korollar er kjernen til RSA-algoritmen, som vi kommer til å se på i den neste delen av kapittelet.

Korollar 6.2.15. La n være et naturlig tall. La a være et heltall slik at $\mathsf{sfd}(a, \phi(n)) = 1$. Ut ifra Korollar 3.4.39, finnes det da et heltall b slik at

$$ab \equiv 1 \pmod{\phi(n)}.$$

La x være et heltall slik at $\mathsf{sfd}(x, n) = 1$. Da er

$$(x^a)^b \equiv x \pmod{n}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Siden

$$ab \equiv 1 \pmod{\phi(n)},$$

har vi: $\phi(n) \mid ab - 1$. Dermed finnes det et naturlig tall k slik at $ab - 1 = k\phi(n)$, altså slik at $ab = 1 + k\phi(n)$.

(2) Da er

$$\begin{aligned}(x^a)^b &= x^{ab} \\ &= x^{1+k\phi(n)} \\ &= x^1 \cdot x^{k\phi(n)} \\ &= x \cdot \left(x^{\phi(n)}\right)^k.\end{aligned}$$

(3) Ut ifra Proposisjon 6.2.10 er

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

Dermed er

$$x \cdot \left(x^{\phi(n)}\right)^k \equiv x \cdot 1^k = x \pmod{n}.$$

(4) Det følger fra (2) og (3) at

$$(x^a)^b \equiv x \pmod{n}.$$

□

Eksempel 6.2.16. Vi har:

(1) $\phi(11) = 10$;

(2) $\mathsf{sfd}(3, 10) = 1$;

(3) $3 \cdot 7 = 21 \equiv 1 \pmod{10}$.

Da fastslår Korollar 6.2.15 at, for et hvilket som helst heltall x slik at $\mathsf{sfd}(x, 11) = 1$, er

$$\left(x^3\right)^7 \equiv x \pmod{11}.$$

For eksempel:

$$\left(6^3\right)^7 \equiv 6 \pmod{11},$$

altså

$$6^{21} \equiv 6 \pmod{11}.$$

Én måte å vise at dette riktignok er sant er å følge beviset for 6.2.15: ut ifra Korollar **??** er

$$6^{10} \equiv 1 \pmod{11},$$

og deretter er

$$6^{21} = \left(6^{10}\right)^2 \cdot 6 \equiv 1^2 \cdot 6 = 6 \pmod{11}.$$

Eksempel 6.2.17. Vi har:

(1) $\phi(34) = \phi(17) \cdot \phi(2) = 16 \cdot 1 = 16$;

(2) $\mathsf{sfd}(5, 16) = 1$;

(3) $5 \cdot 13 = 65 \equiv 1 \pmod{16}$.

Da fastslår Korollar 6.2.15 at, for et hvilket som helst heltall x slik at $\mathsf{sfd}(x, 34) = 1$, er

$$\left(x^5\right)^{13} \equiv x \pmod{34}.$$

For eksempel:

$$\left(9^5\right)^{13} \equiv 9 \pmod{34},$$

altså

$$9^{65} \equiv 9 \pmod{34}.$$

Én måte å vise at dette riktignok er sant er å følge beviset for 6.2.15: ut ifra Proposisjon 6.2.10 er

$$9^{16} \equiv 1 \pmod{34},$$

og deretter er

$$9^{65} = \left(9^{16}\right)^4 \cdot 9 \equiv 1^4 \cdot 9 = 9 \pmod{34}.$$

6.3 Et eksempel på et bevis hvor Eulers teorem benyttes

Merknad 6.3.1. Proposisjon 6.2.10 kan benyttes på en lignende måte som Korollar 4.10.8 ble benyttet i bevisene for Proposisjon 4.11.1 og Proposisjon 4.11.10. La oss se på et eksempel.

Proposisjon 6.3.2. Det naturlige tallet $3^{37639} - 2187$ er delelig med 87808.

Bevis. Vi gjør følgende observasjoner.

(1) En primtallsfaktorisering til 87808 er

$$2^8 \cdot 7^3.$$

(2) Det følger fra (1) og Proposisjon 6.2.2 at $\phi(87808) = \phi\left(2^8\right) \cdot \phi\left(7^3\right)$.

(3) Ut ifra Proposisjon 6.1.18 er

$$\phi\left(2^8\right) = 2^8 - 2^7 = 128.$$

(4) Ut ifra Proposisjon 6.1.18 er

$$\phi\left(7^3\right) = 7^3 - 7^2 = 294.$$

(5) Det følger fra (2) – (4) at

$$\phi(87808) = 128 \cdot 294 = 37632.$$

(6) Ut ifra Proposisjon 6.2.10 er

$$3^{\phi(87808)} \equiv 1 \pmod{87808}.$$

(7) Det følger fra (5) og (6) at

$$3^{37632} \equiv 1 \pmod{87808}.$$

(8) Det følger fra (7) at

$$3^{37639} - 2187 = 3^{37632} \cdot 3^7 - 2187 \equiv 1 \cdot 3^7 - 2187 = 3^7 - 2187 = 0 \pmod{87808},$$

altså

$$3^{37639} - 2187 \equiv 0 \pmod{87808}.$$

Da har vi:

$$87808 \mid 3^{37639} - 2187.$$

□

Oppgaver

O6.1 Oppgaver i eksamens stil

Oppgave O6.1.1. Hvor mange naturlige tall x slik at $x \leq 2925$ og $\mathsf{sfd}(x, 2925) = 1$ finnes det?

Oppgave O6.1.2. Vis uten å regne ut at $4721 \cdot \left(11^{2163}\right) + 5324$ er delelig med 4725.