Forelesning 21 — torsdag den 30. oktober

5.12 Mersenne-primtall

Merknad 5.12.1. Nå kommer vi til å se på et fint tema hvor kvadratisk gjensidighet kan benyttes.

Terminologi 5.12.2. La n være et naturlig tall. Vi sier at $2^n - 1$ er et *Mersenne-tall*. Dersom $2^n - 1$ er et primtall, sier vi at det er et *Mersenne-primtall*.

Eksempel 5.12.3. Den andre kolonnen i følgende tabell viser de første 15 Mersenne-tallene.

n	$2^n - 1$
1	1
2	3
3	7
4	15
5	31
6	63
7	127
8	255
9	511
10	1023
11	2047
12	4095
13	8191
14	16383
15	32767

Merknad 5.12.4. Når er et Mersenne-tall et primtall? Dette spørsmålet har fascinert matematikkere siden Antikkens Hellas. I denne delen av kapittelet kommer vi til å utforske det litt.

Proposisjon 5.12.5. La n være et naturlig tall slik at $n \geq 2$. La a være et naturlig tall. Anta at $a^n - 1$ er et primtall. Da er $a = 2$, og n er et primtall.

Bevis. La oss først bevise at $a = 2$. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 1.13.6 er

$$(a^n - 1) = (a - 1)\left(a^{n-1} + a^{n-2} + \cdots + a + 1\right).$$

(2) Siden $n \geq 2$, er

$$a^{n-1} + a_{n-2} + \cdots + a + 1 \geq a + 1.$$

Siden a er et naturlig tall, er $a + 1 > 1$. Dermed er

$$a^{n-1} + a_{n-2} + \cdots + a + 1 > 1.$$

(3) Siden $a^n - 1$ er et primtall, er 1 og $a^n - 1$ de eneste divisorene til $a^n - 1$.

(4) Det følger fra (1) – (3) at

$$a^{n-1} + a^{n-2} + \cdots + a + 1 = a^n - 1.$$

(5) Det følger fra (1) og (4) at

$$a^n - 1 = (a - 1)\left(a^n - 1\right).$$

Ut ifra Proposisjon 2.2.25 er da

$$a - 1 = 1,$$

altså $a = 2$.

La oss nå bevise at n er et primtall. Anta at det finnes et naturlig tall m slik at $m \mid n$. Da finnes det et naturlig tall k slik at $n = km$. Vi gjør følgende observasjoner.

(1) Da er

$$\begin{aligned} 2^n - 1 &= 2^{km} - 1 \\ &= (2^m)^k - 1. \end{aligned}$$

(2) Ut ifra Proposisjon 1.13.6 er

$$\left((2^m)^k - 1\right) = (2^m - 1)\left((2^m)^{k-1} + (2^m)^{k-2} + \cdots + 2^m + 1\right).$$

(3) Det følger fra (1) og (2) at

$$2^n - 1 = (2^m - 1)\left((2^m)^{k-1} + (2^m)^{k-2} + \cdots + 2^m + 1\right).$$

(4) Dersom $m > 1$, er $2^m - 1 > 1$.

(5) Siden $2^n - 1$ er et primtall, er 1 og $2^n - 1$ de eneste divisorene til $2^n - 1$.

(6) Det følger fra (3) – (5) at $2^m - 1 = 2^n - 1$, altså at $2^m = 2^n$. Da er $m = n$.

Således har vi bevist at, dersom $m \mid n$ og $m > 1$, er $m = n$. Derfor er n et primtall.

□

Eksempel 5.12.6. De eneste naturlige tallene i den andre kolonnen i tabellen i Eksempel 5.12.3 som er primtall er: 3, 7, 31, 127, og 8191. Vi får disse primtallene når n er 2, 3, 5, 7, og 13. Proposisjon 5.12.5 fastslår at alle disse verdiene av n er primtall. Dette er riktignok sant.

Eksempel 5.12.7. Siden 21 ikke er et primtall, fastslår Proposisjon 5.12.5 at det ikke er sant at $2^{21} - 1$ er et primtall. Dette er riktignok sant: $2^{21} - 1 = 2097151$, og $7 \mid 2097151$.

Merknad 5.12.8. Når p er ett av de første fire primtallene, altså 2, 3, 5, og 7, er $2^p - 1$ et primtall. Er $2^p - 1$ alltid et primtall når p er et primtall? Nei! Når $p = 11$, er

$$2^p - 1 = 2^{11} - 1 = 2047.$$

Siden $2047 = 23 \cdot 89$, er 2047 ikke et primtall.

For hvilke primtall p er $2^p - 1$ et primtall? Resten av denne delen av kapittelet handle om dette spørsmålet.

Proposisjon 5.12.9. La p være et primtall. Anta at $2p + 1$ er et primtall. Da har vi: enten $2p + 1 \mid 2^p - 1$ eller $2p + 1 \mid 2^p + 1$.

Bevis. Siden $2p + 1$ er et primtall, følger det fra Korollar 4.10.8 at

$$2^{(2p+1)-1} \equiv 1 \pmod{2p+1},$$

altså at

$$2^{2p} \equiv 1 \pmod{2p+1}.$$

Derfor er

$$2^{2p} - 1 \equiv 0 \pmod{2p+1}.$$

Siden

$$2^{2p} - 1 = (2^p - 1)(2^p + 1),$$

er da

$$(2^p - 1)(2^p + 1) \equiv 0 \pmod{2p+1}.$$

Siden $2p + 1$ er et primtall, følger det fra Proposisjon 4.2.12 at enten

$$2p + 1 \mid 2^p - 1$$

eller

$$2p + 1 \mid 2^p - 1.$$

□

Eksempel 5.12.10. Siden 3 er et primtall og $2 \cdot 3 + 1 = 7$ er et primtall, fastslår Proposisjon 5.12.9 at enten $7 \mid 2^3 - 1$ eller $7 \mid 2^3 + 1$. Siden $2^3 - 1 = 7$ og $7 \mid 7$, er dette riktignok sant.

Eksempel 5.12.11. Siden 5 er et primtall og $2 \cdot 5 + 1 = 11$ er et primtall, fastslår Proposisjon 5.12.9 at enten $11 \mid 2^5 - 1$ eller $11 \mid 2^5 + 1$. Siden $2^5 + 1 = 33$ og $11 \mid 33$, er dette riktignok sant.

Eksempel 5.12.12. Siden 11 er et primtall og $2 \cdot 11 + 1 = 23$ er et primtall, fastslår Proposisjon 5.12.9 at enten $23 \mid 2^{11} - 1$ eller $23 \mid 2^{11} + 1$. Siden $2^{11} - 1 = 2047$ og $23 \mid 2047$, er dette riktignok sant.

Merknad 5.12.13. Vi holder på med å svare på spørsmålet: for hvilke primtall p er $2^p - 1$ et primtall? Proposisjon 5.12.9 henleder oss deretter til spørsmålet: for hvilke primtall p, slik at $2p + 1$ er et primtall, er det tilfellet at $2p + 1 \mid 2^p - 1$? Ved hjelp av Korollar 5.9.21, svarer følgende proposisjon på dette.

Proposisjon 5.12.14. La p være et primtall. Anta at $2p + 1$ er et primtall. Dersom

$$2p + 1 \equiv 1 \pmod 8$$

eller

$$2p + 1 \equiv 7 \pmod 8),$$

har vi: $2p + 1 \mid 2^p - 1$. Ellers har vi: $2p + 1 \mid 2^p + 1$.

Bevis. Anta først at enten

$$2p + 1 \equiv 1 \pmod 8$$

eller

$$2p + 1 \equiv 7 \pmod 8).$$

Siden $2p+1$ er et primtall, følger det fra Korollar 5.9.21 at $\mathbb{L}^2_{2p+1} = 1$. Ut ifra Proposisjon 5.3.2 er da

$$2^{\frac{(2p+1)-1}{2}} \equiv 1 \pmod{2p + 1},$$

altså

$$2^p \equiv 1 \pmod{2p + 1}.$$

Det følger at

$$2^p - 1 \equiv 0 \pmod{2p + 1},$$

altså at

$$2p + 1 \mid 2^p - 1.$$

Anta istedenfor at verken

$$2p + 1 \equiv 1 \pmod 8$$

eller

$$2p + 1 \equiv 7 \pmod 8).$$

Da følger det fra Korollar 5.9.21 at $\mathbb{L}^2_{2p+1} = -1$. Ut ifra Korollar 5.3.12 er da

$$2^{\frac{(2p+1)-1}{2}} \equiv -1 \pmod{2p + 1},$$

altså

$$2^p \equiv -1 \pmod{2p+1}.$$

Det følger at

$$2^p + 1 \equiv 0 \pmod{2p+1},$$

altså at

$$2p+1 \mid 2^p + 1.$$

□

Eksempel 5.12.15. Vi har: 3 er et primtall og $2 \cdot 3 + 1 = 7$ er et primtall. Siden

$$7 \equiv 7 \pmod{8},$$

fastslår Proposisjon 5.12.14 at $7 \mid 2^3 - 1$. Siden $2^3 - 1 = 7$ og $7 \mid 7$, er dette riktignok sant.

Eksempel 5.12.16. Vi har: 5 er et primtall og $2 \cdot 5 + 1 = 11$ er et primtall. Siden

$$11 \equiv 3 \pmod{8},$$

fastslår Proposisjon 5.12.14 at $11 \mid 2^5 + 1$. Siden $2^5 + 1 = 33$ og $11 \mid 33$, er dette riktignok sant.

Eksempel 5.12.17. Vi har: 11 er et primtall og $2 \cdot 11 + 1 = 23$ er et primtall. Siden

$$23 \equiv 7 \pmod{8},$$

fastslår Proposisjon 5.12.14 at $23 \mid 2^{11} - 1$. Siden $2^{11} - 1 = 2047$ og $23 \mid 2047$, er dette riktignok sant.

Korollar 5.12.18. La p være et primtall. Anta at $2p + 1$ er et primtall. Dersom

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

har vi: $2p + 1 \mid 2^p - 1$.

Bevis. Dersom

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

følger det fra Korollar 3.2.63 at ett av følgende er sant:

(A) $p \equiv 3 \pmod{8}$;

(B) $p \equiv 7 \pmod{8}$.

Anta først at (A) er sant. Da er

$$2p + 1 \equiv 7 \pmod 8.$$

Det følger fra Proposisjon 5.12.14 at

$$2p + 1 \mid 2^p - 1.$$

Anta istedenfor at (B) er sant. Da er

$$2p + 1 \equiv 15 \equiv 7 \pmod 8.$$

Igjen følger det fra Proposisjon 5.12.14 at

$$2p + 1 \mid 2^p - 1.$$

□

Eksempel 5.12.19. Vi har: 3 er et primtall og $2 \cdot 3 + 1 = 7$ er et primtall. Siden

$$3 \equiv 3 \pmod 4,$$

fastslår Korollar 5.12.18 at $7 \mid 2^3 - 1$. Siden $2^3 - 1 = 7$ og $7 \mid 7$, er dette riktignok sant.

Eksempel 5.12.20. Vi har: 11 er et primtall og $2 \cdot 11 + 1 = 23$ er et primtall. Siden

$$11 \equiv 3 \pmod 4,$$

fastslår Korollar 5.12.18 at $23 \mid 2^{11} - 1$. Siden $2^{11} - 1 = 2047$ og $23 \mid 2047$, er dette riktignok sant.

Proposisjon 5.12.21. La p være et primtall slik at $p > 2$. La q være et primtall slik at $q \mid 2^p - 1$. Da finnes det et naturlig tall m slik at $q = 2mp + 1$.

Bevis. Vi gjør følgende observasjoner.

(1) La t være ordenen til 2 modulo q. Siden $q \mid 2^p - 1$, er

$$2^p \equiv 1 \pmod q.$$

Ut ifra Proposisjon 4.12.10, har vi da: $t \mid p$.

(2) Siden p er et primtall, er 1 og p de eneste divisorene til p. Derfor følger det fra (1) at enten $t = 1$ eller $t = p$.

(3) Anta at $t = 1$. Da er

$$2^1 \equiv 1 \pmod q,$$

altså $q \mid 2^1 - 1$. Dermed har vi: $q \mid 1$. Siden q er et primtall, er $q > 1$. Siden antakelsen at $t = 1$ fører til motsigelsen at både $q \mid 1$ og $q > 1$, konkluderer vi at det ikke er sant at $t = 1$. Derfor er $t = p$.

(4) Ut ifra Korollar 4.10.8 er

$$2^{q-1} \equiv 1 \pmod{q}.$$

Da følger det fra Proposisjon 4.12.10 at $t \mid q-1$.

(5) Det følger fra (3) og (4) at $p \mid q-1$. Dermed finnes det et naturlig tall k slik at $q-1 = kp$, altså slik at $q = kp+1$.

(6) Anta at

$$k \equiv 1 \pmod{2}.$$

Siden p er et primtall og $p > 2$, er

$$p \equiv 1 \pmod{2}.$$

Da er

$$q \equiv 1 \cdot 1 + 1 = 1 + 1 = 2 \equiv 0 \pmod{2}.$$

Det følger at $2 \mid q$. Siden $q \mid 2^p - 1$, følger det at $2 \mid 2^p - 1$. Da er

$$2^p - 1 \equiv 0 \pmod{2}.$$

Imidlertid er

$$2^p - 1 \equiv 1 \pmod{2}.$$

Ut ifra Proposisjon 3.2.11, kan det ikke være sant at både

$$2^p - 1 \equiv 0 \pmod{2}$$

og at

$$2^p - 1 \equiv 1 \pmod{2}.$$

Siden antakelsen at

$$k \equiv 1 \pmod{2}$$

fører til denne motsigelsen, konkluderer vi at det ikke er sant at

$$k \equiv 1 \pmod{2}.$$

Ut ifra Proposisjon 3.2.1, er da

$$k \equiv 0 \pmod{2},$$

altså har vi: $2 \mid k$. Dermed finnes det et naturlig tall m slik at $k = 2m$.

(7) Det følger fra (5) og (6) at $q = 2mp + 1$.

□

Eksempel 5.12.22. Vi har: $2^{11}-1 = 2047$, og $89 \mid 2047$. Siden 89 er et primtall, fastslår Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $89 = (2m) \cdot 11 + 1$. Dette er riktignok sant: $89 = (2 \cdot 4) \cdot 11 + 1$.

I tillegg har vi: $23 \mid 2047$. Siden 23 er et primtall, fastslår Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $23 = (2m) \cdot 11 + 1$. Dette er riktignok sant: $23 = (2 \cdot 1) \cdot 11 + 1$.

Eksempel 5.12.23. Vi har: $2^{29} - 1 = 536870911$, og en primtallsfaktorisering til 536870911 er

$$233 \cdot 1103 \cdot 2089.$$

Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $233 = (2m) \cdot 29 + 1$. Dette er riktignok sant: $89 = (2 \cdot 4) \cdot 29 + 1$.

I tillegg fastslår Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $1103 = (2m) \cdot 29 + 1$. Dette er riktignok sant: $1103 = (2 \cdot 19) \cdot 29 + 1$.

I tillegg fastslår Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $2089 = (2m) \cdot 29 + 1$. Dette er riktignok sant: $2089 = (2 \cdot 36) \cdot 29 + 1$.

Proposisjon 5.12.24. La p være et primtall slik at $p > 2$. La q være et primtall slik at $q \mid 2^p - 1$. Da er enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 5.12.21, finnes det et naturlig tall m slik at $q = 2mp + 1$.

(2) Ut ifra Proposisjon 5.3.2, er

$$\mathbb{L}_q^2 \equiv 2^{\frac{q-1}{2}} \pmod q.$$

(3) Det følger fra (1) at

$$2^{\frac{q-1}{2}} = 2^{\frac{(2mp+1)-1}{2}} = 2^{mp} = (2^p)^m.$$

Dermed følger det fra (2) at

$$\mathbb{L}_q^2 \equiv (2^p)^m.$$

(4) Siden $q \mid 2^p - 1$, er

$$2^p - 1 \equiv 0 \pmod q,$$

altså er

$$2^p \equiv 1 \pmod q.$$

(5) Det følger fra (3) og (4) at

$$\mathbb{L}_q^2 \equiv 1^m = 1 \pmod p.$$

Ut ifra Proposisjon 5.5.3 er da $\mathbb{L}_q^2 = 1$.

(6) Det følger fra (5) og Korollar 5.9.21 at enten

$$q \equiv 1 \pmod 8,$$

eller

$$q \equiv 7 \pmod 8.$$

□

Eksempel 5.12.25. Vi har: $2^{11} - 1 = 2047$, og $89 \mid 2047$. Siden 89 er et primtall, fastslår Proposisjon 5.12.24 at enten

$$89 \equiv 1 \pmod 8$$

eller

$$89 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$89 \equiv 1 \pmod 8.$$

I tillegg har vi: $23 \mid 2047$. Siden 23 er et primtall, fastslår Proposisjon 5.12.24 at enten

$$23 \equiv 1 \pmod 8$$

eller

$$23 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$23 \equiv 7 \pmod 8.$$

Eksempel 5.12.26. Vi har: $2^{29} - 1 = 536870911$, og en primtallsfaktorisering til 536870911 er

$$233 \cdot 1103 \cdot 2089.$$

Proposisjon 5.12.24 fastslår at enten

$$233 \equiv 1 \pmod 8$$

eller

$$233 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$233 \equiv 1 \pmod 8.$$

I tillegg fastslår Proposisjon 5.12.24 at enten

$$1103 \equiv 1 \pmod 8$$

eller

$$1103 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$1103 \equiv 7 \pmod 8.$$

I tillegg fastslår Proposisjon 5.12.24 at enten

$$2089 \equiv 1 \pmod 8$$

eller

$$2089 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$2089 \equiv 1 \pmod 8.$$

Lemma 5.12.27. La n være et naturlig tall. La m være et naturlig tall slik at $m^2 \leq n$ og $(m+1)^2 > n$. Dersom det finnes et naturlig tall a slik at $a \mid n$, finnes det et naturlig tall b slik at $b \mid n$ og $b \leq m$.

Bevis. Ett av følgende er sant:

(A) $a \leq m$;

(B) $a > m$.

Anta først at (A) er sant. Ved å la b være a, er da lemmaet sant.

Anta istedenfor at (B) er sant. Siden $a \mid n$, finnes det et naturlig tall b slik at $n = ba$. Dersom $b > m$, er

$$n = ba > m \cdot m = m^2.$$

Imidlertid har vi antatt at

$$m^2 \leq n.$$

Siden antakelsen at $b > m$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $b > m$. Derfor er $b \leq m$.

□

Eksempel 5.12.28. La n være 54, og la m være 7. Da er $m^2 = 49 < 54$ og $(m+1)^2 = 8^2 = 64 > 54$. Vi har: $9 \mid 54$. Da fastslår Lemma 5.12.27 at det finnes et naturlig tall b slik at $b \leq 7$ og $b \mid 54$. Dette er riktignok sant: $6 \leq 7$, og $6 \mid 54$.

Eksempel 5.12.29. La n være 86, og la m være 9. Da er $m^2 = 81 < 86$ og $(m+1)^2 = 10^2 = 100 > 86$. Vi har: $43 \mid 86$. Da fastslår Lemma 5.12.27 at det finnes et naturlig tall b slik at $b \leq 9$ og $b \mid 86$. Dette er riktignok sant: $2 \leq 9$, og $2 \mid 86$.

Merknad 5.12.30. For et hvilket som helst naturlig tall n, finnes det faktisk et naturlig tall m slik at $m^2 \leq n$ og $(m+1)^2 > n$, nemlig det størstest naturlige tallet som er mindre enn eller likt $\sqrt{n}$. Når $n = 23$, er for eksempel $\sqrt{23} \approx 4.80$. Derfor er $m = 4$. Det er riktignok sant at $4^2 = 16 \leq 23$ og at $5^2 = 25 > 23$.

Imidlertid er dette resultatet ikke viktig for oss. Derfor kommer vi ikke til å gi et bevis for det.

Korollar 5.12.31. La p være et primtall slik at $p > 2$. La m være et naturlig tall slik at $m^2 \leq 2^p - 1$ og $(m+1)^2 > 2^p - 1$. Dersom $2^p - 1$ ikke er et primtall, finnes det et primtall q slik at $q \mid 2^p - 1$, $q \leq m$, og enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

Bevis. Vi gjør følgende observasjoner.

(1) Dersom $2^p - 1$ ikke er et primtall, finnes det et naturlig tall a slik at $a \mid 2^p - 1$ og $n > 1$. Ut ifra Lemma 5.12.27, finnes det da et naturlig tall b slik at $b \mid 2^p - 1$ og $b \leq m$.

(2) Ut ifra Korollar 4.3.19, finnes det et primtall q slik at $q \mid b$. Ut ifra Proposisjon 2.5.30 er $q \leq b$, altså $q \leq m$.

(3) Det følger fra (1), (2), og Proposisjon 2.5.27 at $q \mid 2^p - 1$.

(4) Det følger fra Proposisjon 5.12.24 at enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

□

Eksempel 5.12.32. La oss bevise at $2^7 - 1$ er et primtall. Vi har: $2^7 - 1 = 127$ og $11^2 = 121 < 127$ og $12^2 = 144 > 127$. Anta at $2^7 - 1$ ikke er et primtall. Da følger det fra Korollar 5.12.31 at det finnes et primtall q slik at $q \mid 127$, $q \leq 11$, og enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

Det eneste primtallet som oppfyller disse kravene er 7. Det er ikke sant at $7 \mid 127$. Vi konkluderer at $2^7 - 1$ er et primtall.

Eksempel 5.12.33. La oss bevise at $2^{13} - 1$ er et primtall. Vi har: $2^{13} - 1 = 8191$ og $90^2 = 8100 < 8191$ og $91^2 = 8281 > 8191$. Anta at $2^{13} - 1$ ikke er et primtall. Vi gjør følgende observasjoner.

(1) Det følger fra Korollar 5.12.31 at det finnes et primtall q slik at $q \mid 8191$, $q \leq 90$, og enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

(2) Det følger fra Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $q = (2m) \cdot 13 + 1$, altså $q = 26m + 1$.

Det eneste naturlige tallene q slik at $q \leq 90$ som oppfyller (2) er: 27, 53, og 79. Det eneste av disse tre naturlige tallene som er kongruent enten til 1 eller til 7 modulo 8 er 79. Det er ikke sant at $79 \mid 8191$. Vi konkluderer at $2^{13} - 1$ er et primtall.

Eksempel 5.12.34. La oss bevise at $2^{17} - 1$ er et primtall. Vi har: $2^{17} - 1 = 131071$ og $362^2 = 131044 < 131071$ og $363^2 = 131769 > 131071$. Anta at $2^{17} - 1$ ikke er et primtall. Vi gjør følgende observasjoner.

(1) Det følger fra Korollar 5.12.31 at det finnes et primtall q slik at $q \mid 131071$, $q \leq 362$, og enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8).$$

(2) Det følger fra Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $q = (2m) \cdot 17 + 1$, altså $q = 34m + 1$.

De eneste naturlige tallene q slik at $q \leq 362$ som oppfyller (2) er:

$$35, 69, 103, 137, 171, 205, 239, 273, 307, 341.$$

De eneste av disse naturlige tallene som er kongruente enten til 1 eller til 7 modulo 8 er: 103, 137, 239, og 273. Ingen av disse fire naturlige tallene deler 131071. Vi konkluderer at $2^{17} - 1$ er et primtall.

Istedenfor å ha sjekket om ett av de fire naturlige tallene 103, 137, 239, og 273 deler 131071, kunne vi ha først observert at 273 ikke er et primtall, og dermed ikke oppfyller (1). Da hadde vært nok å sjekke om ett av de tre naturlige tallene 103, 137, og 239 deler 131071.

Merknad 5.12.35. I Eksempel 5.12.3 fant vi de første fem Mersenne-primtallene: 3, 7, 31, 127, og 8191. Faktisk er det kun 48 kjente Mersenne-primtall! Det 48-ende ble oppdaget i 2013: det er $2^{57885161} - 1$, og har 17425170 sifre. Dette er det største kjente primtallet.

Når datamaskiner leter etter større og større primtall, er Mersenne-primtall hovedsakelig fokuset. Grunnen for dette er at vi kan benytte kvadratisk gjensidighet og andre teoretiske verktøy for å komme fram til resultater som ligner på Proposisjon 5.12.21 og Korollar 5.12.31. Disse resultatene gir oss en bedre forståelse for de naturlige tallene som kan dele et Mersenne-tall enn de naturlige tallene som kan dele et hvilket som helst naturlig tall.

Oppgaver

O5.1 Oppgaver i eksamens stil

Oppgave O5.1.11. Hvilke av følgende Mersenne-tall er primtall? Begrunn svaret.

(1) $2^{18} - 1$.

(2) $2^{19} - 1$.

(3) $2^{41} - 1$.