Mersennetall og deres primtallsfaktorer

Jakob Peder Pettersen

8. juli 2017

Sammendrag

Dette beviset tar for seg Mersennetallene og deres primtallsfaktorer. Spesielt handler dette teoremet om hvilke Mersennetall som er primtall.

Innhold

1 Definisjoner brukt i beviset

1.1 Mersennetallene

1.1.1 Grunnleggende definisjon

For $n \geq 1$, er det n-te Mersennetallet (M_n) definert ved:

$$M_n = 2^n - 1$$

Tallet n kalles heretter indekser til Mersennetallet.

1.1.2 Mersenneprimtall

Dersom M_n er et primtall, kalles da M_n et Mersenneprimtall. n blir da kalt en primtallgenerende indeks.

1.2 Største felles divisor

Største felles divisor mellom to heltall a og b, notert som $\gcd(a, b)$ er definert som det største naturlige tallet som deler både a og b.

1.3 Eulers ϕ-funksjon

La n være et naturlig tall. Da er $\phi(n)$ definert som antall naturlige tall k slik $\gcd(n, k) = 1$

1.4 Delelighet

Dersom $a, b \in \mathbb{Z}$, betyr $a \mid b$ at a deler b, det vil si at det finnes et tall $k \in \mathbb{Z}$ slik at $b = k \cdot a$. I motsatt fall sier vi at a ikke deler b og skriver $a \nmid b$.

2 Teori brukt i beviset

2.1 Eulers teorem

Dersom $\gcd(a, n)$, så gjelder:

$$a^{\phi(n)} \equiv 1 \mod n \tag{1}$$

3 Felles faktorer mellom Mersennetall

Teorem 3.1. *Største felles devisor mellom to Mersennetall er selv et Mersennetall, nærmere bestemt det Mersennetallet som har indeksen som er største felles divisor til indeksene til de to opprinnelige Mersennetallene, altså:*

$$\gcd(M_a, M_b) = M_{\gcd(a,b)}$$

For å vise dette trenger vi følgende lemma:

Lemma 3.2. *For alle $a, b \in \mathbb{N}^+$ så er:*

$$M_a \mid M_{a \cdot b}$$

Bevis. Opplagt gjelder:

$$M_a = 2^a - 1 \equiv 0 \pmod{M_a} \tag{2}$$

Dette kan omformes til:

$$2^a \equiv 1 \pmod{M_a} \tag{3}$$

og igjen til:

$$(2^a)^b \equiv 1^b \equiv 1 \pmod{M_a} \tag{4}$$

Dette er det samme som:

$$M_{a\cdot b} = 2^{a\cdot b} - 1 \equiv 0 \pmod{M_a} \tag{5}$$

og følgelig:

$$M_a \mid M_{a\cdot b} \tag{6}$$

□

Videre til hovedresultatet har vi:

Bevis. Vi vet at vi kan skrive:

$$\gcd(a,b) = t\cdot a + s\cdot b \tag{7}$$

der $t, s \in \mathbb{Z}$. Imidlertid må nøyaktig ett av tallene s og t være positivt og det andre må være null eller negativt. Dersom det ene tallet er null, vil vi da imidlertid ha at

$$\gcd(a,b) = k\cdot \min(a,b) \tag{8}$$

, noe som gir:

$$\gcd(a,b) = \min(a,b) \tag{9}$$

og følgelig $\min(a,b) \mid \max(a,b)$. I dette spesialtilfellet sørger lemmaet for at $M_{\min(a,b)} \mid M_{\max(a,b)}$ og følgelig at

$$\gcd(M_a, M_b) = M_{\gcd(a,b)}$$

Dersom ingen av tallene s og t er null, la da d være en felles divisor av M_a og M_b. Da vet vi: $d \mid M_{|t|\cdot a}$ og $d \mid M_{|s|\cdot b}$ (merk absoluttverditegnene). Av dette har vi at $d \mid \left|M_{|t|\cdot a} - M_{|s|\cdot b}\right|$. Følgelig blir:

$$\left|M_{|t|\cdot a} - M_{|s|\cdot b}\right| = \left|\left(2^{|t|\cdot a} - 1\right) - \left(2^{|s|\cdot b} - 1\right)\right| = \left|2^{|t|\cdot a} - 2^{|s|\cdot b}\right| = \tag{10}$$

$$\left|2^{\min\left(|t|\cdot a,|s|\cdot b\right)} \cdot \left(2^{\max\left(|t|\cdot a,|s|\cdot b\right)-\min\left(|t|\cdot a,|s|\cdot b\right)} - 1\right)\right| = \left|2^{\min\left(|t|\cdot a,|s|\cdot b\right)} \cdot \left(2^{\left||t|\cdot a-|s|\cdot b\right|} - 1\right)\right| = \tag{11}$$

$$\left|2^{\min\left(|t|\cdot a,|s|\cdot b\right)} \cdot \left(2^{t\cdot a+s\cdot b} - 1\right)\right| = 2^{\min\left(|t|\cdot a,|s|\cdot b\right)} \cdot M_{t\cdot a+s\cdot b} = \tag{12}$$

$$2^{\min\left(|t|\cdot a,|s|\cdot b\right)} \cdot M_{\gcd(a,b)} \tag{13}$$

Altså har vi da at $d \mid 2^{\min\left(|t|\cdot a,|s|\cdot b\right)} \cdot M_{\gcd(a,b)}$, men Mersennetallene er alltid oddetall, så $\gcd\left(d, 2^{\min\left(|t|\cdot a,|s|\cdot b\right)}\right) = 1$, så vi får: $d \mid M_{\gcd(a,b)}$. På den annen side har vi av lemmaet at $M_{\gcd(a,b)} \mid M_a$ og $M_{\gcd(a,b)} \mid M_b$. Altså må vi da ha at

$$\gcd(M_a, M_b) = M_{\gcd(a,b)} \tag{14}$$

□