Wiederholung:

Proposition 2.5: Eine gerade Zahl $n \in 2\mathbb{N}$ ist vollkommen
$\Leftrightarrow$ n hat die Form $n = 2^m(2^{m+1}-1)$ $m \in \mathbb{N}$
und $2^{m+1}-1$ ist eine Mersennesche Primzahl.

Für den Beweis brauchen wir

Def: Die Teilersummenfunktion $\sigma: \mathbb{N}^+ \to \mathbb{N}^+$ ist definiert durch

$$\sigma(n) := \sum_{\substack{d \in \mathbb{N}^+ \\ d \mid n}} d$$

Bemerkung: Falls $(a,b) = 1$ gilt $\sigma(ab) = \sigma(a)\sigma(b)$

Beweis der Proposition 2.5:

$\Leftarrow$: (Euklid) Sei $n = 2^m(2^{m+1}-1)$ wobei $2^{m+1}-1 \in \mathbb{P}$

Dann ist $\sigma(n) = \sigma(2^m)\sigma(2^{m+1}-1)$
$= (2^{m+1}-1)\cdot(1 + 2^{m+1}-1)$
$= (2^{m+1}-1)\,2^{m+1}$
$= 2n.$

$\Rightarrow$: (Euler) Sei $n = 2^m b$ eine gerade vollkommene Zahl
mit b ungerade, $m \geq 1$

Dann gilt $2n = \sigma(n) = \sigma(2^m)\sigma(b)$
$= (2^{m+1}-1)\sigma(b)$
$\Rightarrow 2^{m+1} b = (2^{m+1}-1)\sigma(b)$

Da 2^{m+1} ungerade ist, gilt

$$2^{m+1}-1 \mid b$$

d.h. $b = (2^{m+1}-1)\cdot a$ für ein $a \in \mathbb{N}$

Zu zeigen ist, dass $a=1$ und $2^{m+1}-1$ eine Primzahl ist.

Angenommen $a > 1$.

Dann ist $\sigma(b) \geq 1 + (2^{m+1}-1) + a + b$

$= 2^{m+1} + a + (2^{m+1}-1)a$

$= 2^{m+1}(a+1)$

Also ist $2^{m+1} b = (2^{m+1}-1)\sigma(b)$

$\geq (2^{m+1}-1) 2^{m+1}(a+1)$

$\Rightarrow \quad b \geq (2^{m+1}-1)(a+1)$

$= b + 2^{m+1} - 1$ ↯ $(m \geq 1)$

Angenommen $b = 2^{m+1}-1 \notin \mathbb{P}$

Sei c ein nicht-trivialer Teiler.

Dann ist $2n = \sigma(n) = (2^{m+1}-1)\sigma(b)$

$\geq (2^{m+1}-1)(1+c+b)$

$= 2^{m+1} b - b + (2^{m+1}-1)(1+c)$

$= 2^{m+1} b - (2^{m+1}-1) + (2^{m+1}-1)(1+c)$

$= 2^{m+1} b + (2^{m+1}-1)c$

$> 2^{m+1} b$

$> 2n$ ↯

Also ist $b = 2^{m+1}-1$ eine Mersennesche Primzahl. □

Bemerkungen:

- $2^n - 1 \in \mathbb{P} \Rightarrow n \in \mathbb{P}$

  aber die Rückrichtung gilt <u>nicht</u>, z.B. $2^{11} - 1 = 2047 = 23 \cdot 89$

- Es ist nicht bekannt, ob es unendlich viele Mersennesche Primzahlen gibt
  ob es unendlich viele Mersennesche Nichtprimzahlen gibt.

- Man kennt bisher 47 Mersennesche Primzahlen
- Die 9 größten bisher bekannten Primzahlen sind alle Mersennesche Primzahlen.

- Es ist auch unbekannt, ob es ungerade vollkommene Zahlen gibt
  (Es gibt keine kleiner als 10^{1500})

Def: Seien $F_n := 2^{2^n} + 1$ $(n \in \mathbb{N})$ die Fermatsche Zahlen

$F_0 = 3$
$F_1 = 5$
$F_2 = 17$
$F_3 = 257$
$F_4 = 65537$

} sind alle prim.

Fermat hat vermutet, dass jedes F_n prim ist.
Diese Vermutung wurde von Euler widerlegt.

Proposition 2.6: (Euler) $641 \mid F_5 = 2^{32} - 1$

Beweis: $5 \cdot 2^7 = 641 - 1$

$5^4 \cdot 2^{28} = (641-1)^4$

$= a \cdot 641 + (-1)^4$ für ein $a \in \mathbb{N}$

$= 641a + 1$

Es gilt auch $641 = 625 + 16$

$= 5^4 + 2^4$

$\Rightarrow \quad 2^4 = 641 - 5^4$

Also ist $F_5 = 2^{32} + 1$

$= 2^4 \cdot 2^{28} + 1$

$= (641 - 5^4) 2^{28} + 1$

$= 641 \cdot 2^{28} - (641a + 1) + 1$

$= 641 (2^{28} - a)$ □

Bemerkung: • Euler hat sogar bewiesen, dass

$F_5 = 641 \cdot 6700417$

die Primfaktorzerlegung ist.

• keine weiteren Fermatschen Primzahlen ($n \geq 5$) sind bisher bekannt.

• Es ist bekannt, dass für $5 \leq n \leq 32$, F_n nicht prim ist.

Lemma 2.7: Seien $m, n \in \mathbb{N}$, $m \neq n$

Dann ist $(F_m, F_n) = 1$

Beweis: Sei $m < n$ (oBdA)

und $\forall k \in \mathbb{N}$ sei $G_k := F_k - 2 = 2^{2^k} - 1$

Dann ist $F_k G_k = (2^{2^k} + 1)(2^{2^k} - 1)$

$$= (2^{2^k})^2 - 1$$

$$= 2^{2 \cdot 2^k} - 1$$

$$= 2^{2^{k+1}} - 1$$

$$= G_{k+1}$$

Induktiv gilt

$$G_n = G_m \prod_{i=m}^{n-1} F_i$$

Insbesondere $F_m \mid G_n = a \cdot F_m$ für $a = G_m \prod_{i=m+1}^{n-1} F_i$

Sei $d = (F_m, F_n)$

Dann gilt $d \mid (F_n - a F_m) = F_n - G_n = 2$

Also gilt $d = 1$ oder $d = 2$

Aber F_m, F_n sind ungerade

Also ist $d = 1$. □

Korollar: (Satz von Euklid) Es gibt unendlich viele Primzahlen.

Beweis 2: Sei f_n der kleinste Teiler von F_n größer als 1.

Dann sind alle f_n Primzahlen (L 2.1) und paarweise verschieden (L 2.7) □

Verteilung der Primzahlen

Def: Wir bezeichnen die k-te Primzahl mit p_k

$p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ---

Lemma 2.8: Sei $a_k := p_{k+1} - p_k$

Dann ist die Folge $(a_k)_{k \in \mathbb{N}}$ unbeschränkt

d.h. es gibt beliebig große „Lücken" zwischen den Primzahlen.

Beweis: Übungsaufgabe

Allerdings gilt $p_{k+1} \leq \left(\prod_{i=1}^{k} p_i\right) + 1$ (siehe den ersten Beweis vom Satz von Euklid).

Es gilt sogar:

Satz 2.9: $\forall k \in \mathbb{N}$ gilt $p_k < p_{k+1} < 2p_k$

d.h. $a_k < p_k$

Dieser Satz heisst das Postulat von Bertrand und wurde von Tschebyscheff bewiesen.
Wir lassen den Beweis aus.

Def: Wir bezeichnen mit $\mathbb{R}$ die Menge aller reellen Zahlen.

Wir definieren die Primzahlanzahlfunktion $\pi: \mathbb{R} \to \mathbb{N}$ durch

$$\pi(x) = \left|\{p \in \mathbb{P} : p \leq x\}\right|$$

Satz 2.10 (Primzahlsatz von Hadamard)

Es gilt $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$

d.h. $\pi(x) \sim \frac{x}{\ln(x)}$

Bemerkung: Aus der Riemannschen Vermutung würde die stärkere Aussage

$$\pi(x) = \int_2^x \frac{1}{\ln(t)}\,dt + O(\sqrt{x}\ln(x))$$

folgen.

Wir beweisen nur den schwächeren Satz:

Satz 2.11: (Tschebyscheff) $\forall\, n \in \mathbb{N}$ gilt

$$\frac{1}{4}\frac{n}{\ln(n)} \leq \pi(n) \leq 6\frac{n}{\ln(n)}$$

Für den Beweis (nächstes Mal) brauchen wir folgendes

Bemerkung: $2^n < \binom{2n}{n} < 4^n$ für $n > 1$ (Aufgabe)

so gilt auch $n\ln(2) < \ln((2n)!) - 2\ln(n!) < 2n\ln(2)$

Def: Für eine reelle Zahl x bezeichnen wir mit $\lfloor x \rfloor$ die größte ganze Zahl n sodass $n \leq x$

$\nu_p(n)$ bezeichnet die größte Zahl m sodass $p^m \mid n$

Also den Exponent von p in der Primfaktorzerlegung

$$n = \prod_{p\in\mathbb{P}} p^{\nu_p(n)}$$