WiSe '21/'22, hhu
K. Halupczok

# Vorlesung Einführung in die Zahlentheorie

## EZ 15: Fermat- und Mersenne-Primzahlen

**Stichworte:** Fermatzahlen, regelmäßige n-Ecke, Pepins Test, Mersennezahlen, Sophie-Germain-Pz-paare, Lucas-Test, Wieferich-Pz, vollkommene Zahlen

---

15.1. **Einleitung:** Wir führen das Primzahltestproblem fort zur Frage nach Tests für spezielle Pzen:
Gibt es unendliche Folgen von Pzen, die leicht anzugeben sind?
Anscheinend nicht. Fermat vermutete $2^{2^n}+1 = F_n$, und tatsächlich sind $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ prim, aber $641 \mid F_5$, d.h. $F_5$ nicht prim (vgl. ü Aufg. 4 Bl. 9, [Euler 1732]).

15.2. **Bem.:** $2^k+1$ prim $\Rightarrow$ $k$ eine 2er-Potenz $k=p^m$ mit $p>2 \Rightarrow 2^m+1 \mid 2^{mp}+1$,
denn Polynomdiv. liefert Quotienten $\sum_{i=0}^{p-1} (-1)^i 2^{mi} \in \mathbb{Z}$.

15.3. **Def:** $F_n := 2^{2^n}+1$ heißt **n-te Fermatzahl**. Eine Pz dieser Form heißt **Fermatsche Primzahl**.
**Motivation:** Kann man von $F_n$ leicht "testen", ob sie prim/zus.gesetzt ist?

15.4. **Satz** (Gauß, Konstruktion regelmäßiger n-Ecke, aus Algebra-Vor. bekannt):
Ein regelmäßiges n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n$ von der Gestalt $n = 2^\nu p_1 p_2 \cdots p_r$ mit p.w.v. Fermatschen Primzahlen $p_1, \dots, p_r$ ist (und bel. $\nu \in \mathbb{N}_0$, auch $r=0$ zugelassen).

15.5. **Bem.:** (1) So ist z.B. das 17-Eck m.Z.u.L. konstruierbar, das 7-Eck oder 9-Eck hingegen nicht.
(2) Für $n \geq 3$ hat jeder Primteiler von $F_n$ die Gestalt $p = t\,2^{n+2}+1$. (ü Aufg. 4c) Blatt 9)
Damit leicht zu sehen: $F_5 = 2^{32}+1$ ist Produkt von $641 = 5\cdot 2^7+1$ und $52347 \cdot 2^7+1$.
(3) $F_6$ ist nicht prim, sondern teilbar durch $274177 = 1+1072 \cdot 2^9$ [Clausen 1855].
(4) $F_n$ ist nicht prim für $5 \leq n \leq 40$
(5) Derzeit bei 305 Fermatzahlen entschieden, dass sie nicht prim.
Bei allen anderen offen! Die größte: $F_{33297780}$, hat Teiler $193 \cdot 2^{33297780}+1$.
(Stand: 27. Mai 2019)

15.6. **Satz:** $F_{n+1} - 2 = \prod_{k=0}^{n} F_k$. Insb.: $m > n \Rightarrow (F_m, F_n) = 1$.

**Bew.:** (ii) Blatt 2, Aufg. 1. □

15.7. **Bem.:** Für welche ungeraden $n$ ist die Konstruktion des regelmäßigen $n$-Ecks m.Z.u.L. möglich? Laut aktuellem Stand nach Satz 15.4 für $n = 3 \cdot 5 \cdot 17 \cdot 257 \cdot \underbrace{65537}_{F_4} \overset{15.6}{=} F_5 - 2 = 2^{32} - 1 = 4.294.967.295$.
Falls es nach $F_4$ keine weiteren Fermat-Pzen gibt (ist vermutlich so), gibt es kein größeres solches $n$.

Für Fermatzahlen gibt es einen recht effizienten Primalitätstest:

15.8. **Satz (Pepins Test):** Sei $n \geq 2$ und $g$ eine ganze zu $F_n$ teilerfremde Zahl mit $\left(\frac{g}{F_n}\right)_{\text{Jacobi}} = -1$. Dann sind äquivalent:
(i) $F_n$ ist prim, (ii) $g^{\frac{F_n - 1}{2}} \equiv -1 \ (F_n)$, (iii) $\operatorname{ord}(g \bmod F_n) = F_n - 1 = 2^{2^n}$.

**Bew.:** (i) $\Rightarrow$ (ii): Klar nach Euler-Kriterium, (ii) $\Rightarrow$ (iii): Aus (ii) folgt $g^{F_n - 1} \equiv 1 \ (F_n)$, also ist $\operatorname{ord}_{F_n}(g)$ ein Teiler von $F_n - 1 = 2^{2^n}$, d.h. eine Zer-Potenz.
Nach (ii) ist $g^{2^{2^n - 1}} \not\equiv 1 \ (F_n)$, also muss $\operatorname{ord}_{F_n}(g) = 2^{2^n} = F_n - 1$ sein.
(iii) $\Rightarrow$ (i): Aus (iii) folgt $F_n - 1 \mid \varphi(F_n)$, insb. $\varphi(F_n) \geq F_n - 1$. Jede der Zahlen $1, 2, 3, \ldots, F_n - 1$ ist also teilerfremd zu $F_n$, d.h. $F_n$ ist prim. □

15.9. **Bem.:** • Der Test ist anwendbar z.B. mit $g = 3$, 5 oder 10.
Denn $F_n = 2^{2^n} + 1 \equiv 2^{2 \cdot 2^{n-1}} + 1 \equiv 1 + 1 \equiv 2 \ (3)$, also $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$.
Für $n \geq 2$ ist $F_n = 2^{4 \cdot 2^{n-2}} + 1 \equiv 1 + 1 = 2 \ (5)$, also $\left(\frac{5}{F_n}\right) = \left(\frac{F_n}{5}\right) = \left(\frac{2}{5}\right) = -1$.
Weiter $(10, F_n) = 1$ und $\left(\frac{10}{F_n}\right) = \left(\frac{2}{F_n}\right)\left(\frac{5}{F_n}\right) = \left(\frac{5}{F_n}\right) = -1$.
• Pepins Test ist wegen (ii) ein algorithmisch "schneller" Test. Auf ihm (mit Verfeinerungen) beruhen die Ergebnisse aus 15.5 (4), (5).

Weitere interessante nat. Zahlen, für die es (schnelle) spezielle PZ tests gibt, sind diese:

15.10. **Def.:** Für eine PZ $p$ heißt $M_p := 2^p - 1$ eine **Mersennezahl.**
Ist $M_p$ prim, heißt $M_p$ **Mersennesche Primzahl.**
- (Mersenne 1588–1648) untersuchte $M_p$ für $p \leq 257$.
- Leibniz vermutete: alle $M_p$ prim!?

15.11. **Bem.:** (1) $2^k - 1$ prim $\Rightarrow$ $k$ prim [$2^a - 1 \mid 2^{ab} - 1$; Quotient ist $1 + 2^a + 2^{2a} + \ldots + 2^{(b-1)a}$]
(2) $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ prim
(3) $M_{11}$ nicht prim: $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ [Fermat]
(4) Für $23 \leq p \leq 100$ ist nur $M_{31}$, $M_{61}$, $M_{89}$ prim [$M_{61}$ wurde im Jahr 1886 bestätigt]
Fermat zeigte: $M_{37}$ nicht prim.
Euler vermutete: $M_{41}$, $M_{47}$ nicht prim
(5) Mersenne hat 5 Fehler gemacht: $M_{61}$, $M_{89}$, $M_{107}$ "vergessen",
$M_{67}$, $M_{257}$ fälschlicherweise als prim behauptet
(6) Für $100 \leq p \leq 257$ sind nur $M_{107}$, $M_{127}$ prim [$M_{127}$ von Lucas im Jahr 1876 bewiesen]
Bis 1951 war $M_{127}$ die größte (numerisch) bekannte PZ.
(7) Vermuten könnte man: $p$ Mersennesche PZ $\Rightarrow$ $M_p$ prim
Wahr für $M_3$, $M_7$, $M_{31}$, $M_{127}$ prim, aber $M_{8191} = M_{M_{13}}$ nicht prim.
(8) Für $p \leq 12\,000$ sind genau 23 PZen $M_p$, $M_{11213}$ die größte davon.
(9) Bislang >50 Mersenne-PZen bekannt,
aktuell größte (numerisch) bekannte PZ: $M_{82\,589\,933}$
mit 24 862 048 Stellen. [Seit 7.12.2018, www.mersenne.org, Projekt "GIMPS"]

15.12. **Satz** (Euler): Für $p$ prim gilt: $p \equiv 3 \ (4)$ und $2p+1$ prim $\Leftrightarrow$ $2p+1$ teilt $M_p$. [o.B.]

15.13. **Bem.:** • Jeder Primteiler $q$ von $M_p$, $p \geq 3$, hat die Gestalt $q = 2ap + 1$.
**Bew.:** Sei $q \mid 2^p - 1$ $\Rightarrow$ $2^p \equiv 1 \ (q)$ $\Rightarrow$ $p = \mathrm{ord}_q(2)$
$\Rightarrow p \mid q-1$ $\Rightarrow$ $q = 1 + ap$ $\overset{2 \nmid p,q}{\Rightarrow}$ $2 \mid a$, Beh. ✓ □
• $2p + 1 = 2^p - 1 \Rightarrow p = 3$.

15.14. **Def.:** Ein Primzahlpaar $(p, 2p+1) \in \mathbb{P}^2$ bzw. $(\frac{p-1}{2}, p) \in \mathbb{P}^2$ heißt ein **Sophie-Germain-Primzahlpaar.** (Vgl. Bem. 14.7 zu Sophie Germain).

15.15. Bem.: Wie bei PZ-Zwillingspaaren $(p, p+2) \in \mathbb{P}^2$ geht man bei Sophie-Germain-PZpaaren $(p, 2p+1) \in \mathbb{P}^2$ davon aus, dass es $\infty$ viele gibt; diese Vermutungen sind bislang unbewiesen.

15.16. Anwendung auf $p=37$: $q \mid M_{37}$ prim $\overset{15.13}{\Rightarrow}$ $q = 1+2pk$: ~~75~~, 149, 223, ...
- $2^{37} \equiv 1 \ (149)$, da $2^{37 \cdot 2} = 2^{\frac{149-1}{2}} \equiv \left(\frac{2}{149}\right) = -1$.
- $2^{37} \equiv 1 \ (223)$, da $2^8 \equiv 256 \equiv 33 \ (223)$, $2^{16} \equiv 1089 \equiv -26$
$2^{32} \equiv 676 \equiv 7$, $2^{37} \equiv 7 \cdot 2^5 \equiv 7 \cdot 32 = 224 \equiv 1 \ (223)$.

Also: $223 \mid M_{37}$ zus'gesetzt.

Auch für Mersenne-Zahlen gibt es einen sehr schnellen PZtest:

15.17. Satz (Lucas-Test): Def. (Lucas-)Folge $s_1, s_2, s_3, \ldots$ durch $s_1 := 4$, $s_{n+1} := s_n^2 - 2$.
[Also 4, 14, 194, 37634, ...] Dann: $M_p$ prim $\Leftrightarrow s_{p-1} \equiv 0 \ (M_p)$. [o.B.]

Bsp.: $M_7 = 2^7 - 1 = 127$, $s_3 = 194 \equiv 67$, $s_4 \equiv s_3^2 - 2 \equiv 67^2 - 2 \equiv 42$, $s_5 \equiv 42^2 - 2 \equiv 111$, $s_6 \equiv 111^2 - 2 \equiv 0$ ✓

Weiß man, ob Mersenne- oder Fermatzahlen wenigstens quadratfrei sind?
PZquadrate $p^2$ können nur in bestimmten Fällen Teiler von $F_n$ bzw. $M_q$ sein:

15.18. Satz (Wieferich-PZen): Sei $p$ ein Primteiler einer Fermatzahl $F_n$ [bzw. einer Mersennezahl $M_q$]. Genau dann gilt $p^2 \mid F_n$ [bzw. $p^2 \mid M_q$], wenn $2^{p-1} \equiv 1 \ (p^2)$ gilt.

15.19. Def.: Eine PZ $p$ mit $2^{p-1} \equiv 1 \ (p^2)$ heißt Wieferich-Primzahl.
- Bisher sind nur 1093 und 3511 mit dieser Eigenschaft bekannt. Für diese $1093 = 1 + 273 \cdot 2^2$, $3511 = 1 + 1755 \cdot 2^1$, kommen also nicht als Teiler von $F_n$ in Frage. ($p = t \cdot 2^{n+2} + 1$)
[Und auch nicht von $M_q$, o.B.]

Bew. von 15.18: „$\Rightarrow$" im Fermatfall: Haben (1) $2^{2^{n+1}} - 1 = F_n (F_n - 2)$, (15.6.) so dass $p \mid F_n$ äquivalent zu (2) $p \mid 2^{2^{n+1}} - 1$, $p \nmid 2^{2^n} - 1 = F_n - 2$ ist, d.h. $\operatorname{ord}_p(2) = 2^{n+1}$.
Daher ist $2^{n+1}$ Teiler von $p-1$, es folgt (3) $2^{2^{n+1}} - 1 \mid 2^{p-1} - 1$. Somit:
$p^2 \mid F_n \overset{(1),(3)}{\Rightarrow} p^2 \mid 2^{p-1} - 1$, d.h. $p$ ist W-PZ.
„$\Leftarrow$" im Mersennefall: $p \mid M_q \Rightarrow \operatorname{ord}_p(2) = q$, also $q \mid p-1$, somit (3') $2^q - 1 \mid 2^{p-1} - 1$.
Die Ann. $p^2 \mid M_q = 2^q - 1$ zeigt wieder, dass $p$ eine W-PZ ist.

„$\Leftarrow$": Gelte $p^2 \mid 2^{p-1}-1$. Mit Lemma 15.20 folgt $p^2 \mid 2^{2^m-1}-1$.
Mit (1) ist dann $p^2 \mid F_m$, da $p$ in (2) nicht in $2^{2^m}-1 = F_m - 2$ aufgeht.
Im Mersennefall hat man anstelle (2) einfach $p \mid 2^q - 1$. Mit Lemma 15.20 folgt $p^2 \mid 2^q - 1 = M_q$. □

15.20. **Lemma**: $p$ prim, $a \in \mathbb{Z}$. Dann: $p \mid a^m - 1 \wedge p^2 \mid a^{p-1} - 1 \Rightarrow p^2 \mid a^m - 1$.

**Bew.**: $a^m \equiv 1 \,(p) \Rightarrow a^{mp} - 1 = \underbrace{(a^m - 1)}_{\equiv 0 (p)} \cdot \underbrace{(a^{m(p-1)} + \ldots + a^m + 1)}_{\equiv p \equiv 0 (p)} \equiv 0 \,(p^2)$.
Also: $s \mid mp$, $s := \mathrm{ord}_{p^2}(a)$.
Aus $a^{p-1} \equiv 1 \,(p^2)$ folgt $s \mid p-1$. Weil $(p, p-1) = 1$, folgt $s \mid m$,
also ist mit $m = s \cdot t$ dann $a^m = (a^s)^t \equiv 1^t = 1 \,(p^2)$. □

Mersennesche PZ werden seit der Antike untersucht:

15.21. **Satz (Euklid)**: Hat $n$ die Gestalt $n = 2^{k-1}(2^k - 1)$, wo $2^k - 1$ prim ist (also notwendig $k = p$ prim, $M_p = 2^p - 1$ prim), dann ist $n$ vollkommen, d.h. $\sigma(n) = 2n$, wo $\sigma(n) = \sum_{t \mid n} t$ die Teilersummenfkt. bezeichnet.

**Bew.**: $\sigma(n) \overset{\text{kmlt.}}{=} \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1) \cdot \underbrace{(1 + (2^k - 1))}_{\text{da prim}} = (2^k - 1)2^k = 2n$. □

15.22. **Bsp.**: Jede Zahl $2^{p-1}M_p$ mit $M_p$ prim ist vollkommen, z.B.
$n = 2M_2 = 6$, $4M_3 = 28$, $16M_5 = 16 \cdot 31 = 496$, $64M_7 = 64 \cdot 127 = 8128$, ...
Aber: $n = 2^{11-1}M_{11} = 2^{10} \cdot \underbrace{2047}_{23 \cdot 89}$ ist nicht vollkommen. Dies folgt aus:

15.23. **Satz (Euler)**: Die geraden vollkommenen Zahlen $n$ sind genau die Zahlen der Gestalt $n = 2^{p-1}M_p$ mit $M_p$ prim.

**Bew.**: Sei $2 \nmid n$ vollkommen, etwa $n = 2^{k-1}a$ mit $k > 1$, $2 \nmid a$. Dann ist
$\sigma(n) = \sigma(2^{k-1})\sigma(a) = (2^k - 1)\sigma(a) \overset{\text{vor.}}{=} 2n = 2^k a = (2^k - 1)a + a$,
also $\circledast$ $(2^k - 1)(\sigma(a) - a) = a$.
Dann: $\sigma(a) - a \mid a$, wo $0 < \underbrace{\sigma(a) - a}_{\text{Summe aller Teiler} \neq a \text{ von } a} < a$ ($\neq a$, da $2^k - 1 \neq 1$ für $k \geq 2$).
Aber dann ist $\sigma(a) - a$ der einzige Teiler $< a$ von $a$, d.h. $a$ ist prim und $\sigma(a) - a = 1$.
Aus $\circledast$ folgt: $a = 2^k - 1$ ist prim, die Beh. □

15.24. **Bem.:** Die Teilersummenfunktion $\sigma(n)$ ist ein Beispiel für eine zahlentheoretische Funktion. Sie ist multiplikativ, d.h. $(n,m)=1 \Rightarrow \sigma(nm)=\sigma(n)\sigma(m)$, denn
$$\sigma(nm)=\sum_{d/nm} d = \sum_{\substack{d_1/n,\ t_1/m \\ (n,m)=1}} d_1 t_1 = \Big(\sum_{d/n} d\Big)\cdot\Big(\sum_{t/m} t\Big) = \sigma(n)\sigma(m).$$

Dies wurde in den Beweisen von 15.21 und 15.23 benutzt.

Wir haben bereits die Eulersche $\varphi$-Funktion mit dieser Eigenschaft kennengelernt. Zahlentheoretische Funktionen sind Abbildungen $\mathbb{N}\to\mathbb{C}$ mit "Zahlentheorie-Bezug". Ihre interessanten Eigenschaften lassen sich am besten analytisch behandeln, weswegen diese in der Fortsetzungsvorlesung "Analytische Zahlentheorie" ausführlich studiert werden sollen.

15.25. **Ungelöstes Problem:** Gibt es ungerade vollkommene Zahlen? Man weiß:
- Jedes $n \le 10^{200}$, $2\nmid n$, ist nicht vollkommen.
- Jedes $n$, $2\nmid n$, mit weniger als 8 Primfaktoren ist nicht vollkommen.

15.26. **Abschließende Bem.:** Die speziellen Pzen, wie in diesem Kapitel besprochen, sind für die kryptologische Sicherheit von Bedeutung: die Pzen $p,q$ in einem RSA-Modul $N=pq$ sollten nicht von so einer Gestalt sein; ein Angreifer würde für solche Zahlen zuerst testen, ob sie $N$ teilen. Bei der Erzeugung von $p,q$ sollte man dies (mit genannten Tests) am besten gleich ausschließen. Sophie-Germain-Pzen sind einerseits gut geeignet (→"safe prime", vgl. Wikipedia), andererseits auch nicht wegen Satz 15.12.