

Das Lucas Kriterium

Anton Betten

4. Februar 2000

Zusammenfassung

Das Lucas Kriterium erlaubt zu entscheiden, ob eine Mersenne Zahl $M_m = 2^m - 1$ Primzahl ist. Dieses Kriterium wird bewiesen.

1 Einführung

Sei \mathbb{P} die Menge der natürlichen Primzahlen. Sei stets $M = M_m = 2^m - 1$ mit $m > 2$. Das Lucas-Kriterium besagt:

Definiert man rekursiv s_i durch $s_0 = 4, s_{i+1} \equiv s_i^2 - 2 \pmod{M}$ so gilt: $M \in \mathbb{P} \iff s_{m-2} \equiv 0 \pmod{M}. \quad (1)$
--

2 Definitionen

Wir bezeichnen mit \mathbb{F}_q den Körper mit q Elementen (für Primzahlpotenzen q).

Sei L ein quadratischer Zahlkörper, d. h. eine quadratische Erweiterung von \mathbb{Q} . Man kann $L = \mathbb{Q}(\sqrt{d})$ schreiben mit quadratfreiem d . Zu $\alpha = a + b\sqrt{d} \in L$ ist $\alpha^* = a - b\sqrt{d}$ die Konjugierte (diese wird häufig mit $\bar{\alpha}$ bezeichnet, wir behalten dieses Zeichen jedoch für Restklassenelemente vor).

(i) Man hat $s(\alpha) = \alpha + \alpha^*$ die Spur von α . Sie ist \mathbb{Q} -linear und additiv.

(ii) Man hat $n(\alpha) = \alpha \cdot \alpha^*$ die Norm von α . Sie ist multiplikativ.

Sei $\alpha \in \mathcal{O}$. Dann heißt α ganz, wenn $s(\alpha) \in \mathbb{Z}$ und $n(\alpha) \in \mathbb{Z}$ ist. Die Menge der ganzen Zahlen von L bilden einen Ring, der mit \mathcal{O} oder \mathcal{O}_L bezeichnet wird. Dieser Ring heißt auch Maximalordnung.

Eine Zahl $\epsilon \in \mathcal{O} \setminus \{0\}$ heißt Einheit, wenn $\epsilon^{-1} \in \mathcal{O}$ ist. Die Menge der Einheiten von \mathcal{O} wird mit \mathcal{O}^\times bezeichnet.

Ein Zahlenpaar (β_1, β_2) heißt Ganzheitsbasis, wenn $L = \mathbb{Q}\beta_1 + \mathbb{Q}\beta_2$ und $\mathcal{O} = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2$ gilt.

3 Verwendete Sätze

In diesem Abschnitt werden die verwendeten Sätze und Ergebnisse aufgeführt. Auf Beweise wird verzichtet.

Für $a \in \mathbb{Z}, p \in \mathbb{P}$ gilt:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p} \quad (\text{Eulerkriterium})$$

Für $p, q \in \mathbb{P}$ gilt

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

(Gauss'sches Reziprozitätsgesetz für Legendre Symbole).

Für $p, q \in \mathbb{Z}$ gilt

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

(Reziprozitätsgesetz für Jacobi Symbole).

Für $\alpha \in L \setminus \mathbb{Q}$ ist $X^2 - s(\alpha)X + n(\alpha) = X^2 - (\alpha + \alpha^*)X + \alpha\alpha^* = (X - \alpha)(X - \alpha^*)$ die Gleichung von α .

$$\alpha \in \mathcal{O}^\times \iff \alpha \in \mathcal{O} \wedge n(\alpha) \in \{\pm 1\}$$

Sei $L = \mathbb{Q}(\sqrt{d})$ mit quadratfreiem d . Dann ist $(1, \omega)$ Ganzheitsbasis mit

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \iff d \equiv 1 \pmod{4} \\ \sqrt{d} & \iff d \equiv 2, 3 \pmod{4} \end{cases}$$

Der Fall $d \equiv 0 \pmod{4}$ scheidet aus, da d quadratfrei vorausgesetzt war.

Sei $p \in \mathbb{P}$, $L = \mathbb{Q}(\sqrt{d})$, \mathfrak{I} die Menge der ganzen Ideale von \mathcal{O}_L , \mathbb{P}_L die Menge der Primideale von \mathfrak{I} . Zahlen $a \in \mathcal{O}$ definieren Hauptideale $\mathcal{O}a$.

Ideale können multipliziert werden: Man definiert $A \cdot B := \langle \sum_i a_i b_i \mid a_i \in A, b_i \in B \rangle$.

Für ganze Ideale A, B schreibt man $A \mid B$, wenn ein ganzes Ideal C existiert mit $AC = B$. Man schreibt $A \mid a \iff A \mid \mathcal{O}a$ für $a \in \mathcal{O}$. Die Teilbarkeit von Idealen ist die umgekehrte Enthaltenseinsrelation: $A \mid B \iff A \supseteq B$.

Für jedes Ideal $A \in \mathfrak{I}$ ist $A^* := \{a^* \mid a \in A\}$ wieder ein Ideal, das konjugierte Ideal.

Die Norm eines Ideals A ist $n(A) := \text{ggT}(n(a) \mid a \in A)$. Es gilt $A \cdot A^* = n(A)\mathcal{O}$. Die Idealnorm ist multiplikativ. Es ist $n(A) = 1 \iff A = \mathcal{O}$.

Eine Menge der Form $\frac{1}{m}A$ mit $m \in \mathbb{Z}$ und $A \in \mathfrak{I}$ heißt gebrochenes Ideal. Mit ihnen kann das Inverse eines Ideals A angegeben werden: $A^{-1} = \frac{1}{n(A)}A^*$, denn $AA^{-1} = \frac{1}{n(A)}AA^* = \frac{1}{n(A)}n(A)\mathcal{O} = \mathcal{O}$.

Jedes ganze Ideal $A \in \mathfrak{I}$ besitzt eine bis auf Reihenfolge der Faktoren eindeutige Zerlegung $A = P_1^{\text{ord}_{P_1}(A)} \cdot \dots \cdot P_r^{\text{ord}_{P_r}(A)}$ mit Primidealen P_1, \dots, P_r .

Für jedes ganze Ideal $A \in \mathfrak{I}$ ist $\Phi(A) := |(\mathcal{O}/A)^\times|$ die „idealische Phifunktion“.

Es ist wichtig zu untersuchen, wie Primzahlen $p \in \mathbb{P}$ sich verhalten, wenn die zugehörigen Hauptideale $\mathcal{O}p$ in \mathfrak{I} faktorisiert werden. Wir nehmen etwa $\mathcal{O}p = P_1^{n_1} \cdot \dots \cdot P_r^{n_r}$ mit $P_1, \dots, P_r \in \mathbb{P}_L$ an. Wegen $p^2 = n(\mathcal{O}p) = n(P_1^{n_1}) \cdot \dots \cdot n(P_r^{n_r})$ folgt $r \leq 2$. Nun treten drei Fälle auf (es ist $p \in \mathbb{P}$, $P \in \mathbb{P}_L$):

- (i) $\mathcal{O}_p = PP$: man sagt „ p ist verzweigt“.
- (ii) $\mathcal{O}_p = PP^*$ mit $P^* \neq P$: man sagt „ p ist zerlegt“.
- (iii) $\mathcal{O}_p = P$: man sagt „ p ist träge“.

Beispiele: Wir betrachten $L = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q} + \mathbb{Q}i$. Es ist $\mathcal{O}_L = \mathbb{Z}1 + \mathbb{Z}i$.

- (i) $5 = (2 + i)(2 - i)$, also $\mathcal{O}5 = PP^*$ mit $P = \mathcal{O}(2 + i)$ und $P^* = \mathcal{O}(2 - i)$ d. h. 5 ist zerlegt.
- (ii) $2 = (1 + i)(1 - i)$. Achtung: wegen $-(1 + i)i = -(i - 1) = 1 - i$ ist $1 + i$ assoziiert zu $1 - i$ (d. h. beide Zahlen unterscheiden sich nur bis auf Einheitsfaktoren). Demnach ist $\mathcal{O}(1 + i) = \mathcal{O}(1 - i)$, d. h. $\mathcal{O}2 = (\mathcal{O}(1 + i))^2$, mit anderen Worten: 2 ist verzweigt.
- (iii) Die Primzahl 7 kann nicht als Summe zweier Quadrate geschrieben werden. Somit ist 7 träge, d. h. $\mathcal{O}7$ ist Primideal.

Der folgende Satz besagt, wann eine Primzahl verzweigt, zerlegt bzw. träge ist. Sei wieder $L = \mathbb{Q}(\sqrt{d})$ mit quadratfreiem d . Man setzt

$$d_L = \begin{cases} 4d & \iff d \equiv 1 \pmod{4} \\ d & \iff d \equiv 2, 3 \pmod{4} \end{cases}$$

Dann gilt für $p \in \mathbb{P}$:

$$p \text{ ist } \left\{ \begin{array}{l} \text{verzweigt} \\ \text{zerlegt} \\ \text{träge} \end{array} \right\} \text{ in } L \iff \left(\frac{d_L}{p} \right) = \left\{ \begin{array}{l} 0 \\ 1 \\ -1 \end{array} \right\}.$$

Der kleine Satz von Fermat für quadratische Zahlkörper:

- (i) Ist p träge Primzahl, so gilt $\alpha^p \equiv \alpha\alpha^* \pmod{\mathcal{O}_p}$.

Sei wieder $L = \mathbb{Q}(\sqrt{d})$ mit quadratfreiem d . Sei P ein Primideal und p eine Primzahl mit $P \mid p$. Dann gilt

$$\mathcal{O}/P \simeq \begin{cases} \mathbb{F}_p & \iff p \text{ verzweigt oder zerlegt} \\ \mathbb{F}_{p^2} & \iff p \text{ träge} \end{cases}$$

4 Der Beweis des Lucas Kriteriums

4.1 Lemma Sei A ganzes Ideal, $A \nmid 2$, $\overline{\mathcal{O}} = \mathcal{O}/A$, $\epsilon \in \mathcal{O}^\times$. Dann ist $\bar{\epsilon} \in \overline{\mathcal{O}}^\times$ und es gilt für $j \geq 1$

$$s(\epsilon^{2^j}) \equiv 0 \pmod{A} \iff \text{ord}(\bar{\epsilon}) = 2^{j+2} \quad (2)$$

worin ord die Elementordnung in $\overline{\mathcal{O}}$ bezeichnet.

Beweis:

$$\begin{aligned} 0 &\equiv s(\epsilon^{2^j}) = \epsilon^{2^j} + (\epsilon^{2^j})^* \pmod{A} && / \cdot \epsilon^{2^j} \\ \iff 0 &\equiv (\epsilon^{2^j})^2 + \epsilon^{2^j} (\epsilon^{2^j})^* \pmod{A} \\ \iff 0 &\equiv \epsilon^{2^{j+1}} + n(\epsilon^{2^j}) \pmod{A} \\ \iff 0 &\equiv \epsilon^{2^{j+1}} + \underbrace{n(\epsilon)}_{\pm 1} \pmod{A} \\ \iff 0 &\equiv \epsilon^{2^{j+1}} + 1 \pmod{A} \\ \iff \bar{\epsilon}^{2^{j+1}} &= -1_{\overline{\mathcal{O}}^\times} \neq \underbrace{1_{\overline{\mathcal{O}}^\times}}_{A \nmid 2} = 1 \end{aligned}$$

□

Die s_i aus dem Lucas Kriterium können wie folgt gedeutet werden:

4.2 Lemma $s_i = s(\epsilon^{2^i})$ mit $\epsilon = 2 + \sqrt{3} \in \mathcal{O}_L^\times$, $L = \mathbb{Q}(\sqrt{3})$.

Beweis: Wegen $n(\epsilon) = (2 + \sqrt{3})(2 - \sqrt{3}) = 4 - 3 = 1$ folgt $\epsilon \in \mathcal{O}^\times$. Wegen $s(\epsilon^{2^0}) = s(\epsilon) = 2 + \sqrt{3} + 2 - \sqrt{3} = 4 = s_0$ gilt die Gleichung für $i = 0$. Sei der Nachweis für alle Zahlen kleiner oder gleich einem festen i bereits erbracht. Wir zeigen $s_{i+1} = s(\epsilon^{2^{i+1}})$. Für jedes $\alpha \in L$ gilt

$$\alpha^2 - s(\alpha) \cdot \alpha + n(\alpha) = 0.$$

Für ϵ folgt speziell

$$\begin{aligned} \Rightarrow s(\epsilon^2) &= s(s(\epsilon)\epsilon) - s(n(\epsilon)) \\ &= s(\epsilon)s(\epsilon) - 2n(\epsilon) \\ &= s(\epsilon)^2 - 2 \\ \Rightarrow s(\epsilon^{2^{i+1}}) &= s(\epsilon^{2^i \cdot 2}) \\ &= s((\epsilon^{2^i})^2) \\ &= s((\epsilon^{2^i})^2) - 2 \\ \Rightarrow s(\epsilon^{2^{i+1}}) &= s_i^2 - 2 = s_{i+1} \end{aligned}$$

□

Wir beweisen nun das Lucas Kriterium, d. h. (1). Zunächst betrachten wir die Folgerung \Rightarrow :

Sei p eine Primzahl und P ein Primideal mit $P \mid p \mid M$. Wegen M ungerade ist $p \neq 2$ und damit $P \nmid 2$. Nach Voraussetzung gilt

$$\begin{aligned} s(\epsilon^{2^{m-2}}) &\equiv 0 \pmod{M} \\ \Rightarrow s(\epsilon^{2^{m-2}}) &\equiv 0 \pmod{P} \\ \Rightarrow \text{ord}(\epsilon) &= 2^{m-2+2} = 2^m \end{aligned}$$

nach Lemma 4.1. Nun gilt für $\bar{\epsilon}$ in $\bar{\mathcal{O}} = \mathcal{O}/P$:

$$\bar{\epsilon}^{\Phi(P)} = \bar{1},$$

wobei Φ die „idealische“ Phifunktion ist, d. h. $\Phi(A) = |(\mathcal{O}/A)^\times|$ für jedes ganze Ideal A . Wir unterscheiden die Fälle p zerlegt oder verzweigt bzw. p träge.

Sei zunächst p zerlegt oder verzweigt.

Dann ist $\mathcal{O}/P \simeq \mathbb{F}_p$ und

$$\begin{aligned} 2^m \mid \Phi(P) &= |(\mathcal{O}/P)^\times| = |\mathcal{O}/P| - 1 = p - 1 \\ \Rightarrow 2^m &\leq p - 1 \leq M - 1 = 2^m - 2, \end{aligned}$$

ein Widerspruch. Demnach ist p träge und $\mathcal{O}/P \simeq \mathbb{F}_{p^2}$, d. h. $\Phi(P) = |(\mathcal{O}/P)^\times| = p^2 - 1$.

Wir wissen:

$$\begin{aligned} p \text{ träge Primzahl} &\iff \left(\frac{d_L}{p}\right) = -1 \\ &\iff d_L \text{ ist kein quadratischer Rest mod } p \\ &\iff \sqrt{d} \notin \mathbb{F}_p \end{aligned}$$

Wir müssen noch nachweisen, dass M prim ist. Dazu studieren wir $\text{ord}(\bar{\epsilon} \in \mathbb{F}_p^\times)$ in der multiplikativen Faktorgruppe $G = \bar{\mathcal{O}}^\times / \mathbb{F}_p^\times$ der Ordnung $(p^2 - 1)/(p - 1) = p + 1$. Es sei noch einmal an $\bar{\mathcal{O}} \simeq \mathcal{O}/P \simeq \mathbb{F}_p(\bar{\omega}) \simeq \mathbb{F}_{p^2}$ erinnert, mit $(1, \omega)$ Ganzheitsbasis von \mathcal{O} . Das Element $\epsilon^{2^{m-2}}$ besitzt die allgemeine Form

$$\epsilon^{2^{m-2}} = \frac{1}{2}(s + t\sqrt{d})$$

mit $s, t \in \mathbb{Z}$. Nun ist nach Voraussetzung $s(\epsilon^{2^{m-2}}) \equiv 0 \pmod{p}$, also $s = 0$.

$$\Rightarrow \bar{\epsilon}^{2^{m-2}} = \frac{\bar{t}}{2} \underbrace{\sqrt{d}}_{\in \mathcal{O}^\times \setminus \mathbb{F}_p^\times}$$

$$\begin{aligned} \Rightarrow (\bar{\epsilon}\mathbb{F}_p^\times)^{2^{m-2}} &= \frac{\bar{t}}{2}\sqrt{d}\mathbb{F}_p^\times \neq \mathbb{F}_p^\times = 1_G \\ \Rightarrow \bar{\epsilon}^{2^{m-1}}\mathbb{F}_p^\times &= -1\mathbb{F}_p^\times = \mathbb{F}_p^\times = 1_G, \end{aligned}$$

woraus folgt

$$\begin{aligned} \Rightarrow \text{ord}(\bar{\epsilon}\mathbb{F}_p^\times) &= 2^{m-1} \mid |G| = \frac{|\overline{\mathcal{O}}^\times|}{|\mathbb{F}_p^\times|} = \frac{p^2 - 1}{p - 1} = p + 1 \\ \Rightarrow 2^{m-1} &\leq p + 1 \leq M + 1 = 2^m. \end{aligned}$$

Sei nun p der kleinste Primteiler von M . Falls $p \neq M \Rightarrow p \leq \sqrt{M}$. Dann ergibt sich

$$\begin{aligned} 2^{m-1} - 1 &\leq p \leq \sqrt{M} = \sqrt{2^m - 1} \\ \Leftrightarrow (2^{m-1} - 1)^2 &\leq 2^m - 1 \\ \Leftrightarrow 2^{2(m-1)} - 2^m + 1 &\leq 2^m - 1, \end{aligned}$$

was für $m > 2$ ein Widerspruch ist. Damit ist gezeigt, dass M Primzahl ist.

Wir zeigen nun die Richtung \Leftarrow des Kriteriums.

Dazu sei $p = M = 2^m - 1$ prim mit $m > 2$. Notwendigerweise ist $m \in \mathbb{P}$, etwa $m = 2n + 1$. Sei weiter $\epsilon = 2 + \sqrt{3} \in \mathcal{O}_L$ mit $L = \mathbb{Q}(\sqrt{3})$. Es ist $n(\epsilon) = 1$, d. h. $\epsilon \in \mathcal{O}^\times$. Nach dem Reziprozitätsgesetz gilt

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}}$$

und wegen $p \equiv -1 \pmod{4}$ (denn $4 \mid p + 1 = 2^m$) und $3 \equiv -1 \pmod{4}$

$$\begin{aligned} &= \left(\frac{p}{3}\right) \cdot (-1) \\ &= -\left(\frac{2^{2n} \cdot 2 - 1}{3}\right) \end{aligned}$$

hier ist $2^{2n} = 4^n \equiv 1^n \equiv 1 \pmod{3}$, demnach $2^{2n} \cdot 2 \equiv 2 \pmod{3}$ und somit $2^{2n} \cdot 2 - 1 \equiv 1 \pmod{3}$, d. h.

$$= - \left(\frac{1}{3} \right) = -1.$$

Demnach ist p träge.

Wir zeigen nun $\epsilon^{2^{m-1}} \equiv -1 \pmod{p}$ (woraus $\text{ord}(\bar{\epsilon}) = 2^m$ folgt):

Nach dem kleinen Satz von Fermat gilt:

$$\bar{\epsilon}^{2^m} = \bar{\epsilon}^{p+1} = \overline{\epsilon^*} = n(\bar{\epsilon}) = \overline{n(\epsilon)} = \bar{1},$$

und somit

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

Um $\epsilon^{2^{m-1}} \equiv -1 \pmod{p}$ nachzuweisen, genügt der Nachweis von

$$s\left(\epsilon^{2^{m-1}}\right) \equiv -2 \pmod{p}.$$

Dies geschieht mit einem Trick. Wir definieren die Hilfsgröße $\lambda = 1 + \sqrt{3}$ (mit $n(\lambda) = -2$). Dann ist

$$\lambda^2 = 1 + 2\sqrt{3} + 3 = 4 + 2\sqrt{3} = 2(2 + \sqrt{3}) = 2\epsilon.$$

Damit folgt

$$\begin{aligned} 2^{2^{m-1}} \cdot s\left(\epsilon^{2^{m-1}}\right) &= s\left(2^{2^{m-1}} \cdot \epsilon^{2^{m-1}}\right) \\ &= s\left((2\epsilon)^{2^{m-1}}\right) \\ &= s\left((\lambda^2)^{2^{m-1}}\right) \\ &= s\left(\lambda^{2^m}\right) \\ &= s\left(\lambda^{p+1}\right) \end{aligned}$$

$$\begin{aligned}
&\equiv s(\lambda\lambda^*) \pmod{p} \\
&= s(n(\lambda)) \pmod{p} \\
&= s(-2) \pmod{p} \\
&= -4 \pmod{p}.
\end{aligned}$$

Division durch 2 ergibt (Achtung: $2 \nmid p$, d. h. die Division ist erlaubt!):

$$\Rightarrow 2^{2^{m-1}-1} \cdot s(\epsilon^{2^{m-1}}) \equiv -2 \pmod{p}$$

und wegen

$$\begin{aligned}
2^{m-1} &= \frac{2^m}{2} = \frac{p+1}{2} \\
\Rightarrow 2^{2^{m-1}-1} &= 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) = 1 \pmod{p}
\end{aligned}$$

nach dem Eulerkriterium und einem Ergänzungssatz zum Legendre Symbol (wegen $p \equiv -1 \pmod{8}$). Eingesetzt folgt

$$\begin{aligned}
&s(\epsilon^{2^{m-1}}) \equiv -2 \pmod{p} \\
\Rightarrow \epsilon^{2^{m-1}} &\equiv -1 \pmod{p} \\
\Rightarrow \epsilon^{2^m} &\equiv 1 \pmod{p} \\
\Rightarrow \text{ord}(\bar{\epsilon}) &= 2^m
\end{aligned}$$

und nach Lemma 4.1

$$\Rightarrow s(\epsilon^{2^{m-2}}) \equiv 0 \pmod{p}.$$

5 Ergebnisse

i	p_i	M_{p_i} (# Stellen)	
1	5	31 (2)	prim
2	7	127 (3)	prim
3	11	2047 (4)	
4	13	8191 (4)	prim
5	17	131071 (6)	prim
6	19	524287 (6)	prim
7	23	8388607 (7)	
8	29	536870911 (9)	
9	31	2147483647 (10)	prim
10	37	137438953471 (12)	
11	41	2199023255551 (13)	
12	43	8796093022207 (13)	
13	47	140737488355327 (15)	
14	53	9007199254740991 (16)	
15	59	576460752303423487 (18)	
16	61	2305843009213693951 (19)	prim
17	67	147573952589676412927 (21)	
18	71	2361183241434822606847 (22)	
19	73	9444732965739290427391 (22)	
20	79	604462909807314587353087 (24)	
21	83	9671406556917033397649407 (25)	
22	89	618970019642690137449562111 (27)	prim
23	97	158456325028528675187087900671 (30)	
24	101	2535301200456458802993406410751 (31)	
25	103	10141204801825835211973625643007 (32)	
26	107	162259276829213363391578010288127 (33)	prim
27	109	649037107316853453566312041152511 (33)	
28	113	10384593717069655257060992658440191 (35)	
29	127	170141183460469231731687303715884105727 (39)	prim
30	131	2722258935367507707706996859454145691647 (40)	

i	p_i	# Stellen	prim ?	min:sec
1	5	2	prim	
2	7	3	prim	
3	11	4		
4	13	4	prim	
5	17	6	prim	
6	19	6	prim	
7	23	7		
8	29	9		
9	31	10	prim	
10	37	12		
11	41	13		
12	43	13		
13	47	15		
14	53	16		
15	59	18		
16	61	19	prim	
17	67	21		
18	71	22		
19	73	22		
20	79	24		
21	83	25		
22	89	27	prim	
23	97	30		
24	101	31		
25	103	32		
26	107	33	prim	
27	109	33		
28	113	35		
29	127	39	prim	
30	131	40		
31	137	42		
32	139	42		
33	149	45		
34	151	46		
35	157	48		
36	163	50		
37	167	51		0:1
38	173	53		0:1
39	179	54		0:1
40	181	55		0:1
41	191	58		0:1
42	193	59		0:1
43	197	60		0:1
44	199	60		0:1
45	211	64		0:1
46	223	68		0:2
47	227	69		0:2
48	229	69		0:2
49	233	71		0:2
50	239	72		0:2
51	241	73		0:2
52	251	76		0:3
53	257	78		0:3
54	263	80		0:3
55	269	81		0:3
56	271	82		0:3
57	277	84		0:4
58	281	85		0:4
59	283	86		0:4
59	283	86		0:4
60	293	89		0:4
61	307	93		0:5
62	311	94		0:5
63	313	95		0:5
64	317	96		0:5
65	331	100		0:6
66	337	102		0:7
67	347	105		0:7
68	349	106		0:7
69	353	107		0:8
70	359	109		0:8
71	367	111		0:9
72	373	113		0:9
73	379	115		0:9
74	383	116		0:10
75	389	118		0:10
76	397	120		0:11
77	401	121		0:11
78	409	124		0:12
79	419	127		0:13
80	421	127		0:13

i	p_i	# Stellen	prim ?	min:sec	i	p_i	# Stellen	prim ?	min:sec
81	431	130		0:14	121	677	204		0:54
82	433	131		0:14	122	683	206		0:55
83	439	133		0:15	123	691	209		0:56
84	443	134		0:15	124	701	212		0:59
85	449	136		0:16	125	709	214		1:1
86	457	138		0:17	126	719	217		1:3
87	461	139		0:17	127	727	219		1:5
88	463	140		0:17	128	733	221		1:7
89	467	141		0:18	129	739	223		1:8
90	479	145		0:19	130	743	224		1:10
91	487	147		0:20	131	751	227		1:12
92	491	148		0:21	132	757	228		1:13
93	499	151		0:21	133	761	230		1:15
94	503	152		0:22	134	769	232		1:17
95	509	154		0:23	135	773	233		1:18
96	521	157	prim	0:24	136	787	237		1:22
97	523	158		0:25	137	797	240		1:26
98	541	163		0:27	138	809	244		1:30
99	547	165		0:28	139	811	245		1:30
100	557	168		0:30	140	821	248		1:33
101	563	170		0:31	141	823	248		1:34
102	569	172		0:32	142	827	249		1:35
103	571	172		0:32	143	829	250		1:36
104	577	174		0:33	144	839	253		1:40
105	587	177		0:35	145	853	257		1:45
106	593	179		0:36	146	857	258		1:46
107	599	181		0:37	147	859	259		1:47
108	601	181		0:37	148	863	260		1:48
109	607	183	prim	0:38	149	877	265		1:54
110	613	185		0:40	150	881	266		1:56
111	617	186		0:40	151	883	266		1:56
112	619	187		0:41	152	887	268		1:57
113	631	190		0:43	153	907	274		2:5
114	641	193		0:45	154	911	275		2:7
115	643	194		0:45	155	919	277		2:10
116	647	195		0:47	156	929	280		2:15
117	653	197		0:48	157	937	283		2:18
118	659	199		0:49	158	941	284		2:20
119	661	199		0:50	159	947	286		2:22
120	673	203		0:52	160	953	287		2:26

p	# Stellen	prim ?	min:sec
1279	386	prim	5:47
2203	664	prim	29:4
2281	687	prim	32:18