Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Über die Ordnung von Punkten einer Untervarietät einer algebraischen Gruppe über einem endlichen Körper

Masterarbeit

Lukas Fink

Betreuer

Prof. Dr. Richard Pink

Departement Mathematik, ETH Zürich

Zürich, Dezember 2008

Inhaltsverzeichnis

1 Einführung

Sei A eine abelsche Varietät der Dimension d über einem algebraisch abgeschlossenen Körper K der Charakteristik $p \geq 0$. Nehme an, dass entweder $p = 0$ oder $p \nmid n$ gilt. Dann gilt für die Menge der n-Torsionspunkte

$$\{a \in A(K) \mid a^n = 1\} \cong (\mathbb{Z}/n\mathbb{Z})^{2d}.$$

Die Anzahl aller Elemente $a \in A(K)$ der Ordnung n verhält sich also asymptotisch gleich wie n^{2d}, d.h.

$$\#\left\{a \in A\left(\overline{\mathbb{F}}_p\right) \mid \operatorname{ord}(a) = n\right\} \sim n^{2d}.$$

Sei nun aber A eine kommutative algebraische Gruppe über einem endlichen Körper k mit algebraischem Abschluss K. Dann ist $A(K)$ eine abelsche Torsionsgruppe und man interessiert sich für die Verteilung der Ordnungen von Punkten einer Untervarietät $X \subset A$. Da über dieses Thema selbst in eifachen Fällen noch nicht viel bekannt ist, beschäftigen wir uns in dieser Arbeit darüber.

Wir betrachten die algebraische Gruppe $A = \overline{\mathbb{F}}_2^{\times} \times \overline{\mathbb{F}}_2^{\times}$ und die Untervarietät $X = \{(x, y) \in A \mid x + y = 1\}$. Wie angesprochen, untersuchen wir die Menge aller Punkte von X der Ordnung n bzw. dessen Kardinalität $a(n)$:

$$a(n) = \#\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0, 1\} \mid \operatorname{ord}(x, 1 - x) = n\right\}.$$

Des Weiteren definieren wir

$$c(n) = \sum_{m \leq n} a(m).$$

Das Hauptresultat der vorliegenden Arbeit ist eine Aussage über das Verhalten von $c(n)$ für grosse n:

$$c(n) = o\left(n^2\right).$$

Aufgrund expliziter Berechnungen von $a(n)$ stellen wir jedoch die Vermutung auf, dass sich $c(n)$ verhält wie $O(n)$.

Diese Arbeit ist im Wesentlichen in drei Teile gegliedert. Im ersten Teil beschäftigen wir uns mit der Frage, unter welchen Bedingungen an n der Wert von $a(n)$ Null ist. Daraus schliessen wir dann, dass $c(n) = o(n^2)$ gilt. Im zweiten Teil berechnen wir dann $a(n)$ für möglichst viele n. Wir benutzen dazu das Computer-Algebra-System PARI/GP und die portable C++ Bibliothek NTL. Es wird sich aber herausstellen, dass diese Berechnungen sehr zeitaufwändig sind. Wir versuchen darum im letzten Kapitel eine Näherung für $a(n)$ zu konstruieren. Die Ideen für die Berechnungen, die Erabeitung der Kriterien sowie die Konstruktion der Heuristik stammen von Prof. Dr. Richard Pink. An dieser Stelle möchte ich mich bei Herrn Pink für seine Ideen und Motivationen herzlichst bedanken. Ebenfalls danke ich Patrik Hubschmid und Rainer Trachsler für deren Unterstützung.

2 Theoretischer Teil

Wir betrachten im Folgenden die algebraische Gruppe $A = \overline{\mathbb{F}}_2^{\times} \times \overline{\mathbb{F}}_2^{\times}$ und die Untervarietät $X = \{(x, y) \in A \mid x + y = 1\}$. Wir möchten nun das Wachstumsverhalten von

$$\#\left\{x \in X\left(\overline{\mathbb{F}}_2\right) \mid \operatorname{ord}(x) = n\right\}$$

in Abhängikeit von n untersuchen. Wir definieren für $2 \nmid n$

$$a(n) = \#\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \operatorname{ord}(x, 1-x) = n\right\}$$

und

$$b(n) = \#\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \operatorname{ord}(x, 1-x) \mid n\right\}.$$

Es ist dann $b(n) = \sum_{d|n} a(d)$ und mit der Möbius'schen Summationsformel folgt

$$a(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) b(d).$$

Bemerkung

1. Wir betrachten Lösungen der Gleichung $x^n = 1$ in $\overline{\mathbb{F}}_2$. Da es nur endlich viele Lösungen gibt, liegen diese in einer endlichen Erweiterung $\mathbb{F}_{2^k} \supset \mathbb{F}_2$. Der Körper $\mathbb{F}_{2^k}$ ist aber der Zerfällungskörper des Polynoms $X^{2^k} - X \in \mathbb{F}_2[X]$ und wir bekommen folgende Rechnung: $\mathbb{F}_{2^k} = \left\{x \in \overline{\mathbb{F}}_2 \mid x^{2^k} - x = 0\right\} = \left\{x \in \overline{\mathbb{F}}_2 \mid x^{2^k-1} - 1 = 0\right\} \cup \{0\}$. Nun ist $\left\{x \in \overline{\mathbb{F}}_2 \mid x^n = 1\right\}$ genau dann in $\left\{x \in \overline{\mathbb{F}}_2 \mid x^{2^k-1} = 1\right\} = \mathbb{F}_{2^k}^{\times}$ enthalten, wenn $n \mid \left(2^k - 1\right)$ bzw. wenn $2^k \equiv 1 \pmod{n}$. Das kleinste k, für welches also alle Lösungen von $x^n = 1$ in $\mathbb{F}_{2^k}$ liegen, ist somit gleich der multiplikativen Ordnung von $2 \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. Im Folgenden werden wir diese mit $r(n)$ bezeichnen:

$$r : \mathbb{N} \to \mathbb{N},\ n \mapsto r(n) = \min\left\{k \in \mathbb{N} \mid 2^k \equiv 1 \mod n\right\}.$$

2. Für eine ungerade natürliche Zahl n sei $F_n(X) = X^n - 1$ ein Polynom über $\mathbb{F}_2$. Dann ist $b(n) = \#\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid F_n(x) = 0 \text{ und } F_n(1-x) = 0\right\}$.

   Beweis

   Für ein $x \in \overline{\mathbb{F}}_2 \setminus \{0,1\}$ wollen wir zeigen, dass

   $$\operatorname{ord}(x, 1-x) \mid n \Leftrightarrow F_n(x) = 0 \text{ und } F_n(1-x) = 0$$

   gilt.
   Sei $x \in \overline{\mathbb{F}}_2 \setminus \{0,1\}$ mit $\operatorname{ord}(x, 1-x) \mid n$. Da $\operatorname{ord}(x, 1-x) = \operatorname{kgV}(\operatorname{ord}(x), \operatorname{ord}(1-x))$ ist, gilt:

   $$\operatorname{ord}(x) \mid n \text{ und } \operatorname{ord}(1-x) \mid n.$$

   Somit ist $x^n = 1$ und $(1-x)^n = 1$.
   Sei nun umgekehrt $x \in \overline{\mathbb{F}}_2 \setminus \{0,1\}$ mit $x^n = 1 = (1-x)^n$. Es folgt nun, dass $\operatorname{ord}(x)$ und $\operatorname{ord}(1-x)$ Teiler von n sind. Somit ist auch $\operatorname{kgV}(\operatorname{ord}(x), \operatorname{ord}(1-x))$ ein Teiler von n. $\Rightarrow \operatorname{ord}(x, 1-x) \mid n$. □

Im letzten Teil des obigen Beweises haben wir folgendes Lemma benutzt:

Lemma 2.1
Seien $r, s \in \mathbb{N}$ zwei natürliche Zahlen und sei d ein gemeinsames Vielfaches von r und s. Dann ist das kleinste gemeinsame Vielfache von r und s ein Teiler von d.

Beweis

Sei $x = \mathrm{kgV}(r, s)$ und sei d eine natürliche Zahl mit $r \mid d$ und $s \mid d$. Nehmen wir an, es existiere ein $k \in \mathbb{N}$, so dass $kx < d < (k+1)x$. Nach Voraussetzung ist aber $(k+1)x \equiv 0 \mod r$ und $d \equiv 0 \mod r$. Somit ist auch $(k+1)x - d \equiv 0 \mod r$. Dasselbe gilt für s. Es folgt also, dass $(k+1)x - d$ ein gemeinsames Vielfaches von r und s ist. Nun ist aber $(k+1)x - d < (k+1)x - kx = x = \mathrm{kgV}(r, s)$. □

2.1 Kriterien für $a(n) = 0$

In diesem Abschnitt stellen wir drei Sätze vor, die eine Aussage darüber machen, für welche ungeraden Zahlen n die Menge $\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \mathrm{ord}(x, 1-x) = n\right\}$ leer ist, bzw. für welche ungeraden $n \in \mathbb{N}$ die Zahl $a(n)$ Null ist.

Satz 2.2
Sei n eine ungerade natürliche Zahl. Seien $a, b \in \mathbb{Z}$ und $s \in \mathbb{N}$ mit $2 \nmid a, b$ und $n \mid a \cdot 2^s - b$. Falls

- $a, b > 0, a \neq b, ab < r(n)$, *oder*
- $a > 0 > b, |2ab| < r(n)$, *oder*
- $a = b > 1, a \cdot (a-1) < r(n)$,

dann ist $a(n) = 0$.

Für den Beweis benötigen wir folgende Lemmas:

Lemma 2.3
Sei n eine ungerade natürliche Zahl. Seien $a, b \in \mathbb{Z}$ und $s \in \mathbb{N}$ mit $2 \nmid a, b$ und $n \mid a \cdot 2^s - b$. Dann gelten folgende drei Aussagen:

- $a, b > 0, a \neq b \Rightarrow b(n) \leq ab$,
- $a > 0 > b \Rightarrow b(n) \leq |2ab|$,
- $a = b > 1 \Rightarrow a(n) \leq a \cdot (a-1)$.

Beweis

Sei n eine ungerade natürliche Zahl. Seien $2 \nmid a, b \in \mathbb{Z}$, sowie $s \in \mathbb{N}$, so dass $n \mid a \cdot 2^s - b$. Wir möchten nun $b(n)$ abschätzen. Dazu betrachten wir die Gleichungen

$$x^n = 1 \tag{1}$$

$$(1-x)^n = 1. \tag{2}$$

Die Anzahl Lösungen dieser zwei Gleichungen in $\overline{\mathbb{F}}_2 \setminus \{0,1\}$ entspricht $b(n)$. Da n ein Teiler von $a \cdot 2^s - b$ ist, folgt aus diesen zwei Gleichungen, dass $\left(x^{2^s}\right)^a = x^b$ und $(1-x)^{a \cdot 2^s} = \left(1-x^{2^s}\right)^a = (1-x)^b$. Schreiben wir $y = x^{2^s}$, folgt also $y^a = x^b$ und $(1-y)^a = (1-x)^b$. Setzen wir nun $x = z^a$ für ein $z \in \overline{\mathbb{F}}_2$, so ergibt sich aus $y^a = \left(z^b\right)^a$, dass $y = \zeta z^b$ für ein ζ mit $\zeta^a = 1$. Es folgt also, dass

$$\left(1-\zeta z^b\right)^a = (1-z^a)^b. \tag{3}$$

Die Anzahl Lösungen für das Paar (z,ζ) von (3) ist beschränkt, und diese wollen wir nun abschätzen. Dazu betrachten wir folgende Fälle. Wenn

- $a \neq b$ und $a, b > 0$, so ist für ein festes ζ die Anzahl Lösungen für z höchstens ab. Für ζ gibt es aber auch noch a viele Möglichkeiten und wir haben für das Paar (z,ζ) insgesamt höchstens $a^2 b$ viele Lösungen.
- $a \neq b$ und $a > 0 > b$, so können wir die obige Gleichung beidseits mit $(1-z^a)^{-b} \cdot z^{-ab}$ multiplizieren. Dann erhalten wir nämlich die Polynomgleichung $(1-z^a)^{-b} \cdot \left(z^{-b} - \zeta\right)^a = z^{-ab}$ und diese Gleichung hat bei einem festen ζ für z maximal $|2ab|$ viele Lösungen. Wiederum gibt es für ζ genau a viele Möglichkeiten. Somit ist die Anzahl Lösungen für das Paar (z,ζ) beschränkt durch $|2a^2 b|$.
- $a = b > 0$ und $\zeta \neq 1$, so hat die obige Gleichung höchstens ab viele Lösungen für z. Für $\zeta \neq 1$ haben wir $a-1$ viele Möglichkeiten, so dass es für (z,ζ) maximal $ab \cdot (a-1)$ viele Lösungen gibt.

Da wir $x = z^a$ gewählt haben, ist die Anzahl Lösungen für x von (1) und (2) in jedem der drei Fälle beschränkt durch

- ab,
- $|2ab|$ und
- $b \cdot (a-1) = a \cdot (a-1)$.

□

Lemma 2.4
Sei n eine ungerade natürliche Zahl mit $a(n) > 0$. Dann ist $r(n)$ ein Teiler von $a(n)$.

Beweis

Die Gruppe $\mathbb{Z}/r(n)\mathbb{Z}$ operiert auf $A_n = \left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \operatorname{ord}(x, 1-x) = n\right\}$ mittels

$$\mathbb{Z}/r(n)\mathbb{Z} \times A_n \to A_n,\ (a + r(n)\mathbb{Z}, x) \mapsto x^{2^a}.$$

Dass dies in der Tat eine Operation ist, wird im Kapitel über die Heuristik gezeigt. $\mathbb{Z}/r(n)\mathbb{Z}$ operiert frei auf A_n. Sei nämlich $x \in A_n$ und $g = a + r(n)\mathbb{Z} \in \mathbb{Z}/r(n)\mathbb{Z}$, so dass $gx = x$. Dann ist also $x^{2^a} = x$ und daraus folgt, dass $g = 0$ ist, denn für alle $x \in A_n$ ist $\mathbb{F}_2(x) = \mathbb{F}_{2^{r(n)}}$ und somit gilt für alle $0 < a < r(n)$, dass $x^{2^a} \neq x$. Die Wirkung von $\mathbb{Z}/r(n)\mathbb{Z}$ ist also frei, und damit ist für alle $x \in A_n$ der Stabilisator $\operatorname{Stab}_{\mathbb{Z}/r(n)\mathbb{Z}}(x)$ trivial. Mit der Bahnformel folgern wir schliesslich, dass jede Bahn die Länge $r(n)$ hat und somit ist A_n eine Vereinigung von Bahnen der Länge $r(n)$. □

Wir beweisen den Satz 2.1 für die erste Behauptung. Nehmen wir an, dass $a(n) > 0$. $r(n)$ ein Teiler ist von $a(n)$, also insbesondere ist $r(n) \leq a(n)$. Nun gelten aber nach Voraussetzung des Satzes die Ungleichungen $a(n) \leq b(n) \leq ab < r(n)$, was sofort einen Wiederspruch nach sich zieht. Entsprechend werden die zweite und dritte Behauptung bewiesen.

□

Satz 2.5
Sei n eine ungerade natürliche Zahl und es gebe Zahlen i, i', j, j', so dass

1. $2^i + 2^{i'} \equiv 2^j + 2^{j'} \bmod n$ *und*
2. $(i, i') \not\equiv (j, j'), (j', j) \bmod r(n)$.

Dann ist $a(n) = 0$.

Bemerkung

Diesem Satz geben wir in der Folge den Namen *Kriterium*. Wir sagen, eine ungerade natürliche Zahl n *erfüllt das Kriterium*, falls es Zahlen i, i', j, j' gibt, so dass

1. $2^i + 2^{i'} \equiv 2^j + 2^{j'} \bmod n$ und
2. $(i, i') \not\equiv (j, j'), (j', j) \bmod r(n)$.

Andernfalls nennen wir n einen *Kandidaten*.

Beweis

Sei n eine ungerade natürliche Zahl. Nehmen wir an, es existieren Zahlen i, i', j, j' mit $2^i + 2^{i'} \equiv 2^j + 2^{j'} \bmod n$ und $(i, i') \not\equiv (j, j'), (j', j) \bmod r(n)$, so dass $a(n) > 0$. Es gibt also ein $x \in \overline{\mathbb{F}}_2 \setminus \{0, 1\}$ mit $\operatorname{ord}(x, 1-x) = n$. Da n ein Teiler von $2^i + 2^{i'} - 2^j - 2^{j'}$ ist, gelten die Gleichungen

$$x^{2^i+2^{i'}-2^j-2^{j'}} = 1 \text{ und } (1-x)^{2^i+2^{i'}-2^j-2^{j'}} = 1.$$

Die erste Gleichung ist äquivalent zu $x^{2^i}x^{2^{i'}} = x^{2^j}x^{2^{j'}}$ und die zweite zu $(1-x)^{2^i}(1-x)^{2^{i'}} = (1-x)^{2^j}(1-x)^{2^{j'}}$. Unter Berücksichtigung der Charakteristik ist letztere aber äquivalent zu $\left(1-x^{2^i}\right)\left(1-x^{2^{i'}}\right) = \left(1-x^{2^j}\right)\left(1-x^{2^{j'}}\right)$. Multiplizieren wir diese Gleichung aus und setzen $x^{2^i}x^{2^{i'}} = x^{2^j}x^{2^{j'}}$ ein, so ergibt sich $x^{2^{i'}} - x^{2^{j'}} = x^{2^j} - x^{2^i}$ bzw.

$$x^{2^{i'}}\left(1-x^{2^{j'}-2^{i'}}\right) = x^{2^j}\left(1-x^{2^i-2^j}\right).$$

Da nach Voraussetzung des Satzes $x^{2^i-2^j} \neq 1$ ist, kommen wir zu

$$x^{2^j-2^{i'}} = \frac{1-x^{2^{j'}-2^{i'}}}{1-x^{2^i-2^j}}.$$

Da aber $x^{2^i}x^{2^{i'}} = x^{2^j}x^{2^{j'}}$ gilt, ist die rechte Seiter dieser Gleichung 1. Es folgt also, dass $x^{2^j} = x^{2^{i'}}$ bzw $x^{2^{i'}-2^j} = 1$ ist. Somit gilt aber auch die Rechnung $(1-x)^{2^{i'}-2^j} = (1-x)^{2^{i'}\left(1-2^{j-i'}\right)} = \left(1-x^{2^{i'}}\right)^{1-2^{j-i'}} = \frac{1-x^{2^{i'}}}{\left(1-x^{2^{i'}}\right)^{2^{j-i'}}} = \frac{1-x^{2^{i'}}}{1-x^{2^j}} = 1$. Nun ist aber $n = \operatorname{kgv}(\operatorname{ord}(x), \operatorname{ord}(1-x))$ und daher ist $2^{i'}-2^j$ ein Vielfaches von n, was aber ein Widerspruch zu den Voraussetzungen des Satzes ist.

□

Korollar 2.6
Sei n eine ungerade natürliche Zahl. Falls $r(n) > \sqrt{2n+\frac{1}{4}} - \frac{1}{2}$, dann ist $a(n) = 0$.

Beweis

Wir wenden das Schubfachprinzip an. Es ist

$$\#\{(i,j) \mid 0 \leq i \leq j < r(n)\} = \frac{1}{2}r(n)(r(n)+1)$$

und die Anzahl möglicher Restklassen ist n. Gilt nun $\frac{1}{2}r(n)(r(n)+1) > n$, so gibt es eine Restklasse, in der zwei Zahlen $2^i + 2^j$ und $2^{i'} + 2^{j'}$ liegen. Somit hat die Kongruenz $2^i + 2^{i'} \equiv 2^j + 2^{j'} \bmod n$ mit $(i,i') \not\equiv (j,j'), (j',j) \bmod r(n)$ sicher eine Lösung. Nun ist $\frac{1}{2}r(n)(r(n)+1) > n \Leftrightarrow \frac{r(n)(r(n)+1)}{2} > n \Leftrightarrow \left(r(n)+\frac{1}{2}\right)^2 > 2n + \left(\frac{1}{2}\right)^2$. Damit ist $a(n) = 0$ falls $r(n) > \sqrt{2n+\frac{1}{4}} - \frac{1}{2}$. □

Wir definieren eine weitere zahlentheoretische Funktion

$$c : \mathbb{N} \to \mathbb{N},\ n \mapsto c(n) = \sum_{m \leq n} a(m).$$

Über diese Abbildung können wir folgende Aussagen treffen:

Proposition 2.7
Sei n eine natürliche Zahl. Dann gilt

1. $c(n) > \frac{n}{2} - 2$.
2. $c(n) = o(n^2)$.

Für den Beweis des zweiten Teils benötigen wir folgenden Satz:

Satz 2.8
Sei $n \in \mathbb{N}$ eine natürliche Zahl. Dann existiert ein $\delta > 0$, so dass

$$S(n) = \#\left\{1 \leq m \leq n \mid m \text{ ungerade und } r(m) \leq \sqrt{m}\exp\left((\log m)^\delta\right)\right\} = o(n).$$

Ein Beweis findet sich in [KuRu].

Somit können wir nun Proposition 2.6 beweisen:

Beweis

Sei $n \in \mathbb{N}$.

1. Wir betrachten ein $m \in \mathbb{N}$, so dass $2^{m+1} > n \geq 2^m - 1$. Da für jedes $n \in \mathbb{N}$

$$b(n) = \sum_{d|n} a(d) \leq \sum_{m \leq n} a(m) = c(n)$$

gilt, und c monoton steigend ist, gelten folgende Ungleichungen: $c(n) \geq c(2^m - 1) \geq b(2^m - 1)$. Nun ist $b(2^m - 1) = 2^m - 2$, weil $r(2^m - 1) = m$ ist und somit wird $b(2^m - 1) = \#\left\{x \in \mathbb{F}_{2^m} \setminus \{0,1\} \mid x^{2^m-1} = 1 = (1-x)^{2^m-1}\right\}$. In $\mathbb{F}_{2^m} \setminus \{0,1\}$ erfüllt aber jedes Element x die Gleichung $x^{2^m-1} = 1$ und die Anzahl Elemente in $\mathbb{F}_{2^m} \setminus \{0,1\}$ ist $2^m - 2$. Nach der Wahl von m ist nun $2^m - 2 > \frac{n}{2} - 2$, und schliesslich gilt $c(n) > \frac{n}{2} - 2$.

2. Wir betrachten

$$R(n) = \#\left\{1 \leq m \leq n \mid m \text{ ungerade und } r(m) \leq \sqrt{2m + \frac{1}{4}} - \frac{1}{2}\right\}.$$

Sei $\delta > 0$, so dass $S(n) = o(n)$. Nun ist $R(n) \leq S(n)$, denn $\sqrt{2m + \frac{1}{4}} - \frac{1}{2} < \sqrt{2m + m} = \sqrt{3}\sqrt{m}$ und $\sqrt{3}\sqrt{m} < \exp(1)\sqrt{m} \leq \sqrt{m}\exp\left((\log m)^\delta\right)$ für alle $3 \leq m \leq n$. Somit ist also $R(n) = o(n)$ und daraus schliessen wir

$$\lim_{n\to\infty} \frac{c(n)}{n^2} \leq \lim_{n\to\infty} \frac{nR(n)}{n^2} = \lim_{n\to\infty} \frac{R(n)}{n} = 0$$

und somit ist $c(n) = o(n^2)$.

□

3 Berechnungen

3.1 Berechnung von $b(n)$

Sei n eine ungerade natürliche Zahl. In diesem Abschnitt zeigen wir, wie sich der Wert von $b(n)$ berechnen lässt. Sei $F_n(X) = X^n - 1$ ein Polynom über $\mathbb{F}_2$. Wie wir bereits gesehen haben, lässt sich $b(n)$ anhand von $F_n(X)$ und $F_n(1-X)$ für ein ungerades n berechnen. Wir wollen nun explizit angeben, wie sich $b(n)$ berechnen lässt. Dazu betrachten wir folgendes Lemma:

Lemma 3.1
Sei n eine ungerade natürliche Zahl. Dann gilt:

1. $F_n(x) = 0$ und $F_n(1-x) = 0 \Leftrightarrow \mathrm{ggT}(F_n(X), F_n(1-X))(x) = 0$.

2. $F_n(X)$ *ist separabel über* $\mathbb{F}_2$.

Beweis

1. Sei $x \in \overline{\mathbb{F}}_2 \setminus \{0,1\}$ mit $F_n(x) = 0 = F_n(1-x)$ und sei $G(X) = \mathrm{ggT}(F_n(X), F_n(1-X))$. Dann ist $F_n(X) = P(X)G(X)$ und $F_n(1-X) = Q(X)G(X)$ und die Polynome P und Q haben keine gemeinsame Nullstelle. Hätten nämlich P und Q eine gemeinsame Nullstelle x_0, so wäre $(X-x_0)G(X)$ ein gemeinsamer Teiler von $F_n(X)$ und $F_n(1-X)$. Nehmen wir an, es sei $G(x) \neq 0$. Dann ist aber $P(x) = 0 = Q(x)$ und x ist somit eine gemeinsame Nullstelle von P und Q.
Sei nun umgekehrt $x \in \overline{\mathbb{F}}_2 \setminus \{0,1\}$ und $G(X) = \mathrm{ggT}(F_n(X), F_n(1-X))$ mit $G(x) = 0$. Wieder ist $F_n(X) = P(X)G(X)$ und $F_n(1-X) = Q(X)G(X)$. Da $G(x) = 0$ ist, gilt $F_n(x) = 0$ und $F_n(1-x) = 0$.

2. F_n ist separabel über $\mathbb{F}_2$, falls F_n und F_n' in $\overline{\mathbb{F}}_2$ keine gemeinsamen Nullstellen in $\overline{\mathbb{F}}_2$ haben. Nun ist $F_n'(X) = nX^{n-1} = 0 \Leftrightarrow X = 0$, denn n ist ungerade und somit ungleich Null. Weil aber $F_n(0) = 1$ ist, schliessen wir, dass F_n separabel ist.

□

Proposition 3.2
Sei n eine ungerade natürliche Zahl. Für die Anzahl aller Elemente $x \in \overline{\mathbb{F}}_2 \setminus \{0,1\}$, für die $\mathrm{ord}(x, 1-x)$ *ein Teiler von n ist, gilt*

$$b(n) = \deg\left(\mathrm{ggT}\left(X^n - 1, (1-X)^n - 1\right)\right).$$

Beweis

Sei n eine ungerade natürliche Zahl. Wir haben gezeigt, dass

$$b(n) = \#\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \mathrm{ggT}\left(F_n(X), F_n(1-X)\right)(x) = 0\right\}.$$

Nun ist aber auch $G(X) = \mathrm{ggT}(F_n(X), F_n(1-X))$ separabel. Nehmen wir an, es gäbe ein $x \in \overline{\mathbb{F}}_2 \setminus \{0,1\}$ mit $G(x) = 0 = G'(x)$. Schreiben wir $F_n(X) = G(X)P(X)$, so ist $F_n(x) = 0$. Betrachten wir nun $F_n'(X) = G(X)P'(X) + G'(X)P(X)$, so folgern wir, dass auch $F_n'(x) = 0$ ist, was ein Widerspruch zur Separabilität von F_n ist. Da G separabel ist, hat G in $\overline{\mathbb{F}}_2$ genau $\deg(G)$ viele verschiedene Nullstellen. Somit ist dann $b(n) = \deg\left(\mathrm{ggT}\left(X^n - 1, (1-X)^n - 1\right)\right)$. □

Die Berechnung der $b(n)$ lässt sich aber noch vereinfachen. Sei j die kleinste natürliche Zahl mit $n < 2^j$. Dann ist $n = 2^j - m$ für ein $m > 0$. Multiplizieren wir nun $(1-X)^n - 1$ mit $(1-X)^m$, so erhalten wir unter Berücksichtigung, dass in der Faktorzerlegung von $X^n - 1$ der Faktor $1-X$ genau eimal vorkommt und dass $(1-X) \nmid \left((1-X)^n - 1\right)$ folgendes: $\mathrm{ggT}\left(X^n - 1, (1-X)^n - 1\right) = \frac{1}{1-X}\,\mathrm{ggT}\left(X^n - 1, (1-X)^{2^j} - (1-X)^m\right)$. Zu $(1-X)^{2^j} - (1-X)^m$ addieren wir nun $(X^n - 1)X^m = X^{2j} - X^m$. Dies ergibt dann

$$b(n) = \deg\left(\frac{1}{1-X}\,\mathrm{ggT}\left(X^n - 1, 1 - X^m - (1-X)^m\right)\right)$$

$$= \deg\left(\mathrm{ggT}\left(X^n - 1, 1 - X^m - (1-X)^m\right)\right) - 1.$$

Eine zweite Möglichkeit bietet sich an, wenn wir j als die grösste natürliche Zahl mit $n > 2^j$ wählen. Schreiben wir $n = 2^j + m$ mit $m > 0$ und multiplizieren wir das Polynom $(1-X)^n - 1$ mit X^m, dann ist $\mathrm{ggT}\left(X^n - 1, (1-X)^n - 1\right) = \mathrm{ggT}\left(X^n - 1, \right.$ $\left.(1-X)^{2^j} X^m (1-X)^m - X^m\right)$. Nun ist aber $(1-X)^{2^j} X^m = \left(1 - X^{2^j}\right) X^m = X^m - X^n$. Zu berechnen bleibt also

$$\mathrm{ggT}\left(X^n - 1, \left(X^m - X^n\right)(1-X)^m - X^m\right).$$

Addieren wir nun zu $\left(X^m - X^n\right)(1-X)^m - X^m$ das Polynom $(1-X)^m\left(X^n - 1\right)$, so erhalten wir in diesem Fall

$$b(n) = \deg\left(\mathrm{ggT}\left(X^n - 1, \left(X^m - 1\right)(1-X)^m - X^m\right)\right).$$

Zusammengefasst erhalten wir:

Proposition 3.3
Sei n eine ungerade natürliche Zahl.

1. *Sei j die kleinste natürliche Zahl mit $n < 2^j$ und $m > 0$, so dass $n = 2^j - m$. Dann gilt $b(n) = \deg\left(\mathrm{ggT}\left(X^n - 1, 1 - X^m - (1-X)^m\right)\right) - 1$.*
2. *Sei j die grösste natürliche Zahl mit $n > 2^j$ und $m > 0$, so dass $n = 2^j + m$. Dann ist $b(n) = \deg\left(\mathrm{ggT}\left(X^n - 1, \left(X^m - 1\right)(1-X)^m - X^m\right)\right)$.*

Wollen wir nun für eine ungerade natürliche Zahl n den Wert $b(n)$ berechnen, so wählen wir jene der zwei Möglichkeiten, bei der der Grad des zweiten Polynoms in der Berechnung des grössten gemeinsamen Teilers kleiner ist. Um eine Aussage über diesen Grad zu treffen, betrachten wir jetzt die folgende Abbildung:

$$m : \mathbb{N} \to \mathbb{N},\ n \mapsto m(n) = \min\left\{m_1, 2m_2\right\},$$

wobei sich für eine ungerade natürliche Zahl n die Werte m_1 und m_2 wie folgt berechnen: $m_1 = 2^{j_1} - n$ mit $j_1 = \min\left\{k \in \mathbb{N} \mid n < 2^k\right\}$ und $m_2 = n - 2^{j_2}$ mit $j_2 = \max\left\{k \in \mathbb{N} \mid n > 2^k\right\}$.

Proposition 3.4
Sei n eine ungerade natürliche Zahl. Dann gilt: $m(n) \leq \frac{n}{2}$.

Beweis

Sei n eine ungerade natürliche Zahl. Wir betrachten den Fall $m(n) = m_1 = 2m_2$. Dies ist äquivalent zu $2^j - n = 2\left(n - 2^{j-1}\right)$ mit $j = j_1$ und $j_2 = j - 1$. Diese Gleichung führt uns zu $n = \frac{2}{3}2^j$. Ist nun $n > \frac{2}{3}2^j$, so wird $m(n) = m_1$. Andernfalls ist $m(n) = 2m_2$.

- Sei $n > \frac{2}{3}2^j$. Dann ist $m(n) = m_1 = 2^j - n < \frac{3}{2}n - n = \frac{n}{2}$.
- Sei $n \leq \frac{2}{3}2^j$. Dann ist $m(n) = 2n - 2^j \leq 2n - \frac{3}{2}n = \frac{n}{2}$.

□

Wir zeigen nun noch den Verlauf der Abbildung m in Abhänigkeit von n, sowie eine Graphik, die uns zeigt, um wieviel mal schneller die Berechnung von $b(n)$ mittels Proposition 3.3 ist als mittels Proposition 3.2.

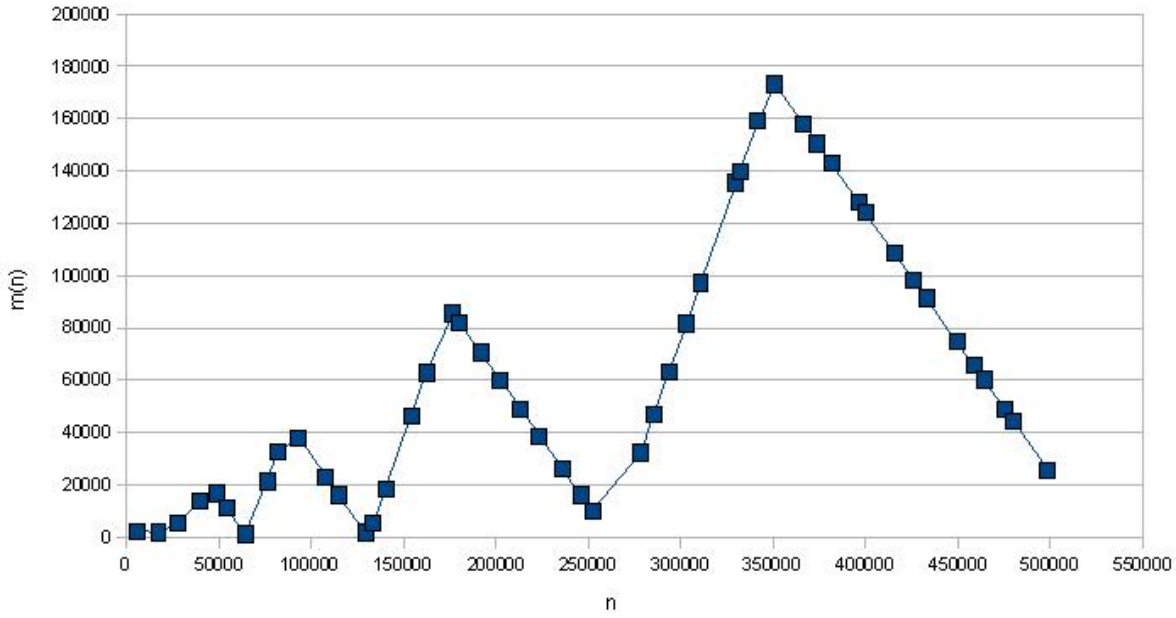

Abbildung 1: Verlauf von m

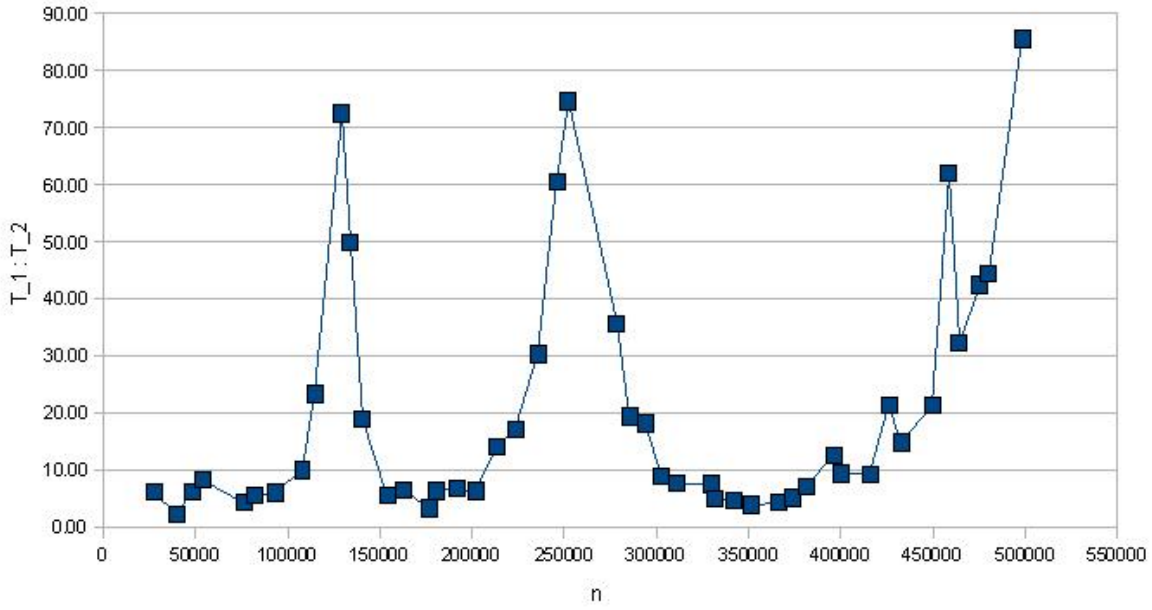

Abbildung 2: Verbesserung der Laufzeit zur Berechnung von $b(n)$. Dabei ist T_1 die Laufzeit zur Berechnung von $b(n)$ mittels Proposition 3.2 und T_2 diejenige mittels Proposition 3.3.

3.2 Algorithmen zur Berechnung von $b(n)$ bzw. $a(n)$

In diesem Kapitel stellen wir drei Algorithmen vor. Wir wollen für jede ungerade natürliche Zahl n zwischen 1 und einer gegebenen oberen Grenze $N \in \mathbb{N}$ das $a(n)$ berechnen. Wir betrachten dazu die Menge

$$M = \{n \in \mathbb{N} \mid 1 \leq n \leq N, \text{ n ungerade}\}.$$

Die Berechnung von $a(n)$ für $n \in M$ erfolgt nun in drei Schritten:

1. Prüfe für alle $n \in M$, ob n das Kriterium erfüllt oder nicht. Wir betrachten dann die Mengen

   $$M_0 = \{n \in M \mid n \text{ erfüllt das Kriterium}\} \text{ und } M_1 = M \setminus M_0.$$

   Für jedes $n \in M_0$ ist dann $a(n) = 0$ und für jedes $n \in M_1$ möchten wir $a(n)$ berechnen.

2. Berechne für jede Zahl $n \in M_1$ das $b(n)$.

3. Berechne für jedes $n \in M_1$ das $a(n)$.

3.2.1 Kriterium

Als erstes stellen wir einen Algorithmus vor, der mittels dem Kriterium entscheidet, welche ungeraden Zahlen $n \in M$ das Kriterium nicht erfüllen. Dies ergibt dann die Menge von Kandidaten M_1. Dazu betrachten wir folgende äquivalente Formulierung des Kriteriums:

Proposition 3.5
Sei n eine ungerade natürliche Zahl. Äquivalent sind

1. *Es existieren Zahlen i, i', j, j', so dass $2^i + 2^{i'} \equiv 2^j + 2^{j'} \mod n$ und $(i, i') \not\equiv (j, j'), (j', j) \mod r(n)$*

2. *Es existieren Zahlen x, y, z, so dass $(1 + 2^x)^{r(n)} \equiv (1 + 2^y)^{r(n)} \mod n$ und $1 + 2^y \equiv 2^z (1 + 2^x) \mod n$. Des Weiteren erfüllen x, y und z die Bedingungen $z \not\equiv 0 \mod r(n)$, $z + x \not\equiv 0 \mod r(n)$, $z \not\equiv y \mod r(n)$ und $z + x \not\equiv y \mod r(n)$.*

Beweis

1. 1. $\Rightarrow$ 2.
   Nehmen wir an, n erfülle das Kriterium. Es gibt also Zahlen i, i', j, j' mit $(i, i') \not\equiv (j, j'), (j', j) \bmod r(n)$, so dass

   $$2^i + 2^{i'} \equiv 2^j + 2^{j'} \bmod n.$$

   Schriben wir $2^i \left(1 + 2^{i'-i}\right) \equiv 2^j \left(1 + 2^{j'-j}\right) \bmod n$ und potenzieren beide Seiten mit $r(n)$, so folgt

   $$\left(1 + 2^{i'-i}\right)^{r(n)} \equiv \left(1 + 2^{j'-j}\right)^{r(n)} \bmod n,$$

denn $(2^i)^{r(n)}$ beziehungsweise $(2^j)^{r(n)}$ ist kongruent $1 \bmod n$. Setzen wir nun $x = i' - i$ und $y = j' - j$, erhalten wir die Kongruenz

$$(1 + 2^x)^{r(n)} \equiv (1 + 2^y)^{r(n)} \bmod n.$$

Nun wählen wir $z = i - j$. Dann erfüllen die Zahlen x, y, z die geforderten Bedingungen.

2. 2. $\Rightarrow$ 1.
Nehmen wir an, es gibt Zahlen x, y, z, so dass $(1 + 2^x)^{r(n)} \equiv (1 + 2^y)^{r(n)} \mod n$ und $1 + 2^y \equiv 2^z (1 + 2^x) \mod n$ mit $z \not\equiv 0 \mod r(n)$, $z + x \not\equiv 0 \mod r(n)$, $z \not\equiv y \mod r(n)$ und $z + x \not\equiv y \mod r(n)$. Setzen wir $i = 0$, $i' = y$, $j' = z + x$ und $j = z$, so folgt aus $1 + 2^y \equiv 2^z (1 + 2^x) \mod n$, dass $1 + 2^{i'} \equiv 2^j + 2^j \bmod n$ und die geforderten Bedingungen an i, i', j, j' sind ebenfalls erfüllt.

□

Bemerkung

Die Beding
ungen $z \not\equiv 0 \mod r(n)$, $z + x \not\equiv 0 \mod r(n)$, $z \not\equiv y \mod r(n)$ und $z + x \not\equiv y \mod r(n)$ an x, y und z sind äquivalent zu den folgenden Bedingungen:

- $0 \leq x \leq y \leq \frac{r(n)}{2}$
- $x \neq \frac{r(n)}{2} \vee y \neq \frac{r(n)}{2} \vee z \neq \frac{r(n)}{2}$.

Wir benutzen nun Proposition 3.4 um das Kriterium zu implementieren. Sei $n \in M$. Der Algorithmus besteht im Wesentlichen aus zwei Teilen:

1. Untersuche, ob $r(n) \leq \sqrt{2n + \frac{1}{4}} - \frac{1}{2}$. Falls $r(n) > \sqrt{2n + \frac{1}{4}} - \frac{1}{2}$ ist, ist $a(n) = 0$.

2. Falls $r(n) \leq \sqrt{2n + \frac{1}{4}} - \frac{1}{2}$ ist: Finde $0 \leq x \leq y \leq \frac{r(n)}{2}$ und $0 \leq z < r(n)$:

   - $(1 + 2^x)^{r(n)} \equiv (1 + 2^y)^{r(n)} \mod n$, und
   - $1 + 2^y \equiv 2^z (1 + 2^x) \mod n$, und
   - $x \neq \frac{r(n)}{2} \vee y \neq \frac{r(n)}{2} \vee z \neq \frac{r(n)}{2}$.

   Falls so ein Tripel gefunden wurde, dann ist $a(n) = 0$. Andernfalls ist n ein Kandidat, d.h. es ist $n \in M_1$.

Der Output dieses Algorithmus ist also die Menge M_1. Das nächste Programm berechnet für alle $n \in M_1$ das $b(n)$.

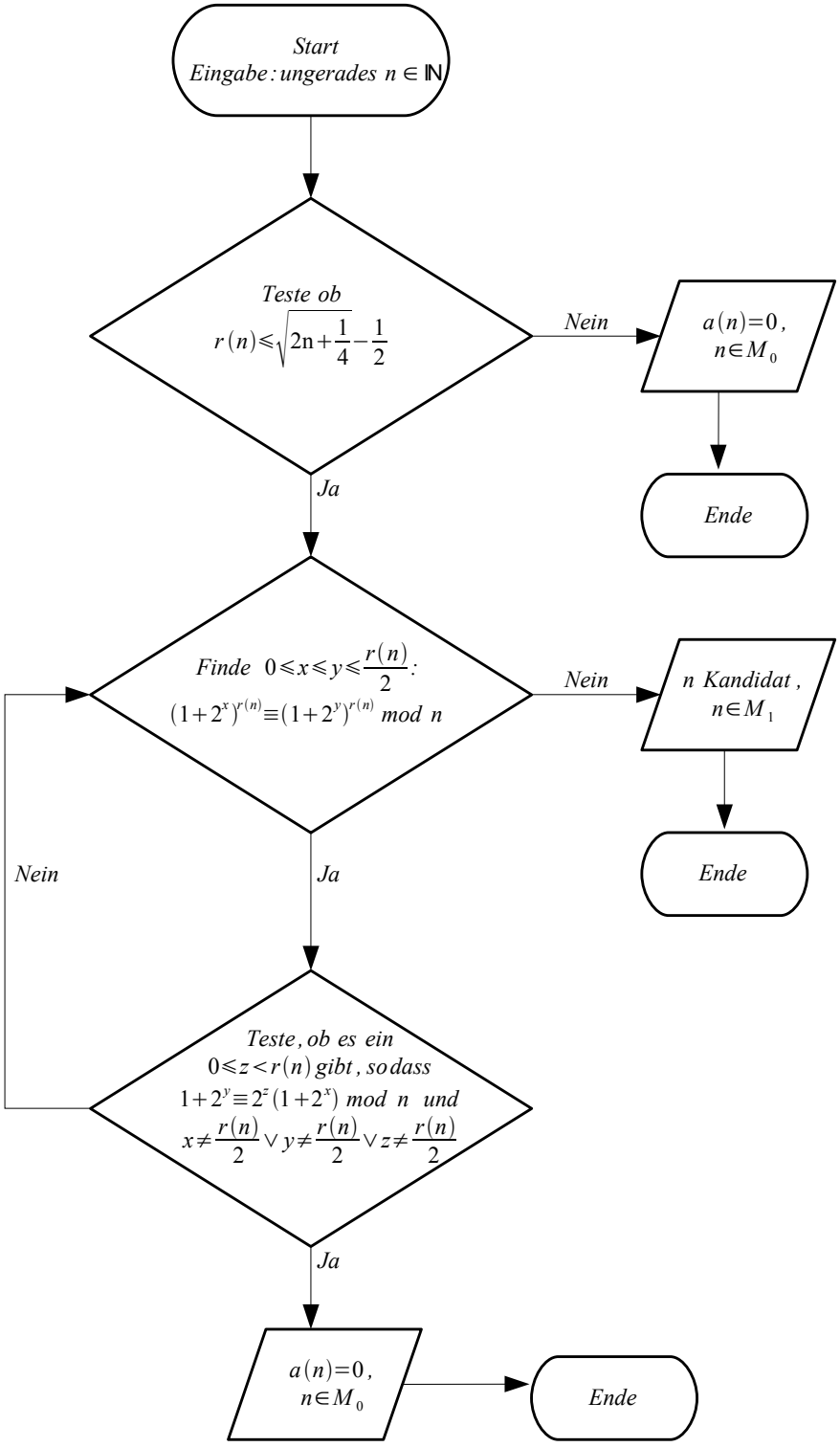

Abbildung 3: Programmablaufplan für das Kriterium

3.2.2 Berechnung von $b(n)$

In diesem Kapitel stellen wir einen Algorithmus zur Berechnung der $b(n)$ vor. Sei also n eine ungerade natürliche Zahl. Die Berechnung von $b(n)$ erfolgt in zwei Schritten:

1. Berechnung der kleinsten Zahl j_1, so dass $2^{j_1} > n$. Dann ist $j_2 = j_1 - 1$ die grösste Zahl mit $2^{j_2} < n$. Definiere $m_1 = 2^{j_1} - n$ und $m_2 = n - 2^{j_2}$.

2. Falls $2m_2 \geq m_1$, dann rechnen wir

$$b(n) = \deg\left(\mathrm{ggT}\left(X^n - 1, 1 - X^{m_1} - (1-X)^{m_1}\right)\right) - 1.$$

   Falls $2m_2 < m_1$, dann berechnen wir

$$b(n) = \deg\left(\mathrm{ggT}\left(X^n - 1, \left(X^{m_2} - 1\right)(1-X)^{m_2} - X^{m_2}\right)\right).$$

Die Berechnung des grössten gemeinsamen Teilers zweier Polynome über $\mathbb{F}_2$, erfolgt mit der portablen C++ Bibliothek NTL. Die beiden Polynome müssen dabei als Vektoren, dessen Komponenten die Koeffizienten der Polynome sind, eingelesen werden. Wir haben also für eine natürliche Zahl n die Koeffizienten der Polynome $X^n - 1, 1 - X^n - (1-X)^n, (X^n - 1)(1-X)^n - X^n \in \mathbb{F}_2[X]$ zu berechnen. Sei $(1-X)^n = p_0 + p_1 X + \cdots + p_n X^n$. mit $p_i \in \mathbb{F}_2$. Betrachten wir nun dieses Polynom als Vektor $[p_0, \ldots, p_n]$, so erhalten wir:

- $X^n - 1 = [1, \ldots, 1]$,
- $1 - X^n - (1-X)^n = [1 + p_0, p_1, \ldots, p_{n-1}, 1 + p_n]$,
- $(X^n - 1)(1-X)^n - X^n = [p_0, \ldots, p_{n-1}, p_0 + p_n + 1, p_1 \ldots, p_n]$.

3.2.3 Berechnung von $a(n)$

Wir zeigen nun, wie wir für alle $n \in M_1$ das $a(n)$ berechnen. Aus den Definitionen von $a(n)$ und $b(n)$ folgt $b(n) = \sum_{d|n} a(d)$ und somit ist

$$a(n) = b(n) - \sum_{\substack{d<n \\ d|n}} a(d).$$

Schreiben wir $M_1 = \{n_1, \ldots, n_q\}$ mit $n_1 < n_2 < \cdots < n_q$, so hat man folgende Rekursion:

$$a(n_1) = b(n_1) \text{ und}$$

$$a(n_k) = b(n_k) - \sum_{\substack{d<k \\ n_d|n_k}} a(n_d) \text{ für } k = 2, \ldots, q.$$

Berechnen wir nun $a(n)$ und $c(n)$ für alle ungeraden n zwischen 1 und $2'000'000$, so stellen wir damit die Vermutung auf, dass

$$c(n) = O(n)$$

ist.

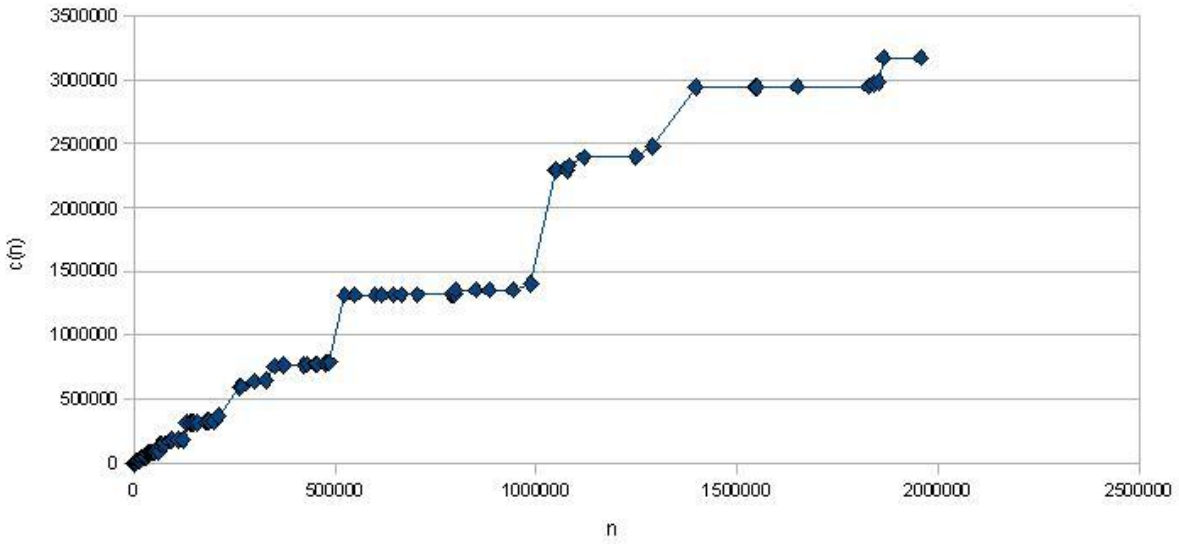

Abbildung 4: Verlauf der Abbildung c

Algorithm 1 Koeffizienten von $(1-X)^n$ über $\mathbb{F}_2$ mittels Binärdarstellung von $n = \sum_i a_i 2^i$.

```
1:  procedure KOEFF(n)
2:      i ← 0
3:      k ← 1                                          ▷ k = 2^i
4:      m ← n                                          ▷ m = ⌊n/2^i⌋
5:      w[0] ← 1
6:      d ← 0                                          ▷ d = deg(w)
7:      while m > 0 do
8:          if m odd then                              ▷ dann ist a_i = 1
9:              for j = 0 to d do
10:                 w[j + k] ← w[j]                    ▷ w ← w · (1 + x^{2^i})
11:             end for
12:             m ← (m − 1)/2
13:             d ← k + d
14:             i ← i + 1
15:             k ← 2k
16:         else                                       ▷ dann ist a_i = 0
17:             m ← m/2
18:             i ← i + 1
19:             k ← 2k
20:         end if
21:     end while
22:     return w
23: end procedure
```

n	a(n)	c(n)	r(n)	(2^r(n)-1)/n
3	2	2	2	1
7	6	8	3	1
15	12	20	4	1
31	30	50	5	1
63	54	104	6	1
73	18	122	9	7
85	24	146	8	3
127	126	272	7	1
255	216	488	8	1
273	24	512	12	15
341	90	602	10	3
511	486	1088	9	1
585	72	1160	12	7
819	108	1268	12	5
1023	900	2168	10	1
1057	60	2228	15	31
1365	396	2624	12	3
1387	36	2660	18	189
2047	2046	4706	11	1
2359	42	4748	21	889
3133	48	4796	24	5355
4095	3420	8216	12	1
4161	72	8288	18	63
4369	240	8528	16	15
4681	540	9068	15	7
5461	1722	10790	14	3
6765	60	10850	20	155
8191	8190	19040	13	1
8525	120	19160	20	123
9399	48	19208	24	1785
9709	270	19478	18	27
11275	180	19658	20	93
12483	486	20144	18	21
13107	2256	22400	16	5
13797	594	22994	18	19
13981	180	23174	20	75
16383	14532	37706	14	1
16513	210	37916	21	127
19065	240	38156	20	55
21845	6960	45116	16	3
21931	96	45212	24	765
25575	420	45632	20	41

Abbildung 5: $a\,(n)$ und $c\,(n)$ für $n = 1, \ldots, 2'000'000$

28197	144	45776	24	595
29127	2700	48476	18	9
32767	32130	80606	15	1
33825	960	81566	20	31
37449	4752	86318	18	7
41943	1380	87698	20	25
42799	1134	88832	21	49
46995	72	88904	24	357
47127	726	89630	22	89
49981	120	89750	30	21483
51319	72	89822	36	1339065
53261	72	89894	24	315
60787	1914	91808	22	69
65535	55824	147632	16	1
65793	288	147920	24	255
69905	4500	152420	20	15
75915	144	152564	24	221
76627	72	152636	36	896805
87381	25110	177746	18	3
95325	7620	185366	20	11
109655	216	185582	24	153
121369	156	185738	39	4529623
131071	131070	316808	17	1
140911	168	316976	28	1905
140985	1224	318200	24	119
143395	1080	319280	24	117
149943	120	319400	30	7161
151183	72	319472	36	454545
158369	168	319640	28	1695
159783	936	320576	24	105
178481	2484	323060	23	47
182361	6072	329132	22	23
184365	2016	331148	24	91
197379	1584	332732	24	85
209715	35040	367772	20	5
262143	227556	595328	18	1
262657	1026	596354	27	511
266305	3960	600314	24	63
299593	41454	641768	21	7
328965	5832	647600	24	51
349525	111180	758780	20	3
349867	540	759320	30	3069
372827	7848	767168	24	45

Abbildung 6: $a\,(n)$ und $c\,(n)$ für $n = 1, \ldots, 2'000'000$

422733	840	768008	28	635
430185	9720	777728	24	39
449829	360	778088	30	2387
453549	144	778232	36	151515
475107	588	778820	28	565
479349	11808	790628	24	35
486579	96	790724	48	578477445
486737	174	790898	29	1103
524287	524286	1315184	19	1
549791	270	1315454	30	1953
599479	528	1315982	33	14329
617093	1596	1317578	28	435
646443	270	1317848	30	1661
664335	108	1317956	36	103441
704555	1260	1319216	28	381
790097	990	1320206	30	1359
791845	2184	1322390	28	339
796593	84	1322474	42	5521071
798915	33984	1356458	24	21
849583	156	1356614	39	647089
883227	288	1356902	36	77805
942305	108	1357010	36	72927
986895	47664	1404674	24	17
1048575	885660	2290334	20	1
1049601	1200	2291534	30	1023
1077699	216	2291750	36	63765
1082401	34650	2326400	25	31
1118481	65880	2392280	24	15
1248537	4284	2396564	28	215
1290555	82800	2479364	24	13
1398101	462528	2941892	22	3
1545103	102	2941994	51	1457378449
1549411	1980	2943974	30	693
1649373	1440	2945414	30	651
1826203	168	2945582	42	2408301
1838599	23814	2969396	27	73
1851279	10836	2980232	28	145
1864135	190944	3171176	24	9
1957095	216	3171392	36	35113

Abbildung 7: $a\,(n)$ und $c\,(n)$ für $n = 1, \ldots, 2'000'000$

4 Heuristik

4.1 Erste Heuristik

Sei n eine ungerade natürliche Zahl und sei $A_n = \left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \operatorname{ord}(x, 1-x) = n\right\}$. In diesem Kapitel wollen wir einen heuristischen Wert für $a(n) = |A_n|$ herleiten. Dazu betrachten wir die Menge

$$W_{r(n)} = \left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \mathbb{F}_2(x) = \mathbb{F}_{2^{r(n)}}\right\},$$

über die wir die folgenden Aussagen treffen können:

Proposition 4.1
Es gilt:

1. $A_n \subseteq W_{r(n)}$.
2. $x \in W_{r(n)} \Rightarrow 1 - x \in W_{r(n)}$.

Des Weiteren definieren wir die Menge

$$T_n = \left\{x \in W_{r(n)} \mid x^n = 1\right\}.$$

Dies sind alle Elemente von $\overline{\mathbb{F}}_2 \setminus \{0,1\}$ der Ordnung n' für einen Teiler n' von n, der nicht schon Teiler von $2^{r'} - 1$ ist für einen echten Teiler r' von $r(n)$. Die nächste Proposition zeigt uns, wie wir die Kardinalitäten von $W_{r(n)}$ und T_n für eine ungerade natürliche Zahl n berechnen.

Proposition 4.2
Es gilt:

1. $\left|W_{r(n)}\right| = \sum_{d \mid r(n)} \mu(d)\, 2^{\frac{r(n)}{d}}$.
2. $|T_n| = \sum_{d \mid r(n)} \mu(d)\, \operatorname{ggT}\left(n, 2^{\frac{r(n)}{d}} - 1\right)$.

Beweis

1. Sei $W_d = \{x \in \mathbb{F}_{2^d} \mid \mathbb{F}_2(x) = \mathbb{F}_{2^d}\}$. Wir zeigen nun, dass

$$\mathbb{F}_{2^k} = \coprod_{d \mid k} W_d$$

ist. Sei $x \in \mathbb{F}_{2^k}$. Dann gibt es ein natürliches d mit $d \mid k$, so dass $\mathbb{F}_2(x) = \mathbb{F}_{2^d}$. Damit liegt x in W_d und somit ist $x \in \bigcup_{d \mid k} W_d$. Sei nun $x \in W_d$ für ein $d \mid k$. Dann liegt x in $\mathbb{F}_{2^d}$. Da d ein Teiler von k ist, liegt x auch in $\mathbb{F}_{2^k}$. Nehmen wir an, es gäbe ein $x \in W_d \cap T_{d'}$ für zwei verschiedene Teiler d und d' von k. Damit ist $\mathbb{F}_2(x) = \mathbb{F}_{2^d}$ und $\mathbb{F}_2(x) = \mathbb{F}_{2^{d'}}$. Somit ist $\mathbb{F}_{2^d} = \mathbb{F}_{2^{d'}}$ und $d = d'$. Damit ist nun $2^k = \sum_{d \mid k} |W_d|$. Mit $k = r(n)$ und der Möbius'schen Umkehrformel folgt die Behauptung.

2. Sei $T_{n,d} = \{x \in W_d \mid x^n = 1\}$. Dann gilt: $\sum_{d|r(n)} |T_{n,d}| = |\{x \in \mathbb{F}_{2^{r(n)}} \mid x^n = 1\}| = \left|\left\{x \in \overline{\mathbb{F}}_2 \mid x^n = 1 \text{ und } x^{2^{r(n)}-1} = 1\right\}\right| = \left|\left\{x \in \overline{\mathbb{F}}_2 \mid x^{\mathrm{ggT}\left(n, 2^{r(n)}-1\right)} = 1\right\}\right| = \mathrm{ggT}\left(n, 2^{r(n)} - 1\right)$. Wiederum mit der Möbius'schen Umkehrformel folgt die Behauptung. □

Für die Heuristik gehen wir davon aus, dass für $x \in W_{r(n)}$ die Ereignisse $x \in T_n$ und $1 - x \in T_n$ stochastisch unabhängig sind. Dann ist die heuristische Anzahl der Punkte $(x, 1-x) \in T_n \times T_n$ gleich $\frac{|T_n|^2}{|W_{r(n)}|}$. Dies ist nun der heuristische Wert für die Summe der $a(n')$ für alle Teiler n' von n, die nicht schon Teiler von $2^{r'} - 1$ sind für einen echten Teiler r' von $r(n)$. Aus diesen berechnet man zuletzt den heuristischen Wert für $a(n)$.

Wie im letzten Kapitel betrachten wir nun die Menge M aller ungeraden natürlichen Zahlen n zwischen 1 und einer fixen oberen Grenze N. Sei wiederum

$$M_1 = \{k \in M \mid k \text{ erfüllt das Kriterium nicht}\}.$$

Wir möchten nun die heuristischen Werte für alle Zahlen aus M_1 berechnen. Die aus diesen Berechnungen resultierende Liste beinhaltet die heuristischen Werte aller Zahlen aus M_1, für die der exakt errechnete Wert und dessen heuristische Schätzung nicht beide Null sind. Die Liste zeigt uns aber, dass diese Heuristik verbessert werden kann. Es fällt auf, dass manchmal der exakte Wert von $a(n)$ grösser als Null ist, während der heuristische Wert fast verschwindet. Dies geschieht tendenziell dann, wenn n ein Teiler von $2^{2i} + 2^i + 1$ ist mit $r(n) = 3i$ (siehe z.B. $n = 73, 273, 1057, 1387, 2359, 3133, ...$). Wir wollen daher im nächsten Unterkapitel versuchen, die Heuristik zu verbessern.

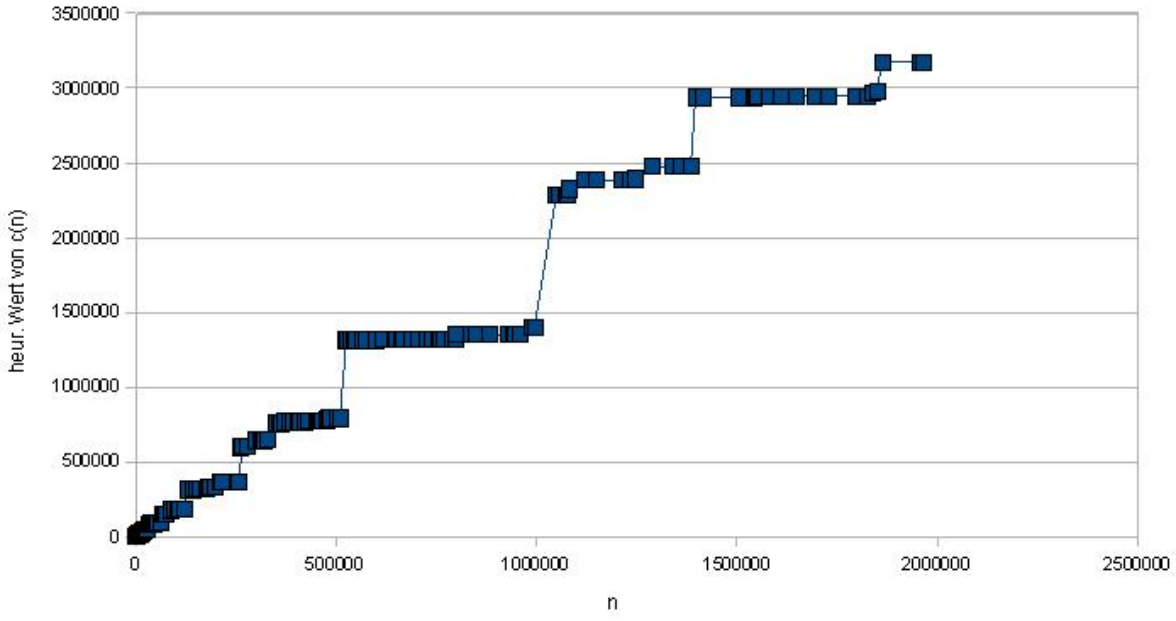

Abbildung 8: Heuristischer Verlauf von c

n	a(n)	aheur(n)	a(n)-aheur(n)	r(n)	(2^r(n)-1)/n
3	2	2.00	0.00	2	1
7	6	6.00	0.00	3	1
15	12	10.67	1.33	4	1
31	30	30.00	0.00	5	1
63	54	50.67	3.33	6	1
73	18	10.29	7.71	9	7
85	24	25.60	-1.60	8	3
127	126	126.00	0.00	7	1
255	216	204.80	11.20	8	1
273	24	13.76	10.24	12	15
341	90	96.97	-6.97	10	3
511	486	493.71	-7.71	9	1
585	72	68.35	3.65	12	7
819	108	123.80	-15.80	12	5
1023	900	888.48	11.52	10	1
1057	60	33.00	27.00	15	31
1353	0	1.47	-1.47	20	775
1365	396	370.24	25.76	12	3
1387	36	6.60	29.40	18	189
1971	0	12.39	-12.39	18	133
2047	2046	2041.98	4.02	11	1
2255	0	4.57	-4.57	20	465
2325	0	4.07	-4.07	20	451
2359	42	2.58	39.42	21	889
3133	48	0.00	48.00	24	5355
3813	0	11.73	-11.73	20	275
4095	3420	3370.89	49.11	12	1
4161	72	57.14	14.86	18	63
4369	240	289.13	-49.13	16	15
4681	540	659.95	-119.95	15	7
5461	1722	1750.33	-28.33	14	3
6223	0	17.41	-17.41	21	337
6765	60	36.54	23.46	20	155
8191	8190	8190.00	0.00	13	1
8435	0	3.96	-3.96	24	1989
8525	120	61.54	58.46	20	123
9399	48	4.62	43.38	24	1785
9709	270	316.78	-46.78	18	27
10845	0	5.93	-5.93	24	1547
11275	180	115.23	64.77	20	93
12483	486	522.91	-36.91	18	21
13107	2256	2313.04	-57.04	16	5
13797	594	594.55	-0.55	18	19
13981	180	175.96	4.04	20	75

Abbildung 9: Erste Heuristik: heuristische Werte von $a\,(n)$ für $n = 1, \ldots, 2'000'000$

15665	0	13.85	-13.85	24	1071
15709	0	58.58	-58.58	22	267
16383	14532	14498.79	33.21	14	1
16513	210	127.28	82.72	21	127
18631	0	10.30	-10.30	25	1801
18705	0	1.10	-1.10	28	14351
19065	240	292.89	-52.89	20	55
21845	6960	6939.11	20.89	16	3
21931	96	27.69	68.31	24	765
24295	0	2.10	-2.10	28	11049
25305	0	31.65	-31.65	24	663
25575	420	492.31	-72.31	20	41
28197	144	41.54	102.46	24	595
29127	2700	2742.54	-42.54	18	9
32767	32130	32035.38	94.62	15	1
33825	960	921.81	38.19	20	31
37449	4752	4737.02	14.98	18	7
41943	1380	1407.64	-27.64	20	25
42799	1134	868.27	265.73	21	49
43053	0	6.03	-6.03	28	6235
46995	72	110.77	-38.77	24	357
47127	726	469.63	256.37	22	89
49981	120	2.31	117.69	30	21483
51319	72	0.00	72.00	36	1339065
53261	72	167.37	-95.37	24	315
55245	0	9.58	-9.58	28	4859
55831	0	92.70	-92.70	25	601
60787	1914	878.71	1035.29	22	69
65535	55824	55512.85	311.15	16	1
65793	288	221.54	66.46	24	255
69905	4500	4398.42	101.58	20	15
71827	0	4.67	-4.67	30	14949
72885	0	16.82	-16.82	28	3683
75915	144	284.84	-140.84	24	221
76627	72	0.00	72.00	36	896805
87381	25110	25099.52	10.48	18	3
95325	7620	7376.92	243.08	20	11
104643	0	8.67	-8.67	30	10261
109655	216	664.62	-448.62	24	153
121369	156	0.00	156.00	39	4529623
131071	131070	131070.00	0.00	17	1
140911	168	73.80	94.20	28	1905
140985	1224	996.94	227.06	24	119
143395	1080	1147.20	-67.20	24	117
149943	120	18.58	101.42	30	7161

Abbildung 10: Erste Heuristik: heuristische Werte von $a\,(n)$ für $n = 1, \ldots, 2'000'000$

151183	72	0.00	72.00	36	454545
158369	168	87.05	80.95	28	1695
159783	936	1338.96	-402.96	24	105
178481	2484	3797.43	-1313.43	23	47
182361	6072	7044.98	-972.98	22	23
184365	2016	1719.12	296.88	24	91
197379	1584	1993.87	-409.87	24	85
209715	35040	35187.35	-147.35	20	5
215265	0	146.85	-146.85	28	1247
215481	0	37.53	-37.53	30	4983
256999	0	123.02	-123.02	29	2089
262143	227556	227376.83	179.17	18	1
262657	1026	514.00	512.00	27	511
266305	3960	4016.89	-56.89	24	63
279527	0	2.27	-2.27	35	122921
299593	41454	41892.54	-438.54	21	7
310323	0	1.24	-1.24	36	221445
316017	0	1.28	-1.28	36	217455
319865	0	1.38	-1.38	36	214839
328965	5832	5317.00	515.00	24	51
349525	111180	110673.92	506.08	20	3
349867	540	111.00	429.00	30	3069
358065	0	1.59	-1.59	36	191919
359233	0	1.74	-1.74	36	191295
364635	0	1.63	-1.63	36	188461
372827	7848	8037.71	-189.71	24	45
383135	0	2.04	-2.04	36	179361
391419	0	1.90	-1.90	36	175565
403845	0	2.01	-2.01	36	170163
411255	0	2.07	-2.07	36	167097
422733	840	590.37	249.63	28	635
430185	9720	9177.63	542.37	24	39
449829	360	167.42	192.58	30	2387
453549	144	2.60	141.40	36	151515
454545	0	2.46	-2.46	36	151183
461871	0	2.60	-2.60	36	148785
463419	0	173.12	-173.12	30	2317
475107	588	696.43	-108.43	28	565
479349	11808	12055.72	-247.72	24	35
486737	174	441.27	-267.27	29	1103
501291	0	3.13	-3.13	36	137085
510489	0	3.13	-3.13	36	134615
524287	524286	524286.00	0.00	19	1
526695	0	3.42	-3.42	36	130473
536389	0	4.08	-4.08	36	128115

Abbildung 11: Erste Heuristik: heuristische Werte von $a(n)$ für $n = 1, \ldots, 2'000'000$

544455	0	3.68	-3.68	36	126217
549791	270	279.03	-9.03	30	1953
565383	0	4.01	-4.01	36	121545
575757	0	4.14	-4.14	36	119355
599479	528	41.84	486.16	33	14329
617093	1596	1392.85	203.15	28	435
646443	270	338.27	-68.27	30	1661
652365	0	5.14	-5.14	36	105339
664335	108	5.30	102.70	36	103441
667147	0	6.39	-6.39	36	103005
689643	0	6.13	-6.13	36	99645
704555	1260	1771.96	-511.96	28	381
726921	0	6.77	-6.77	36	94535
737373	0	6.81	-6.81	36	93195
755915	0	7.93	-7.93	36	90909
762237	0	7.35	-7.35	36	90155
769785	0	7.27	-7.27	36	89271
790097	990	563.56	426.44	30	1359
791845	2184	2213.62	-29.62	28	339
796593	84	0.00	84.00	42	5521071
798915	33984	32135.14	1848.86	24	21
835485	0	8.46	-8.46	36	82251
849583	156	1.29	154.71	39	647089
850815	0	8.72	-8.72	36	80769
883227	288	10.08	277.92	36	77805
930969	0	11.12	-11.12	36	73815
942305	108	12.03	95.97	36	72927
948051	0	11.50	-11.50	36	72485
959595	0	11.06	-11.06	36	71613
986895	47664	47852.99	-188.99	24	17
996151	0	14.30	-14.30	36	68985
1048575	885660	885391.37	268.63	20	1
1049601	1200	892.00	308.00	30	1023
1058281	0	15.63	-15.63	36	64935
1074195	0	14.28	-14.28	36	63973
1077699	216	13.89	202.11	36	63765
1082401	34650	34916.02	-266.02	25	31
1118481	65880	64301.67	1578.33	24	15
1149405	0	16.34	-16.34	36	59787
1211535	0	18.05	-18.05	36	56721
1233765	0	18.70	-18.70	36	55699
1248537	4284	5152.35	-868.35	28	215
1290555	82800	82659.16	140.84	24	13
1339065	0	21.58	-21.58	36	51319
1360647	0	23.44	-23.44	36	50505

Abbildung 12: Erste Heuristik: heuristische Werte von $a(n)$ für $n = 1, \ldots, 2'000'000$

1385613	0	23.44	-23.44	36	49595
1398101	462528	463959.71	-1431.71	22	3
1415583	0	25.74	-25.74	36	48545
1503873	0	28.13	-28.13	36	45695
1542025	0	2.08	-2.08	40	713031
1545103	102	0.00	102.00	51	1457378449
1549411	1980	2219.97	-239.97	30	693
1551615	0	29.70	-29.70	36	44289
1580085	0	30.75	-30.75	36	43491
1609167	0	32.68	-32.68	36	42705
1649373	1440	2233.06	-793.06	30	651
1696149	0	36.06	-36.06	36	40515
1727271	0	37.28	-37.28	36	39785
1796165	0	43.60	-43.60	36	38259
1826203	168	0.00	168.00	42	2408301
1838599	23814	24672.19	-858.19	27	73
1851279	10836	11142.82	-306.82	28	145
1864135	190944	192905.00	-1961.00	24	9
1957095	216	46.31	169.69	36	35113
1965379	0	55.63	-55.63	36	34965

Abbildung 13: Erste Heuristik: heuristische Werte von $a\,(n)$ für $n = 1, \ldots, 2'000'000$

4.2 Zweite Heuristik

Wir möchten nun die Eingangs erarbeitete Heuristik verbessern. Dazu betrachten wir die symmetrische Gruppe $S_3 : x \mapsto x, x \mapsto 1-x, x \mapsto \frac{1}{x}, x \mapsto 1-\frac{1}{x}, x \mapsto \frac{x}{x-1}, x \mapsto \frac{1}{1-x}$ und definieren

$$G = S_3 \times \mathbb{Z}/r(n)\mathbb{Z}.$$

Proposition 4.3
Es gilt

1. *Die Gruppe G operiert auf A_n.*
2. *Für jedes $x \in A_n$ ist $Stab_G(x)$ isomorph zu einer Untergruppe von S_3.*

Beweis

1. S_3 operiert auf $\overline{\mathbb{F}}_2 \setminus \{0,1\}$ und lässt $\operatorname{ord}(x, 1-x)$ fest. Es ist also $\operatorname{ord}(x,1-x) = \operatorname{ord}(\sigma x, \sigma(1-x))$ für jedes $\sigma \in S_3$:

   - Für $\sigma = \mathrm{id}$ und $\sigma = (x \mapsto 1-x)$ ist die Aussage klar.
   - Sei $\sigma = \left(x \mapsto \frac{1}{x}\right)$. Dann ist $\operatorname{ord}\left(\frac{1}{x}, \frac{1}{1-x}\right) = \operatorname{kgV}\left(\operatorname{ord}\left(\frac{1}{x}\right), \operatorname{ord}\left(\frac{1}{1-x}\right)\right) = \operatorname{kgV}(\operatorname{ord}(x), \operatorname{ord}(1-x)) = \operatorname{ord}(x, 1-x)$.
   - Für $\sigma = \left(x \mapsto 1-\frac{1}{x}\right)$ gilt $\operatorname{ord}\left(1-\frac{1}{x}, 1-\frac{1}{1-x}\right) = \operatorname{ord}\left(\frac{x-1}{x}, \frac{x}{x-1}\right) = \operatorname{ord}\left(\frac{x-1}{x}\right) = \operatorname{kgV}(\operatorname{ord}(x), \operatorname{ord}(1-x)) = \operatorname{ord}(x, 1-x)$.
   - Für $\sigma = \left(x \mapsto \frac{x}{x-1}\right)$ ist $\operatorname{ord}\left(\frac{x}{x-1}, \frac{1-x}{1-x-1}\right) = \operatorname{ord}\left(\frac{x}{1-x}\right) = \operatorname{kgV}(\operatorname{ord}(x), \operatorname{ord}(1-x)) = \operatorname{ord}(x, 1-x)$.
   - Für $\sigma = \left(x \mapsto \frac{1}{1-x}\right)$ gilt $\operatorname{ord}\left(\frac{1}{1-x}, 1-\frac{1}{1-(1-x)}\right) = \operatorname{kgV}\left(\operatorname{ord}\left(\frac{1}{1-x}\right), \operatorname{ord}\left(\frac{1}{x}\right)\right) = \operatorname{ord}(x, 1-x)$.

   S_3 operiert also auf $\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \operatorname{ord}(x,1-x) = n\right\} = A_n$.

   Ebenfalls wirkt $\mathbb{Z}/r(n)\mathbb{Z}$ auf A_n mittels

   $$(x, a + r(n)\mathbb{Z}) \mapsto x^{2^a}.$$

   Sind nämlich $g = a + r(n)\mathbb{Z}$ und $h = b + r(n)\mathbb{Z}$, so ist $g(h,x) = g\left(x^{2^b}\right) = \left(x^{2^b}\right)^{2^a} = gh(x)$ und $(0,x) \mapsto x^{2^0} = x$ für jedes $x \in A_n$. Des Weiteren ist $\operatorname{ord}\left(x^{2^a}\right) = \operatorname{ord}(x)$ für alle $a \in \mathbb{Z}/r(n)\mathbb{Z}$ und $x \in A_n$. Wäre nämlich $\operatorname{ord}\left(x^{2^a}\right) = q < \operatorname{ord}(x)$, hätte dies $\left(x^{2^a}\right)^q = 1$ zur Folge. Damit wäre also $\left(x^q - 1\right)^{2^a} = 0$ und somit $x^q = 1$, was ein Widerspruch zu $\operatorname{ord}(x) > q$ ist. Daraus folgt, dass für jedes $g + r(n)\mathbb{Z}$ das Bild gx von $x \in A_n$ wieder in A_n liegt. G operiert nun auf A_n, denn die Operationen von S_3 bzw. $\mathbb{Z}/r(n)\mathbb{Z}$ auf A_n kommutieren.

2. Seien $x \in A_n$ und $g = (\sigma, a + r(n)\mathbb{Z}) \in \operatorname{Stab}_G(x) \cap (\{\mathrm{id}\} \times \mathbb{Z}/r(n)\mathbb{Z})$. $\Rightarrow g = (\mathrm{id}, a + r(n)\mathbb{Z})$ mit $x^{2^a} = x$. Da aber $\operatorname{ord}(x, 1-x) = n$ ist, folgt $\mathbb{F}_2(x) = \mathbb{F}_{2^{r(n)}}$. Somit ist $x^{2^{r(n)}} = x$ und insbesondere $x^{2^a} \neq x$ für alle $0 < a < r(n)$. Damit ist also

$g = (\mathrm{id}, 0)$. Betrachtet man nun die Projektion $\mathrm{pr}_1 : S_3 \times \mathbb{Z}/r(n)\mathbb{Z} \to S_3$, so ist dessen Einschränkung auf $\mathrm{Stab}_G(x)$

$$\mathrm{pr}_1 |_{\mathrm{Stab}_G(x)} \colon \mathrm{Stab}_G(x) \hookrightarrow S_3$$

injektiv, denn $\ker\left(\mathrm{pr}_1 |_{\mathrm{Stab}_G(x)}\right) = \mathrm{Stab}_G(x) \cap (\{\mathrm{id}\} \times \mathbb{Z}/r(n)\mathbb{Z}) = \{(\mathrm{id}, 0)\}$.

□

Für die Heuristik gehen wir a-priori von Bahnen der Länge

a) $r(n)$,
b) $2r(n)$,
c) $3r(n)$ und
d) $6r(n)$

aus und leiten für jeden dieser Fälle einen heuristischen Wert für die Anzahl Punkte von $\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \mathrm{ord}(x, 1-x) = n\right\}$ her, die in einer Bahn der gegebenen Länge liegen. Der heuristische Wert von $a(n) = \#\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \mathrm{ord}(x, 1-x) = n\right\}$ ergibt sich dann aus der Summation dieser einzelnen heuristischen Werte.

4.2.1 a) x liegt in einer Bahn der Länge $r(n)$

Proposition 4.4
Sei n eine ungerade natürliche Zahl und sei $x \in A_n$. Äquivalent sind

1. $|Gx| = r(n)$.
2. $n = 3$.

Beweis

1. 1. $\Rightarrow$ 2.
   Sei also x in einer Bahn der Länge $r(n)$. Dann hat $\mathrm{Stab}_G(x)$ die Ordnung 6. Daraus folgt, dass $\mathrm{Stab}_G(x)$ isomorph zu S_3 ist. Nun ist $\mathrm{Stab}_G(x) \supset [\mathrm{Stab}_G(x), \mathrm{Stab}_G(x)] = A_3 \times \{0\}$. Insbesondere liegt also das Element $\left(x \mapsto 1 - \frac{1}{x}, 0\right)$ in $\mathrm{Stab}_G(x)$. Das heisst also $x = 1 - \frac{1}{x}$ respektive $x^2 + x + 1 = 0$. Beidseitiges Multiplizieren mit $x - 1$ ergibt $x^3 - 1 = 0$. Daraus folgt, dass $x \in \mathbb{F}_4$ und dass $n = 3$ ist.

2. 2. $\Rightarrow$ 1.
   Sei $n = 3$. Dann ist $r(n) = 2$ und somit $G = S_3 \times \mathbb{Z}/2\mathbb{Z}$. Sei $x \in \overline{\mathbb{F}}_2 \setminus \{0,1\}$ mit $x^3 = 1 = (1-x)^3$. Dann liegen folgende Elemente in $\mathrm{Stab}_G(x)$: $(x \mapsto x, 0)$, $\left(x \mapsto 1 - \frac{1}{x}, 0\right)$, $\left(x \mapsto \frac{1}{1-x}, 0\right)$, $\left(x \mapsto \frac{1}{x}, 1\right)$, $(x \mapsto 1 - x, 1)$, $\left(x \mapsto \frac{x}{x-1}, 1\right)$. Damit ist $|\mathrm{Stab}_G(x)| = 6$ und damit $|Gx| = 2$.

   □

4.2.2 b) x liegt in einer Bahn der Länge $2r(n)$

Sei nun x in einer Bahn der Länge $2r(n)$. $\mathrm{Stab}_G(x)$ hat also Ordnung 3 und ist somit als einzige Untergruppe von S_3 der Ordnung 3 isomorph zu A_3. Nun gilt folgende Proposition:

Proposition 4.5
Sei n eine ungerade natürliche Zahl. Und liege $x \in A_n$ in einer Bahn der Länge $2r(n)$. Dann gilt

1. $3 \mid r(n)$.
2. $1 - \frac{1}{x} = x^{2^i}$ *oder* $\frac{1}{1-x} = x^{2^i}$ *mit* $i = \frac{r(n)}{3}$.
3. $x^{2^{2i}+2^i+1} = 1 = (1-x)^{2^{2i}+2^i+1}$ *mit* $i = \frac{r(n)}{3}$.
4. $n \mid (2^{2i} + 2^i + 1)$ *mit* $i = \frac{r(n)}{3}$.

Beweis

1. Sei nun $\mathrm{Stab}_G(x)$ der Graph eines Homomorphismus $\varphi : A_3 \mapsto \mathbb{Z}/r(n)\mathbb{Z}$. Wäre φ trivial, hätte dies zur Folgerung, dass $\mathrm{Stab}_G(x) = \{(\mathrm{id}, 0), (x \mapsto 1 - \frac{1}{x}, 0), (x \mapsto \frac{1}{1-x}, 0)\}$. Dies zieht aber $x^3 = 1$ nach sich, und somit liegt x in einer Bahn der Länge $r(n)$. Wir können also annehmen, dass φ nicht trivial ist. Als nächstes zeigen wir, dass $r(n)$ durch 3 teilbar ist. Sei $\sigma_1 = \mathrm{id}, \sigma_2 = (x \mapsto 1 - \frac{1}{x})$ und $\sigma_3 = (x \mapsto \frac{1}{1-x})$. Wir möchten zeigen, dass φ injektiv ist. Nehmen wir an, $\varphi(\sigma_2) = 0$. Dann wäre $\varphi(\sigma_3) = \varphi(\sigma_2^2) = \varphi(\sigma_2)^2 = 0$ und somit φ trivial. Unter Annahme, dass $\varphi(\sigma_3) = 0$ ist, folgt $\varphi(\sigma_2) = \varphi(\sigma_3^2) = \varphi(\sigma_3)^2 = 0$. Wiederum wäre dann φ trivial. Somit ist φ injektiv und $|\mathrm{im}(\varphi)| = 3$. Weil $\mathrm{im}(\varphi)$ eine Untergruppe von $\mathbb{Z}/r(n)\mathbb{Z}$ ist, folgt $3 \mid r(n)$.

2. Schreiben wir $r(n) = 3i$, so liegen folgende Elemente in $\mathrm{Stab}_G(x)$: $(x \mapsto 1 - \frac{1}{x}, 0 + r(n)\mathbb{Z})$, $(x \mapsto 1 - \frac{1}{x}, i + r(n)\mathbb{Z})$ und $(x \mapsto 1 - \frac{1}{x}, 2i + r(n)\mathbb{Z})$. Für das erste Element erhalten wir die Gleichung $x^3 = 1$. Für das zweite Element die Gleichung $1 - \frac{1}{x} = x^{2^i}$ und für das letzte Element die Gleichung $1 - \frac{1}{x} = x^{2^{2i}}$. Aus $1 - \frac{1}{x} = x^{2^{2i}}$ folgt $x = \frac{1}{1-x^{2^{2i}}} = \left(\frac{1}{1-x}\right)^{2^{2i}}$. Potenzieren wir beide Seiten mit 2^i, ergibt sich die Gleichung $x^{2^i} = \left(\frac{1}{1-x}\right)^{2^{2i}2^i} = \left(\frac{1}{1-x}\right)^{2^{3i}} = \frac{1}{1-x}$.

3. Es ist $x^{2^{2i}+2^i+1} = x^{2^{2i}}x^{2^i}x = \frac{1}{1-x}\left(1 - \frac{1}{x}\right)x = 1$. Und $(1-x)^{2^{2i}+2^i+1} = \left(1 - x^{2^{2i}}\right)\left(1 - x^{2^i}\right)(1-x) = \left(1 - \frac{1}{1-x}\right)\left(1 - \left(1 - \frac{1}{x}\right)\right)(1-x) = 1$.

4. n ist die kleinste natürliche Zahl mit $\mathrm{ord}(x) \mid n$ und $\mathrm{ord}(1-x) \mid n$. Wegen $x^{2^{2i}+2^i+1} = 1 = (1-x)^{2^{2i}+2^i+1}$ folgt nun $n \mid (2^{2i} + 2^i + 1)$.

□

Proposition 4.6
Sei $3 \neq n$ eine ungerade natürliche Zahl und sei $x \in A_n$. Nehme an, es existiere ein $i \in \mathbb{N}$, so dass $n \mid 2^{2i} + 2^i + 1$. Sei i minimal mit dieser Eigenschaft. Dann gilt

1. $x^{2^i} = 1 - \frac{1}{x}$ *oder* $x^{2^i} = \frac{1}{1-x}$.
2. $|Gx| = 2r(n)$.
3. $\mathrm{ord}(x) = \mathrm{ord}(1-x)$.

4. $r(n) = 3i$.

Beweis

1. Sei i eine natürliche Zahl, so dass n ein Teiler von $2^{2i} + 2^i + 1$ ist und sei i minimal gewählt. Sei $x \in A_n$. Es gilt $1 = (1-x)^{2^{2i}+2^i+1} = \left(1 + x^{2^{2i}}\right)\left(1 + x^{2^i}\right)(1+x)$. Multiplizieren wir diese Gleichung mit x^{2^i+1} und bemerken, dass $x^{2^i+1}\left(1 + x^{2^{2i}}\right) = x^{2^i+1} + 1$, bekommen wir
$$x^{2^i}x = \left(x^{2^i}x + 1\right)\left(1 + x^{2^i}\right)(1+x),$$
was äquivalent ist zu
$$\left(x^{2^i}x + x + 1\right)\left(x^{2^i}x + x^{2^i} + 1\right) = 0.$$
Daraus folgt nun, dass $x^{2^i} = \frac{x+1}{x}$ oder $x^{2^i} = \frac{1}{1+x}$.

2. $\mathrm{Stab}_G(x)$ hat Ordnung 3, denn es liegen folgende Elemente in $\mathrm{Stab}_G(x)$: $\left(x \mapsto \frac{1}{1-x}, i\right)$, $\left(x \mapsto 1 - \frac{1}{x}, i\right)$ und $(x \mapsto x, 0)$. Da $n \neq 3$ ist, besitzt $\mathrm{Stab}_G(x)$ keine weiteren Elemente.

3. Es ist $\mathrm{ord}(1-x) = \mathrm{ord}\left(\frac{1}{1-x}\right) = \mathrm{ord}\left(x^{2^i}\right) = \mathrm{ord}(x)$.

4. Es gilt $(2^{3i}-1) = (2^{2i} + 2^i + 1)(2^i - 1)$. Daraus folgt, dass $2^{3i} \equiv 1 \mod n$ ist. Da $|Gx| = 2r(n)$ ist, folgt wegen obiger Proposition, dass $r(n)$ durch 3 teilbar ist. Sei also $r(n) = 3j$ und nehmen wir an, dass $j < i$ sei. Dann ist $2^{3j} - 1 \equiv 0 \mod n$, was äquivalent zu $(2^j - 1)(2^{2j} + 2^j + 1) \equiv 0 \mod n$ ist. Daraus folgt nun, dass $(2^{2j} + 2^j + 1) \equiv 0 \mod n$ ist, weil $(2^j - 1) \not\equiv 0 \mod n$. $(2^{2j} + 2^j + 1) \equiv 0 \mod n$ zieht aber einen Widerspruch zur Minimalität von i nach sich.

□

Korollar 4.7
Sei $3 \neq n$ eine ungerade natürliche Zahl und sei $x \in A_n$. Äquivalent sind

1. $|Gx| = 2r(n)$.

2. $\exists i \in \mathbb{N} : n \mid 2^{2i} + 2^i + 1$.

Wir betrachten nun die Menge
$$K_i = \left\{ x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \mathbb{F}_2(x) = \mathbb{F}_{2^{3i}} \text{ und } x^{2^i} \in \left\{ 1 + \frac{1}{x}, \frac{1}{1+x} \right\} \right\},$$
sowie deren Kardinalität $K(i) = \#K_i$.

Proposition 4.8
Sei $i \in \mathbb{N}$. Dann gilt
$$K(i) = \sum_{\substack{d \mid i \\ 3d \nmid i}} \mu\left(\frac{i}{d}\right)\left(2^d + 2 + 2(-1)^{d+1}\right).$$

Beweis

1. Es ist $\#\left\{x \in \overline{\mathbb{F}}_2 \mid x^{2^i} = 1 + \frac{1}{x}\right\} = 2^i + 1$ und $\#\left\{x \in \overline{\mathbb{F}}_2 \mid x^{2^i} = \frac{1}{1+x}\right\} = 2^i + 1$. Die Anzahl gemeinsamer Nullstellen der zwei Gleichungen $x^{2^i} = 1 + \frac{1}{x}$ und $x^{2^i} = \frac{1}{1+x}$ ist 0, falls i ungerade, oder 2, falls i gerade ist. Denn es gilt $\mathrm{ggT}\left(x^{2^i}x + x + 1, x^{2^i}x + x^{2^i} + 1\right) = \mathrm{ggT}\left(x\left(x^{2^i} - 1\right) + x^2 + x + 1, x^{2^i} - x\right) = \mathrm{ggT}\left(x^2 + x + 1, x^{2^i} - x\right) = \frac{1}{x-1}\mathrm{ggT}\left(x^3 - 1, x^{2^i-1} - 1\right)$. Nun entsprechen die Nullstellen von $X^3 - 1$ der Menge $\mathbb{F}_4^\times$ und die Nullstellen von $X^{2^i-1} - 1$ entsprechen der Menge $\mathbb{F}_{2^i}^\times$. Falls nun i gerade ist, ist $\mathbb{F}_4^\times \subset \mathbb{F}_{2^i}^\times$ und die Nullstellen von $\mathrm{ggT}\left(X^3 - 1, X^{2^i-1} - 1\right)$ sind $\mathbb{F}_4^\times \setminus \{1\}$. In diesem Fall gibt es also 2 gemeinsame Nullstellen. Sei nun i ungerade. Dann ist $\mathbb{F}_4^\times \cap \mathbb{F}_{2^i}^\times = \{1\}$. In diesem Fall ist $\mathrm{ggT}\left(X^3 - 1, X^{2^i-1} - 1\right) = 1$ und wir haben keine gemeinsamen Nullstellen. Dies ergibt nun

$$\left\{x \in \overline{\mathbb{F}}_2 \setminus \mathbb{F}_4 \mid x^{2^i} = 1 + \frac{1}{x} \,\mathrm{oder}\, x^{2^i} = \frac{1}{1+x}\right\} = 2 + 2^i + 2\left(-1\right)^{i+1}.$$

2. Jedes $x \in \overline{\mathbb{F}}_2 \setminus \mathbb{F}_4$ mit $x^{2^i} = 1 + \frac{1}{x}$ oder $x^{2^i} = \frac{1}{1+x}$ erzeugt den Körper $\mathbb{F}_{2^{3d}}$ über $\mathbb{F}_2$, falls $d \mid i$ und $3d \nmid i$. Somit ist

$$\sum_{\substack{d \mid i \\ 3d \nmid i}} K\left(d\right) = 2 + 2^i + 2\left(-1\right)^{i+1}.$$

3. Daraus lässt sich dann $K\left(i\right)$ berechnen:

$$K\left(i\right) = \sum_{\substack{d \mid i \\ 3d \nmid i}} \mu\left(\frac{i}{d}\right) 2\left(2^d + \left(-1\right)^{d+1}\right).$$

□

Der letzte Teil des Beweises ist eine Konsequenz aus dem folgenden Lemma:

Lemma 4.9
Seien $F : \mathbb{N} \to \mathbb{R}^+$ und $K : \mathbb{N} \to \mathbb{R}^+$ zwei arithmetische Funktionen mit der Eingenschaft, dass für jedes $n \in \mathbb{N}$

$$F\left(n\right) = \sum_{\substack{d \mid n \\ 3d \nmid n}} K\left(d\right)$$

gilt. Dann ist für jedes $n \in \mathbb{N}$

$$K\left(n\right) = \sum_{\substack{d \mid n \\ 3d \nmid n}} \mu\left(\frac{n}{d}\right) F\left(d\right).$$

Beweis

Sei $n \in \mathbb{N}$. Dann ist

$$\sum_{\substack{d|n \\ 3d\nmid n}} \mu\left(\frac{n}{d}\right) F(d) = \sum_{\substack{d|n \\ 3d\nmid n}} \mu\left(\frac{n}{d}\right) \sum_{\substack{c|d \\ 3c\nmid d}} K(c) = \sum_{\substack{c|n \\ 3c\nmid n}} K(c) \sum_{\substack{d:c|d|n \\ 3d\nmid n}} \mu\left(\frac{n}{d}\right).$$

Aus $c \mid d \mid n$ und $3c \nmid n$ folgt $3d \nmid n$. Somit fällt die Bedingung $3d \nmid n$ weg. Des Weiteren ist

$$\sum_{d:c|d|n} \mu\left(\frac{n}{d}\right) = \sum_{d'|\frac{n}{c}} \mu(d').$$

Diese Summe ist Null, falls $\frac{n}{c} > 1$ und 1, falls $\frac{n}{c} = 1$. Somit ist

$$\sum_{\substack{c|n \\ 3c\nmid n}} K(c) \sum_{d'|\frac{n}{c}} \mu(d') = K(n).$$

□

Nun betrachten wir

$$B(i) = \#\left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid x^{2^{2i}+2^i+1} = 1 \text{ und } \mathbb{F}_2(x) = \mathbb{F}_{2^{3i}}\right\}.$$

Es gilt

$$\sum_{\substack{j|i \\ 3j\nmid i}} B(j) = 2^{2i} + 2^i + (-1)^{i+1},$$

und somit

$$B(i) = \sum_{\substack{j|i \\ 3j\nmid i}} \mu(j) \left(2^{\frac{2i}{j}} + 2^{\frac{i}{j}} + (-1)^{\frac{i}{j}+1}\right).$$

Die Wahrscheinlichkeit, dass ein $x \in \overline{\mathbb{F}}_2 \setminus \{0,1\}$ mit $x^{2^{2i}+2^i+1} = 1 \text{ und } \mathbb{F}_2(x) = \mathbb{F}_{2^{3i}}$ die Ordnung n hat beträgt $\frac{\varphi(n)}{B(i)}$. Multiplizieren wir diese Wahrscheinlichkeit mit der Anzahl Kandidaten, so bekommen wir den heuristischen Wert

$$a^{\mathrm{b}}_{\mathrm{heur}}(n) = \frac{\varphi(n)}{B(i)} K(i).$$

4.2.3 c) x liegt in einer Bahn der Länge $3r(n)$

Nun untersuchen wir den Fall, wo $x \in A_n$ in einer Bahn der Länge $3r(n)$ liegt. Die Stabilisatorenuntergruppe $\mathrm{Stab}_G(x)$ hat die Ordnung 2 und ist isomorph zu $S_2 \subset S_3$. Die Bahn von x besteht aus $3\,\mathbb{Z}/r(n)\,\mathbb{Z}$-Bahnen und für genau eine von denen ist $\mathrm{Stab}_G(x) = \left(x \mapsto \frac{1}{x^{2^i}}\right)$ für ein $0 \leq i < r(n)$. Daraus folgt, dass $x = x^{-2^i} = x^{2^{2i}} = x$ und somit $r(n) \mid 2i$. Entweder ist nun $r = 2i$ oder $i = 0$. Der zweite Fall impliziert aber $x = \frac{1}{x}$, was $x = 1$ nach sich zieht und somit zu einem Widerspruch führt. $r(n)$ ist somit gleich $2i$. Wir erhalten somit die folgende Aussage:

Proposition 4.10
Sei n eine ungerade natürliche Zahl und sei $x \in A_n$ mit $|Gx| = 3r(n)$. Dann ist $r(n)$ durch 2 teilbar.

Das folgende Lemma benutzen wir, um die nächste Proposition zu beweisen.

Lemma 4.11
Sei H eine endliche Gruppe. Seien $a, b \in H$ mit

- $ab \neq 1$ *und*
- $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$.

Dann ist $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.

Beweis

Seien $a, b \in H$ mit $ab \neq 1$ und $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$. Seien $\mathrm{ord}(a) = n$ und $\mathrm{ord}(b) = m$. Wir wollen zeigen, dass $\mathrm{ord}(ab) = nm$ ist. Nehmen wir an, es gäbe eine natürliche Zahl $k < nm$ mit $(ab)^k = 1$. Dann ist $a^k = (b^{-1})^k$. Da aber nach Voraussetzung $a \neq b^{-1}$ ist, folgt, dass $a^k \neq (b^{-1})^k$ für alle k mit $k < \mathrm{ord}(a)$ und $k < \mathrm{ord}(b)$. Somit muss also $a^k = 1$ und $(b^{-1})^k = 1$ sein. k ist also ein Vielfaches von $\mathrm{ord}(a)$ und von $\mathrm{ord}(b)$. Damit ist $k \geq \mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b)) = \frac{nm}{\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b))} = nm$. □

Nun betrachten wir die Menge

$$\widetilde{K}_i = \left\{ x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \mathbb{F}_2(x) = \mathbb{F}_{2^{2i}} \text{ und } x^{2^i+1} = 1 \right\}.$$

Proposition 4.12
Sei n eine ungerade natürliche Zahl mit $r(n) = 2i$ und sei $x \in \widetilde{K}_i$. Dann ist $\mathrm{ord}(1-x) = \mathrm{ord}(x, 1-x)$.

Beweis

Wir wollen zeigen, dass $\mathrm{ord}\left(x\left(x + x^{2^i}\right)\right) = \mathrm{ord}(x)\,\mathrm{ord}\left(x + x^{2^i}\right)$ ist.

- Nehmen wir an, es sei $x + x^{2^i} = x^{-1}$. Da $x^{2^i} = x^{-1}$ ist, wäre dann $x = 0$.
- Es ist $x + x^{2^i} \in \mathbb{F}_{2^i}^{\times}$, denn $\left(x + x^{2^i}\right)^{2^i} = x^{2^i} + \left(x^{2^i}\right)^{2^i} = x^{2^i} + x^{2^{2i}} = x^{2^i} + x$. Somit ist $\left(x + x^{2^i}\right)^{2^i - 1} = 1$, und damit ist $\mathrm{ord}\left(x + x^{2^i}\right)$ ein Teiler von $2^i - 1$. Nun ist aber $\mathrm{ord}(x)$ ein Teiler von $2^i + 1$. Des Weiteren ist $\mathrm{ggT}(2^i + 1, 2^i - 1) = \mathrm{ggT}(2^i + 1, 2^i - 1 - (2^i + 1)) = \mathrm{ggT}(2^i + 1 - 2) = 1$. Nehmen wir nun an, es sei $\mathrm{ggT}\left(\mathrm{ord}(x),\ \mathrm{ord}\left(x + x^{2^i}\right)\right) = h > 1$. Dann gilt aber $h \mid 2^i + 1$ und $h \mid 2^i - 1$ mit $h > 1$, was aber ein Widerspruch zu $\mathrm{ggT}(2^i + 1, 2^i - 1) = 1$ ist. Damit haben wir gezeigt, dass $\mathrm{ggT}\left(\mathrm{ord}(x), \mathrm{ord}\left(x + x^{2^i}\right)\right) = 1$.
- Somit bekommen wir die folgende Rechnung: $\mathrm{ord}(1-x) = \mathrm{ord}\left((1-x)^2\right) = \mathrm{ord}\left(x\left(x + x^{-1}\right)\right) = \mathrm{ord}\left(x\left(x + x^{2^i}\right)\right) = \mathrm{ord}(x)\,\mathrm{ord}\left(x + x^{2^i}\right)$. Damit ist also

$\operatorname{ord}(x) \mid \operatorname{ord}(1-x)$ und wir erhalten $\operatorname{ord}((x,1-x)) = \operatorname{kgV}(\operatorname{ord}(x), \operatorname{ord}(1-x)) = \operatorname{ord}(1-x)$. Wir erhalten somit:

$$\operatorname{ord}((x,1-x)) = n = \operatorname{ord}(x) \operatorname{ord}\left(x + x^{2^i}\right).$$

□

Sei nun $\operatorname{ord}(x) = n'$ und $\operatorname{ord}\left(x + x^{2^i}\right) = n''$. Damit ist $(n', n'') = 1$ und wir erhalten für die heuristische Anzahl von Punkten in einer Bahn der Länge $3r(n)$:

$$a^c_{\text{heur}}(n) = 3\varphi(n') \frac{\varphi(n'')}{\#\{x \in \mathbb{F}_{2^i} \mid \mathbb{F}_2(x) = \mathbb{F}_{2^i}\}} = \frac{3\varphi(n)}{\#\{x \in \mathbb{F}_{2^i} \mid \mathbb{F}_2(x) = \mathbb{F}_{2^i}\}}.$$

4.2.4 d) x liegt in einer Bahn der Länge $6r(n)$

Gehen wir noch auf den letzten Fall ein, wo x in einer Bahn der Länge $6r(n)$ liegt. In diesem Fall können wir folgende Aussage machen:

Proposition 4.13
Sei n eine ungerade natürliche Zahl und sei $x \in A_n$. Dann sind äquvalent:

1. $|Gx| = 6r(n)$
2. *G operiert frei auf A_n.*

Wir betrachten die Mengen

$$A = \left\{x \in \overline{\mathbb{F}}_2 \setminus \{0,1\} \mid \mathbb{F}_2(x) = \mathbb{F}_{2^{r(n)}} \text{ und } \operatorname{Stab}_G(x) = 1\right\}$$

und

$$B = \{x \in A \mid x^n = 1\}.$$

Der heuristische Wert für die Summe der $a(n')$ für alle Teiler n' von n, für die $r(n') = r(n)$ gilt, ist nun $\frac{|B|^2}{|A|}$:

$$\sum_{\substack{n' \mid n \\ r(n') = r(n)}} a^{\text{d}}_{\text{heur}}(n') = \frac{|\,B\,|^2}{|\,A\,|}$$

Und daraus berechnet man zuletzt den heuristischen Wert für $a^{\text{d}}_{\text{heur}}(n)$.

Kriterium

```
/*Eingabe: Gerade obere Grenze N=ogr>1. => M={1<n<=ogr| n ungerade}.
  Ausgabe: Menge M_1={n\in M| n ist Kandidat} in Form des Vektors
           kand_n=[n_1,...,n_q].
           Vektor r_n, für den gilt r[k]=r(n_k)*/

krit(ogr)={
kand=vector(ogr/2);
/*Falls 2*k-1 Kandidat, dann kand[k]=0. Sonst: kand[k]=1*/

r=vector(ogr/2);
/*Falls 2*k-1 Kandidat, dann r[k]=r(2*k-1).*/


for(k=1,ogr/2, n=2*k-1;     /*1<=n<=ogr*/
    a=-1;
    gr=sqrt(2*n+1/4)-1/2;
    v=vector(truncate(gr)+1);
    /*v[i+1]=(1+2^i)%n*/
    v[1]=2%n;
    ex=1;
    potmodn=2%n;
    /*potmodn=(2^ex)%n*/


/*Berechnung von r(n), falls dieses nicht grösser wird als gr*/

    while((ex<=gr)&&(potmodn!=1),
        v[ex+1]=(potmodn+1)%n;
        potmodn=(2*potmodn)%n;
        ex=ex+1);
    if(ex>gr,
        a=0;kand[k]=1,
        r[k]=ex);            /*r[k]=r(n)*/


/*Kontrolle, ob es x,y gibt mit (1+2^x)^r kongruent zu (1+2^y)^r mod n.
Wenn ja, wird kontrolliert ob es ein z gibt mit (1+2^y) kongruent zu
2^z(1+2^x) mod n*/

    if(a!=0,
        xvec=vector(truncate(ex/2)+1);
        /*xvec[m+1]=(1+2^m)^r mod n*/
        for(m=0,truncate(ex/2),xvec[m+1]=lift((Mod(v[m+1],n))^ex);

        key=vecsort(xvec,,1);
        /*Permutation, die xvec sortiert*/

        for(j=1,truncate(ex/2)+1,
            for(i=1,j,
                if(xvec[key[i]]==xvec[key[j]],
                    x=key[i]-1;
                    y=key[j]-1;
                    z=1;
                    w=(2*v[x+1])%n;          /*w=2^z*(1+2^x)*/
                    while((v[y+1]!=w)&&(z<ex),
```

```
                        z=z+1;
                        w=(2*w)%n);
                        if((z<ex)&&((x!=ex/2)||(y!=ex/2)||(z!=ex/2)),
                            a=0;
                            kand[k]=1;
                            z=ex;
                            j=truncate(ex/2)+2;i=j+1)))))));


/*Ausgabe*/

q=0;   /*q=Anzahl Kandidaten*/
print("kand_n=");print1("{");
for(k=1,ogr/2,
    if(kand[k]==0,q=q+1;
                  print1(2*k-1);print1(",")));print("}");
print(Anzahl_Kandidaten);
print(q);

print("r_n=");print1("[");
for(k=1,ogr/2,
    if(kand[k]==0,print1(r[k]);print1(",")));print("]");

}
```

Berecnung von b(n)

```
//Eingabe: Menge M_1 in Form des Vektors kand_n=[n_1,...,n_q] und dessen
           //Anzahl Komponenten q//
//Ausgabe: Vektor b=[b_1,...,b_q] mit b[b_k]=b(n_k) für 1<=k<=q//

#include <NTL/GF2X.h>
#include <NTL/vec_GF2.h>
#include <iostream.h>
#include <fstream.h>

//Berechnet die Koeffizienten von (1-X)^n//

vec_GF2 koeff(long n)
{
  vec_GF2 w;
  w.SetLength(n+1);
  w[0]=1;
  long k=1;         //k=2^i//
  long d=0;      //d=deg(w)//
  long m=n;         //m=Ganzteil von n/2^i//
                    //w=(1+X)^(n-(2^i)*m)//
  while(m>0)
  {
    if((m%2)!=0)
      {
        for(long j=0;j<d+1;j++)
          {
            w[j+k]=w[j];
          }
        d=d+k;
```

```
        k=2*k;
        m=(m-1)/2;
      }
   else
      {
        m=m/2;
        k=2*k;
      }
  }
return w;
}

//Berechnet die Koeffizienten von (1-X)^n-1 falls n=2^j-m//

vec_GF2 degmin_first(long m)
{
  vec_GF2 w;
  w=koeff(m);     //w=(1-X)^m//
  w[0]=w[0]-1;    //w=(1-X)^m-1//
  w[m]=w[m]-1;    //w=(1-X)^m-X^m-1//
  return w;
}

//Berechnet die Koeffizienten von (1-X)^n-1 falls n=2^j+m//

vec_GF2 degmin_sec(long m)
{
  vec_GF2 v,w;
  w=koeff(m);           //w=(1-X)^m//
  v.SetLength(2*m+1);
  for(int k=m;k<2*m+1;k++)
    v[k]=w[k-m];        //v=X^m*(1-X)^m//
  for(k=0;k<m+1;k++)
    v[k]=v[k]-w[k];     //v=X^m*(1-X)^m-(1-X)^m//
  v[m]=v[m]-1;          //v=X^m*(1-X)^m-(1-X)^m-X^m//
  return v;
}

//Berechnet b(n)//

long ber_b(long n)
{
  long x;
  vec_GF2 u,v;
  GF2X f,g;
  u.SetLength(n+1);
  u[0]=1;
  u[n]=1;
  long k=1;
  while(k<=n)
    k=2*k;        //k:kleinste natürliche Zahl grösser als n//
  long d=k-n;
  long dd=n-k/2;  //k/2: grösste natürliche Zahl kleiner als n//
  if(d<=2*dd)     //Vergleich der Grade der zwei Polynome//
  {
    v=degmin_first(d);
    conv(f,u);
    conv(g,v);
```

```
    x=deg(GCD(f,g))-1;
  }
  else
  {
    v=degmin_sec(dd);
    conv(f,u);
    conv(g,v);
    x=deg(GCD(f,g));
  }
  return x;
}

int main()
{
  long x;
  long q=14;
  long kand_n[14]={3,7,15,31,63,73,85,127,255,273,341,511,585,819};
  ofstream myfile;
  myfile.open ("Berechnete_b_n.txt");
  myfile<<"b=[";
  for(int k=0;k<q;k++)
    {
      x=ber_b(kand_n[k]);
      myfile<<x;myfile<<",";
    }
  myfile<<"]";
  myfile.close();
  return 0;
}
```

Berechnung von a(n)

```
/*Eingabe: Menge M_1 in Form des Vektors kand_n=[n_1,...,n_q], q, und den
           Vektor b=[b_1,...,b_q], wobei b[b_k]=b(n_k) für 1<=k<=q.
  Ausgabe: Vektor a=[a_1,...,a_q] mit der Eigenschaft a[a_k]=a(n_k) für
           alle 1<=k<=q.*/

ber_a()={

q=14;

kand_n=[3,7,15,31,63,73,85,127,255,273,341,511,585,819];

b=[2,6,14,30,62,18,24,126,254,32,120,510,86,194];
a=vector(q);

for(k=1,q,s=0;
  for(m=1,k-1,
    if(kand_n[k]%kand_n[m]==0,
       s=s+a[m]));
  a[k]=b[k]-s);

print("a=");
print(a);
}
```

Heuristik

```
/*Eingabe: Die Menge der Kandidaten M_1 in Form des Vektors
           kand_n=[n_1,...,n_q], für dessen Komponenten wir den
           heuristischen Wert berechnen wollen, dessen Anzahl
           Komponenten q, sowie ein Vektor hilfvec, der sämtliche Teiler
           von  n_1,...,n_q enthält, und dessen Länge anz. Ein  Vektor
           r_n, für den gilt, dass r_n[k]=r(kand_n[k]) und ein Vektor
           hilf_r_n für den gilt, dass hilf_r_n[k]=r(hilfvec[k]).
 Ausgabe:  Vektor aheur, dessen Komponenten die heuristischen Werte von
           den Komponenten von kand_n sind.*/


heuristik()={

t=1; /*Toleranz t. Falls aheur(k)<t, dann setze aheur(k)=0*/

q=14;
anz=27;
aheur=vector(anz);

kand_n=[3, 7, 15, 31, 63, 73, 85, 127, 255, 273, 341, 511, 585, 819];

r_n=[2,3,4,5,6,9,8,7,8,12,10,9,12,12];


hilfvec=[3, 5, 7, 9, 11, 13, 15, 17, 21, 31, 39, 45, 51, 63, 65, 73, 85,
91, 117, 127, 195, 255, 273, 341, 511, 585, 819];

hilf_r_n=[2, 4, 3, 6, 10, 12, 4, 8, 6, 5, 12, 12, 8, 6, 12, 9, 8, 12, 12,
7, 12, 8, 12, 10, 9, 12, 12];

/*Berechnung der heuristischen Werte*/

for(k=1,anz,
    wr=sumdiv(hilf_r_n[k],v,moebius(v)*2^(hilf_r_n[k]/v));
    tn=sumdiv(hilf_r_n[k],v,
              moebius(v)*gcd(hilfvec[k],2^(hilf_r_n[k]/v)-1));
    quot=tn^2/wr;quot=1.*quot;
    s=0;
    for(m=1,k-1,
      if(hilfvec[k]%hilfvec[m]==0,kontr=1;
        fordiv(hilf_r_n[k],d,
          if(d<hilf_r_n[k],
            if((2^d-1)%hilfvec[m]==0,kontr=0)));
          if(kontr==1,s=s+aheur[m])));
    aheur[k]=quot-s);


for(k=1,anz,if(abs(aheur[k])<t,aheur[k]=0));

/*Ausgabe*/

print("n");
for(k=1,q,print(kand_n[k]));
print();
```

```
print(heuristischer_Wert);
for(k=1,q,m=1;
  while(kand_n[k]!=hilfvec[m],m=m+1);
  print(aheur[m]));
print();

print(Expontent);
for(k=1,q,print(r_n[k]));
print();

print("(2^r-1)/n");
for(k=1,q,print((2^r_n[k]-1)/kand_n[k]));
print();
}
```

Die Berechnung der Vektoren hilfvec und hilf_r_n kann mittels folgender Prozedur umgesetzt werden:

```
/*Eingabe: Vektor kand_n=[n_1,...,n_q] der Länge q.
  Ausgabe: Vektor hilfvec, der alle Teiler ausser 1 von den Zahlen
           n_1,...,n_q enthält. Sowie ein Vektor hilf_r_n, für den gilt,
           dass hilf_r_n[k]=r(hilfvec[k]) für alle k.*/

teiler()={

q=14;

kand_n=[3,7,15,31,63,73,85,127,255,273,341,511,585,819];

/*Berechnung der Gesamtanzahl Teiler*/

z=0;
for(k=1,q,z=length(divisors(kand_n[k]))+z);

nvec=vector(z);

/*Speichern aller Teiler in einem Vektor nvec*/

stelle=0;
for(k=1,q,
 fordiv(kand_n[k],d,stelle=stelle+1;nvec[stelle]=d));

/*Sortieren von nvec*/

nvec=vecsort(nvec);

anz=0;
vecn=vector(z);
for(k=2,z, if(nvec[k]!=nvec[k-1],anz=anz+1;vecn[anz]=nvec[k]));

/*Aufstellen des hilfvec*/

hilfvec=vector(anz);
for(k=1,anz,hilfvec[k]=vecn[k]);
print("hilfvec=");
```

```
print(hilfvec);
print();

print(Anzahl Teiler);
print(anz);

hilf_r_n=vector(anz);

/*Berechnung von r(hilfvec[k]) für k=1,...,anz*/

for(k=1,anz,
 expot=1;
 pot=2;
 while(pot%hilfvec[k]!=1,pot=2*pot;expot=expot+1);
 hilf_r_n[k]=expot);
print();
print("hilf_r_n=");
print(hilf_r_n);
print();
}
```

Literatur

[PiRo] P. Kurlberg and Z. Rudenick, *On quantum ergodicity for linear maps of the torus*, Comm. Math. Phys. **222** (2001), 201-227.