

Geometrien des Faktorisierungsproblems: Ein analytischer Zugang über KQ- Gruppen

Version 3

**Zur funktionalen Nutzbarmachung strukturierter
Gruppierungsräume für Faktorisierungsfragen**

Version 1: Datum Veröffentlichung: 18.07.2025

Version 2: Datum Veröffentlichung: 19.07.2025

Version 3: Datum Veröffentlichung: 22.07.2025

Achim Meißner

Email:

service@ameis-web.de

Abstract

Diese Arbeit untersucht die Bedingungen semiprimier Zahlen $N = p \cdot q$, für die sich der größere Primfaktor q deterministisch und ohne Iteration aus N berechnen lässt, diese N-Werte werden im folgenden „SPeQ-Semiprimes“ genannt und können direkt durch $q = V + \sqrt{V^2 - N}$ gelöst werden (V ist hier der Vorkommawert der Wurzel von N um 1 erhöht). Die Reduktion auf eine Quadratdifferenzform erlaubt es, den Primfaktor q direkt zu bestimmen, wenn die Differenz $q - p$ eine definierte Schwelle nicht überschreitet. Die Funktion wurde im Kontext der KQ-Gruppenstruktur hergeleitet und mit der Fermat-Methode verglichen. Die Berechnungen und Tests erfolgten vollständig mit selbsterstellten p- und q-Werten die mit Python und GMPY2 erzeugt wurden.

Schlüsselwörter / Keywords

Semiprime-Struktur, symmetrische Primprodukte, quadratische Zentren, Strukturparameter, analytische Faktorisierung, große Zahlenräume, mathematische Rekonstruktion

Vorwort

Diese Arbeit greift zentrale Analysefähigkeiten auf, wie sie im Rahmen des KQ-KFS-Papiers entwickelt wurden, und wendet sie auf das Faktorisierungsproblem an.

Ziel war es herauszufinden, ob man mit „KQ“ das Problem der Faktorisierung analytisch betrachten kann. Der Fokus liegt auf dem Auffinden systematischer Muster und algorithmisch nutzbarer Eigenschaften semiprimer Zahlen.

Das zugrunde liegende KQ-KFS-Paper wird für die Lektüre dieses Textes als bekannt vorausgesetzt (Meißner, 2025a).

Ergänzend sei darauf hingewiesen, dass das Konzept der Monoinformation bereits eine erste konkrete Anwendung der KQ- und KFS-Prinzipien beschreibt und deren informationstheoretisches Potenzial auslotet (Meißner, 2025b).

Hinweis: In dieser Version 3 wurden so weitreichende Änderungen vorgenommen, dass auf eine genaue Änderungshistorie verzichtet wurde.

Inhalt

1	Analytische Lösung semiprimen Zahlen im Bereich quadratischer Schranken	4
1.1	Analytische Vorüberlegungen	4
1.2	Schranke der Symmetriebindung	5
1.3	Identität der Primfaktoren in KQ	6
1.4	Testreihe	8
1.5	Laufzeitverhalten	14
2	Reduktion auf die Quadratdifferenzform der SPeQ-Semiprimes	16
3	Ausblick	20
4	Lizenzhinweis zur Nutzung dieses Dokuments	21
5	Literaturverzeichnis	23

1 Analytische Lösung semiprimer Zahlen im Bereich quadratischer Schranken

Das klassische Faktorisierungsproblem wird in diesem Abschnitt daraufhin untersucht, ob und in welchem Umfang es sich mit den Mitteln der KQ-Gruppensystematik analytisch erfassen lässt. Dabei dienen semiprime Zahlen als Anwendungsfall. Ziel ist es, die Eigenschaften dieser Zahlen mit Hilfe der KQ-Parameter zu analysieren und zu prüfen, ob sich darin Merkmale erkennen lassen.

Unter einem Semiprime versteht man eine natürliche Zahl, die genau zwei Primfaktoren besitzt, wobei diese entweder verschieden oder gleich sein können (Wolfram, o.J.).

1.1 Analytische Vorüberlegungen

Ausgangspunkt der folgenden Betrachtung ist die strukturelle Analyse von Zahlen der Form $N = p \cdot q$, wobei p und q zwei voneinander verschiedene Primzahlen mit $p < q$ sind. Wird dabei die Differenz $d = \frac{q-p}{2}$ als Maß der arithmetischen Asymmetrie gewählt, so ergibt sich der arithmetische Mittelpunkt der beiden Faktoren zu $M = \frac{p+q}{2}$. Dieses symmetrisch zwischen p und q gelegene Zentrum bildet die Grundlage der weiteren Betrachtung. Es ist zunächst ein rein algebraisch definierter Mittelwert, besitzt jedoch in Verbindung mit dem Produkt N eine Eigenschaft.

Quadratiert man den Mittelpunkt M , so ergibt sich $M^2 = \left(\frac{p+q}{2}\right)^2$, was sich durch elementare Umformung zu

$$M^2 = \frac{p^2 + 2pq + q^2}{4}$$

ausschreiben lässt. Vergleicht man diesen Ausdruck mit $N = p \cdot q$, ergibt sich

$$M^2 - N = \left(\frac{p+q}{2}\right)^2 - pq = \left(\frac{q-p}{2}\right)^2 = d^2$$

Der Produktwert N liegt also exakt um den quadratischen Abstand d^2 unterhalb des Quadrats des Mittelpunkts M . Diese Identität ist allgemeingültig und unabhängig von der Größe der beteiligten Primzahlen.

Die Bedeutung dieser Feststellung liegt darin, dass jede semiprime Zahl mit kleiner Faktorendifferenz notwendigerweise knapp unterhalb eines echten Quadrats liegt. Die Tiefe dieser Unterschreitung hängt ausschließlich vom Abstand $q - p$ ab. Solange dieser Abstand klein bleibt, bleibt auch d klein, und N bleibt in unmittelbarer Nähe von M^2 . In dieser Konstellation ist das Produkt N formal nichts anderes als ein echtes Quadrat, reduziert um einen exakt quantifizierbaren Term d^2 . Damit ergibt sich eine systematische Asymmetrie in der Lage semiprimer Zahlen: sie liegen, solange die Differenz zwischen ihren Faktoren beschränkt ist, strikt unterhalb eines echten Quadrats, genauer: unterhalb des Quadrats ihres arithmetischen Mittelpunkts.

Je größer jedoch d wird, desto weiter entfernt sich N von M^2 . In Grenzfällen, bei sehr ungleichen Primfaktoren, kann N sogar zwischen weit auseinanderliegenden Quadraten zu liegen kommen, ohne noch erkennbare Nähe zu einem Zentrum zu besitzen. Dennoch bleibt die Gleichung $M^2 - N = d^2$ immer gültig, sie verliert lediglich an funktionaler Verwertbarkeit, wenn d überhandnimmt. Entscheidend ist also die Bindung des Produkts N an die Mitte seiner beiden Faktoren: Sie ist strukturell stabil nur dann, wenn die beiden Faktoren hinreichend symmetrisch um diese Mitte angeordnet sind.

1.2 Schranke der Symmetriebindung

Ausgehend von der Beziehung $N = M^2 - d^2$, lässt sich eine exakte Bedingung dafür ableiten, bis zu welcher Differenz $q - p$ die semiprime Zahl N strukturell eng an das Quadrat ihres arithmetischen Mittelpunkts gebunden bleibt. Diese Bindung geht verloren, wenn $\sqrt{N} = \sqrt{M^2 - d^2}$ in den nächstniedrigeren Ganzzahlbereich unterhalb von M übertritt. Der ganzzahlige Vorkommateil von $\sqrt{N}$ weicht dann von $M - 1$ ab, was den Übergang in eine unsymmetrischere Faktorlage markiert.

Setzt man

$$\sqrt{M^2 - d^2} = M - 1$$

so ergibt sich durch Umformung

$$M^2 - d^2 = (M - 1)^2$$

woraus folgt $d^2 = 2M - 1$ und damit $d > \sqrt{2M - 1}$. Die strukturelle Nähe zu M^2 bleibt demnach nur erhalten, solange $d \leq \sqrt{2M - 1}$. Diese Ungleichung lässt sich grob in eine Schranke für $q - p$ überführen. Setzt man $M \approx \sqrt{N}$, was für kleine Faktorendifferenzen eine brauchbare Näherung ist, so ergibt sich $d \leq \sqrt{2\sqrt{N}}$, also

$$q - p \leq 2\sqrt{2} \cdot N^{1/4} = \mathcal{O}(N^{1/4})$$

Diese Schranke ist nicht linear, sondern folgt einer quartischen Wurzel in Bezug auf N . Für typische N -Werte lassen sich daraus konkrete Bitdifferenzgrenzen ableiten. Bei N mit 2048 bit liegt die Grenze für $q - p$ bei etwa $\mathcal{O}(2^{513})$, bei 4096 bit entsprechend bei $\mathcal{O}(2^{1021})$. Diese theoretisch hergeleitete Obergrenze stimmt mit den empirisch beobachteten Schwellen sehr gut überein, bis zu denen eine eindeutige strukturelle Nähe von N zu seinem Mittelpunktquadrat erhalten bleibt.

1.3 Identität der Primfaktoren in KQ

Im Rahmen umfangreicher Untersuchungen zu kanonisch-quadratischen Gruppenstrukturierungen zeigte sich, dass sich der größere Primfaktor q eines semiprimen Produkts $N = p \cdot q$ über die Gleichung

$$q = T_q + \sqrt{SP} \tag{1}$$

beschreiben lässt. Diese Beziehung wurde nicht theoretisch postuliert, sondern ergibt sich aus einer Vielzahl empirischer Prüfungen, in denen jeweils N durch fest definierte p -, q -Paare konstruiert wurde und anschließend die zugehörigen KQ-Parameter T_q und SP berechnet wurden. Die Gleichung (1) stellte sich dabei als direkt nutzbare, deterministische Struktur heraus, die den Wert von q bis auf die letzte Stelle korrekt liefert, solange bestimmte Bedingungen eingehalten werden.

In den Testreihen wurde insbesondere sichtbar, dass die Strukturbindung an T_q vom N-Wert nur dann erhalten bleibt, wenn q und p in einem symmetrischen Verhältnis zu diesem T_q stehen, das sich durch die quadratische Abweichung SP eindeutig quantifizieren lässt. Entscheidend ist hierbei, dass q und p nicht bloß als Faktoren, sondern als eigene Gruppennummern G oder T_q in Form von T_{q_p} und T_{q_q} betrachtet werden können.

In diesem Kontext kann man die Differenz zwischen T_q des N-Werts und eben T_{q_q} und T_{q_p} „messen“.

Ein Beispiel:

Ein exemplarischer Fall ist $N = 391$ mit T_{q20} , $GP11$ und $SP = 9$ (das Minuszeichen bedeutet im KQ-Kontext: der Wert ist NL für $N391$, der N-Wert liegt links vom quadratischen Zentrum) mit der Zerlegung $p = 17$, $q = 23$. Damit liegt $T_{q_q} = 23$ und $T_{q_p} = 17$ jeweils im exakten Abstand 3 zu dem T_q vom $NL391$ also gilt:

$$T_{q_q} - T_q = 3 \text{ und } T_q - T_{q_p} = 3$$

Dieser symmetrische Abstand ist durch $SP = 9$ exakt kodiert, da

$$\sqrt{SP} = 3$$

SP fungiert hier also als quadratische Abweichung beider Faktoren vom strukturellen Zentrum T_q des N-Werts. Die Bedeutung liegt darin, dass q nicht isoliert betrachtet wird, sondern als ein vom Zentrum aus abgeleiteter Punkt, dessen Abstand durch

$$\sqrt{SP}$$

exakt bestimmt ist.

Diese Beobachtung ist nicht auf kleine Zahlen beschränkt. Für 2048-bit-lange semiprime N-Werte konnte gezeigt werden, dass diese Gleichung für alle Konstellationen mit

$$q - p \leq 513$$

Zahlendifferenz in Bit Differenz vollständig gültig bleibt. In diesem Bereich stimmt der berechnete Wert der Gleichung (1) mit dem tatsächlichen q über alle rund 310 Stellen exakt überein. Bereits bei einer Differenz von 514 bit fiel die Übereinstimmung drastisch auf etwa 154 gemeinsame Stellen. Dasselbe Muster zeigte sich bei 4096-bit-N-Werten: Bei Zahlendifferenzen

$$q - p \leq 1025$$

in Bit, es blieben bis zu 618 Dezimalstellen identisch. Erst bei einer Bitdifferenz von genau 1026 fiel die Übereinstimmung auf 307 Stellen.

1.4 Testreihe

Die Motivation dieser Tests war, herauszufinden, warum alle erstellten p- und q-Werte immer das KQ-Attribut NL hatten, ob das also reiner Zufall der Testdaten war oder ob sich die Lage NL für die benannten Bit-Differenzen als systematisch erweisen sollte. In Abbildung 1 und Abbildung 2 sind die jeweilige Anzahl für 2048 bit und 4096 bit lange N-Werte zu sehen:

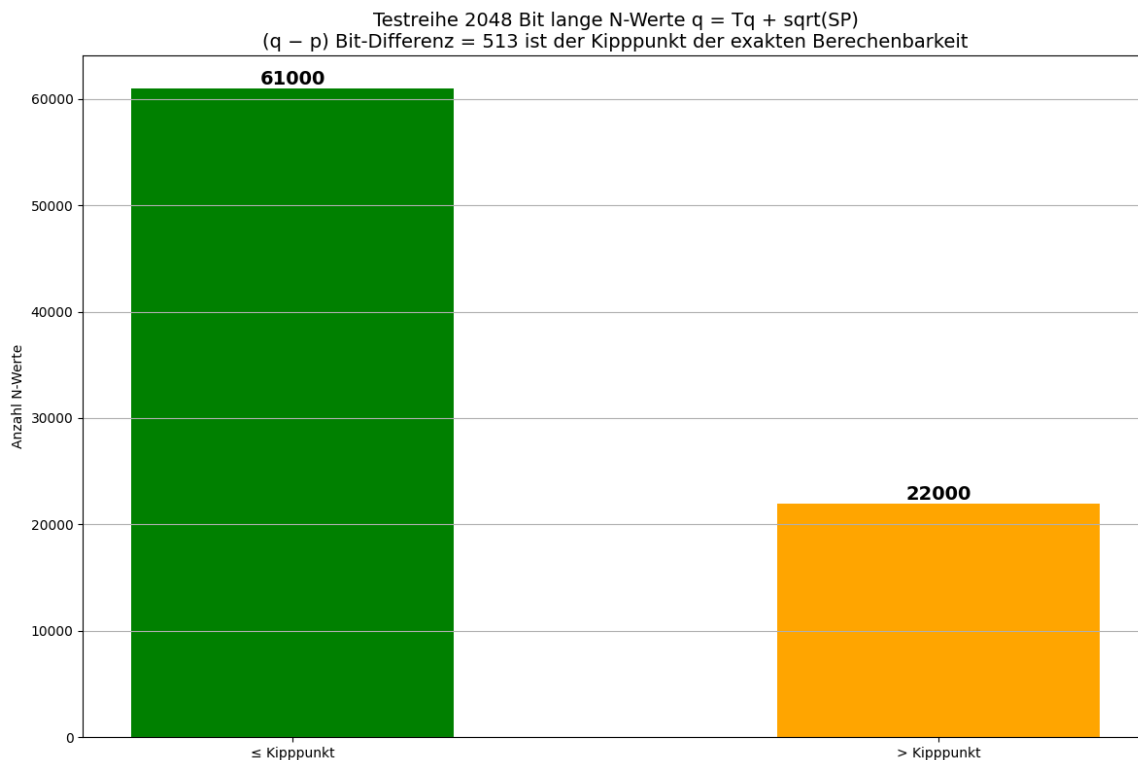


Abbildung 1: Testreihe Versuchs N-Werte 2048 bit lang

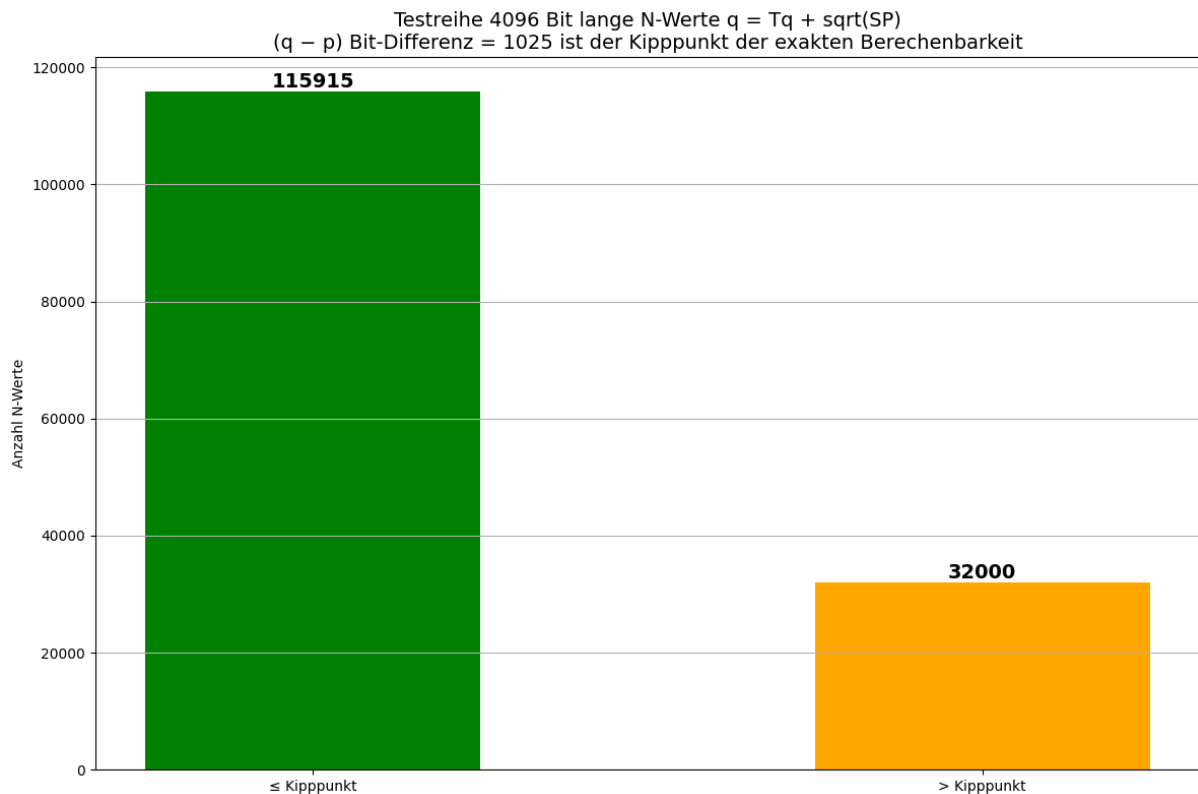


Abbildung 2: Testreihe Versuchs N-Werte 4096 bit lang

Der Testreihenaufbau war wie folgt:

- Gestartet wurde bei $q - p$ bit Rechendifferenz in 10er Schritte, also z.B. 1-10, dann 11-20 etc.
- In jedem Intervall wurden 1000 p- und q-Werte zufällig erzeugt, das N dann mit der Gleichung (1) geprüft und die Anzahl der übereinstimmenden Ziffern mit q gezählt.
- Kurz vor und nach der jeweiligen Kippunkten (513, 1025), ca. 10 Zähler jeweils, wurde das Intervall in 1 bit Schritten verkleinert, um den Kippunkt genau herausfinden zu können.
- Damit der lineare und beobachtete Abfall der übereinstimmenden Treffer der Gleichung (1) vs. q ebenfalls erkundet werden konnte, wurde nach dem Kippunkt + 10 in 50er Schritten die Intervalle umgesetzt, also z.B. 824 bis 873 bit Rechendifferenz bis zum doppelten Wert der Kippunkte ($2 \cdot 513$ und $2 \cdot 1025$).

Ein weitere Motivation war auch, herauszufinden wo genau dieser beschriebene Kippunkt genau liegt und ob es da Streubereiche gibt.

Die beobachteten Kippunkte werden in der Abbildung 3 und Abbildung 4 dargestellt:

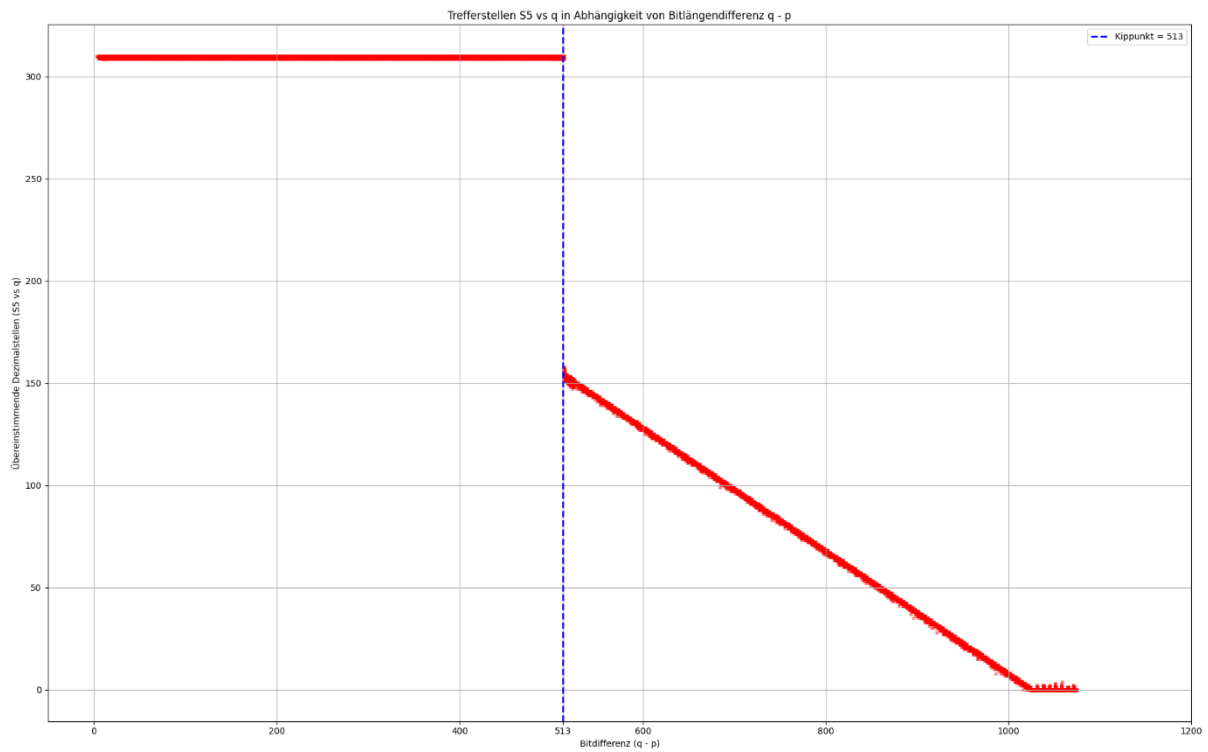


Abbildung 3: Treffer Gleichung (1) Ziffern mit q für 2048 bit N

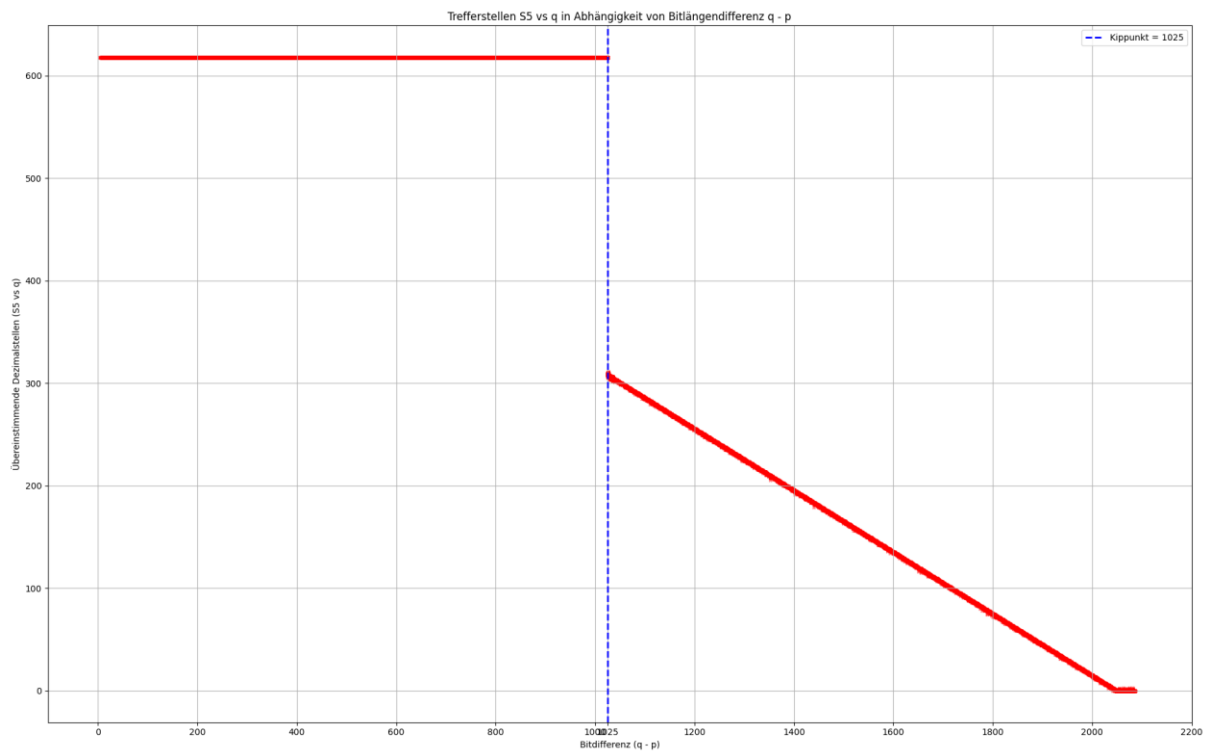


Abbildung 4: Treffer Gleichung (1) Ziffern mit q für 4096 bit N

Der abfallende rechte Teil der Diagramme und die zugehörige Regressionslinie (siehe Abbildung 5 und Abbildung 6):

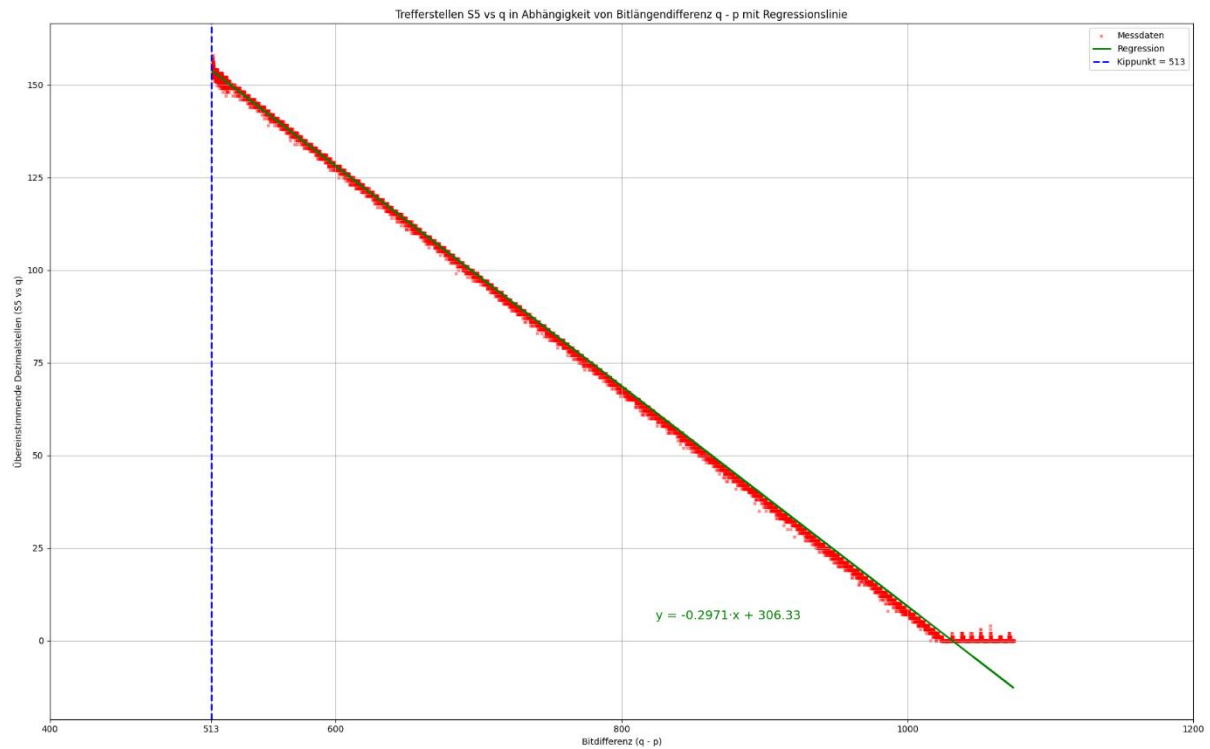


Abbildung 5: Regresssionslinie für 2048 bit N

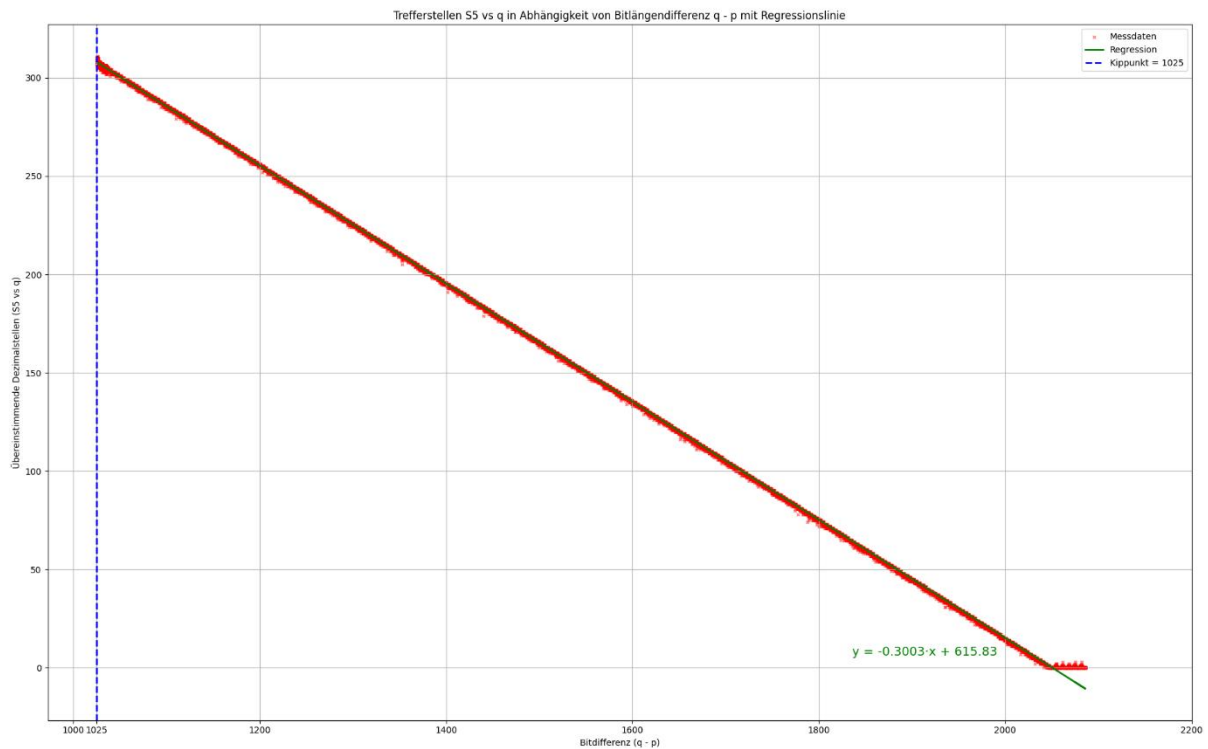


Abbildung 6: Regressionslinie für 4096 bit N

Für 2048 bit lange N-Werte wurde auch noch die Abweichung der SP-Werte von echten Quadratzahlen in Abhängigkeit der Bitdifferenzen betrachtet (siehe Abbildung 7):

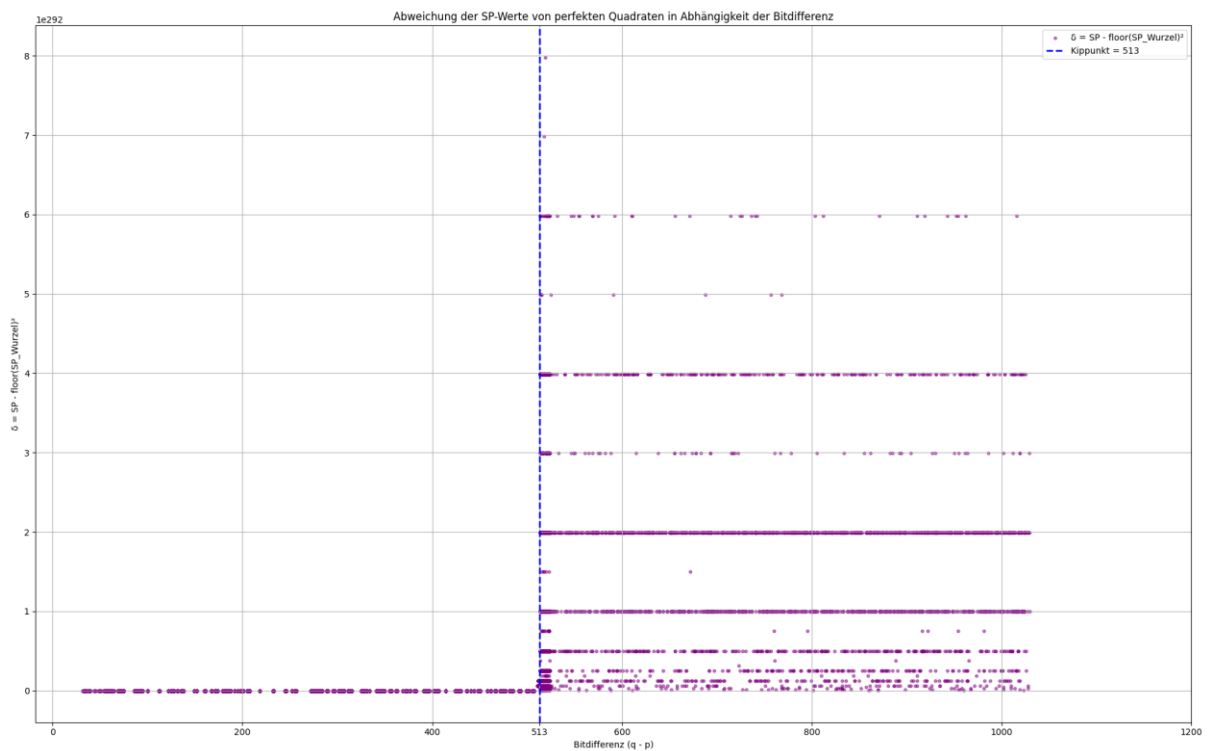


Abbildung 7: 2048 bit N Regressionslinie

Diese sprunghafte Verschlechterung jenseits der Kippunkte zeigt, dass die Gleichung (1) eine reale Grenze der Symmetriebindung und ihrer Gültigkeit markiert. Solange sich p und q über einen gemeinsamen Mittelpunkt T_q eindeutig rekonstruieren lassen, etwa in der Form Tq_p und Tq_q und der zugehörige SP-Wert eine exakte Quadratstruktur bildet, bleibt die Berechnung von q reproduzierbar. Solche N-Werte werden unter dem vorläufigen Arbeitstitel „SPeQ-Semiprimes“ zusammengefasst. Sobald diese Bedingung verletzt wird, verliert die Identität ihre deterministische Präzision. Die Bindung des N-Werts über $\sqrt{SP}$ ist daher keine Näherung, sondern eine direkte Abhängigkeit in N , die durch empirische Verfahren erkannt, bestätigt und für alle getesteten Fälle quantifizierbar gemacht wurde.

Alle erfolgreichen Treffer der Gleichung (1) vs. q sind NL Werte und haben echte SP-Quadratzahlen. N-Werte nach dem Kippunkten sind entweder NL oder NR und besitzen keine echten quadratischen SP-Werte mehr im Testumfang. Natürlich ist die statistische Auswertung von gerade mal knapp über 100.000 4096 bit langen N-Werten vermutlich nicht repräsentativ, aber durch die rein zufällige Auswahl von p- und q-Werten lässt sich durchaus ein Trend erkennen, der sich mit den in „1.1 Analytische Vorüberlegungen“ gewonnenen Erkenntnissen deckt.

Im bisherigen Verlauf wurde gezeigt, wie sich die kanonisch-quadratische Gruppierung als analytisches Werkzeug im Kontext semiprimer Zahlen einsetzen lässt. Erstaunlich ist dabei, dass KQ selbst in sehr großen Zahlenbereichen problemlos anwendbar bleibt und auch Differenzen von nur 1 zwischen z.B. N-Werten mit über 1230 Dezimalstellen noch klar und zuverlässig erkennbar umgesetzt. Die bisher analysierten Konstellationen zeigen, dass sich die algebraischen Marker Tq und SP innerhalb des KQ-Schemas nicht nur bestimmen, sondern auch funktional nutzen lassen, um die internen Eigenschaften solcher Zahlen exakt zu beschreiben.

Die KQ-Gruppenstrukturen wurden ursprünglich als analytisches Hilfsmittel im Rahmen anderer Untersuchungen entwickelt. Die dabei eingeführten Parameter wie Tq , Tp , GP und insbesondere SP entstanden nicht aus einem vorgefassten Modell, sondern ergaben sich nebenläufig aus der systematischen Analyse der KQ-Struktur selbst. Der Parameter SP , der den Abstand eines gegebenen N-Werts zur mittensymmetrischen echten Quadratzahl Tq^2 beschreibt, hat sich dabei als zentrale

Größe herauskristallisiert. Dass sich dieser eigens definierte Parameter nun in sämtlichen durchgeführten Testreihen exakt entsprechend den in dieser Arbeit hergeleiteten Zusammenhängen verhält, insbesondere durch die Identifikation echter Quadratzahlen bei spezifischen Klassen von Semiprimes, zeigt das Analysevermögen der KQ-Gruppen in überraschender Deutlichkeit.

1.5 Laufzeitverhalten

Für jede untersuchte Zahl N wurde im Rahmen der Analyse eine definierte Abfolge von vier Kernwerten berechnet, die zur vollständigen Ermittlung des größeren Primfaktors q notwendig sind. Ausgangspunkt ist der Wert Tp , Tq von N , GP und SP . Die vollständige Berechnung all dieser Größen erfolgt deterministisch und in fester Abfolge, wobei jede Zwischenoperation exakt definiert und vollständig rekonstruktiv ist. In systematischen Testreihen wurde die gesamte Berechnungskette, von der Eingabe des Produkts N bis zur expliziten Ermittlung des Werts q , hinsichtlich ihres Zeitverhaltens untersucht. Selbst bei sehr großen Zahlen N mit einer Länge von 4096 Bit beträgt die durchschnittlich benötigte Rechenzeit bis zur Bestimmung von q etwa 0,05 bis 0,1 Millisekunden (in Python). Dieser Wert umfasst bereits die vollständige Auswertung aller genannten Zwischenparameter einschließlich der Berechnung der Quadratwurzel und der exakten Addition zur Bestimmung von q . (siehe Abbildung 8 und Abbildung 9):

	J	K	L	M	N	O	P	Q
	Bitlänge_N	Bitdiff_q_minus_p	Trefferstellen_S5_q	Volltreffer_q	SP_Quadrat	SP_Wurzel	N_Lage	Laufzeit_ms
0	4096	282	618	True	True	19426688922	NL	0.059
1	4095	285	618	True	True	15541351137	NL	0.048
4	4095	291	618	True	True	99464647281	NL	0.055
3	4095	290	618	True	True	49732323640	NL	0.055
0	4095	286	618	True	True	31082702275	NL	0.055
3	4095	288	618	True	True	12433080910	NL	0.056
1	4095	283	618	True	True	38853377844	NL	0.05
4	4096	288	618	True	True	12433080910	NL	0.055
0	4095	289	618	True	True	24866161820	NL	0.058

Abbildung 8: Bit ZiffernDiff q-p ca. 290

J	K	L	M	N	O	P	Q
Bitlänge_N	Bitdiff_q_minus_p	Trefferstellen_S5_q	Volltreffer_q	SP_Quadrat	SP_Wurzel	N_Lage	Laufzeit_ms
4096	1023	618	True	True	22471164185	NL	0.117
4095	1023	618	True	True	22471164185	NL	0.121
4095	1023	618	True	True	22471164185	NL	0.116
4096	1023	618	True	True	22471164185	NL	0.081
4096	1023	618	True	True	22471164185	NL	0.114
4095	1023	618	True	True	22471164185	NL	0.104
4095	1023	618	True	True	22471164185	NL	0.118
4096	1023	618	True	True	22471164185	NL	0.11
4096	1023	618	True	True	22471164185	NL	0.112
4095	1023	618	True	True	22471164185	NL	0.113
4095	1023	618	True	True	22471164185	NL	0.111
4095	1023	618	True	True	22471164185	NL	0.117
4096	1023	618	True	True	22471164185	NL	0.113
4095	1023	618	True	True	22471164185	NL	0.145
4096	1023	618	True	True	22471164185	NL	0.399

Abbildung 9: Bit ZiffernDiff q-p ca. 1023

2 Reduktion auf die Quadratdifferenzform der SPeQ-Semiprimes

Die hier hergeleitete Methode zur Bestimmung des Faktors q aus einem gegebenen semiprimen N (SPeQ-Semiprimes), basierend auf der Gruppenstruktur der KQ-Systematik, kann durch eine elementare Umformung auf eine überraschend einfache analytische Form reduziert werden. Diese Formulierung erlaubt nicht nur eine methodische Trennung von der KQ-Systematik, sondern verdeutlicht zugleich, dass der Mechanismus zur Bestimmung von q in einem speziellen, aber sehr breiten Bereich als reine Quadratdifferenzrelation gefasst werden kann.

Zentraler Ausgangspunkt ist der aus dem vorhergehenden Kapitel definierte Wert T_q , der für alle gültigen Fälle die Gruppenidentität zu einem gegebenen N festlegt. Dieser Wert wird deterministisch aus N berechnet als:

$$T_q = (\sqrt{4 \cdot N + 1} + 1) \div 2$$

Dieser Ausdruck basiert auf den KQ-Gruppenstrukturen selbst. Für den betrachteten Wertebereich ist allerdings entscheidend, dass jeder dieser SPeQ-Semiprimes notwendigerweise vor dem Quadratzentrum T_q^2 liegt. Diese Konstellation wird in der KQ-Terminologie als NL-Lage bezeichnet. Aus dieser Lage ergibt sich unmittelbar:

$$SP = T_q^2 - N$$

mit der zentralen Eigenschaft, dass SP in diesen Fällen stets eine echte Quadratzahl ist. Die Berechnung von q erfolgt deterministisch über die bereits gezeigte Gleichung (1) die hier nochmals gezeigt wird, um die Umformungsschritte besser zu verdeutlichen:

$$q = T_q + \sqrt{SP}$$

Da aber für N -Werte die NL sind gilt $T_q = \lfloor \sqrt{N} \rfloor + 1$, kann man die gesamte Formel alternativ in eine vollständig unabhängige Darstellung überführen. Bezeichne man:

$$V := \lfloor \sqrt{N} \rfloor + 1$$

so folgt daraus:

$$SP = V^2 - N$$

und schließlich:

$$q = V + \sqrt{V^2 - N} \quad (2)$$

Diese Formulierung erfasst exakt denselben Mechanismus wie die vorhergehende Herleitung über die KQ-Struktur, erfordert jedoch keinerlei Kenntnis von Gruppenparametern oder deren Ableitungen. Sie ist elementar und basiert ausschließlich auf der Differenz zwischen einem quadratischen Oberwert V^2 und dem gegebenen N , wobei V in jedem gültigen Fall als $\lfloor \sqrt{N} \rfloor + 1$ bestimmt wird. Diese Reduktion ist zugleich auch die direkte funktionale Entsprechung zum Startwert a in der klassischen Fermat-Methode, da auch dort der initiale Versuchswert durch Aufrunden der Quadratwurzel von N gebildet wird, man könnte auch schreiben:

$$q = a + \sqrt{|a^2 - N|} \quad (3)$$

Man kann daher auch argumentieren, dass die hier gefundene Relation:

$$q = \lfloor \sqrt{N} \rfloor + 1 + \sqrt{(\lfloor \sqrt{N} \rfloor + 1)^2 - N} \quad (4)$$

eine Art „Nebenfunktion“ der Fermat-Methode darstellt, sofern man sich auf die Klasse der SPeQ-Semiprimes beschränkt. Die Fermat-Methode liefert hier direkt bereits im Null-Schritten die Auflösung (wie ein Professor in einer Email anmerkte). SPeQ in KQ ist also im Grunde die Semiprime-Klasse die direkt im ersten Durchlauf der Fermat-Methode gelöst werden kann.

Die aus den KQ-Analysen hergeleitete SPeQ-Gleichung (1) ist auch als Funktion interessant und zeigt die geometrische Ausrichtung (die lila Funktion siehe Abbildung 10):

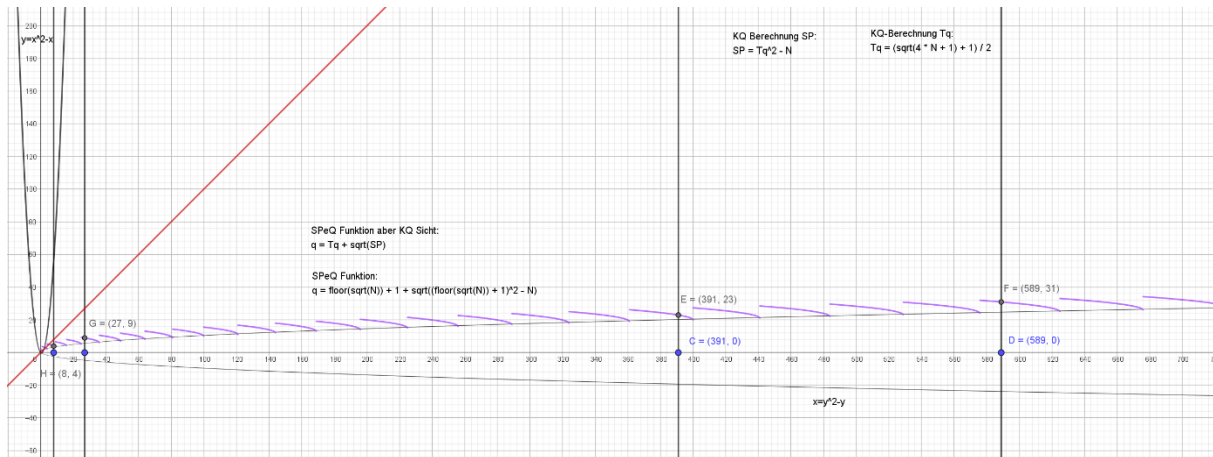


Abbildung 10: SPeQ Gleichung

Die SPeQ-Funktion gleicht sich über den Zahlenverlauf immer mehr der invertierten $x = y^2 - y$ Funktion an (siehe Abbildung 11 und Abbildung 12):

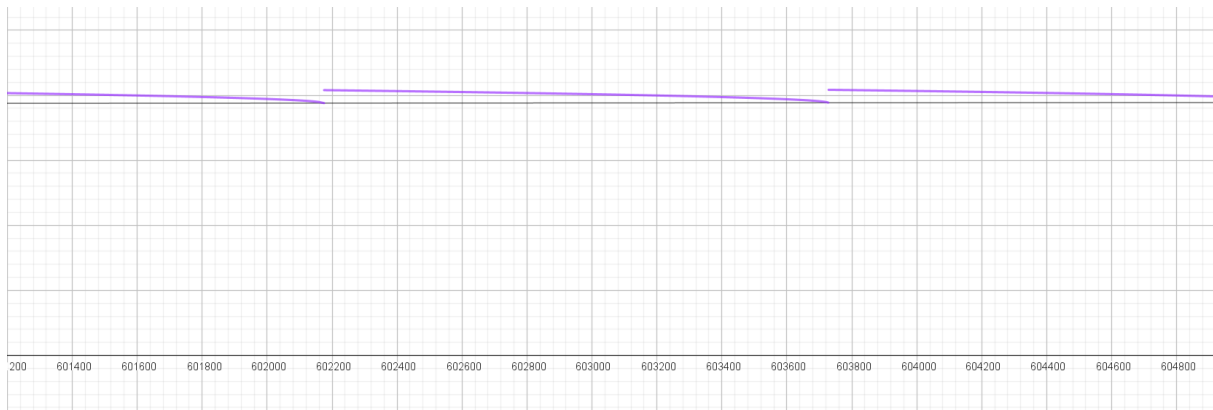


Abbildung 11: SPeQ Funktionsverlauf 1

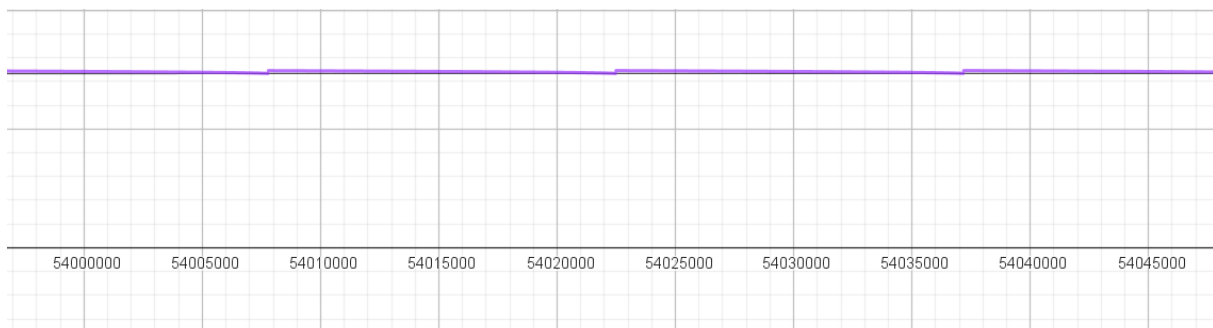


Abbildung 12: SPeQ Funktionsverlauf 2

Abschließend sei darauf hingewiesen, dass die im Rahmen der KQ-Gruppenstrukturierungen entwickelten Gruppierungsmechanismen, wie in der Arbeit gezeigt, ein bislang ungenutztes analytisches Potenzial innerhalb der Zahlentheorie besitzen könnten. Durch ihre Fähigkeit, jedem natürlichen N-Wert eindeutig zuordenbare Strukturparameter (Metadaten) wie Tq , Tp , GP oder SP und einer genauen Gruppe G ($G = Tq$) zuzuweisen, entsteht ein konsistentes Ordnungssystem, das sich nicht nur zur Klassifikation, sondern auch zur präzisen funktionalen Analyse eignet, denn mit den KQ-Parametern kann man selbst auch algorithmisch rechnen, z.B. in Python-Codes, wie in „KQ-KFS-Strukturen“ ebenfalls demonstriert wurde, mit der Erzeugung garantiert Teilerfremder Zahlenpaare ohne benötigte ggT Prüfungen (Meißner, 2025a, S. 60–61).

3 Ausblick

Weitere bisherige Analysen innerhalb der KQ-Gruppierungsstruktur deuten darauf hin, dass sich über die SP-Parameter prinzipiell auch weiterreichende Zusammenhänge zwischen den Primfaktoren p und q abbilden lassen, insbesondere im Hinblick auf deren numerischen Abstand. Die bislang untersuchten SPeQ-Semiprimes markieren dabei vermutlich lediglich eine besonders klar abgrenzbare Teilstruktur innerhalb einer umfassenderen Ordnung, dessen systematische Erschließung Gegenstand künftiger Untersuchungen sein wird.

Es sei ausdrücklich festgehalten, dass die hier beschriebene Methode sogenannte Fermat-sichere Semiprimes mathematisch nicht auflösen vermag. Eine solche Generalisierung ist jedoch weder beabsichtigt noch Teil des Untersuchungsziels dieser Arbeit. Ziel war es, zu zeigen, dass sich mithilfe der KQ-Gruppierungsstruktur alternative analytische Zugänge zum semiprimen Produktraum eröffnen lassen und dass sich aus diesen strukturellen Erkenntnissen konkrete Beziehungen ableiten lassen, wie sie exemplarisch in den Gleichungen (2), (3) und (4) dargestellt wurden.

Hinweis zur Einordnung der Arbeit:

Der Verfasser ist weder ausgebildeter Mathematiker noch Kryptologe. Etwaige Abweichungen von etablierten Herleitungen, Konventionen oder Fachtermini der formalen Mathematik sind vor diesem Hintergrund zu verstehen. Die verwendeten Begriffe und Zugänge beruhen auf eigener Analyse und begrifflicher Setzung im Rahmen einer unabhängigen Untersuchung.

4 Lizenzhinweis zur Nutzung dieses Dokuments

Das vorliegende Werk einschließlich aller darin enthaltenen Begriffe, Modelle und Darstellungen, insbesondere die Konzepte der Kanonisch-Quasiquadratischen Gruppenstruktur (KQ), der K-Fokalen Schalensymmetrie (KFS), der Monoinformation, der geometrisch motivierten Zugänge zum Faktorisierungsproblem, der Quadratrouutenanalyse, sowie sämtliche weiteren benannten oder implizierten Strukturansätze, ist urheberrechtlich geschützt.

Die Nutzung ist unter folgenden Bedingungen gestattet:

- Die wissenschaftliche Nutzung (einschließlich Zitierung, Weiterentwicklung in akademischen Kontexten, Verwendung zu Lehr- und Forschungszwecken) ist uneingeschränkt gestattet, sofern auf den Ursprung des Werks in angemessener Weise verwiesen wird.
- Die private Nutzung, d. h. die nicht-kommerzielle Verwendung im persönlichen, nicht-institutionellen Rahmen (z. B. individuelle Anwendungen, private Weiterverarbeitung, nicht öffentliche Weitergabe), ist ebenfalls gestattet, unter Beibehaltung der vollständigen Herkunftsangabe.
- Kommerzielle Nutzung, darunter fallen unter anderem jede Art von kommerzieller Softwareintegration, kommerzielle Beratung, industrielle Anwendung, Lizenzweitergabe oder technische Implementierung in Produkten oder Dienstleistungen, ist nur nach ausdrücklicher schriftlicher Zustimmung des Urhebers und dem Abschluss eines entsprechenden Lizenzvertrags zulässig.

Jegliche Form der kommerziellen Verwertung ohne Lizenz stellt eine Verletzung des Urheberrechts dar und kann/wird rechtlich verfolgt werden.

Dieses Werk steht unter der Creative-Commons-Lizenz CC BY-NC 4.0 International.

Wissenschaftliche und private Nutzung sind unter Namensnennung gestattet.

Kommerzielle Nutzung nur mit vorheriger schriftlicher Zustimmung des Autors.

Lizenztext: <https://creativecommons.org/licenses/by-nc/4.0/>

Zitierhinweis:

A. Meißner: Geometrien des Faktorisierungsproblems: Ein analytischer Zugang über KQ-Gruppen. Zur funktionalen Nutzbarmachung strukturierter Gruppierungsräume für Faktorisierungsfragen. DOI: 10.5281/zenodo.16318813

(online verfügbar unter: <https://doi.org/10.5281/zenodo.16318813>)

5 Literaturverzeichnis

- Meißner, A. (2025a). *KQ-KFS-Strukturen: Zur geometrischen Emergenz arithmetischer Realität. Eine Analyse Kanonisch-Quasiquadratischer Gruppen (KQ) und K-Fokaler-Schalenstrukturen (KFS) als Strukturformen informationstragender Räume*. Zenodo.
<https://doi.org/10.5281/ZENODO.15683651>
- Meißner, A. (2025b). *Monoinformation: Architektur rekursiv erzeugter Informationsräume. Fokale Raumadressierung (KRA) aus der Emergenz strukturierter Superpositionierung*. Zenodo.
<https://doi.org/10.5281/ZENODO.15711824>
- Wolfram. (o.J.). *Semiprime -- from Wolfram MathWorld*. Zugriff am 22.07.2025.
Verfügbar unter: <<https://mathworld.wolfram.com/Semiprime.html>>