Sicheres Einkaufen im Internet dank großer Primzahlen

MINT-Lehrerfortbildung, Fachvortrag Mathematik

PD Dr. Karin Halupczok

11. März 2020, Heinrich Heine Universität Düsseldorf

Zusammenfassung:

Die Suche nach Mustern in der Menge der Primzahlen führt zu mathematischen Vermutungen über die pseudozufällige Häufigkeit ihres Auftretens. Einige dieser Vermutungen sind derzeit unbewiesen und Gegenstand intensiver mathematischer Forschung, ihre Aussagen werden aber in bestimmten algorithmischen Anwendungen benutzt.

Diese modernen Anwendungen betreffen etwa die Sicherheit digital verfügbarer Daten und beruhen typischerweise auf dem mathematischen Faktorisierungsproblem bzw. dem Problem der Berechnung des diskreten Logarithmus in bestimmten algebraischen Strukturen. Ohne der Verwendung großer Primzahlen sind heute z. B. Online-Banking, Einkaufen im Internet, Kryptowährungen etc. undenkbar. Kurz gehen wir auch auf die derzeitige Entwicklung des Quantencomputers und dessen Bedeutung für die Datensicherheit im Internet ein.

Primzahlen

Sei $\mathbb{N} = \{1, 2, \dots\}$ die Menge der natürlichen Zahlen.

$a \in \mathbb{N}$ heißt Teiler von $b \in \mathbb{N}$, falls es ein $c \in \mathbb{N}$ gibt mit $ac = b$

Primzahlen

Sei $\mathbb{N} = \{1, 2, \dots\}$ die Menge der natürlichen Zahlen.

$a \in \mathbb{N}$ heißt Teiler von $b \in \mathbb{N}$, falls es ein $c \in \mathbb{N}$ gibt mit $ac = b$

Eine natürliche Zahl p heißt *prim* bzw. Primzahl, wenn sie genau zwei natürliche Teiler hat (nämlich 1 und $p \neq 1$).

Primzahlen

Sei $\mathbb{N} = \{1, 2, \dots\}$ die Menge der natürlichen Zahlen.

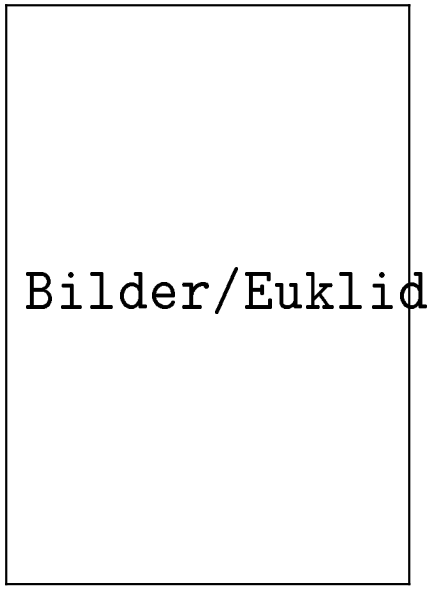
$a \in \mathbb{N}$ heißt Teiler von $b \in \mathbb{N}$, falls es ein $c \in \mathbb{N}$ gibt mit $ac = b$

Eine natürliche Zahl p heißt *prim* bzw. Primzahl, wenn sie genau zwei natürliche Teiler hat (nämlich 1 und $p \neq 1$).

Folge der Primzahlen:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Euklid

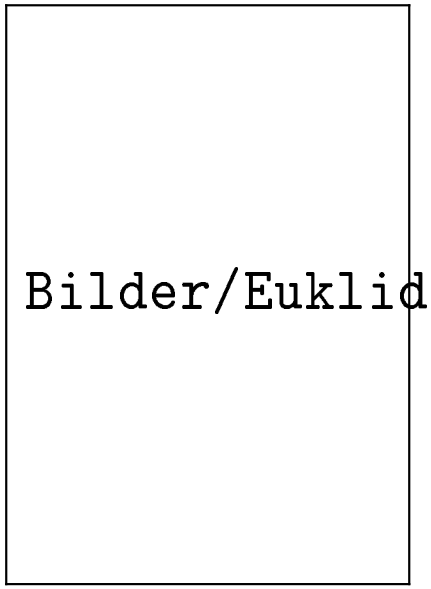


Euklid von Alexandria, ca. 300 v. Chr.

Satz von Euklid:

Es existieren unendlich viele Primzahlen.

Euklid

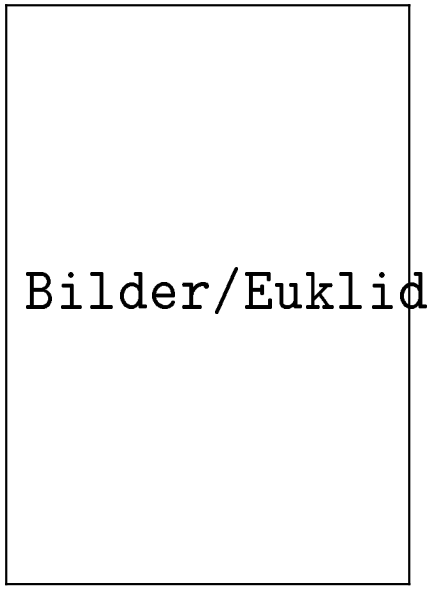


Euklid von Alexandria, ca. 300 v. Chr.

Satz von Euklid:
Es existieren unendlich viele Primzahlen.

Beweis: Sind $p_1, \ldots, p_n$ Primzahlen, so gibt es einen Primteiler p_{n+1} von $p_1 \cdots p_n + 1$, der von den $p_1, \ldots, p_n$ verschieden ist.
Auf diese Weise werden unendlich viele verschiedene Primzahlen $p_1, p_2, \ldots$ konstruiert.

Euklid



Euklid von Alexandria, ca. 300 v. Chr.

Satz von Euklid:
Es existieren unendlich viele Primzahlen.

Beweis: Sind $p_1, \ldots, p_n$ Primzahlen, so gibt es einen Primteiler p_{n+1} von $p_1 \cdots p_n + 1$, der von den $p_1, \ldots, p_n$ verschieden ist.
Auf diese Weise werden unendlich viele verschiedene Primzahlen $p_1, p_2, \ldots$ konstruiert.

Größte numerisch bekannte Primzahl

Größte numerisch bekannte Primzahl aktuell:

$$2^{82\,589\,933} - 1$$

Ein Zahlenmonster mit 24 862 048 Dezimalstellen !
(Vgl. vermutete Anzahl der Teilchen im Universum: 10^{100})

Größte numerisch bekannte Primzahl

Größte numerisch bekannte Primzahl aktuell:

$$2^{82\,589\,933} - 1$$

Ein Zahlenmonster mit 24 862 048 Dezimalstellen !
(Vgl. vermutete Anzahl der Teilchen im Universum: 10^{100})

Bekannt seit 07.12.2018 durch das Internet-Projekt GIMPS
GIMPS: Great Internet Mersenne Prime Search

`http://www.mersenne.org/`

Wozu sind große Primzahlen nützlich? Sind sooo große Primzahlen wie diese hier nützlich?

Erstellung von Primzahllisten

Antikes Sieb des Eratosthenes (ca. 273–194 v. Chr.):
Verfahren zur Erstellung von Primzahllisten

Erstellung von Primzahllisten

Antikes Sieb des Eratosthenes (ca. 273–194 v. Chr.):
Verfahren zur Erstellung von Primzahllisten

z. B. die Liste aller Primzahlen zwischen 10 und 100, wenn die Primzahlen bis 10 bekannt sind $(2, 3, 5, 7)$:

Erstellung von Primzahllisten

Antikes Sieb des Eratosthenes (ca. 273–194 v. Chr.):
Verfahren zur Erstellung von Primzahllisten

z. B. die Liste aller Primzahlen zwischen 10 und 100, wenn die Primzahlen bis 10 bekannt sind $(2, 3, 5, 7)$:

Jede zusammengesetzte Zahl $n \leq 100$ hat einen Primteiler $\leq 10 = \sqrt{100}$,

Erstellung von Primzahllisten

Antikes Sieb des Eratosthenes (ca. 273–194 v. Chr.):
Verfahren zur Erstellung von Primzahllisten

z. B. die Liste aller Primzahlen zwischen 10 und 100, wenn die Primzahlen bis 10 bekannt sind $(2, 3, 5, 7)$:

Jede zusammengesetzte Zahl $n \leq 100$ hat einen Primteiler $\leq 10 = \sqrt{100}$, denn wären sonst p, q zwei Primteiler > 10 von n, so wäre $n \geq pq > 10 \cdot 10 = 100$.

Erstellung von Primzahllisten

Antikes Sieb des Eratosthenes (ca. 273–194 v. Chr.):
Verfahren zur Erstellung von Primzahllisten

z. B. die Liste aller Primzahlen zwischen 10 und 100, wenn die Primzahlen bis 10 bekannt sind $(2, 3, 5, 7)$:

Jede zusammengesetzte Zahl $n \leq 100$ hat einen Primteiler $\leq 10 = \sqrt{100}$, denn wären sonst p, q zwei Primteiler > 10 von n, so wäre $n \geq pq > 10 \cdot 10 = 100$.

Idee: Streiche in der Liste 1,2,. . . ,100 alle Vielfachen von $2, 3, 5, 7$

Animation des Siebes von Eratosthenes

~~01~~ 02 03 04 05 06 07 08 09 10
11 12 13 14 15 16 17 18 19 20
21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50
51 52 53 54 55 56 57 58 59 60
61 62 63 64 65 66 67 68 69 70
71 72 73 74 75 76 77 78 79 80
81 82 83 84 85 86 87 88 89 90
91 92 93 94 95 96 97 98 99 100

Animation des Siebes von Eratosthenes

~~01~~	~~02~~	03	~~04~~	05	~~06~~	07	~~08~~	09	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

Streiche alle n, für die n durch 2 teilbar sind.

Animation des Siebes von Eratosthenes

~~01~~	~~02~~	~~03~~	~~04~~	05	~~06~~	07	~~08~~	~~09~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

Streiche alle n, für die n durch 3 teilbar sind.

Animation des Siebes von Eratosthenes

~~01~~	~~02~~	~~03~~	~~04~~	~~05~~	~~06~~	07	~~08~~	~~09~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Streiche alle n, für die n durch 5 teilbar sind.

Animation des Siebes von Eratosthenes

~~01~~	~~02~~	~~03~~	~~04~~	~~05~~	~~06~~	~~07~~	~~08~~	~~09~~	10
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	20
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	30
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	40
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	50
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	60
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	70
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	80
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	90
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	100

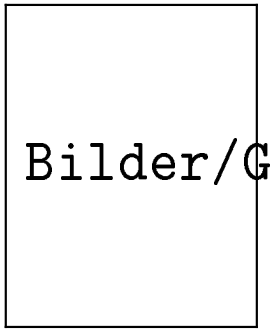
Streiche alle n, für die n durch 7 teilbar sind.

Animation des Siebes von Eratosthenes

~~01~~	~~02~~	~~03~~	~~04~~	~~05~~	~~06~~	~~07~~	~~08~~	~~09~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Ergebnis: Alle Primzahlen $10 < p < 100$

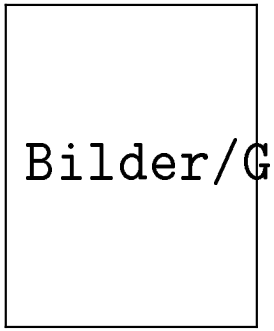
Numerische Beobachtungen



Carl Friedrich Gauß, 1777–1855

Vermutung von Gauß (1849):
Bis zu einer Schranke x gibt es ziemlich genau
$x/\log x$ bzw. $\mathrm{li}(x)$ viele Primzahlen

Numerische Beobachtungen



Carl Friedrich Gauß, 1777–1855

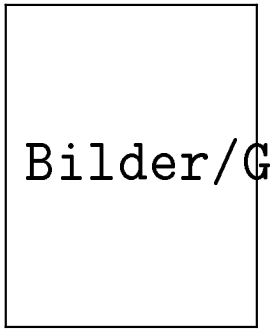
Vermutung von Gauß (1849):
Bis zu einer Schranke x gibt es ziemlich genau
$x/\log x$ bzw. $\mathrm{li}(x)$ viele Primzahlen

$\mathrm{li}(x)$ bezeichnet das logarithmische Integral

$$\mathrm{li}(x) := \int_2^x \frac{dt}{\log t} \approx \frac{x}{\log x},$$

wobei log der natürliche Logarithmus zur Basis $e = 2.71828182845\ldots$ ist.

Numerische Beobachtungen



Carl Friedrich Gauß, 1777–1855

Vermutung von Gauß (1849):
Bis zu einer Schranke x gibt es ziemlich genau
$x/\log x$ bzw. $\mathrm{li}(x)$ viele Primzahlen

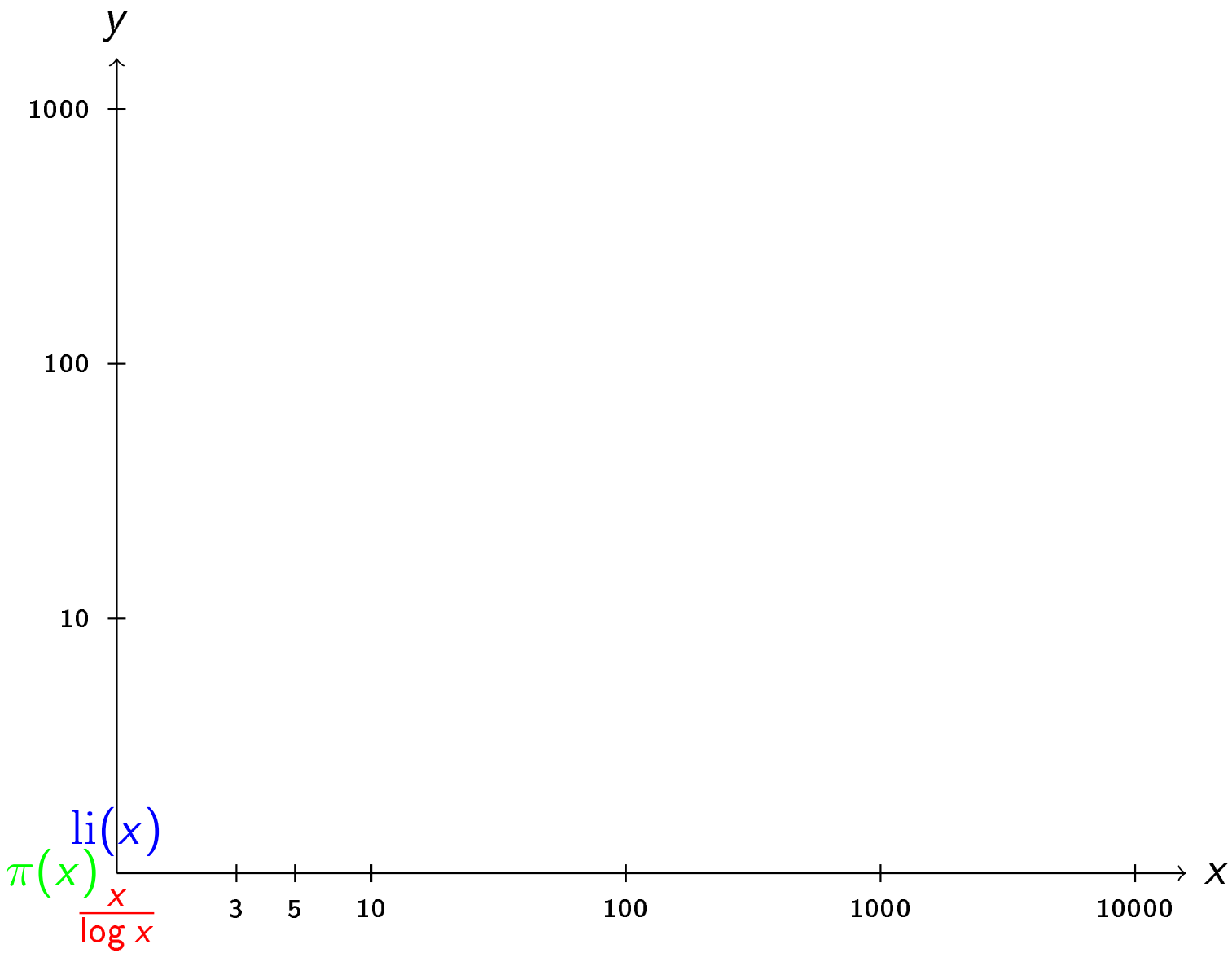
$\mathrm{li}(x)$ bezeichnet das logarithmische Integral

$$\mathrm{li}(x) := \int_2^x \frac{dt}{\log t} \approx \frac{x}{\log x},$$

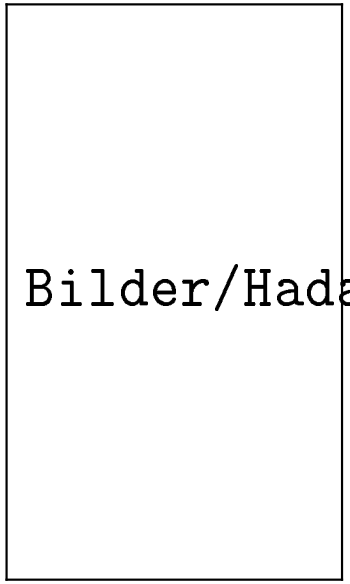
wobei log der natürliche Logarithmus zur Basis $e = 2.71828182845...$ ist.

Die Funktionen $\mathrm{li}(x)$ und $\frac{x}{\log x}$ im Schaubild zusammen mit der Anzahl $\pi(x)$ der Primzahlen $\leq x$:

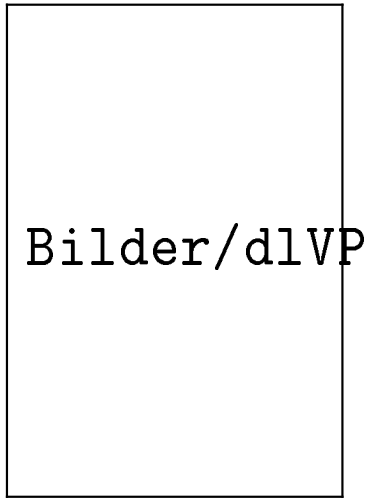
Schaubild von $\pi(x)$, $\mathrm{li}(x)$ und $x/\log x$:



Der Primzahlsatz



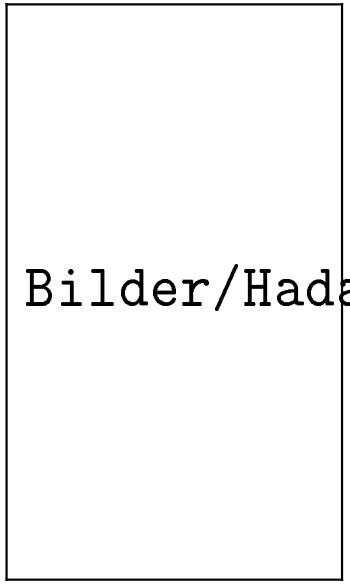
Jacques Hadamard, 1865–1963



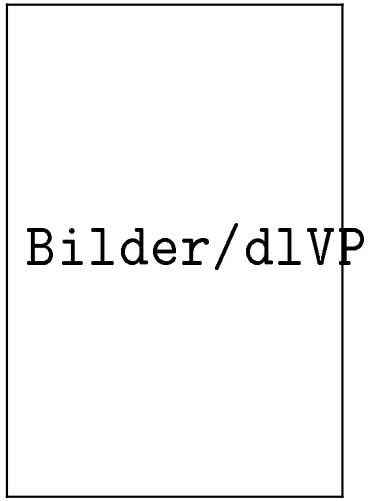
Charles-Louis-Joseph-Xavier de la Vallée-Poussin, 1827–1903

Hadamard und de la Vallée–Poussin (1896):
Beweis der Gaußschen Vermutung, heute bekannt als:

Der Primzahlsatz



Jacques Hadamard, 1865–1963



Charles-Louis-Joseph-Xavier de la Vallée-Poussin, 1827–1903

Hadamard und de la Vallée–Poussin (1896):
Beweis der Gaußschen Vermutung, heute bekannt als:

Primzahlsatz:

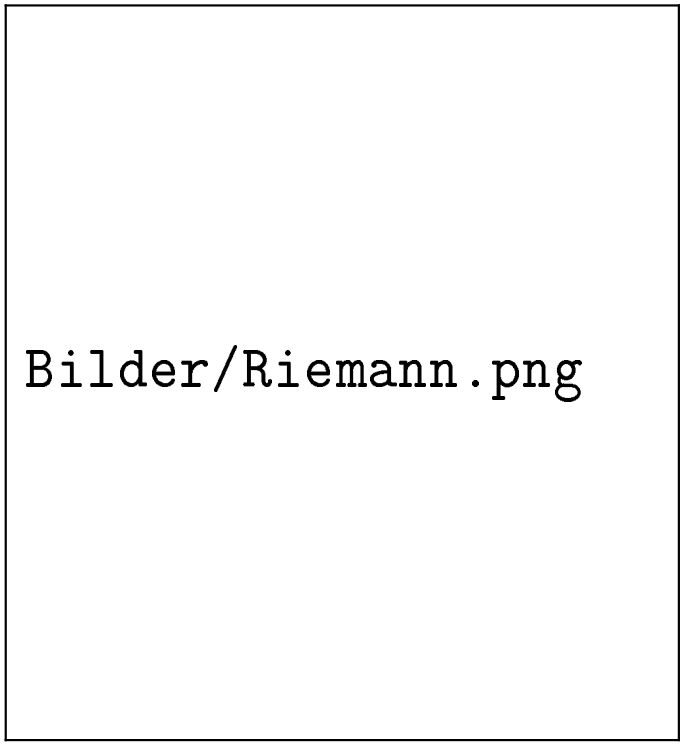
$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1.$$

Die Riemannsche Vermutung

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?

Die Riemannsche Vermutung

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?



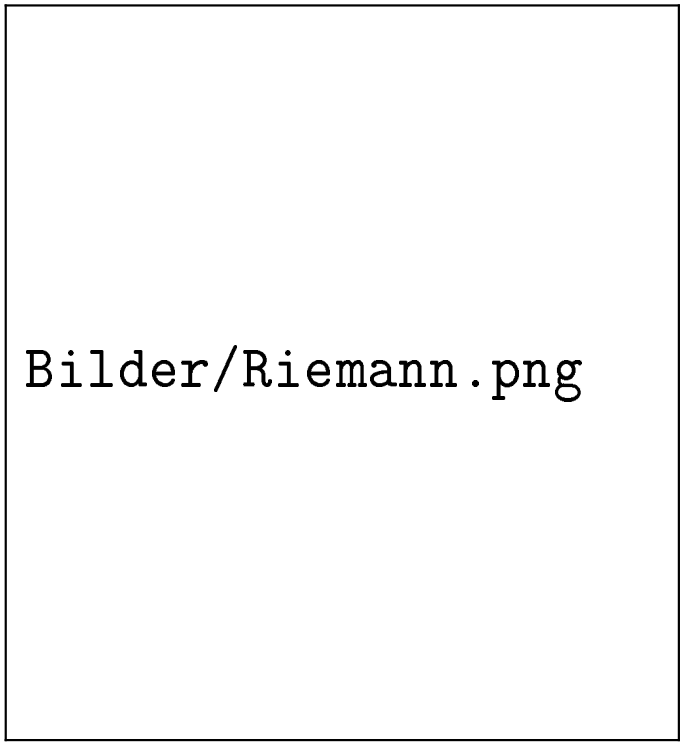
Bernhard Riemann, 1826–1866

Die Riemannsche Vermutung

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?

Riemannsche Vermutung:

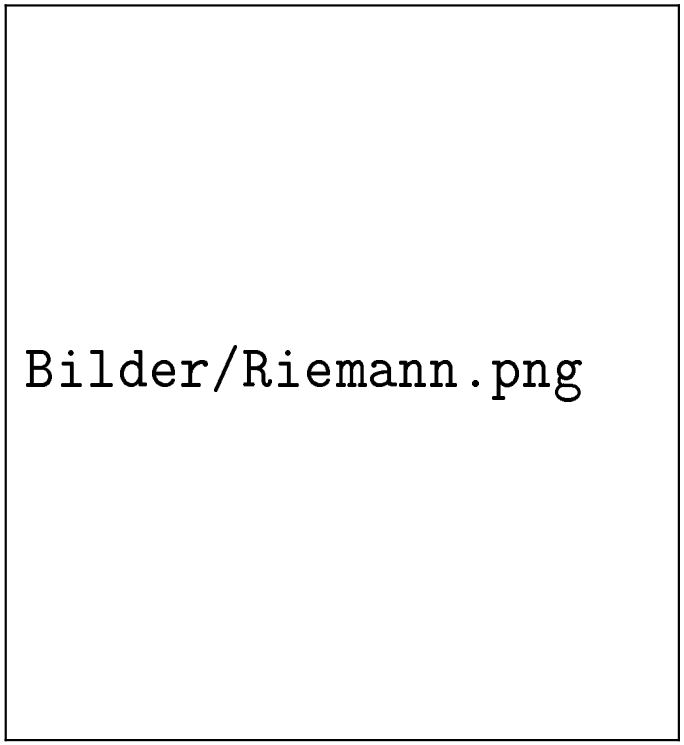
$$|\pi(x) - \mathrm{li}(x)| \leq C\sqrt{x}\log x$$



Bernhard Riemann, 1826–1866

Die Riemannsche Vermutung

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?



Bernhard Riemann, 1826–1866

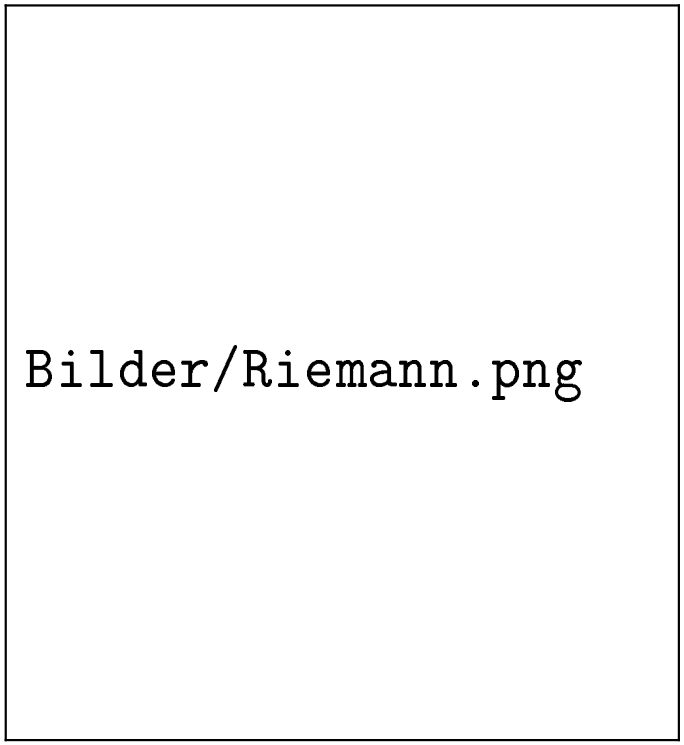
Riemannsche Vermutung:

$$|\pi(x) - \mathrm{li}(x)| \leq C\sqrt{x}\log x$$

Bis heute ungelöst, eines der sieben Millennium-Probleme des Clay Mathematics Institute, die 2000 bekanntgegeben wurden (Preisgeld jeweils: 1 Million US-Dollar)

Die Riemannsche Vermutung

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?



Bernhard Riemann, 1826–1866

Riemannsche Vermutung:

$$|\pi(x) - \mathrm{li}(x)| \leq C\sqrt{x}\log x$$

Bis heute ungelöst, eines der sieben Millennium-Probleme des Clay Mathematics Institute, die 2000 bekanntgegeben wurden (Preisgeld jeweils: 1 Million US-Dollar)

Zum Vergleich das geschätzte Einkommen von George Clooney im Jahr 2020: 170 Millionen US-Dollar

Strukturen und Muster in der Menge der Primzahlen

Wie können Strukturen und Muster in der Menge $\mathbb{P}$ der Primzahlen gefunden und untersucht werden?

Strukturen und Muster in der Menge der Primzahlen

Wie können Strukturen und Muster in der Menge $\mathbb{P}$ der Primzahlen gefunden und untersucht werden?

Strukturen sind interessante Konstellationen endlich vieler natürlicher Zahlen, z. B. Paare mit festem Abstand oder Zahlen in einer Restklasse $\equiv a \bmod q$ (d. h. Zahlen, die alle bei Division durch q denselben Rest a zwischen 0 und $q-1$ lassen)

Strukturen und Muster in der Menge der Primzahlen

Wie können Strukturen und Muster in der Menge $\mathbb{P}$ der Primzahlen gefunden und untersucht werden?

Strukturen sind interessante Konstellationen endlich vieler natürlicher Zahlen, z. B. Paare mit festem Abstand oder Zahlen in einer Restklasse $\equiv a \bmod q$ (d. h. Zahlen, die alle bei Division durch q denselben Rest a zwischen 0 und $q-1$ lassen)

Muster sind sich wiederholende Strukturen in einer beliebigen Teilmenge T der natürlichen Zahlen und sind interessant, wenn sie unendlich oft auftauchen. Dann soll ihre Häufigkeit, mit der diese in T auftreten, auch quantitativ untersucht werden.

Strukturen und Muster in der Menge der Primzahlen

Wie können Strukturen und Muster in der Menge $\mathbb{P}$ der Primzahlen gefunden und untersucht werden?

Strukturen sind interessante Konstellationen endlich vieler natürlicher Zahlen, z. B. Paare mit festem Abstand oder Zahlen in einer Restklasse $\equiv a \bmod q$ (d. h. Zahlen, die alle bei Division durch q denselben Rest a zwischen 0 und $q-1$ lassen)

Muster sind sich wiederholende Strukturen in einer beliebigen Teilmenge T der natürlichen Zahlen und sind interessant, wenn sie unendlich oft auftauchen. Dann soll ihre Häufigkeit, mit der diese in T auftreten, auch quantitativ untersucht werden.

Wir sprechen von Primzahlstrukturen und Primzahlmustern, wenn die untersuchte Menge $T = \mathbb{P}$ ist.

Ein bekanntes Ergebnis zum einfachsten Primzahlmuster: Primzahlen in Restklassen

Satz von Dirichlet (1837):

Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $p \equiv a \bmod q$.

Ein bekanntes Ergebnis zum einfachsten Primzahlmuster: Primzahlen in Restklassen

Satz von Dirichlet (1837):

Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $p \equiv a \bmod q$.

Konsequenz u. a.: Unendlich viele Primzahlen haben jeweils die Endziffer 1, 3, 7, oder 9, und zwar mit einem Anteil von jeweils 25% unter allen Primzahlen (laut Primzahlsatz in arithmetischen Progressionen, der eine quantitative Version des Satzes von Dirichlet darstellt).

Ein bekanntes Ergebnis zum einfachsten Primzahlmuster: Primzahlen in Restklassen

Satz von Dirichlet (1837):

Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $p \equiv a \bmod q$.

Konsequenz u. a.: Unendlich viele Primzahlen haben jeweils die Endziffer 1, 3, 7, oder 9, und zwar mit einem Anteil von jeweils 25% unter allen Primzahlen (laut Primzahlsatz in arithmetischen Progressionen, der eine quantitative Version des Satzes von Dirichlet darstellt).

Analog für andere Basen als 10.

Weitere einfache Primzahlmuster:

Gibt es unendlich viele Primzahlpaare $p, p + 2k$?

(Zwillingsvermutung von de Polignac, 1849)

Weitere einfache Primzahlmuster:

Gibt es unendlich viele Primzahlpaare $p, p + 2k$?

(Zwillingsvermutung von de Polignac, 1849)

Gibt es unendlich viele Sophie-Germain-Primzahlpaare $p, 2p + 1$?

(Sophie Germain, 1805)

Weitere einfache Primzahlmuster:

Gibt es unendlich viele Primzahlpaare $p, p+2k$?

(Zwillingsvermutung von de Polignac, 1849)

Gibt es unendlich viele Sophie-Germain-Primzahlpaare $p, 2p+1$?

(Sophie Germain, 1805)

Ist jede gerade Zahl $n \geq 4$ Summe zweier Primzahlen?
Oder umformuliert: Gibt es für jedes gerade $n \geq 4$ eine Primzahl p so, dass $n-p$ auch prim ist?

(Goldbach-Vermutung, 1742)

Weitere einfache Primzahlmuster:

Gibt es unendlich viele Primzahlpaare $p, p + 2k$?

(Zwillingsvermutung von de Polignac, 1849)

Gibt es unendlich viele Sophie-Germain-Primzahlpaare $p, 2p + 1$?

(Sophie Germain, 1805)

Ist jede gerade Zahl $n \geq 4$ Summe zweier Primzahlen?
Oder umformuliert: Gibt es für jedes gerade $n \geq 4$ eine Primzahl p so, dass $n - p$ auch prim ist?

(Goldbach-Vermutung, 1742)

Wir wissen es nicht!

Bis heute sind diese Fragen unbeantwortet! (Aber alle sind vermutlich mit "Ja" zu beantworten, sogar auf eine sehr präzise Art.)

Eine Vermutung zu linearen Primzahlmustern

Die Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems zu einem gemeinsamen "linearen" Primzahlmusterproblem im Stil des Dirichletschen Satzes ist möglich.

Eine Vermutung zu linearen Primzahlmustern

Die Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems zu einem gemeinsamen "linearen" Primzahlmusterproblem im Stil des Dirichletschen Satzes ist möglich.

Diese heißt Prim-k-Tupel-Vermutung oder auch Vermutung von Dickson-Hardy-Littlewood, kurz "DHL"-Vermutung.

Eine Vermutung zu linearen Primzahlmustern

Die Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems zu einem gemeinsamen "linearen" Primzahlmusterproblem im Stil des Dirichletschen Satzes ist möglich.

Diese heißt Prim-k-Tupel-Vermutung oder auch Vermutung von Dickson-Hardy-Littlewood, kurz "DHL"-Vermutung.

Im Falle der Sophie-Germain-Primzahlen besagt diese Vermutung, dass die Anzahl dieser Primzahlen p (mit $2p+1$ auch prim) bis zu einer Schranke $x > 1$

$$\approx \underbrace{2 \prod_{p>2} \frac{p(p-2)}{(p-1)^2}}_{\approx 1.32032} \cdot \frac{x}{\log^2(x)}$$

beträgt.

Eine Vermutung zu linearen Primzahlmustern

Die Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems zu einem gemeinsamen "linearen" Primzahlmusterproblem im Stil des Dirichletschen Satzes ist möglich.

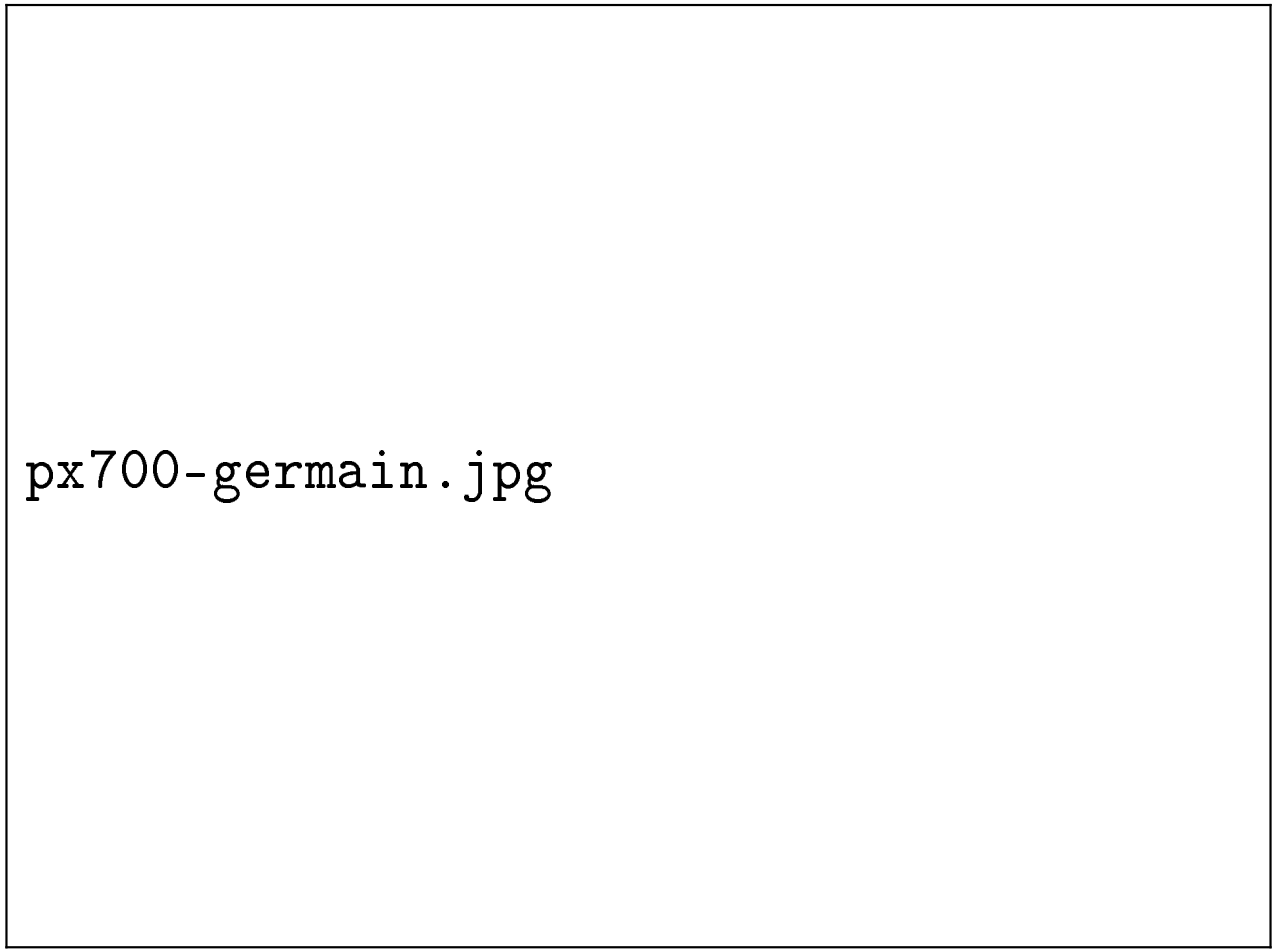
Diese heißt Prim-k-Tupel-Vermutung oder auch Vermutung von Dickson-Hardy-Littlewood, kurz "DHL"-Vermutung.

Im Falle der Sophie-Germain-Primzahlen besagt diese Vermutung, dass die Anzahl dieser Primzahlen p (mit $2p+1$ auch prim) bis zu einer Schranke $x > 1$

$$\approx \underbrace{2 \prod_{p>2} \frac{p(p-2)}{(p-1)^2}}_{\approx 1.32032} \cdot \frac{x}{\log^2(x)}$$

beträgt. Heute spielen Sophie-Germain-Primzahlen eine große Rolle in der Verschlüsselungstechnik und heißen dort "safe primes".

Sophie Germain (1776–1831, Paris)



1805 bewies Sophie Germain, dass der Fermatsche Satz (im sogenannten 1. Fall) für Sophie-Germain-Primzahlen zutrifft.

Siebtheorie

Die genannten ungelösten Probleme können mit der Grundidee des Siebs von Eratosthenes behandelt werden. Die mathematische Behandlung laut Siebtheorie, die als Teilgebiet der additiven Zahlentheorie angesehen wird, bringt quantitative Formulierungen der Vermutungen zutage.
Anhand des Zwillingsproblems zeigen wir, wie Siebtheorie eingesetzt werden kann: Durch eine Abwandlung des Eratosthenes-Siebs.

Siebtheorie

Die genannten ungelösten Probleme können mit der Grundidee des Siebs von Eratosthenes behandelt werden. Die mathematische Behandlung laut Siebtheorie, die als Teilgebiet der additiven Zahlentheorie angesehen wird, bringt quantitative Formulierungen der Vermutungen zutage.
Anhand des Zwillingsproblems zeigen wir, wie Siebtheorie eingesetzt werden kann: Durch eine Abwandlung des Eratosthenes-Siebs.

Gestrichen wird in der Liste der ungeraden Zahlen von 1 bis 199 jede Zahl n, wenn n Vielfaches von p oder wenn $n+2$ Vielfaches von p ist, wobei $p = 3, 5, 7, 11, 13$.

Siebtheorie

Die genannten ungelösten Probleme können mit der Grundidee des Siebs von Eratosthenes behandelt werden. Die mathematische Behandlung laut Siebtheorie, die als Teilgebiet der additiven Zahlentheorie angesehen wird, bringt quantitative Formulierungen der Vermutungen zutage.
Anhand des Zwillingsproblems zeigen wir, wie Siebtheorie eingesetzt werden kann: Durch eine Abwandlung des Eratosthenes-Siebs.

Gestrichen wird in der Liste der ungeraden Zahlen von 1 bis 199 jede Zahl n, wenn n Vielfaches von p oder wenn $n+2$ Vielfaches von p ist, wobei $p = 3, 5, 7, 11, 13$.

Übrig im Sieb bleiben so alle $14 < p < 200$ prim, für die $p+2$ auch prim ist, d. h. genau die Primzahlzwillinge in diesem Bereich.
(Beachten $\sqrt{199} \approx 14.1$)

Animation des Zwillingssiebs

~~001~~ 003 005 007 009 011 013 015 017 019
021 023 025 027 029 031 033 035 037 039
041 043 045 047 049 051 053 055 057 059
061 063 065 057 069 071 073 075 077 079
081 083 085 067 089 091 093 095 097 099
101 103 105 107 109 111 113 115 117 119
121 123 125 127 129 131 133 135 137 139
141 143 145 147 149 151 153 155 157 159
161 163 165 167 169 171 173 175 177 179
181 183 185 187 189 191 193 195 197 199

Animation des Zwillingssiebs

~~001~~ ~~003~~ 005 ~~007~~ ~~009~~ 011 ~~013~~ ~~015~~ 017 ~~019~~
~~021~~ 023 ~~025~~ ~~027~~ 029 ~~031~~ ~~033~~ 035 ~~037~~ ~~039~~
041 ~~043~~ ~~045~~ 047 ~~049~~ ~~051~~ 053 ~~055~~ ~~057~~ 059
~~061~~ ~~063~~ 065 ~~067~~ ~~069~~ 071 ~~073~~ ~~075~~ 077 ~~079~~
~~081~~ 083 ~~085~~ ~~087~~ 089 ~~091~~ ~~093~~ 095 ~~097~~ ~~099~~
101 ~~103~~ ~~105~~ 107 ~~109~~ ~~111~~ 113 ~~115~~ ~~117~~ 119
~~121~~ ~~123~~ 125 ~~127~~ ~~129~~ 131 ~~133~~ ~~135~~ 137 ~~139~~
~~141~~ 143 ~~145~~ ~~147~~ 149 ~~151~~ ~~153~~ 155 ~~157~~ ~~159~~
161 ~~163~~ ~~165~~ 167 ~~169~~ ~~171~~ 173 ~~175~~ ~~177~~ 179
~~181~~ ~~183~~ 185 ~~187~~ ~~189~~ 191 ~~193~~ ~~195~~ 197 ~~199~~

Streiche alle n, für die n oder $n+2$ durch 3 teilbar ist.

Animation des Zwillingssiebs

~~001~~	~~003~~	~~005~~	~~007~~	~~009~~	011	~~013~~	~~015~~	017	~~019~~
~~021~~	~~023~~	~~025~~	~~027~~	029	~~031~~	~~033~~	~~035~~	~~037~~	~~039~~
041	~~043~~	~~045~~	047	~~049~~	~~051~~	~~053~~	~~055~~	~~057~~	059
~~061~~	~~063~~	~~065~~	~~067~~	~~069~~	071	~~073~~	~~075~~	077	~~079~~
~~081~~	~~083~~	~~085~~	~~087~~	089	~~091~~	~~093~~	~~095~~	~~097~~	~~099~~
101	~~103~~	~~105~~	107	~~109~~	~~111~~	~~113~~	~~115~~	~~117~~	119
~~121~~	~~123~~	~~125~~	~~127~~	~~129~~	131	~~133~~	~~135~~	137	~~139~~
~~141~~	~~143~~	~~145~~	~~147~~	149	~~151~~	~~153~~	~~155~~	~~157~~	~~159~~
161	~~163~~	~~165~~	167	~~169~~	~~171~~	~~173~~	~~175~~	~~177~~	179
~~181~~	~~183~~	~~185~~	~~187~~	~~189~~	191	~~193~~	~~195~~	197	~~199~~

Streiche alle n, für die n oder $n+2$ durch 5 teilbar ist.

Animation des Zwillingssiebs

001	003	005	007	009	011	013	015	017	019
021	023	025	027	029	031	033	035	037	039
041	043	045	047	049	051	053	055	057	059
061	063	065	067	069	071	073	075	077	079
081	083	085	087	089	091	093	095	097	099
101	103	105	107	109	111	113	115	117	119
121	123	125	127	129	131	133	135	137	139
141	143	145	147	149	151	153	155	157	159
161	163	165	167	169	171	173	175	177	179
181	183	185	187	189	191	193	195	197	199

Streiche alle n, für die n oder $n+2$ durch 7 teilbar ist.

Animation des Zwillingssiebs

001	003	005	007	009	011	013	015	017	019
021	023	025	027	029	031	033	035	037	039
041	043	045	047	049	051	053	055	057	059
061	063	065	067	069	071	073	075	077	079
081	083	085	087	089	091	093	095	097	099
101	103	105	107	109	111	113	115	117	119
121	123	125	127	129	131	133	135	137	139
141	143	145	147	149	151	153	155	157	159
161	163	165	167	169	171	173	175	177	179
181	183	185	187	189	191	193	195	197	199

Streiche alle n, für die n oder $n+2$ durch 11 teilbar ist.

Animation des Zwillingssiebs

001	003	005	007	009	011	013	015	017	019
021	023	025	027	029	033	035	037	039	
041	043	045	047	049	051	053	055	057	059
061	063	065	067	069	071	073	075	077	079
081	083	085	087	089	091	093	095	097	099
101	103	105	107	109	111	113	115	117	119
121	123	125	127	129	131	133	135	137	139
141	143	145	147	149	151	153	155	157	159
161	163	165	167	169	171	173	175	177	179
181	183	185	187	189	191	193	195	197	199

Streiche alle n, für die n oder $n+2$ durch 13 teilbar ist.

Animation des Zwillingssiebs

001	003	005	007	009	011	013	015	017	019
021	023	025	027	029	031	033	035	037	039
041	043	045	047	049	051	053	055	057	059
061	063	065	067	069	071	073	075	077	079
081	083	085	087	089	091	093	095	097	099
101	103	105	107	109	111	113	115	117	119
121	123	125	127	129	131	133	135	137	139
141	143	145	147	149	151	153	155	157	159
161	163	165	167	169	171	173	175	177	179
181	183	185	187	189	191	193	195	197	199

Ergebnis: Alle $14 < p < 200$ prim, für die $p + 2$ auch prim ist.

Austausch sensibler Daten...

...zwischen zwei Kommunikationspartnern, z. B. über das Internet

Problem: der reine Datenaustausch ist für Unbefugte grundsätzlich stets einsehbar und lesbar, unter Umständen sogar manipulierbar.

- Ein Kunde will ein Produkt in einem online-Shop im Internet einkaufen, dazu müssen etwa die Kreditkartendaten sicher übertragen werden.
- Ein Bankkunde möchte seine Kontodaten online abrufen.
- Ein selbstfahrendes Auto soll Kontakt mit anderen selbstfahrenden Autos aufnehmen.
- Ein Haushaltsgerätehersteller möchte ein Sicherheitsupdate für seine "smarten" Produkte über das WLAN aufspielen.
- Berechtige Personen sollen sich autentifizieren können, etwa durch die Übersendung von Passwörtern.
- Der elektronischen Personalausweis soll die Identifizierung einer Person ermöglichen und nicht manipulierbar sein.
- Sichere Übertragung von Gesundheitsdaten...

Wählen einer Kodierung

In der Kryptographie heißen die beiden Kommunikationspartner immer *Alice* und *Bob*. Alice möchte geheime Daten an Bob senden, etwa einen kurzen Text t (dieser kann auch in Blöcke einer festen Länge b eingeteilt werden).

Wählen einer Kodierung

In der Kryptographie heißen die beiden Kommunikationspartner immer *Alice* und *Bob*. Alice möchte geheime Daten an Bob senden, etwa einen kurzen Text t (dieser kann auch in Blöcke einer festen Länge b eingeteilt werden).

Man benutzt eine Kodierung des verwendeten Alphabets, bei dem jedem Buchstaben genau eine Zahl zugeordnet wird, z. B.:

$$\textit{Leerzeichen} \mapsto \underline{00},\ \mathrm{A} \mapsto \underline{01},\ \mathrm{B} \mapsto \underline{02},\ \mathrm{C} \mapsto \underline{03},\ \ldots,$$
$$\mathrm{Z} \mapsto \underline{26},\ \ddot{\mathrm{A}} \mapsto \underline{27},\ \ddot{\mathrm{O}} \mapsto \underline{28},\ \ddot{\mathrm{U}} \mapsto \underline{29}$$

Jeder Buchstabe des Klartextes t kann so in eine "Ziffer" zwischen $\underline{00}$ und $\underline{29}$ umgewandelt werden (und zurück).

Wählen einer Kodierung

In der Kryptographie heißen die beiden Kommunikationspartner immer *Alice* und *Bob*. Alice möchte geheime Daten an Bob senden, etwa einen kurzen Text t (dieser kann auch in Blöcke einer festen Länge b eingeteilt werden).

Man benutzt eine Kodierung des verwendeten Alphabets, bei dem jedem Buchstaben genau eine Zahl zugeordnet wird, z. B.:

$$\textit{Leerzeichen} \mapsto \underline{00},\ \mathrm{A} \mapsto \underline{01},\ \mathrm{B} \mapsto \underline{02},\ \mathrm{C} \mapsto \underline{03},\ \ldots,$$
$$\mathrm{Z} \mapsto \underline{26},\ \ddot{\mathrm{A}} \mapsto \underline{27},\ \ddot{\mathrm{O}} \mapsto \underline{28},\ \ddot{\mathrm{U}} \mapsto \underline{29}$$

Jeder Buchstabe des Klartextes t kann so in eine "Ziffer" zwischen $\underline{00}$ und $\underline{29}$ umgewandelt werden (und zurück).

Nun soll der Text t buchstabenweise in einen Geheimtext w verschlüsselt werden, so, dass Bob aus w wieder eindeutig t zurückübersetzen kann.

Verschlüsseln mit einem Verschiebeschlüssel

Üblich ist das folgende Verfahren: Alice und Bob besitzen einen gemeinsamen Verschiebeschlüssel s. Dieser ist ein Wort des verwendeten Alphabets einer bestimmten Länge k, also eine Folge $s_1, s_2, \ldots, s_k$ von Ziffern zwischen $\underline{00}$ und $\underline{29}$.

Verschlüsseln mit einem Verschiebeschlüssel

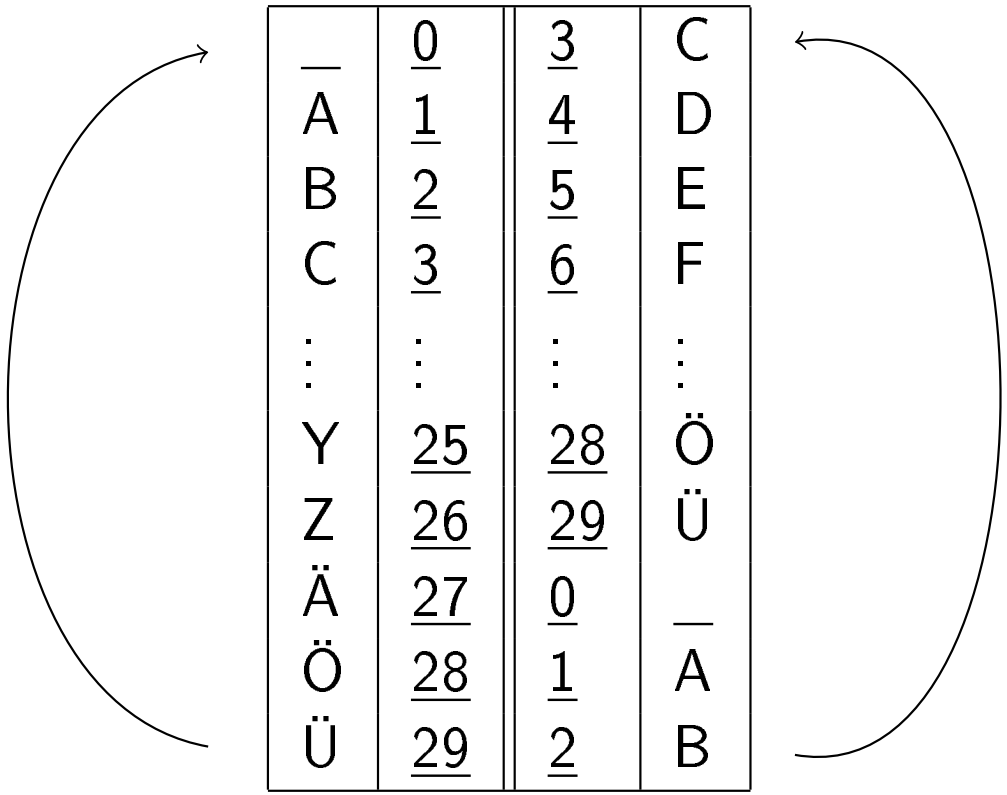
Üblich ist das folgende Verfahren: Alice und Bob besitzen einen gemeinsamen Verschiebeschlüssel s. Dieser ist ein Wort des verwendeten Alphabets einer bestimmten Länge k, also eine Folge $s_1, s_2, \ldots, s_k$ von Ziffern zwischen $\underline{00}$ und $\underline{29}$.

Jeder Buchstabe des Verschiebeschlüssels besagt, um wieviele Buchstaben das Alphabet verschoben werden muss, um den verschlüsselten Buchstaben zu bekommen (ev. zyklisch).
Bsp.: s =GEHEIM= $\underline{7}, \underline{5}, \underline{8}, \underline{5}, \underline{9}, \underline{13}$ mit $k = 6$

t_j	E	C	H	T	E	R	_	T	E	X	T
z_j	$\underline{05}$	$\underline{03}$	$\underline{08}$	$\underline{20}$	$\underline{05}$	$\underline{18}$	$\underline{00}$	$\underline{20}$	$\underline{05}$	$\underline{24}$	$\underline{20}$
s	G	E	H	E	I	M	G	E	H	E	I
s_j	+7	+5	+8	+5	+9	+13	+7	+5	+8	+5	+9
v_j	$\underline{12}$	$\underline{8}$	$\underline{16}$	$\underline{25}$	$\underline{14}$	$\underline{31} = \underline{1}$	$\underline{7}$	$\underline{25}$	$\underline{13}$	$\underline{29}$	$\underline{29}$
w_j	L	H	P	Y	N	A	G	Y	M	Ü	Ü

Zyklische Alphabet-Verschiebung im Beispiel

Hier wird die Verschiebung um $s_1 = \underline{03} = C$ dargestellt:



_	0	3	C
A	1	4	D
B	2	5	E
C	3	6	F
⋮	⋮	⋮	⋮
Y	25	28	Ö
Z	26	29	Ü
Ä	27	0	_
Ö	28	1	A
Ü	29	2	B

Verwendete zyklische Struktur

Die Zahlenuhr mit den Ziffern von $\underline{0}$ bis $\underline{n-1}$ (im Bsp. $n = 30$) heißt Restklassenring modulo n und wird in der Mathematik mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet.

Verwendete zyklische Struktur

Die Zahlenuhr mit den Ziffern von $\underline{0}$ bis $\underline{n-1}$ (im Bsp. $n = 30$) heißt Restklassenring modulo n und wird in der Mathematik mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet. Wir vereinbaren, dass wir auch dann $\underline{\ell}$ für eine Ziffer schreiben wollen, wenn m eine natürliche Zahl $> n$ ist, es soll $\underline{\ell} = \underline{k}$ sein, wenn k der Rest der Division von m durch n ist, der zwischen 0 und $n-1$ liegt. (Bsp. $\underline{32} = \underline{2}$ für $n = 30$.)

Verwendete zyklische Struktur

Die Zahlenuhr mit den Ziffern von $\underline{0}$ bis $\underline{n-1}$ (im Bsp. $n = 30$) heißt Restklassenring modulo n und wird in der Mathematik mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet. Wir vereinbaren, dass wir auch dann $\underline{\ell}$ für eine Ziffer schreiben wollen, wenn m eine natürliche Zahl $> n$ ist, es soll $\underline{\ell} = \underline{k}$ sein, wenn k der Rest der Division von m durch n ist, der zwischen 0 und $n-1$ liegt. (Bsp. $\underline{32} = \underline{2}$ für $n = 30$.)

$$\underline{\ell} = \underline{k} \;\Leftrightarrow\; \ell \equiv k \bmod n$$

Die Restklassen mod n (also anschaulich die Ziffern auf der Uhr) können addiert, multipliziert, sogar potenziert werden:

$$\underline{\ell} + \underline{k} := \underline{\ell + k}, \quad \underline{\ell} \cdot \underline{k} := \underline{\ell \cdot k}, \quad \underline{\ell}^{\,k} := \underline{\ell^k}$$

Es gelten die für Zahlen üblichen Rechengesetze...

Satz: Genau wenn $n = p$ eine Primzahl ist, kann uneingeschränkt durch Restklassen $\neq \underline{0}$ dividiert werden.

Der Verschiebe-Schlüssel ist eine geheime Zeichenkette

Die Verschlüsselung gilt als sicher, wenn der Verschiebeschlüssel s aus zufälligen Buchstaben besteht und darüberhinaus mindestens so lang wie die Botschaft/Block ist, oder wenigstens so lang, dass durch statistische Ermittlungen ein Rückschluss auf den Klartext der Botschaft praktisch unmöglich ist.

Der Verschiebe-Schlüssel ist eine geheime Zeichenkette

Die Verschlüsselung gilt als sicher, wenn der Verschiebeschlüssel s aus zufälligen Buchstaben besteht und darüberhinaus mindestens so lang wie die Botschaft/Block ist, oder wenigstens so lang, dass durch statistische Ermittlungen ein Rückschluss auf den Klartext der Botschaft praktisch unmöglich ist.

Problem: Wie können sich Alice und Bob vor ihrer Kommunikation auf eine gemeinsame geheime Zeichenkette einigen?
Ein solches geheimes Wort müsste ja auch gesendet werden!

Der Verschiebe-Schlüssel ist eine geheime Zeichenkette

Die Verschlüsselung gilt als sicher, wenn der Verschiebeschlüssel s aus zufälligen Buchstaben besteht und darüberhinaus mindestens so lang wie die Botschaft/Block ist, oder wenigstens so lang, dass durch statistische Ermittlungen ein Rückschluss auf den Klartext der Botschaft praktisch unmöglich ist.

Problem: Wie können sich Alice und Bob vor ihrer Kommunikation auf eine gemeinsame geheime Zeichenkette einigen?
Ein solches geheimes Wort müsste ja auch gesendet werden!

Lösung: Die Mathematik kennt eine Möglichkeit, dass sich Alice und Bob auf eine gemeinsame Zahl s (also ein gemeinsames Wort) einigen können, ohne dass es jemals übersendet werden muss!

Der Verschiebe-Schlüssel ist eine geheime Zeichenkette

Die Verschlüsselung gilt als sicher, wenn der Verschiebeschlüssel s aus zufälligen Buchstaben besteht und darüberhinaus mindestens so lang wie die Botschaft/Block ist, oder wenigstens so lang, dass durch statistische Ermittlungen ein Rückschluss auf den Klartext der Botschaft praktisch unmöglich ist.

Problem: Wie können sich Alice und Bob vor ihrer Kommunikation auf eine gemeinsame geheime Zeichenkette einigen?
Ein solches geheimes Wort müsste ja auch gesendet werden!

Lösung: Die Mathematik kennt eine Möglichkeit, dass sich Alice und Bob auf eine gemeinsame Zahl s (also ein gemeinsames Wort) einigen können, ohne dass es jemals übersendet werden muss!

Sie glauben, das geht nicht? Doch, geht!

Die Diffie-Hellmann-Schlüsselerzeugung: Vorbereitung

Alice und Bob einigen sich (öffentlich) auf eine (multiplikative) Gruppe G und einen Erzeuger x, d. h. jedes Element a von G ist als eine Potenz von x schreibbar.

Die Diffie-Hellmann-Schlüsselerzeugung: Vorbereitung

Alice und Bob einigen sich (öffentlich) auf eine (multiplikative) Gruppe G und einen Erzeuger x, d. h. jedes Element a von G ist als eine Potenz von x schreibbar.

Die Auffindung von Erzeugern ist allerdings sehr schwer. Am besten nimmt man anstelle G die von einem Element x erzeugte Untergruppe der Potenzen $\{x, x^2, \ldots, x^{n-1}, 1\}$, wenn n minimal mit $x^n = 1$ in G ist.

Die Diffie-Hellmann-Schlüsselerzeugung: Vorbereitung

Alice und Bob einigen sich (öffentlich) auf eine (multiplikative) Gruppe G und einen Erzeuger x, d. h. jedes Element a von G ist als eine Potenz von x schreibbar.

Die Auffindung von Erzeugern ist allerdings sehr schwer. Am besten nimmt man anstelle G die von einem Element x erzeugte Untergruppe der Potenzen $\{x, x^2, \ldots, x^{n-1}, 1\}$, wenn n minimal mit $x^n = 1$ in G ist.

Z. B. haben die Gruppen $G_p = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\underline{0}\}$ für jede Primzahl p mindestens einen Erzeuger ("Primitivwurzel").

Die Diffie-Hellmann-Schlüsselerzeugung: Vorbereitung

Alice und Bob einigen sich (öffentlich) auf eine (multiplikative) Gruppe G und einen Erzeuger x, d. h. jedes Element a von G ist als eine Potenz von x schreibbar.

Die Auffindung von Erzeugern ist allerdings sehr schwer. Am besten nimmt man anstelle G die von einem Element x erzeugte Untergruppe der Potenzen $\{x, x^2, \ldots, x^{n-1}, 1\}$, wenn n minimal mit $x^n = 1$ in G ist.

Z. B. haben die Gruppen $G_p = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\underline{0}\}$ für jede Primzahl p mindestens einen Erzeuger ("Primitivwurzel").

(Für $p = 31$ ist beispielsweise $x = \underline{17}$ ein Erzeuger. Die Gruppe $(\mathbb{Z}/30\mathbb{Z}) \setminus \{\underline{0}\}$ hat keinen Erzeuger. Die Gruppe $(\mathbb{Z}/9\mathbb{Z}) \setminus \{\underline{0}\}$ mit zusammengesetzten Modul hat den Erzeuger $x = \underline{2}$.)

Die Diffie-Hellmann-Schlüsselerzeugung: Durchführung

(Öffentlich) gegeben: Gruppe G, Erzeuger x.

Die Diffie-Hellmann-Schlüsselerzeugung: Durchführung

(Öffentlich) gegeben: Gruppe G, Erzeuger x.

1. Schritt: Alice denkt sich eine Zahl a zwischen 0 und $n-1$ und schickt x^a an Bob. Geheim: a, öffentlich: x^a. Bob denkt sich eine Zahl b zwischen 0 und $n-1$ und schickt x^b an Alice. Geheim: b, öffentlich: x^b.

Die Diffie-Hellmann-Schlüsselerzeugung: Durchführung

(Öffentlich) gegeben: Gruppe G, Erzeuger x.

1. Schritt: Alice denkt sich eine Zahl a zwischen 0 und $n-1$ und schickt x^a an Bob. Geheim: a, öffentlich: x^a. Bob denkt sich eine Zahl b zwischen 0 und $n-1$ und schickt x^b an Alice. Geheim: b, öffentlich: x^b.

2. Schritt: Alice berechnet mit a das Gruppenelement $(x^b)^a$. Bob berechnet mit b das Gruppenelement $(x^a)^b$.

Die Diffie-Hellmann-Schlüsselerzeugung: Durchführung

(Öffentlich) gegeben: Gruppe G, Erzeuger x.

1. Schritt: Alice denkt sich eine Zahl a zwischen 0 und $n-1$ und schickt x^a an Bob. Geheim: a, öffentlich: x^a. Bob denkt sich eine Zahl b zwischen 0 und $n-1$ und schickt x^b an Alice. Geheim: b, öffentlich: x^b.

2. Schritt: Alice berechnet mit a das Gruppenelement $(x^b)^a$. Bob berechnet mit b das Gruppenelement $(x^a)^b$.

Dann ist $(x^a)^b = x^{ab} = x^{ba} = (x^b)^a$, also kennen Alice und Bob dieses gemeinsame geheime Gruppenelement, das sie s nennen und anschließend zur verschlüsselten Kommunikation verwenden. Dabei wurde $s = x^{ab}$ niemals gesendet!

Der diskrete Logarithmus

Kann aus Abhören der Zahl $y = x^a$ oder $z = x^b$ auf die geheimen Daten $s = x^{ab}$, a bzw. b geschlossen werden?

Der diskrete Logarithmus

Kann aus Abhören der Zahl $y = x^a$ oder $z = x^b$ auf die geheimen Daten $s = x^{ab}$, a bzw. b geschlossen werden?

Die Zahl a mit $x^a = y$ heißt diskreter Logarithmus von y (in G, bzw. zum Erzeuger x modulo p in $\mathbb{Z}/p\mathbb{Z}$.)

Der diskrete Logarithmus

Kann aus Abhören der Zahl $y = x^a$ oder $z = x^b$ auf die geheimen Daten $s = x^{ab}$, a bzw. b geschlossen werden?

Die Zahl a mit $x^a = y$ heißt diskreter Logarithmus von y (in G, bzw. zum Erzeuger x modulo p in $\mathbb{Z}/p\mathbb{Z}$.)

Die Berechnung des diskreten Logarithmus in $\mathbb{Z}/p\mathbb{Z}$ ist ein schwieriges mathematisches Problem, wenn p sehr groß ist.

Der diskrete Logarithmus

Kann aus Abhören der Zahl $y = x^a$ oder $z = x^b$ auf die geheimen Daten $s = x^{ab}$, a bzw. b geschlossen werden?

Die Zahl a mit $x^a = y$ heißt diskreter Logarithmus von y (in G, bzw. zum Erzeuger x modulo p in $\mathbb{Z}/p\mathbb{Z}$.)

Die Berechnung des diskreten Logarithmus in $\mathbb{Z}/p\mathbb{Z}$ ist ein schwieriges mathematisches Problem, wenn p sehr groß ist.

Ein paar hundert Stellen reichen für p aus, damit die Berechnung mit bekannten Algorithmen auf einem klassischen Computer einige tausend Jahre bräuchte!

Der diskrete Logarithmus

Kann aus Abhören der Zahl $y = x^a$ oder $z = x^b$ auf die geheimen Daten $s = x^{ab}$, a bzw. b geschlossen werden?

Die Zahl a mit $x^a = y$ heißt diskreter Logarithmus von y (in G, bzw. zum Erzeuger x modulo p in $\mathbb{Z}/p\mathbb{Z}$.)

Die Berechnung des diskreten Logarithmus in $\mathbb{Z}/p\mathbb{Z}$ ist ein schwieriges mathematisches Problem, wenn p sehr groß ist.

Ein paar hundert Stellen reichen für p aus, damit die Berechnung mit bekannten Algorithmen auf einem klassischen Computer einige tausend Jahre bräuchte!

Die verschlüsselte Kommunikation mit dem Diffie–Hellmann-Verfahren in $\mathbb{Z}/p\mathbb{Z}$ ist also um so sicherer, je größere Primzahlen p man nimmt. Allzu groß darf p natürlich auch nicht sein, damit die Schlüsselerzeugung, d. h. das Potenzieren in der Gruppe nicht zu rechenintensiv wird.

Safe primes – Sichere Primzahlen

Zur praktischen Umsetzung und Machbarkeit des Diffie–Hellmann-Verfahrens spielt die benutzte Rechenstruktur, also die verwendete Gruppe G, eine große Rolle.

Safe primes – Sichere Primzahlen

Zur praktischen Umsetzung und Machbarkeit des Diffie–Hellmann-Verfahrens spielt die benutzte Rechenstruktur, also die verwendete Gruppe G, eine große Rolle.

Betrachten wir $\mathbb{Z}/p'\mathbb{Z}$, wenn $p' = 2p + 1$ prim, also p eine Sophie-Germain-Primzahl ist. Dann hat $\mathbb{Z}/p'\mathbb{Z}$ eine Untergruppe G mit p Elementen, also vergleichsweise groß im Vergleich zum Modul p', bzw. der Modul p' ist vergleichsweise klein.

Safe primes – Sichere Primzahlen

Zur praktischen Umsetzung und Machbarkeit des Diffie–Hellmann-Verfahrens spielt die benutzte Rechenstruktur, also die verwendete Gruppe G, eine große Rolle.

Betrachten wir $\mathbb{Z}/p'\mathbb{Z}$, wenn $p' = 2p + 1$ prim, also p eine Sophie-Germain-Primzahl ist. Dann hat $\mathbb{Z}/p'\mathbb{Z}$ eine Untergruppe G mit p Elementen, also vergleichsweise groß im Vergleich zum Modul p', bzw. der Modul p' ist vergleichsweise klein.

Man nennt dann p' safe prime, also eine sichere Primzahl. Diese sind außerordentlich gut geeignet zur Verschlüsselung.

Safe primes – Sichere Primzahlen

Zur praktischen Umsetzung und Machbarkeit des Diffie–Hellmann-Verfahrens spielt die benutzte Rechenstruktur, also die verwendete Gruppe G, eine große Rolle.

Betrachten wir $\mathbb{Z}/p'\mathbb{Z}$, wenn $p' = 2p + 1$ prim, also p eine Sophie-Germain-Primzahl ist. Dann hat $\mathbb{Z}/p'\mathbb{Z}$ eine Untergruppe G mit p Elementen, also vergleichsweise groß im Vergleich zum Modul p', bzw. der Modul p' ist vergleichsweise klein.

Man nennt dann p' safe prime, also eine sichere Primzahl. Diese sind außerordentlich gut geeignet zur Verschlüsselung.

Die Auffindung solcher Primzahlen ist etwas schwieriger als die Auffindung irgendwelcher Primzahlen bestimmter Größe, mit dem Aufkommen immer schnellerer Rechner aber heute gut machbar.

Safe primes – Sichere Primzahlen

Zur praktischen Umsetzung und Machbarkeit des Diffie–Hellmann-Verfahrens spielt die benutzte Rechenstruktur, also die verwendete Gruppe G, eine große Rolle.

Betrachten wir $\mathbb{Z}/p'\mathbb{Z}$, wenn $p' = 2p + 1$ prim, also p eine Sophie-Germain-Primzahl ist. Dann hat $\mathbb{Z}/p'\mathbb{Z}$ eine Untergruppe G mit p Elementen, also vergleichsweise groß im Vergleich zum Modul p', bzw. der Modul p' ist vergleichsweise klein.

Man nennt dann p' safe prime, also eine sichere Primzahl. Diese sind außerordentlich gut geeignet zur Verschlüsselung.

Die Auffindung solcher Primzahlen ist etwas schwieriger als die Auffindung irgendwelcher Primzahlen bestimmter Größe, mit dem Aufkommen immer schnellerer Rechner aber heute gut machbar.

Zur Einschätzung, wie sicher die Verwendung von G ist, sind u. a. die vermutete Häufigkeit dieser Primzahlen entscheidend, nämlich genau die quantitative Vermutung von oben.

Andere geeignete Gruppen: Punkte elliptischer Kurven

Welche Gruppen eignen sich noch für sensible Kryptograpie-Anwendungen?

Andere geeignete Gruppen: Punkte elliptischer Kurven

Welche Gruppen eignen sich noch für sensible Kryptograpie-Anwendungen?

Neben Restklassengruppen eignen sich weiter die Gruppen der Punkte auf elliptischen Kurven.

Andere geeignete Gruppen: Punkte elliptischer Kurven

Welche Gruppen eignen sich noch für sensible Kryptograpie-Anwendungen?

Neben Restklassengruppen eignen sich weiter die Gruppen der Punkte auf elliptischen Kurven.

Eine elliptische Kurve $E(K)$ über einem Körper K, etwa $K = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p, ist eine nichtsinguläre, irreduzible projektive Kurve vom Grad 3, die einen K-rationalen Wendepunkt enthält.

Andere geeignete Gruppen: Punkte elliptischer Kurven

Welche Gruppen eignen sich noch für sensible Kryptograpie-Anwendungen?

Neben Restklassengruppen eignen sich weiter die Gruppen der Punkte auf elliptischen Kurven.

Eine elliptische Kurve $E(K)$ über einem Körper K, etwa $K = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p, ist eine nichtsinguläre, irreduzible projektive Kurve vom Grad 3, die einen K-rationalen Wendepunkt enthält.

Für die meisten elliptischen Kurven gibt es die vereinfachte Form nach Weierstraß:

$$E_{a,b}(K) = \{(x, y) \in K^2;\ y^2 = x^3 + ax + b\}$$

mit geeigneten $a, b \in K$ als Kurvenparametern.
Solche Gruppen werden heutzutage im großen Stil "industriell" für kryptographische Zwecke genutzt.

Vorteile elliptischer Kurven

Vorteile der elliptischen Kurven-Gruppen gegenüber Restklassengruppen:

- schnell berechenbare Verknüpfung "+" der Punkte, rechnerisch leicht umsetzbar, damit perfekt geeignet für technische Systeme und (billige) Hardware mit wenig Rechenressourcen (z. B. Chips in Smart-Cards ohne Koprozessor).
- viel kürzere Schlüssellänge für ausreichende Sicherheit nötig (die verwendeten Schlüssel S sind bei einem EC-Verfahren nur etwa so groß wie die dritte Wurzel eines Schlüssels bei einer Verschlüsselung mit einer Restklassengruppe bei gleicher Sicherheit)
- Speicheraufwand ist (grob geschätzt) um 1/3 kleiner

Nachteile elliptischer Kurven

Nachteile der elliptischen Kurven-Gruppen gegenüber Restklassengruppen:

- gelegentlich werden bestimmte Klassen von elliptischen Kurven entdeckt, für die das diskrete Logarithmus-Problem leicht gelöst werden kann, so dass sich diese Kurven danach nicht mehr zu kryptographischen Zwecken eignen (z.B. supersinguläre oder anomale Kurven).
- Implementationen sind patentiert
- Kurvenparameter werden von verschiedenen Organisationen veröffentlicht und empfohlen:
  • NIST = U.S.-National Institute for Standards and Technology
  • SECG = Standards for Efficient Cryptography Group
  • BSI = Bundesamt für Sicherheit in der Informationstechnik

Andere Kryptographieverfahren, z.B. RSA

Andere verwendete Verschlüsselungsmethoden wie z. B. das bekannte RSA-Verschlüsselungsverfahren beruhen nicht auf dem Berechnungsproblem des diskreten Logarithmus, sondern dem

Andere Kryptographieverfahren, z.B. RSA

Andere verwendete Verschlüsselungsmethoden wie z. B. das bekannte RSA-Verschlüsselungsverfahren beruhen nicht auf dem Berechnungsproblem des diskreten Logarithmus, sondern dem

Faktorisierungsproblem: Für eine große zusammengesetzte Zahl n finde man echte Teiler t von n mit $1 < t < n$.

Andere Kryptographieverfahren, z.B. RSA

Andere verwendete Verschlüsselungsmethoden wie z. B. das bekannte RSA-Verschlüsselungsverfahren beruhen nicht auf dem Berechnungsproblem des diskreten Logarithmus, sondern dem

Faktorisierungsproblem: Für eine große zusammengesetzte Zahl n finde man echte Teiler t von n mit $1 < t < n$.

Die Faktorisierung großer Zahlen ist schwer!

Andere Kryptographieverfahren, z.B. RSA

Andere verwendete Verschlüsselungsmethoden wie z. B. das bekannte RSA-Verschlüsselungsverfahren beruhen nicht auf dem Berechnungsproblem des diskreten Logarithmus, sondern dem

Faktorisierungsproblem: Für eine große zusammengesetzte Zahl n finde man echte Teiler t von n mit $1 < t < n$.

Die Faktorisierung großer Zahlen ist schwer!

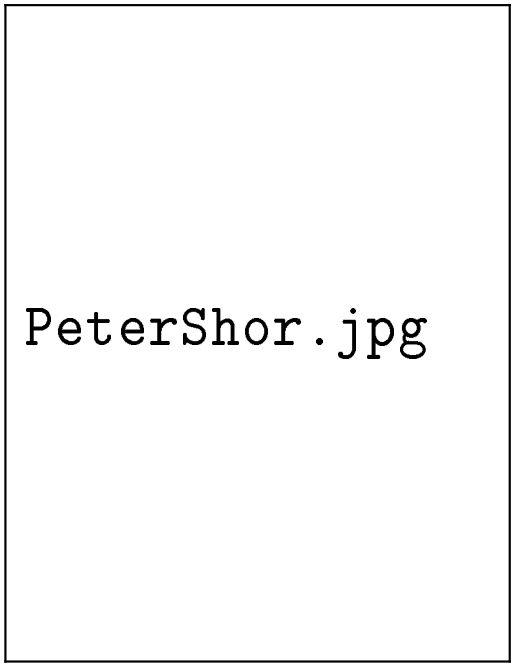
Der beste bekannte Algorithmus zur Auffindung eines echten Teilers einer Zahl n ist das Zahlkörpersieb und hat eine Laufzeit von

$$\exp(C(\log n)^{1/3}(\log\log n)^{2/3}))$$

Damit ist das RSA-Verfahren zwar sicher, wenn die Schlüssel lang genug sind. Für bestimmte (Hardware-)Anwendungen ist es aber zu langsam, da zu rechenintensiv.

Aufkommen der Quantencomputer

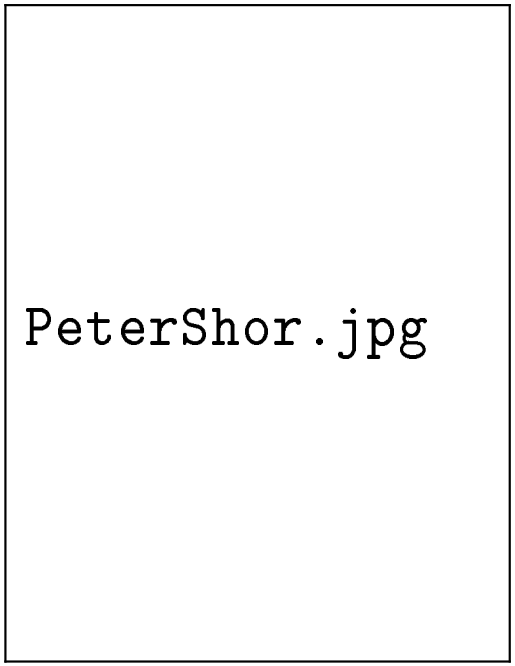
Peter Shor zeigte im Jahr 1994: Ein Quantencomputer benötigt zur Faktorisierung großer Zahlen (Sicherheit bei RSA) und zur Berechnung eines diskreten Logarithmus in einer Restklassengruppe (Sicherheit bei Diffie-Hellmann) nur wenige Sekunden...



Peter Shor

Aufkommen der Quantencomputer

Peter Shor zeigte im Jahr 1994: Ein Quantencomputer benötigt zur Faktorisierung großer Zahlen (Sicherheit bei RSA) und zur Berechnung eines diskreten Logarithmus in einer Restklassengruppe (Sicherheit bei Diffie-Hellmann) nur wenige Sekunden...

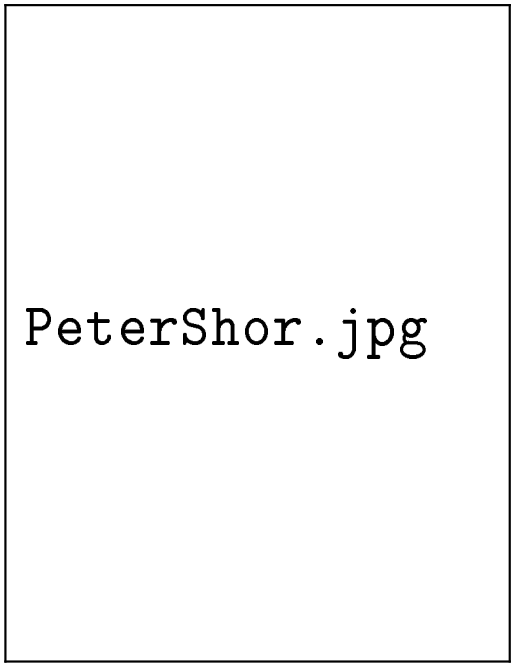


Peter Shor

- Er gab einen Algorithmus an, der im Rahmen der Quantenmechanik durch Kombination bestimmter Sätze der Mathematik formuliert werden kann.

Aufkommen der Quantencomputer

Peter Shor zeigte im Jahr 1994: Ein Quantencomputer benötigt zur Faktorisierung großer Zahlen (Sicherheit bei RSA) und zur Berechnung eines diskreten Logarithmus in einer Restklassengruppe (Sicherheit bei Diffie-Hellmann) nur wenige Sekunden...



Peter Shor

- Er gab einen Algorithmus an, der im Rahmen der Quantenmechanik durch Kombination bestimmter Sätze der Mathematik formuliert werden kann.
- Er wurde für seine Entdeckungen 1998 auf der ICM in Berlin mit dem Nevanlinna-Preis ausgezeichnet.

Aufkommen der Quantencomputer

Peter Shor zeigte im Jahr 1994: Ein Quantencomputer benötigt zur Faktorisierung großer Zahlen (Sicherheit bei RSA) und zur Berechnung eines diskreten Logarithmus in einer Restklassengruppe (Sicherheit bei Diffie-Hellmann) nur wenige Sekunden...

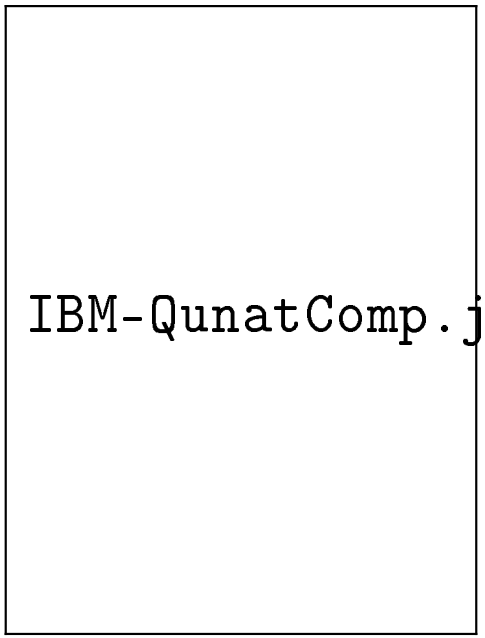
PeterShor.jpg

Peter Shor

- Er gab einen Algorithmus an, der im Rahmen der Quantenmechanik durch Kombination bestimmter Sätze der Mathematik formuliert werden kann.
- Er wurde für seine Entdeckungen 1998 auf der ICM in Berlin mit dem Nevanlinna-Preis ausgezeichnet.
- Mittlerweile werden erste Prototypen entwickelt, obwohl Quantencomputer bei -273°C (fast absolut Null) operieren.

Erste Prototypen der Quantencomputer

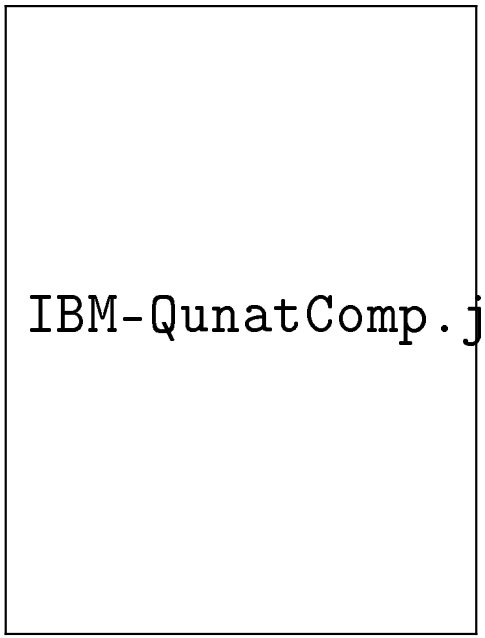
Quantencomputer funktionieren anders als klassische Computer. Sie nutzen Quanteneffekte sehr kalter Atome. Sie können als kleinste Informationseinheit qubits benutzen, die 0, 1 und einen Superpositionszustand dazwischen annehmen können. Bei Messungen nehmen sie die Werte 0 oder 1 an. Klassische Computer rechnen mit bits, die jeweils entweder 0 oder 1 sind.



IBM Quantencomputer

Erste Prototypen der Quantencomputer

Quantencomputer funktionieren anders als klassische Computer. Sie nutzen Quanteneffekte sehr kalter Atome. Sie können als kleinste Informationseinheit qubits benutzen, die 0, 1 und einen Superpositionszustand dazwischen annehmen können. Bei Messungen nehmen sie die Werte 0 oder 1 an. Klassische Computer rechnen mit bits, die jeweils entweder 0 oder 1 sind.

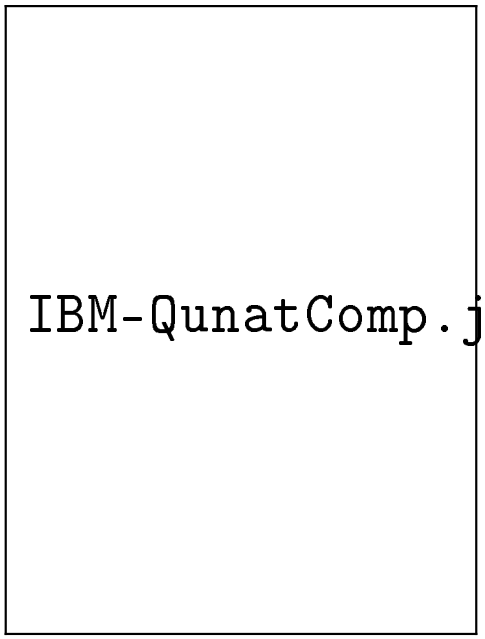


IBM Quantencomputer

Google und IBM haben jeweils bereits einen funktionsfähigen Quantencomputer gebaut.

Erste Prototypen der Quantencomputer

Quantencomputer funktionieren anders als klassische Computer. Sie nutzen Quanteneffekte sehr kalter Atome. Sie können als kleinste Informationseinheit qubits benutzen, die 0, 1 und einen Superpositionszustand dazwischen annehmen können. Bei Messungen nehmen sie die Werte 0 oder 1 an. Klassische Computer rechnen mit bits, die jeweils entweder 0 oder 1 sind.

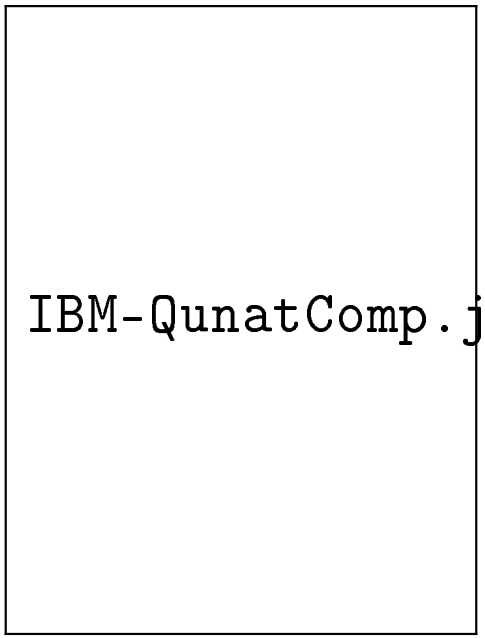


IBM Quantencomputer

Google und IBM haben jeweils bereits einen funktionsfähigen Quantencomputer gebaut.
Im Oktober 2019 gab Google bekannt, die sogenannte "quantum supremacy" überwunden zu haben, was von IBM bezweifelt wird.

Erste Prototypen der Quantencomputer

Quantencomputer funktionieren anders als klassische Computer. Sie nutzen Quanteneffekte sehr kalter Atome. Sie können als kleinste Informationseinheit qubits benutzen, die 0, 1 und einen Superpositionszustand dazwischen annehmen können. Bei Messungen nehmen sie die Werte 0 oder 1 an. Klassische Computer rechnen mit bits, die jeweils entweder 0 oder 1 sind.



IBM Quantencomputer

Google und IBM haben jeweils bereits einen funktionsfähigen Quantencomputer gebaut.
Im Oktober 2019 gab Google bekannt, die sogenannte "quantum supremacy" überwunden zu haben, was von IBM bezweifelt wird.
Der Quantencomputer "Q System One" von IBM soll 2021 nach Deutschland kommen, nämlich in die deutsche IBM-Zentrale in Ehningen.

Quantencomputer und Kryptographie

Der Quantencomputer benötigt zur Berechnung des diskreten Logarithmus in einer kryptographisch geeigneten elliptischen Kurve

nur ca. ein Drittel der Zeit

als dies in einer Restklassengruppe nötig wäre
[Proos und Zalka, 2003].

Quantencomputer und Kryptographie

Der Quantencomputer benötigt zur Berechnung des diskreten Logarithmus in einer kryptographisch geeigneten elliptischen Kurve

nur ca. ein Drittel der Zeit

als dies in einer Restklassengruppe nötig wäre
[Proos und Zalka, 2003].

Bei Aufkommen der Quantencomputer sind die Verfahren ohne elliptischer Kurven demnach etwas sicherer: die auf elliptischen Kurven basierenden Verschlüsselungen sind “schneller geknackt”.

Quantencomputer und Kryptographie

Der Quantencomputer benötigt zur Berechnung des diskreten Logarithmus in einer kryptographisch geeigneten elliptischen Kurve

nur ca. ein Drittel der Zeit

als dies in einer Restklassengruppe nötig wäre
[Proos und Zalka, 2003].

Bei Aufkommen der Quantencomputer sind die Verfahren ohne elliptischer Kurven demnach etwas sicherer: die auf elliptischen Kurven basierenden Verschlüsselungen sind "schneller geknackt".

Zahlreiche weitere Algorithmen, die mathematische Probleme auf Quantencomputern viel schneller lösen als auf klassichen Computern sind seither erschienen (z. B. im Bereich "Big Data" und Künstliche Intelligenz).

Aktuelle Entwicklungen zum Quantencomputer

Es werden Forschungsstellen zu “Post-Quantum-cryptology” geschaffen und ausgeschrieben, z.B. PQCRYPTO, ein Zusammenschluss von Forschergruppen, die nach Verschlüsselungsalternativen suchen, die sicher von Angriffen des Quantencomputers sind.

Aktuelle Entwicklungen zum Quantencomputer

Es werden Forschungsstellen zu “Post-Quantum-cryptology” geschaffen und ausgeschrieben, z.B. PQCRYPTO, ein Zusammenschluss von Forschergruppen, die nach Verschlüsselungsalternativen suchen, die sicher von Angriffen des Quantencomputers sind. Bisher gefundene Lösungen sind inpraktikabel, da sie zu rechenintensiv sind – ein echter Durchbruch ist bislang (noch) nicht zu verzeichnen.

Aktuelle Entwicklungen zum Quantencomputer

Es werden Forschungsstellen zu “Post-Quantum-cryptology” geschaffen und ausgeschrieben, z.B. PQCRYPTO, ein Zusammenschluss von Forschergruppen, die nach Verschlüsselungsalternativen suchen, die sicher von Angriffen des Quantencomputers sind. Bisher gefundene Lösungen sind inpraktikabel, da sie zu rechenintensiv sind – ein echter Durchbruch ist bislang (noch) nicht zu verzeichnen.

Forschungsgelder fließen: ein 300 Millionen Euro schweres Programm des Bundesministeriums für Bildung und Forschung wurde Anfang Februar 2020 vorgestellt.

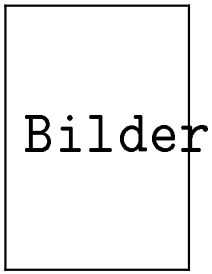
Aktuelle Entwicklungen zum Quantencomputer

Es werden Forschungsstellen zu “Post-Quantum-cryptology” geschaffen und ausgeschrieben, z.B. PQCRYPTO, ein Zusammenschluss von Forschergruppen, die nach Verschlüsselungsalternativen suchen, die sicher von Angriffen des Quantencomputers sind. Bisher gefundene Lösungen sind inpraktikabel, da sie zu rechenintensiv sind – ein echter Durchbruch ist bislang (noch) nicht zu verzeichnen.

Forschungsgelder fließen: ein 300 Millionen Euro schweres Programm des Bundesministeriums für Bildung und Forschung wurde Anfang Februar 2020 vorgestellt.

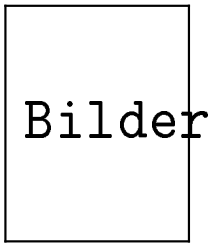
Schon 2018 wurde mit einem Regierungsprogamm 650 Millionen Euro für die Quantenforschung der laufenden Legislaturperiode in Aussicht gestellt (in USA und China hingegen wird mit Milliardenbeträgen operiert).

Quellennachweise 1/2



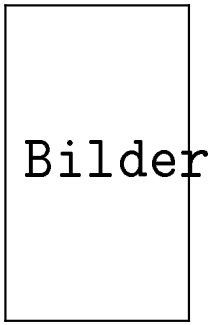
Bilder/Euklid.jpg

Euklid von Alexandria,
https://commons.wikimedia.org/wiki/File:Artgate_Fondazione_Cariplo_-_Cifrondi_Antonio,_Euclide.jpg



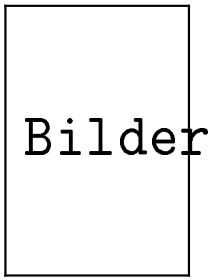
Bilder/Gauss.png

Carl Friedrich Gauß,
https://commons.wikimedia.org/wiki/File:Carl_Friedrich_Gauss.jpg



Bilder/Hadamard.png

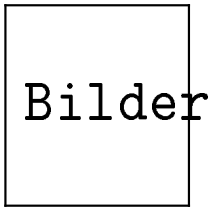
Jacques Hadamard,
https://upload.wikimedia.org/wikipedia/commons/a/ae/Hadamard2_cropped.jpg



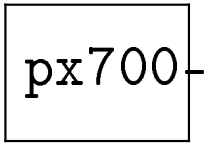
Bilder/dlVP.png

Charles-Louis-Joseph-Xavier de la Vallée-Poussin,
https://commons.wikimedia.org/wiki/File:C-L_de_La_Vallee_Poussin.jpg

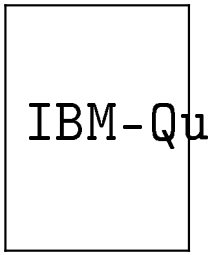
Quellennachweise 2/2



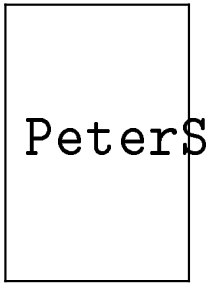
Bilder/Riemann.png
Bernhard Riemann,
https://commons.wikimedia.org/wiki/File:Georg_Friedrich_Bernhard_Riemann.jpeg



px700-germain.jpg
Sophie Germain, http://jeff560.tripod.com/images/germain.jpg



IBM-QunatComp.jpg
MIT Technology Review
https://www.technologyreview.com/s/609451/
ibm-raises-the-bar-with-a-50-qubit-quantum-computer



PeterShor.jpg

Peter Shor http://www-math.mit.edu/~shor

Vielen Dank für Ihre Aufmerksamkeit!

Karin Halupczok