Moderne Siebtheorie

Karin Halupczok

Ringvorlesung 1. Juli 2015

Mathematisches Institut
WWU Münster

Was ist Siebtheorie?

Startpunkt: Das antike Sieb des Eratosthenes:
Erstellung der Primzahlliste $10 < p < 100$:

Was ist Siebtheorie?

Startpunkt: Das antike Sieb des Eratosthenes:
Erstellung der Primzahlliste $10 < p < 100$:

Sei $A = \{1, \ldots, 100\}$,

Was ist Siebtheorie?

Startpunkt: Das antike Sieb des Eratosthenes:
Erstellung der Primzahlliste $10 < p < 100$:

Sei $A = \{1, \ldots, 100\}$,

Was ist Siebtheorie?

Startpunkt: Das antike Sieb des Eratosthenes:
Erstellung der Primzahlliste $10 < p < 100$:

Sei $A = \{1, \ldots, 100\}$,
streiche alle $n \in A$ mit $2 \mid n$,

Was ist Siebtheorie?

Startpunkt: Das antike Sieb des Eratosthenes:
Erstellung der Primzahlliste $10 < p < 100$:

Sei $A = \{1, \ldots, 100\}$,
streiche alle $n \in A$ mit $2 \mid n$,
dann alle $n \in A$ mit $3 \mid n$,

Was ist Siebtheorie?

Startpunkt: Das antike Sieb des Eratosthenes:
Erstellung der Primzahlliste $10 < p < 100$:

Sei $A = \{1, \ldots, 100\}$,
streiche alle $n \in A$ mit $2 \mid n$,
dann alle $n \in A$ mit $3 \mid n$,
dann alle $n \in A$ mit $5 \mid n$
(Vielfache von 4 sind bereits gestrichen),

Was ist Siebtheorie?

Startpunkt: Das antike Sieb des Eratosthenes:
Erstellung der Primzahlliste $10 < p < 100$:

Sei $A = \{1, \ldots, 100\}$,
streiche alle $n \in A$ mit $2 \mid n$,
dann alle $n \in A$ mit $3 \mid n$,
dann alle $n \in A$ mit $5 \mid n$
(Vielfache von 4 sind bereits gestrichen),
usw. ...

Was ist Siebtheorie?

Startpunkt: Das antike Sieb des Eratosthenes:
Erstellung der Primzahlliste $10 < p < 100$:

Sei $A = \{1, \ldots, 100\}$,
streiche alle $n \in A$ mit $2 \mid n$,
dann alle $n \in A$ mit $3 \mid n$,
dann alle $n \in A$ mit $5 \mid n$
(Vielfache von 4 sind bereits gestrichen),
usw. ...

Ende des Verfahrens, sobald alle Vielfachen der Primzahlen $\leq 10 = \sqrt{100}$, d. h. von $2, 3, 5, 7$, gestrichen sind.

Was ist Siebtheorie?

Startpunkt: Das antike Sieb des Eratosthenes:
Erstellung der Primzahlliste $10 < p < 100$:

Sei $A = \{1, \ldots, 100\}$,
streiche alle $n \in A$ mit $2 \mid n$,
dann alle $n \in A$ mit $3 \mid n$,
dann alle $n \in A$ mit $5 \mid n$
(Vielfache von 4 sind bereits gestrichen),
usw. ...

Ende des Verfahrens, sobald alle Vielfachen der Primzahlen
$\leq 10 = \sqrt{100}$, d. h. von $2, 3, 5, 7$, gestrichen sind.

Die übriggebliebenen Zahlen sind die Primzahlen $\in \{10, \ldots, 100\}$,
da jede zusammengesetzte Zahl ≤ 100 einen Primteiler
$\leq 10 = \sqrt{100}$ besitzt und deswegen beim Sieben gestrichen wurde.

Animation des Siebes des 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

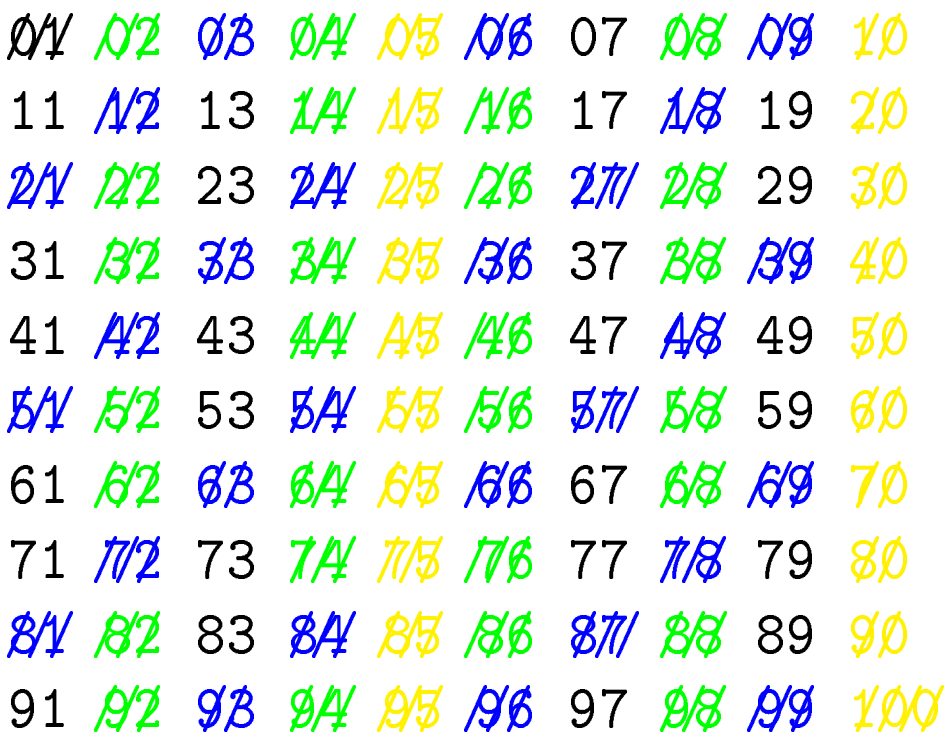
Animation des Siebes des Eratosthenes

~~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 des 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 des Eratosthenes



Animation des Siebes des 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 des 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~~

Grundlegende Siebnotation

Betrachte eine endliche Menge von Objekten $\mathcal{A}$ und sei $\mathcal{P}$ die Menge der Primzahlen so dass es für jedes $p \in \mathcal{P}$ eine zugehörige Teilmenge $\mathcal{A}_p$ von $\mathcal{A}$ gibt.

Grundlegende Siebnotation

Betrachte eine endliche Menge von Objekten $\mathcal{A}$ und sei $\mathcal{P}$ die Menge der Primzahlen so dass es für jedes $p \in \mathcal{P}$ eine zugehörige Teilmenge $\mathcal{A}_p$ von $\mathcal{A}$ gibt.

Das allgemeine Siebproblem ist dann, untere und obere Schranke der Kardinalität der gesiebten Menge anzugeben, d. h. für

$$\mathcal{S}(\mathcal{A}, \mathcal{P}) := \mathcal{A} \setminus \bigcup_{p \in \mathcal{P}} \mathcal{A}_p.$$

Grundlegende Siebnotation

Betrachte eine endliche Menge von Objekten $\mathcal{A}$ und sei $\mathcal{P}$ die Menge der Primzahlen so dass es für jedes $p \in \mathcal{P}$ eine zugehörige Teilmenge $\mathcal{A}_p$ von $\mathcal{A}$ gibt.

Das allgemeine Siebproblem ist dann, untere und obere Schranke der Kardinalität der gesiebten Menge anzugeben, d. h. für

$$\mathcal{S}(\mathcal{A}, \mathcal{P}) := \mathcal{A} \setminus \bigcup_{p \in \mathcal{P}} \mathcal{A}_p.$$

Für reelles $z \geq 1$ definiere $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$. Ziel: Abschätzung der Siebfunktion $S(\mathcal{A}, \mathcal{P}, z) := \#\left(\mathcal{A} \setminus \bigcup_{p \mid P(z)} \mathcal{A}_p\right)$.

Die Siebfunktion im Sieb des Eratosthenes

Das Sieb des Eratosthenes liefert ein Standardbeispiel:

Für $x \geq 1$ reell (oben: $x = 100$) sei $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, sei $\mathcal{P}$ die Menge aller Primzahlen, sei $\sqrt{x} < z \leq x$ und $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.

Die Siebfunktion im Sieb des Eratosthenes

Das Sieb des Eratosthenes liefert ein Standardbeispiel:

Für $x \geq 1$ reell (oben: $x = 100$) sei $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, sei $\mathcal{P}$ die Menge aller Primzahlen, sei $\sqrt{x} < z \leq x$ und $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.

Weiter sei $\mathcal{A}_p := \{n \in \mathcal{A};\ p \mid n\}$.

Die Siebfunktion im Sieb des Eratosthenes

Das Sieb des Eratosthenes liefert ein Standardbeispiel:

Für $x \geq 1$ reell (oben: $x = 100$) sei $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, sei $\mathcal{P}$ die Menge aller Primzahlen, sei $\sqrt{x} < z \leq x$ und $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.
Weiter sei $\mathcal{A}_p := \{n \in \mathcal{A};\ p \mid n\}$. Die Siebfunktion ist dann

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, z) &= \#\Big(\mathcal{A} \setminus \bigcup_{p \mid P(z)} \mathcal{A}_p\Big) \\ &= \#\{n \in \mathcal{A};\ (p \mid n \Rightarrow p \geq z) \text{ für alle } p \in \mathcal{P}\} \\ &= \#\{n \leq x;\ \gcd(n, P(z)) = 1\} \\ &= \pi(x) - \pi(z), \end{aligned}$$

wobei $\pi(x) := \#\{p \leq x;\ p \text{ prim}\}$ die Primzahlzählfunktion bezeichnet.

Ergebnisse für die Primzahlzählfunktion

Mittels Siebmethoden kann die Schranke $C_1 \frac{x}{\log x} \leq \pi(x) \leq C_2 \frac{x}{\log x}$ mit Konstanten $0 < C_1 < 1 < C_2$ gezeigt werden, aber der Primzahlsatz in der Form

$$\pi(x) \sim \frac{x}{\log x} \quad \Leftrightarrow \quad \lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$$

kann so nicht bewiesen werden.

Ergebnisse für die Primzahlzählfunktion

Mittels Siebmethoden kann die Schranke $C_1 \frac{x}{\log x} \leq \pi(x) \leq C_2 \frac{x}{\log x}$ mit Konstanten $0 < C_1 < 1 < C_2$ gezeigt werden, aber der Primzahlsatz in der Form

$$\pi(x) \sim \frac{x}{\log x} \quad \Leftrightarrow \quad \lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$$

kann so nicht bewiesen werden.

Ist aber $z \leq \log x$, zeigen Siebmethoden, dass

$$\#\{n \leq x;\ \gcd(n, P(z)) = 1\} \sim \frac{e^{-\gamma} x}{\log z}$$

gilt, wobei $\gamma := \lim_{n \to \infty} (\sum_{k=1}^{n} \frac{1}{k} - \log n) = 0,57721\ldots$ die Euler–Mascheroni-Konstante ist.

Ein Beispiel für ein anderes Sieb

Das (Primzahl-)Zwillingssieb:

Für $x \geq 1$ reell sei $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, sei $\mathcal{P}$ die Menge aller Primzahlen $p \neq 2$, sei $\sqrt{x} < z \leq x$ und $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p<z}} p$.

Ein Beispiel für ein anderes Sieb

Das (Primzahl-)Zwillingssieb:

Für $x \geq 1$ reell sei $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, sei $\mathcal{P}$ die Menge aller Primzahlen $p \neq 2$, sei $\sqrt{x} < z \leq x$ und $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p<z}} p$.

Nun setzen wir $\mathcal{A}_p := \{n \in \mathcal{A};\ n \equiv 0 \bmod p \text{ oder } n \equiv -2 \bmod p\}$.

Ein Beispiel für ein anderes Sieb

Das (Primzahl-)Zwillingssieb:

Für $x \geq 1$ reell sei $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, sei $\mathcal{P}$ die Menge aller Primzahlen $p \neq 2$, sei $\sqrt{x} < z \leq x$ und $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p<z}} p$.

Nun setzen wir $\mathcal{A}_p := \{n \in \mathcal{A};\ n \equiv 0 \bmod p \text{ oder } n \equiv -2 \bmod p\}$.

Dann ist $\pi_2(x) \leq \pi(z) + S(\mathcal{A}, \mathcal{P}, z)$, wobei

$$\pi_2(x) := \#\{p \leq x;\ p, p+2 \text{ prim}\}$$

die Primzahlzwillingszählfunktion bezeichnet.

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

~~01~~	~~03~~	~~05~~	~~07~~	~~09~~	011	~~13~~	~~15~~	017	~~19~~
~~21~~	~~23~~	~~25~~	~~27~~	029	~~31~~	~~33~~	~~35~~	~~37~~	~~39~~
041	~~43~~	~~45~~	047	~~49~~	~~51~~	~~53~~	~~55~~	~~57~~	059
~~61~~	~~63~~	~~65~~	~~67~~	~~69~~	071	~~73~~	~~75~~	077	~~79~~
~~81~~	~~83~~	~~85~~	~~87~~	089	~~91~~	~~93~~	~~95~~	~~97~~	~~99~~
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

~~01~~	~~03~~	~~05~~	~~07~~	~~09~~	~~11~~	~~13~~	~~15~~	017	~~19~~
~~21~~	~~23~~	~~25~~	~~27~~	029	~~31~~	~~33~~	~~35~~	~~37~~	~~39~~
041	~~43~~	~~45~~	~~47~~	~~49~~	~~51~~	~~53~~	~~55~~	~~57~~	059
~~61~~	~~63~~	~~65~~	~~67~~	~~69~~	071	~~73~~	~~75~~	~~77~~	~~79~~
~~81~~	~~83~~	~~85~~	~~87~~	~~89~~	~~91~~	~~93~~	~~95~~	~~97~~	~~99~~
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	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

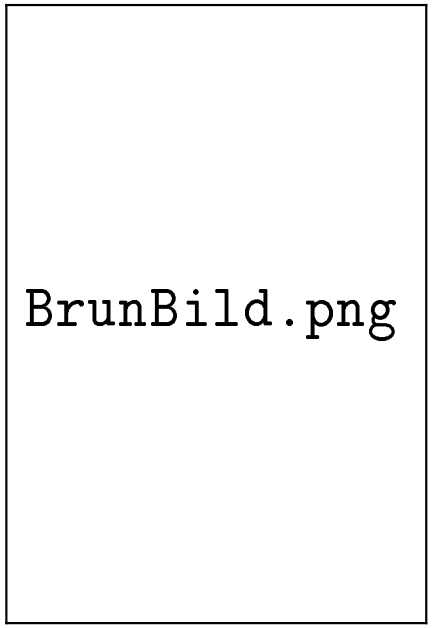
Streiche alle n, für die n oder $n+2$ durch 13 teilbar ist.

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

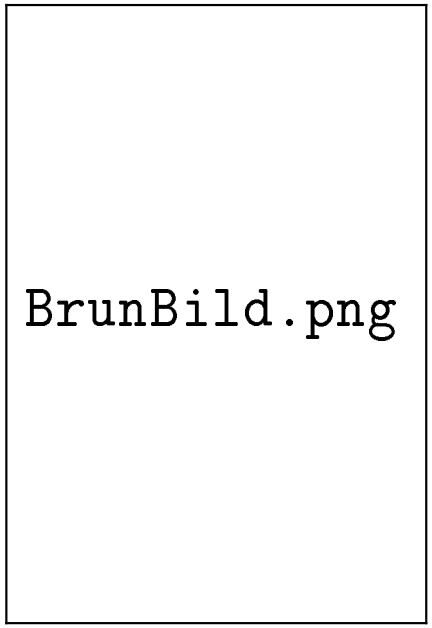
Ergebnis: Alle $14 < p < 200$ prim, für die $p + 2$ auch prim ist.

Bruns Sieb



Viggo Brun, 1885–1978

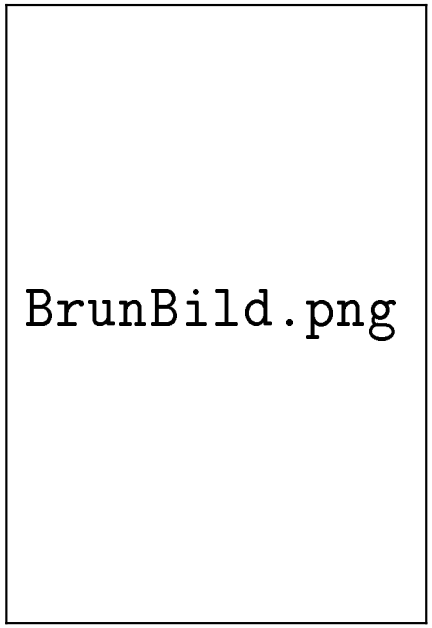
Bruns Sieb



Viggo Brun, 1885–1978

Der Startpunkte der enormen Entwicklungen der modernen Siebtheorie war Bruns Sieb um 1920.

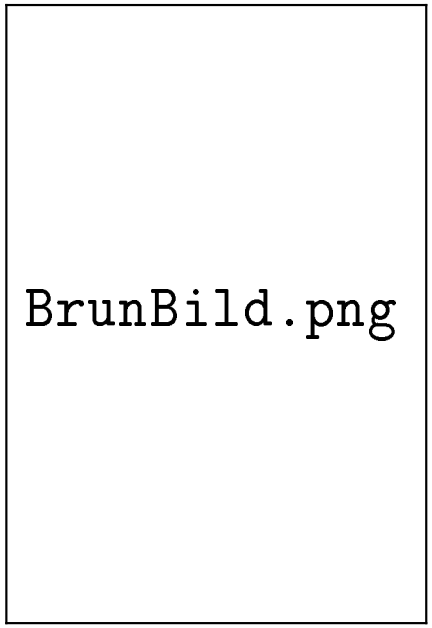
Bruns Sieb



Viggo Brun, 1885–1978

Der Startpunkte der enormen Entwicklungen der modernen Siebtheorie war Bruns Sieb um 1920.
Auf das Zwillingsproblem angewandt, zeigt es, dass die Menge der Primzahlzwillinge klein ist im Vergleich der Menge aller Primzahlen: $\pi_2(x) \ll \frac{x}{\log^2 x}$.

Bruns Sieb

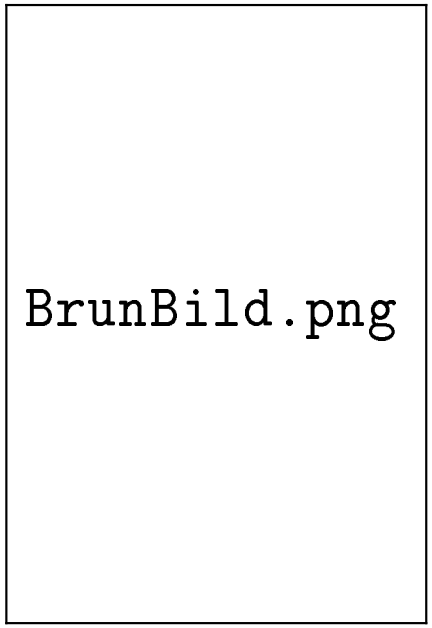


Viggo Brun, 1885–1978

Der Startpunkte der enormen Entwicklungen der modernen Siebtheorie war Bruns Sieb um 1920.
Auf das Zwillingsproblem angewandt, zeigt es, dass die Menge der Primzahlzwillinge klein ist im Vergleich der Menge aller Primzahlen: $\pi_2(x) \ll \frac{x}{\log^2 x}$.

Folgerung: $\sum_{p \in \mathcal{T}} \frac{1}{p}$ konvergiert, wenn p die Menge $\mathcal{T}$ der Primzahlzwillinge durchläuft.

Bruns Sieb



Viggo Brun, 1885–1978

Der Startpunkte der enormen Entwicklungen der modernen Siebtheorie war Bruns Sieb um 1920.
Auf das Zwillingsproblem angewandt, zeigt es, dass die Menge der Primzahlzwillinge klein ist im Vergleich der Menge aller Primzahlen: $\pi_2(x) \ll \frac{x}{\log^2 x}$.

Folgerung: $\sum_{p \in \mathcal{T}} \frac{1}{p}$ konvergiert, wenn p die Menge $\mathcal{T}$ der Primzahlzwillinge durchläuft.
Die numerische Bestimmung dieser Brunschen Konstanten $\sum_{p \in \mathcal{T}} \frac{1}{p} \approx 1.9021605822\ldots$ ist ein schwieriges Problem.

Die Brunsche Konstante

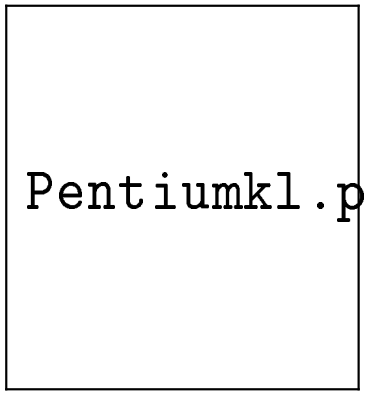
Thomas R. Nicely (Lynchburg College, USA) versuchte um 1994 eine genaue numerische Berechnung der Brunschen Konstante.

Die Brunsche Konstante

Thomas R. Nicely (Lynchburg College, USA) versuchte um 1994 eine genaue numerische Berechnung der Brunschen Konstante. Er machte eine bemerkenswerte Entdeckung:

Die Brunsche Konstante

Thomas R. Nicely (Lynchburg College, USA) versuchte um 1994 eine genaue numerische Berechnung der Brunschen Konstante.
Er machte eine bemerkenswerte Entdeckung:

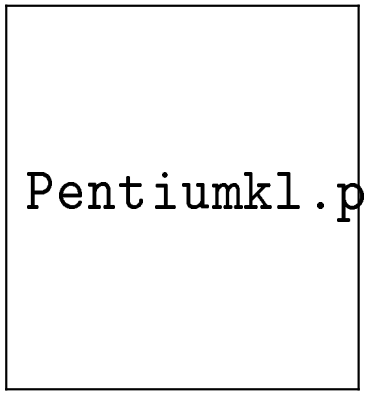


Pentium 66 (SX837) mit FDIV-Bug

Den Pentium-FDIV-Bug: Einen Hardwarefehler des Pentium-Prozessors von Intel, anderthalb Jahre nach Markteinführung, der für fehlerhafte Nachkommastellen in Anwendungen sorgte, bei denen hohe Genauigkeit erforderlich ist.

Die Brunsche Konstante

Thomas R. Nicely (Lynchburg College, USA) versuchte um 1994 eine genaue numerische Berechnung der Brunschen Konstante. Er machte eine bemerkenswerte Entdeckung:



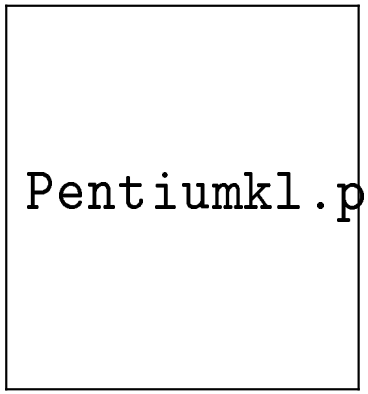
Pentium 66 (SX837) mit FDIV-Bug

Den Pentium-FDIV-Bug: Einen Hardwarefehler des Pentium-Prozessors von Intel, anderthalb Jahre nach Markteinführung, der für fehlerhafte Nachkommastellen in Anwendungen sorgte, bei denen hohe Genauigkeit erforderlich ist.

Allein der Umtausch von ca. einer Million fehlerhafter Prozessoren hat die Herstellerfirma Intel über 475 Millionen Dollar gekostet.

Die Brunsche Konstante

Thomas R. Nicely (Lynchburg College, USA) versuchte um 1994 eine genaue numerische Berechnung der Brunschen Konstante. Er machte eine bemerkenswerte Entdeckung:



Pentium 66 (SX837) mit FDIV-Bug

Den Pentium-FDIV-Bug: Einen Hardwarefehler des Pentium-Prozessors von Intel, anderthalb Jahre nach Markteinführung, der für fehlerhafte Nachkommastellen in Anwendungen sorgte, bei denen hohe Genauigkeit erforderlich ist.

Allein der Umtausch von ca. einer Million fehlerhafter Prozessoren hat die Herstellerfirma Intel über 475 Millionen Dollar gekostet. Intel erntete viel Schadenfreude: “Wieviele Intel-Mitarbeiter braucht man, um eine Glühbirne zu wechseln? 1,9999983256”

Siebsätze

Heutzutage liefert moderne Siebtheorie eine Sammlung verschiedener Siebsätze zur Abschätzung von Siebfunktionen. Oft enthalten ihre Beweise sehr ausgefeilte Ideen. Diese Sätze können in Anwendungen als Werkzeug benutzt werden, oftmals wie eine “black box”.

Siebsätze

Heutzutage liefert moderne Siebtheorie eine Sammlung verschiedener Siebsätze zur Abschätzung von Siebfunktionen. Oft enthalten ihre Beweise sehr ausgefeilte Ideen. Diese Sätze können in Anwendungen als Werkzeug benutzt werden, oftmals wie eine "black box". Beispielsweise kann das Brunsche Sieb als solch ein Siebsatz formuliert werden.

Siebsätze

Heutzutage liefert moderne Siebtheorie eine Sammlung verschiedener Siebsätze zur Abschätzung von Siebfunktionen. Oft enthalten ihre Beweise sehr ausgefeilte Ideen. Diese Sätze können in Anwendungen als Werkzeug benutzt werden, oftmals wie eine "black box". Beispielsweise kann das Brunsche Sieb als solch ein Siebsatz formuliert werden.

Viele dieser Sätze wurden im klassischen Zweig der Primzahltheorie entwickelt, heute erscheinen sie aber auch in verschiedenen anderen Zweigen der Mathematik.

Siebsätze

Heutzutage liefert moderne Siebtheorie eine Sammlung verschiedener Siebsätze zur Abschätzung von Siebfunktionen. Oft enthalten ihre Beweise sehr ausgefeilte Ideen. Diese Sätze können in Anwendungen als Werkzeug benutzt werden, oftmals wie eine "black box". Beispielsweise kann das Brunsche Sieb als solch ein Siebsatz formuliert werden.

Viele dieser Sätze wurden im klassischen Zweig der Primzahltheorie entwickelt, heute erscheinen sie aber auch in verschiedenen anderen Zweigen der Mathematik.

Ein bekannter starker Siebsatz, der vielfältige Anwendungen hat, ist das Selberg-Sieb bzw. Λ^2-Sieb:

Beispiel für einen Siebsatz

Selberg-Sieb:

Beispiel für einen Siebsatz

Selberg-Sieb:

Für $\mathcal{A}_d := \bigcap_{p|d} \mathcal{A}_p$ gelte die Approximationsformel $\#\mathcal{A}_d = g(d)X + R_d$ mit einer multiplikativen Funktion g, für die $0 < g(p) < 1$ für alle $p \in \mathcal{P}$ gilt.

Sei $F(z) := \sum_{\substack{d|P(z) \\ d<z}} \frac{1}{f(d)}$ mit der Funktion $f(k) := \sum_{d|k} \frac{\mu(d)}{g(k/d)}$.

Beispiel für einen Siebsatz

Selberg-Sieb:

Für $\mathcal{A}_d := \bigcap_{p|d} \mathcal{A}_p$ gelte die Approximationsformel $\#\mathcal{A}_d = g(d)X + R_d$ mit einer multiplikativen Funktion g, für die $0 < g(p) < 1$ für alle $p \in \mathcal{P}$ gilt.

Sei $F(z) := \sum_{\substack{d|P(z) \\ d<z}} \frac{1}{f(d)}$ mit der Funktion $f(k) := \sum_{d|k} \frac{\mu(d)}{g(k/d)}$.

Dann gilt

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{X}{F(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\nu(d)} |R_d|,$$

wobei $\nu(d) := \#\{p \mid d\}$ die Anzahl der verschiedenen Primteiler von d bezeichnet.

1. Primzahlen in kurzen Intervallen

Enthält das reelle Intervall $[n, n + \sqrt{n}[$ Primzahlen für alle $n \in \mathbb{N}$?
Das ist eine offene Vermutung.

1. Primzahlen in kurzen Intervallen

Enthält das reelle Intervall $[n, n + \sqrt{n}[$ Primzahlen für alle $n \in \mathbb{N}$?
Das ist eine offene Vermutung.

Unter Annahme der Riemannschen Vermutung gibt es bei fest gewähltem $\varepsilon > 0$ Primzahlen in allen Intervallen $[n, n + n^{1/2+\varepsilon}[$, für die n hinreichend groß ist.

1. Primzahlen in kurzen Intervallen

Enthält das reelle Intervall $[n, n + \sqrt{n}[$ Primzahlen für alle $n \in \mathbb{N}$? Das ist eine offene Vermutung.

Unter Annahme der Riemannschen Vermutung gibt es bei fest gewähltem $\varepsilon > 0$ Primzahlen in allen Intervallen $[n, n + n^{1/2+\varepsilon}[$, für die n hinreichend groß ist.

Ohne Annahme unbewiesener Vermutungen (o.A.u.V) wurde mit Siebmethoden gezeigt, dass es Primzahlen in Intervallen der Form $[n, n + n^{11/20}[$ für alle hinreichend großen n gibt [G. Harman 2007].

1. Primzahlen in kurzen Intervallen

Enthält das reelle Intervall $[n, n+\sqrt{n}[$ Primzahlen für alle $n \in \mathbb{N}$? Das ist eine offene Vermutung.

Unter Annahme der Riemannschen Vermutung gibt es bei fest gewähltem $\varepsilon > 0$ Primzahlen in allen Intervallen $[n, n+n^{1/2+\varepsilon}[$, für die n hinreichend groß ist.

Ohne Annahme unbewiesener Vermutungen (o.A.u.V) wurde mit Siebmethoden gezeigt, dass es Primzahlen in Intervallen der Form $[n, n+n^{11/20}[$ für alle hinreichend großen n gibt [G. Harman 2007].

Wird die Riemannsche Vermutung angenommen, enthalten fast alle Intervalle $[n, n+\log^2 n[$ mit $n \leq X$ Primzahlen (mit Ausnahme von höchstens $o(X)$ vielen).

2. Primzahlen, die durch Polynome dargestellt werden

Ist $f(x) \in \mathbb{Z}[x]$ ein nichtkonstantes irreduzibles Polynom mit positivem Leitkoeffizient und hat $f(n)$ keinen festen Primteiler, wenn $n \in \mathbb{N}$ durchläuft, nimmt $f(n)$ dann unendlich oft Primzahlwerte an? Dies ist eine offene Vermutung.

2. Primzahlen, die durch Polynome dargestellt werden

Ist $f(x) \in \mathbb{Z}[x]$ ein nichtkonstantes irreduzibles Polynom mit positivem Leitkoeffizient und hat $f(n)$ keinen festen Primteiler, wenn $n \in \mathbb{N}$ durchläuft, nimmt $f(n)$ dann unendlich oft Primzahlwerte an? Dies ist eine offene Vermutung.

Der Satz von Dirichlet über Primzahlen in Progressionen zeigt dass dies wahr ist für lineares f, aber es gibt kein bekanntes Ergebnis für höheren Grad, außer in Spezialfällen.

2. Primzahlen, die durch Polynome dargestellt werden

Ist $f(x) \in \mathbb{Z}[x]$ ein nichtkonstantes irreduzibles Polynom mit positivem Leitkoeffizient und hat $f(n)$ keinen festen Primteiler, wenn $n \in \mathbb{N}$ durchläuft, nimmt $f(n)$ dann unendlich oft Primzahlwerte an? Dies ist eine offene Vermutung.

Der Satz von Dirichlet über Primzahlen in Progressionen zeigt dass dies wahr ist für lineares f, aber es gibt kein bekanntes Ergebnis für höheren Grad, außer in Spezialfällen.

Für Polynome in zwei Variablen, ist der Fall $m^2 + n^2$ gut verstanden, ebenso andere quadratische Fälle.

2. Primzahlen, die durch Polynome dargestellt werden

Ist $f(x) \in \mathbb{Z}[x]$ ein nichtkonstantes irreduzibles Polynom mit positivem Leitkoeffizient und hat $f(n)$ keinen festen Primteiler, wenn $n \in \mathbb{N}$ durchläuft, nimmt $f(n)$ dann unendlich oft Primzahlwerte an? Dies ist eine offene Vermutung.

Der Satz von Dirichlet über Primzahlen in Progressionen zeigt dass dies wahr ist für lineares f, aber es gibt kein bekanntes Ergebnis für höheren Grad, außer in Spezialfällen.

Für Polynome in zwei Variablen, ist der Fall $m^2 + n^2$ gut verstanden, ebenso andere quadratische Fälle.

Andere Ergebnisse in Richtung höhergradige Analoga: $m^2 + n^4$ nimmt unendlich oft Primzahlwerte an [J. Friedlander und H. Iwaniec 1989].

2. Primzahlen, die durch Polynome dargestellt werden

Ist $f(x) \in \mathbb{Z}[x]$ ein nichtkonstantes irreduzibles Polynom mit positivem Leitkoeffizient und hat $f(n)$ keinen festen Primteiler, wenn $n \in \mathbb{N}$ durchläuft, nimmt $f(n)$ dann unendlich oft Primzahlwerte an? Dies ist eine offene Vermutung.

Der Satz von Dirichlet über Primzahlen in Progressionen zeigt dass dies wahr ist für lineares f, aber es gibt kein bekanntes Ergebnis für höheren Grad, außer in Spezialfällen.

Für Polynome in zwei Variablen, ist der Fall $m^2 + n^2$ gut verstanden, ebenso andere quadratische Fälle.

Andere Ergebnisse in Richtung höhergradige Analoga: $m^2 + n^4$ nimmt unendlich oft Primzahlwerte an [J. Friedlander und H. Iwaniec 1989].
$x^3 + 2y^3$ ebenso [D. R. Heath-Brown 2001].

3. Diophantische Approximation

Bekannt ist: Ist $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ irrational, dann gibt es unendlich viele Paare teilerfremder ganzer Zahlen m, n mit $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$.

3. Diophantische Approximation

Bekannt ist: Ist $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ irrational, dann gibt es unendlich viele Paare teilerfremder ganzer Zahlen m, n mit $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$.

Können wir auch unendlich viele Lösungen der Ungleichung $|\alpha - \frac{m}{p}| < \frac{1}{p^{1+\theta}}$ erhalten, für ein festes $0 < \theta \leq 1$?

3. Diophantische Approximation

Bekannt ist: Ist $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ irrational, dann gibt es unendlich viele Paare teilerfremder ganzer Zahlen m, n mit $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$.

Können wir auch unendlich viele Lösungen der Ungleichung $|\alpha - \frac{m}{p}| < \frac{1}{p^{1+\theta}}$ erhalten, für ein festes $0 < \theta \leq 1$?

Nimmt man noch strengere Vermutungen als die GRH (verallgemeinerte Riemannsche Vermutung) an, ist dies wahr für $0 < \theta < 1/3$.

3. Diophantische Approximation

Bekannt ist: Ist $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ irrational, dann gibt es unendlich viele Paare teilerfremder ganzer Zahlen m, n mit $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$.

Können wir auch unendlich viele Lösungen der Ungleichung $|\alpha - \frac{m}{p}| < \frac{1}{p^{1+\theta}}$ erhalten, für ein festes $0 < \theta \leq 1$?

Nimmt man noch strengere Vermutungen als die GRH (verallgemeinerte Riemannsche Vermutung) an, ist dies wahr für $0 < \theta < 1/3$.

Die Behauptung ist falsch für $\theta = 1$: Es gibt überabzählbar viele α so dass

$$\|\alpha p\| < \frac{\log p}{500 p \log\log p}$$

nur endlich viele Lösungen in Primzahlen p hat, wobei $\|x\| := \min_{m \in \mathbb{Z}} |x - m|$ [G. Harman 1995].

4. Primzahlen in arithmetischen Progressionen

Frage: Was ist die kleinste Primzahl in einer arithmetischen Progression?

4. Primzahlen in arithmetischen Progressionen

Frage: Was ist die kleinste Primzahl in einer arithmetischen Progression?

Für eine gegebene Restklasse $a \bmod q$ mit $\gcd(a, q) = 1$, fragen wir nach der Größe von $p_{\min(q,a)} := \min\{p \text{ prim};\ p \equiv a \bmod q\}$.

4. Primzahlen in arithmetischen Progressionen

Frage: Was ist die kleinste Primzahl in einer arithmetischen Progression?

Für eine gegebene Restklasse a mod q mit $\gcd(a, q) = 1$, fragen wir nach der Größe von $p_{\min(q,a)} := \min\{p \text{ prim};\ p \equiv a \bmod q\}$.

Y. Linnik zeigte [1944] dass es eine absolute Konstante $L > 0$ mit $p_{\min(q,a)} \ll q^L$ gibt, die wir heute Linniks Konstante nennen.

4. Primzahlen in arithmetischen Progressionen

Frage: Was ist die kleinste Primzahl in einer arithmetischen Progression?

Für eine gegebene Restklasse a mod q mit $\gcd(a, q) = 1$, fragen wir nach der Größe von $p_{\min(q,a)} := \min\{p \text{ prim};\ p \equiv a \bmod q\}$.

Y. Linnik zeigte [1944] dass es eine absolute Konstante $L > 0$ mit $p_{\min(q,a)} \ll q^L$ gibt, die wir heute Linniks Konstante nennen.

linnikSchrift.png

Ausschnitt der Inschrift auf Linniks Grabstein

Ergebnisse von Linnik

Der Beweis der Existenz der Linnik-Konstanten kann mit dem klassischen nullstellenfreien Gebiet für L-funktionen geführt werden:

Ergebnisse von Linnik

Der Beweis der Existenz der Linnik-Konstanten kann mit dem klassischen nullstellenfreien Gebiet für L-funktionen geführt werden:

Es gilt $L(s, \chi) \neq 0$ für jeden primitiven Charakter χ mod q und $s = \sigma + it$ mit $\sigma > 1 - c/\log(q(|t| + 2))$, wobei c eine positive, absolute Konstante ist, außer für höchstens eine einfache reelle Nullstelle von $L(s, \chi)$ – wobei χ dann ein reeller Charakter ist.

Ergebnisse von Linnik

Der Beweis der Existenz der Linnik-Konstanten kann mit dem klassischen nullstellenfreien Gebiet für L-funktionen geführt werden:

Es gilt $L(s, \chi) \neq 0$ für jeden primitiven Charakter χ mod q und $s = \sigma + it$ mit $\sigma > 1 - c/\log(q(|t| + 2))$, wobei c eine positive, absolute Konstante ist, außer für höchstens eine einfache reelle Nullstelle von $L(s, \chi)$ – wobei χ dann ein reeller Charakter ist.

Ein weiteres Problem von Y. Linnik ist die Größe des kleinsten nichtquadratischen Rests mod p, nämlich von $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Ergebnisse von Linnik

Der Beweis der Existenz der Linnik-Konstanten kann mit dem klassischen nullstellenfreien Gebiet für L-funktionen geführt werden:

Es gilt $L(s, \chi) \neq 0$ für jeden primitiven Charakter χ mod q und $s = \sigma + it$ mit $\sigma > 1 - c/\log(q(|t| + 2))$, wobei c eine positive, absolute Konstante ist, außer für höchstens eine einfache reelle Nullstelle von $L(s, \chi)$ – wobei χ dann ein reeller Charakter ist.

Ein weiteres Problem von Y. Linnik ist die Größe des kleinsten nichtquadratischen Rests mod p, nämlich von $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Vinogradovs Vermutung: $\forall \varepsilon > 0\ \forall p > p_0(\varepsilon) :\ \ q(p) < p^{\varepsilon}$.

Ergebnisse von Linnik

Der Beweis der Existenz der Linnik-Konstanten kann mit dem klassischen nullstellenfreien Gebiet für L-funktionen geführt werden:

Es gilt $L(s, \chi) \neq 0$ für jeden primitiven Charakter χ mod q und $s = \sigma + it$ mit $\sigma > 1 - c/\log(q(|t| + 2))$, wobei c eine positive, absolute Konstante ist, außer für höchstens eine einfache reelle Nullstelle von $L(s, \chi)$ – wobei χ dann ein reeller Charakter ist.

Ein weiteres Problem von Y. Linnik ist die Größe des kleinsten nichtquadratischen Rests mod p, nämlich von $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Vinogradovs Vermutung: $\forall \varepsilon > 0\ \forall p > p_0(\varepsilon) :\ \ q(p) < p^{\varepsilon}$.

Unter Annahme der GRH wurde $q(p) \ll (\log p)^2$ gezeigt [Ankeny 1952]

Ergebnisse von Linnik

Der Beweis der Existenz der Linnik-Konstanten kann mit dem klassischen nullstellenfreien Gebiet für L-funktionen geführt werden:

Es gilt $L(s,\chi) \neq 0$ für jeden primitiven Charakter χ mod q und $s = \sigma + it$ mit $\sigma > 1 - c/\log(q(|t|+2))$, wobei c eine positive, absolute Konstante ist, außer für höchstens eine einfache reelle Nullstelle von $L(s,\chi)$ – wobei χ dann ein reeller Charakter ist.

Ein weiteres Problem von Y. Linnik ist die Größe des kleinsten nichtquadratischen Rests mod p, nämlich von $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Vinogradovs Vermutung: $\forall \varepsilon > 0\ \forall p > p_0(\varepsilon):\ \ q(p) < p^{\varepsilon}$.

Unter Annahme der GRH wurde $q(p) \ll (\log p)^2$ gezeigt [Ankeny 1952] $\rightarrow$ ein wichtiges Ergebnis für Primzahltest-Anwendungen!

5. Das große Sieb

5. Das große Sieb

Linnik zeigte [1941], dass Ausnahmen der Vermutung von Vinogradov sehr selten sind: $\#\{p \leq x;\ q(p) \geq p^{\varepsilon}\} \ll_{\varepsilon} \log\log x$.

5. Das große Sieb

Linnik zeigte [1941], dass Ausnahmen der Vermutung von Vinogradov sehr selten sind: $\#\{p \leq x;\ q(p) \geq p^{\varepsilon}\} \ll_{\varepsilon} \log\log x$.

Er führte dazu eine neue Siebmethode ein, die nach ihm intensiv weiterentwickelt wurde. Man nennt sie heute die Methode des großen Siebs.

5. Das große Sieb

Linnik zeigte [1941], dass Ausnahmen der Vermutung von Vinogradov sehr selten sind: $\#\{p \leq x;\ q(p) \geq p^{\varepsilon}\} \ll_{\varepsilon} \log\log x$.

Er führte dazu eine neue Siebmethode ein, die nach ihm intensiv weiterentwickelt wurde. Man nennt sie heute die Methode des großen Siebs.

Eine der wichtigsten Anwendungen des großen Siebs (zusammen mit bestimmten kombinatorischen Identitäten) ist der Satz von Bombieri–Vinogradov über die Verteilung von Primzahlen in Progressionen.

5. Das große Sieb

Linnik zeigte [1941], dass Ausnahmen der Vermutung von Vinogradov sehr selten sind: $\#\{p \leq x;\ q(p) \geq p^{\varepsilon}\} \ll_{\varepsilon} \log\log x$.

Er führte dazu eine neue Siebmethode ein, die nach ihm intensiv weiterentwickelt wurde. Man nennt sie heute die Methode des großen Siebs.

Eine der wichtigsten Anwendungen des großen Siebs (zusammen mit bestimmten kombinatorischen Identitäten) ist der Satz von Bombieri–Vinogradov über die Verteilung von Primzahlen in Progressionen.

Er besagt, dass die Riemannsche Vermutung für alle Moduln q bis zu einer bestimmten Schranke im Schnitt stimmt.

Der Satz von E. Bombieri und A. I. Vinogradov [1965/66]:

Für reelle $A, Q, x > 1$ gilt

$$\sum_{q \le Q} \sup_{y \le x} \max_{a \bmod q} |E(y; q, a)| \ll_A \frac{x}{(\log x)^A} + Q\sqrt{x}(\log(Qx))^3$$

Der Satz von E. Bombieri und A. I. Vinogradov [1965/66]:

Für reelle $A, Q, x > 1$ gilt

$$\sum_{q \le Q} \sup_{y \le x} \max_{a \bmod q} |E(y; q, a)| \ll_A \frac{x}{(\log x)^A} + Q\sqrt{x}(\log(Qx))^3$$

wobei

$$E(y; q, a) := \psi(y; q, a) - \frac{y}{\varphi(q)} \text{ mit } \psi(y; q, a) := \sum_{\substack{n \le y \\ n \equiv a \bmod \varphi^q}} \Lambda(n),$$

Der Satz von E. Bombieri und A. I. Vinogradov [1965/66]:

Für reelle $A, Q, x > 1$ gilt

$$\sum_{q \le Q} \sup_{y \le x} \max_{a \bmod q} |E(y; q, a)| \ll_A \frac{x}{(\log x)^A} + Q\sqrt{x}(\log(Qx))^3$$

wobei

$$E(y; q, a) := \psi(y; q, a) - \frac{y}{\varphi(q)} \text{ mit } \psi(y; q, a) := \sum_{\substack{n \le y \\ n \equiv a \bmod \varphi^q}} \Lambda(n),$$

so dass die nichttriviale obere Schranke $\ll_A x(\log x)^{-A}$ für $Q \le x^{1/2}(\log x)^{-3-A}$ gilt.

Der Satz von E. Bombieri und A. I. Vinogradov [1965/66]:

Für reelle $A, Q, x > 1$ gilt

$$\sum_{q \le Q} \sup_{y \le x} \max_{a \bmod q} |E(y; q, a)| \ll_A \frac{x}{(\log x)^A} + Q\sqrt{x}(\log(Qx))^3$$

wobei

$$E(y; q, a) := \psi(y; q, a) - \frac{y}{\varphi(q)} \text{ mit } \psi(y; q, a) := \sum_{\substack{n \le y \\ n \equiv a \bmod \varphi^q}} \Lambda(n),$$

so dass die nichttriviale obere Schranke $\ll_A x(\log x)^{-A}$ für $Q \le x^{1/2}(\log x)^{-3-A}$ gilt.

Der Exponent $1/2$ müsste laut der Elliott–Halberstam-Vermutung durch $1 - \varepsilon$ ersetzbar sein, von einem Beweis davon ist man weit entfernt.

Über den Satz von Bombieri–Vinogradov

Über den Satz von Bombieri–Vinogradov

Über diesen Satz können Siebmethoden Ergebnisse liefern, die mit der Annahme der Riemannschen Vermutung konkurrieren können: Der Satz von Bombieri–Vinogradov hat viele Anwendungen.

Über den Satz von Bombieri–Vinogradov

Über diesen Satz können Siebmethoden Ergebnisse liefern, die mit der Annahme der Riemannschen Vermutung konkurrieren können: Der Satz von Bombieri–Vinogradov hat viele Anwendungen.

Z. B.: Heute wissen wir aufgrund des Satzes von Bombieri–Vinogradov, dass im Linnik-Problem zur kleinsten Primzahl in einer Progession die Abschätzung $p_{\min(q,a)} \ll q^{2+\varepsilon}$ wahr ist für fast alle q. Diese Schranke müsste unter Annahme der GRH für alle q gelten.

Über den Satz von Bombieri–Vinogradov

Über diesen Satz können Siebmethoden Ergebnisse liefern, die mit der Annahme der Riemannschen Vermutung konkurrieren können: Der Satz von Bombieri–Vinogradov hat viele Anwendungen.

Z. B.: Heute wissen wir aufgrund des Satzes von Bombieri–Vinogradov, dass im Linnik-Problem zur kleinsten Primzahl in einer Progession die Abschätzung $p_{\min(q,a)} \ll q^{2+\varepsilon}$ wahr ist für fast alle q. Diese Schranke müsste unter Annahme der GRH für alle q gelten.

Eine andere, sehr neue Anwendung des Satzes von Bombieri–Vinogradov: Die neuen Durchbrüche zur Primzahlzwillingslückenschranke nach GPY/Zhang/Tao/Maynard, vgl. später.

Die große Siebungleichung

Der wichtigste Schritt eines Fourier-analytischen Beweises des Großen Siebs (und damit des Satzes von Bombieri–Vinogradov) ist eine Ungleichung mit Exponentialsummen, die sogenannte große-Sieb-Ungleichung:

Die große Siebungleichung

Der wichtigste Schritt eines Fourier-analytischen Beweises des Großen Siebs (und damit des Satzes von Bombieri–Vinogradov) ist eine Ungleichung mit Exponentialsummen, die sogenannte große-Sieb-Ungleichung:

Sei $\{v_n\}$ eine Folge komplexer Zahlen, seien $M, N \in \mathbb{N}$ und sei $Q \geq 1$ eine reelle Zahl. Dann ist

$$\sum_{q \leq Q} \sum_{\substack{1 \leq a \leq q \\ \gcd(a,q)=1}} \left| \sum_{M < n \leq M+N} v_n e\left(\frac{a}{q} n\right) \right|^2 \leq (Q^2 + N) \|v\|^2,$$

wobei $\|v\|^2 := \sum_{M<n\leq M+N} |v_n|^2$, $e(\alpha) := \exp(2\pi i \alpha)$ für $\alpha \in \mathbb{R}$.

1. p-adische Nullstellen quadratischer Formen

Ein Problem von J.-P. Serre [1990] bzgl. der quadratischen Form $\varphi_{a,b}(X, Y, Z) = aX^2 + bY^2 - Z^2$ lautet: Für wieviele natürliche Zahlen a und b hat $\varphi_{a,b}$ eine nichttriviale rationale Nullstelle? Im Sinne des Lokal-Global-Prinzips von Minkowski fragt man dann nach den p-adischen Lösungen für jede Primzahl p. Es gibt eine p-adische Lösung genau dann wenn für das Hilbertsymbol $\left(\frac{a,b}{p}\right) = 1$ erfüllt ist.

1. p-adische Nullstellen quadratischer Formen

Ein Problem von J.-P. Serre [1990] bzgl. der quadratischen Form $\varphi_{a,b}(X,Y,Z) = aX^2 + bY^2 - Z^2$ lautet: Für wieviele natürliche Zahlen a und b hat $\varphi_{a,b}$ eine nichttriviale rationale Nullstelle? Im Sinne des Lokal-Global-Prinzips von Minkowski fragt man dann nach den p-adischen Lösungen für jede Primzahl p. Es gibt eine p-adische Lösung genau dann wenn für das Hilbertsymbol $\left(\frac{a,b}{p}\right) = 1$ erfüllt ist.

Antwort: Die Anzahl Paare (a,b) mit $1 \leq a,b \leq H$, für die $\varphi_{a,b}$ eine nichttriviale rationale Nullstelle hat, ist $\ll H^2/\log\log H$.

1. p-adische Nullstellen quadratischer Formen

Ein Problem von J.-P. Serre [1990] bzgl. der quadratischen Form $\varphi_{a,b}(X,Y,Z) = aX^2 + bY^2 - Z^2$ lautet: Für wieviele natürliche Zahlen a und b hat $\varphi_{a,b}$ eine nichttriviale rationale Nullstelle? Im Sinne des Lokal-Global-Prinzips von Minkowski fragt man dann nach den p-adischen Lösungen für jede Primzahl p. Es gibt eine p-adische Lösung genau dann wenn für das Hilbertsymbol $\left(\frac{a,b}{p}\right) = 1$ erfüllt ist.

Antwort: Die Anzahl Paare (a,b) mit $1 \leq a,b \leq H$, für die $\varphi_{a,b}$ eine nichttriviale rationale Nullstelle hat, ist $\ll H^2/\log\log H$.

Genauer: Sei $\mathcal{P}$ eine unendliche Menge ungerader Primzahlen. Ist die Menge $\mathcal{P}_b := \{p \in \mathcal{P};\ (\frac{b}{p}) = -1\}$ hinreichend groß, so dass $\sum_{p\in\mathcal{P}_b} \frac{1}{p} = \infty$, dann hat für fast alle quadratfreien a, die teilerfremd zu $2b$ sind, die quadratische Form $\varphi_{a,b}$ keine nichttriviale p-adische Nullstelle für mindestens ein $p \in \mathcal{P}$.

2. Rationale Punkte auf kubischen Flächen

Wir betrachten kubische Flächen $F(x) = \varphi(u, v)$, wobei F ein kubisches Polynom und $\varphi(u, v)$ eine binäre quadratische Form ist.

2. Rationale Punkte auf kubischen Flächen

Wir betrachten kubische Flächen $F(x) = \varphi(u, v)$, wobei F ein kubisches Polynom und $\varphi(u, v)$ eine binäre quadratische Form ist.

Nimmt man bestimmte harmlose Bedingungen an, wurde gezeigt, dass es unendlich viele rationale Punkte auf Châtelet-Oberflächen gibt, wobei $\varphi(u, v) = u^2 - cv^2$ [H. Iwaniec und R. Munshi, 2010]. Für die Anzahl solcher Punkte mit beschränkter Höhe können einige starke Abschätzungen gezeigt werden.

2. Rationale Punkte auf kubischen Flächen

Wir betrachten kubische Flächen $F(x) = \varphi(u, v)$, wobei F ein kubisches Polynom und $\varphi(u, v)$ eine binäre quadratische Form ist.

Nimmt man bestimmte harmlose Bedingungen an, wurde gezeigt, dass es unendlich viele rationale Punkte auf Châtelet-Oberflächen gibt, wobei $\varphi(u, v) = u^2 - cv^2$ [H. Iwaniec und R. Munshi, 2010]. Für die Anzahl solcher Punkte mit beschränkter Höhe können einige starke Abschätzungen gezeigt werden.

Z. B. im Fall $c = -1$: Sei $F(X) = X^3 + \alpha X^2 + \beta X + \gamma \in \mathbb{Z}[X]$ mit $\alpha + \beta + \gamma \equiv 0 \bmod 4$. Dann enthält $F(x) = u^2 + v^2$ unendlich viele rationale Punkte (x, u, v). Die Anzahl solcher rationaler Punkte mit Nenner $\leq y$ ist $\gg y(\log y)^{-3/2}$.

3. Punkte auf elliptischen Kurven

Ein Problem vom Primzahlzwilllingstyp kann wie folgt auf elliptischen Kurven formuliert werden:
Betrachte eine elliptische Kurve $E(\mathbb{Q})$.

3. Punkte auf elliptischen Kurven

Ein Problem vom Primzahlzwilllingstyp kann wie folgt auf elliptischen Kurven formuliert werden:
Betrachte eine elliptische Kurve $E(\mathbb{Q})$.

Vermutung von Koblitz: Es gibt unendlich viele p, so dass die Ordnung $\#E(\mathbb{F}_p)$ eine Primzahl ist ($E(\mathbb{Q})$ ohne CM und nicht $\mathbb{Q}$-isogen zu einer elliptischen Kurve mit nichttrivialer $\mathbb{Q}$-Torsion).
Die Vermutung von Koblitz wahr „im Mittel“
[A. Balog, A. C. Cojocaru, C. David 2011].

3. Punkte auf elliptischen Kurven

Ein Problem vom Primzahlzwilllingstyp kann wie folgt auf elliptischen Kurven formuliert werden:
Betrachte eine elliptische Kurve $E(\mathbb{Q})$.

Vermutung von Koblitz: Es gibt unendlich viele p, so dass die Ordnung $\#E(\mathbb{F}_p)$ eine Primzahl ist ($E(\mathbb{Q})$ ohne CM und nicht $\mathbb{Q}$-isogen zu einer elliptischen Kurve mit nichttrivialer $\mathbb{Q}$-Torsion).
Die Vermutung von Koblitz wahr „im Mittel“
[A. Balog, A. C. Cojocaru, C. David 2011].

Z. B. kann für die Kurve $E : y^2 = x^3 - x$, gezeigt werden, dass

$$\#\{p \leq x;\ p \equiv 1\ (4),\ \#E(\mathbb{F}_p) = 8P_2\} \gg x(\log x)^2,$$

wobei P_2 eine natürliche Zahl mit höchstens zwei Primfaktoren ist.

3. Punkte auf elliptischen Kurven

Ein Problem vom Primzahlzwilllingstyp kann wie folgt auf elliptischen Kurven formuliert werden:
Betrachte eine elliptische Kurve $E(\mathbb{Q})$.

Vermutung von Koblitz: Es gibt unendlich viele p, so dass die Ordnung $\#E(\mathbb{F}_p)$ eine Primzahl ist ($E(\mathbb{Q})$ ohne CM und nicht $\mathbb{Q}$-isogen zu einer elliptischen Kurve mit nichttrivialer $\mathbb{Q}$-Torsion).
Die Vermutung von Koblitz wahr „im Mittel“
[A. Balog, A. C. Cojocaru, C. David 2011].

Z. B. kann für die Kurve $E : y^2 = x^3 - x$, gezeigt werden, dass

$$\#\{p \leq x;\ p \equiv 1\ (4),\ \#E(\mathbb{F}_p) = 8P_2\} \gg x(\log x)^2,$$

wobei P_2 eine natürliche Zahl mit höchstens zwei Primfaktoren ist.
Die erwartete asymptotische Formel, in der P_2 durch eine Primzahl ersetzt ist, ist eine offene Vermutung, die möglicherweise ebenso schwer wie das Zwillingsproblem selbst ist.

4. Probabilistische Galoistheorie

Sei $f(x) \in \mathbb{Z}[x]$ ein Polynom mit Leitkoeffizient 1.
Wir erwarten: $\mathrm{Gal}(f|\mathbb{Q}) \cong S_n$ mit Wahrscheinlichkeit 1.

4. Probabilistische Galoistheorie

Sei $f(x) \in \mathbb{Z}[x]$ ein Polynom mit Leitkoeffizient 1.
Wir erwarten: $\mathrm{Gal}(f|\mathbb{Q}) \cong S_n$ mit Wahrscheinlichkeit 1.
Betrachte

$$E_n(H) := \#\{(z_1, \ldots, z_n);\ |z_i| \leq H,\ 1 \leq i \leq n,$$
$$\text{so dass } f(x) = x^n + z_1 x^{n-1} + \cdots + z_n$$
$$\underline{\text{nicht}}\ S_n \text{ als Galoisgruppe hat}\}.$$

Man kann leicht zeigen, dass die Anzahl reduzibler f, für die $|z_i| \leq H$ gilt, $\gg H^{n-1}$ ist, so dass $E_n(H) \gg H^{n-1}$.

4. Probabilistische Galoistheorie

Sei $f(x) \in \mathbb{Z}[x]$ ein Polynom mit Leitkoeffizient 1.
Wir erwarten: $\mathrm{Gal}(f|\mathbb{Q}) \cong S_n$ mit Wahrscheinlichkeit 1.
Betrachte

$$E_n(H) := \#\{(z_1, \ldots, z_n);\ |z_i| \leq H,\ 1 \leq i \leq n,$$
$$\text{so dass } f(x) = x^n + z_1 x^{n-1} + \cdots + z_n$$
$$\underline{\text{nicht}}\ S_n \text{ als Galoisgruppe hat}\}.$$

Man kann leicht zeigen, dass die Anzahl reduzibler f, für die $|z_i| \leq H$ gilt, $\gg H^{n-1}$ ist, so dass $E_n(H) \gg H^{n-1}$.

Es wird vermutet, dass $E_n(H) \ll_{n,\varepsilon} H^{n-1+\varepsilon}$.
Für $n = 2, 3, 4$ konnte diese Schranke bestätigt werden [P. Lefton 1979, R. Dietmann 2012].

4. Probabilistische Galoistheorie

Sei $f(x) \in \mathbb{Z}[x]$ ein Polynom mit Leitkoeffizient 1.
Wir erwarten: $\mathrm{Gal}(f|\mathbb{Q}) \cong S_n$ mit Wahrscheinlichkeit 1.
Betrachte

$$E_n(H) := \#\{(z_1, \ldots, z_n);\ |z_i| \leq H,\ 1 \leq i \leq n,$$
$$\text{so dass } f(x) = x^n + z_1 x^{n-1} + \cdots + z_n$$
$$\underline{\text{nicht}}\ S_n \text{ als Galoisgruppe hat}\}.$$

Man kann leicht zeigen, dass die Anzahl reduzibler f, für die $|z_i| \leq H$ gilt, $\gg H^{n-1}$ ist, so dass $E_n(H) \gg H^{n-1}$.

Es wird vermutet, dass $E_n(H) \ll_{n,\varepsilon} H^{n-1+\varepsilon}$.
Für $n = 2, 3, 4$ konnte diese Schranke bestätigt werden [P. Lefton 1979, R. Dietmann 2012].

Die beste zur Zeit bekannte obere Schranke ist $E_n(H) \ll H^{n-1/2}$ [D. Zywina 2010].

5. Beispiel aus der Gruppentheorie

Frage: “Für wieviele $n \leq x$ ist jede Gruppe der Ordnung n zyklisch?”

5. Beispiel aus der Gruppentheorie

Frage: “Für wieviele $n \leq x$ ist jede Gruppe der Ordnung n zyklisch?”

Die Liste der Isomorphieklassen von Gruppen nach ihrer Ordnung sortiert beginnt mit

1	2	3	4	5	6	7
C_1	C_2	C_3	$C_4,\ C_2^2$	C_5	$C_6 = C_3 \times C_2,\ S_3$	C_7

8	9	10	
$C_8,\ C_4 \times C_2,\ C_2^3,\ \mathrm{Dih}_4,\ \mathrm{Q}_8$	$C_9,\ C_3^2$	$C_{10} = C_5 \times C_2,\ \mathrm{Dih}_5$	$\ldots$

5. Beispiel aus der Gruppentheorie

Frage: "Für wieviele $n \leq x$ ist jede Gruppe der Ordnung n zyklisch?"

Die Liste der Isomorphieklassen von Gruppen nach ihrer Ordnung sortiert beginnt mit

1	2	3	4	5	6	7
C_1	C_2	C_3	$C_4,\ C_2^2$	C_5	$C_6 = C_3 \times C_2,\ S_3$	C_7

8	9	10	
$C_8,\ C_4 \times C_2,\ C_2^3,\ \mathrm{Dih}_4,\ \mathrm{Q}_8$	$C_9,\ C_3^2$	$C_{10} = C_5 \times C_2,\ \mathrm{Dih}_5$	...

Wir erhalten die Anzahl von Isomorphieklassen von Gruppen der Ordnung $1, 2, 3, 4, \ldots$ wie folgt:

1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, 5, 1, 2, 1, 14, 1, 5, 1, 5, 2, 2, 1, 15, 2, 2, 5, 4, 1, 4, 1, 51, 1, 2, 1, 14, 1, 2, 2, 14, 1, 6, 1, 4, 2, 2, 1, 52, 2, 5, 1, 5, 1, 15, 2, 13, 2, 2, 1, 13, 1, 2, 4, 267, 1, 4, 1, 5, 1, 4, 1, 50, 1, 2, 3, 4, 1, 6, 1, 52, 15, 2, 1, 15, 1, 2, 1, 12, ...

5. Beispiel aus der Gruppentheorie

Frage: "Für wieviele $n \leq x$ ist jede Gruppe der Ordnung n zyklisch?"

Die Liste der Isomorphieklassen von Gruppen nach ihrer Ordnung sortiert beginnt mit

1	2	3	4	5	6	7
C_1	C_2	C_3	$C_4,\ C_2^2$	C_5	$C_6 = C_3 \times C_2,\ S_3$	C_7

8	9	10	
$C_8,\ C_4 \times C_2,\ C_2^3,\ \mathrm{Dih}_4,\ \mathrm{Q}_8$	$C_9,\ C_3^2$	$C_{10} = C_5 \times C_2,\ \mathrm{Dih}_5$	...

Wir erhalten die Anzahl von Isomorphieklassen von Gruppen der Ordnung $1, 2, 3, 4, \ldots$ wie folgt:

1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, 5, 1, 2, 1, 14, 1, 5, 1, 5, 2, 2, 1, 15, 2, 2, 5, 4, 1, 4, 1, 51, 1, 2, 1, 14, 1, 2, 2, 14, 1, 6, 1, 4, 2, 2, 1, 52, 2, 5, 1, 5, 1, 15, 2, 13, 2, 2, 1, 13, 1, 2, 4, 267, 1, 4, 1, 5, 1, 4, 1, 50, 1, 2, 3, 4, 1, 6, 1, 52, 15, 2, 1, 15, 1, 2, 1, 12, ...

Siebargumentation

Für welche n gibt es genau eine Isomorphieklasse (nämlich nur die zyklische Gruppe)?

Siebargumentation

Für welche n gibt es genau eine Isomorphieklasse (nämlich nur die zyklische Gruppe)?

Ein Satz der Gruppentheorie besagt, dass dies genau dann der Fall ist, wenn $\gcd(n, \varphi(n)) = 1$ gilt [Szele 1947].

Betrachte $A(x) := \#\{n \leq x;\ \gcd(n, \varphi(n)) = 1\}$.

Siebargumentation

Für welche n gibt es genau eine Isomorphieklasse (nämlich nur die zyklische Gruppe)?

Ein Satz der Gruppentheorie besagt, dass dies genau dann der Fall ist, wenn $\gcd(n, \varphi(n)) = 1$ gilt [Szele 1947].

Betrachte $A(x) := \#\{n \leq x;\ \gcd(n, \varphi(n)) = 1\}$.
Beobachtung: n mit $\gcd(n, \varphi(n)) = 1$ ist nicht teilbar durch eine Primzahl $q \equiv 1 \bmod p$ für $p \mid n$, sonst wäre $p \mid \gcd(n, \varphi(n))$.

Siebargumentation

Für welche n gibt es genau eine Isomorphieklasse (nämlich nur die zyklische Gruppe)?

Ein Satz der Gruppentheorie besagt, dass dies genau dann der Fall ist, wenn $\gcd(n, \varphi(n)) = 1$ gilt [Szele 1947].

Betrachte $A(x) := \#\{n \leq x;\ \gcd(n, \varphi(n)) = 1\}$.
Beobachtung: n mit $\gcd(n, \varphi(n)) = 1$ ist nicht teilbar durch eine Primzahl $q \equiv 1 \bmod p$ für $p \mid n$, sonst wäre $p \mid \gcd(n, \varphi(n))$.

Diese Beobachtung kann für ein Siebargument benutzt werden: Für jede Primzahl p betrachte die Menge der n, die p als kleinsten Primteiler hat. Streiche in dieser Menge alle Vielfachen von Primzahlen $q \equiv 1 \bmod p$.

Ein Ergebnis von Erdős

Erdős benutzte dieses Siebargument und teilte die Menge der n auf nach der Größe ihres kleinsten Primteilers p auf.

Ein Ergebnis von Erdős

Erdős benutzte dieses Siebargument und teilte die Menge der n auf nach der Größe ihres kleinsten Primteilers p auf.

Durch Anwendung einer trickreichen Kombination des Brunschen Siebs mit dem obigen Ergebnis zur Anzahl der n ohne kleinen Primfaktoren zeigte er:

Ein Ergebnis von Erdős

Erdős benutzte dieses Siebargument und teilte die Menge der n auf nach der Größe ihres kleinsten Primteilers p auf.

Durch Anwendung einer trickreichen Kombination des Brunschen Siebs mit dem obigen Ergebnis zur Anzahl der n ohne kleinen Primfaktoren zeigte er:

Theorem [Erdős 1948]:

Die Anzahl $A(x)$ der $n \leq x$, für die jede Gruppe der Ordnung n zyklisch ist, ist

$$A(x) \sim \frac{e^{-\gamma} x}{\log \log \log x}$$

für $x \to \infty$, wobei γ die Euler–Mascheroni-Konstante ist.

6. Neue Richtungen der großen-Sieb-Methode

Das folgende Problem kann als Analogon des Linnik-Problems im Kontext elliptischer Kurven verstanden werden:

6. Neue Richtungen der großen-Sieb-Methode

Das folgende Problem kann als Analogon des Linnik-Problems im Kontext elliptischer Kurven verstanden werden:
Gegeben seien zwei nichtisogene elliptische Kurven E_1 und E_2 über $\mathbb{Q}$, was ist die kleinste Primzahl p mit guter Reduktion, so dass $\#E_1(\mathbb{F}_p) \neq \#E_2(\mathbb{F}_p)$?

6. Neue Richtungen der großen-Sieb-Methode

Das folgende Problem kann als Analogon des Linnik-Problems im Kontext elliptischer Kurven verstanden werden:
Gegeben seien zwei nichtisogene elliptische Kurven E_1 und E_2 über $\mathbb{Q}$, was ist die kleinste Primzahl p mit guter Reduktion, so dass $\#E_1(\mathbb{F}_p) \neq \#E_2(\mathbb{F}_p)$?

Diese Frage wurde [1981] von J.-P. Serre untersucht. Er zeigt unter Annahme der GRH (für Dedekindsche Zeta-Funktionen): Es gibt so ein $p \ll (\log D)^2$, wenn D eine gemeinsame obere Schranke der Führungszahl von E_1 und E_2 ist.

6. Neue Richtungen der großen-Sieb-Methode

Das folgende Problem kann als Analogon des Linnik-Problems im Kontext elliptischer Kurven verstanden werden:
Gegeben seien zwei nichtisogene elliptische Kurven E_1 und E_2 über $\mathbb{Q}$, was ist die kleinste Primzahl p mit guter Reduktion, so dass $\#E_1(\mathbb{F}_p) \neq \#E_2(\mathbb{F}_p)$?

Diese Frage wurde [1981] von J.-P. Serre untersucht. Er zeigt unter Annahme der GRH (für Dedekindsche Zeta-Funktionen): Es gibt so ein $p \ll (\log D)^2$, wenn D eine gemeinsame obere Schranke der Führungszahl von E_1 und E_2 ist.

O.A.u.V. zeigten W. Duke und E. Kowalski [2000] eine statistische Version vom Linnik-Typ dieser Behauptung.

6. Neue Richtungen der großen-Sieb-Methode

Das folgende Problem kann als Analogon des Linnik-Problems im Kontext elliptischer Kurven verstanden werden:
Gegeben seien zwei nichtisogene elliptische Kurven E_1 und E_2 über $\mathbb{Q}$, was ist die kleinste Primzahl p mit guter Reduktion, so dass $\#E_1(\mathbb{F}_p) \neq \#E_2(\mathbb{F}_p)$?

Diese Frage wurde [1981] von J.-P. Serre untersucht. Er zeigt unter Annahme der GRH (für Dedekindsche Zeta-Funktionen): Es gibt so ein $p \ll (\log D)^2$, wenn D eine gemeinsame obere Schranke der Führungszahl von E_1 und E_2 ist.

O.A.u.V. zeigten W. Duke und E. Kowalski [2000] eine statistische Version vom Linnik-Typ dieser Behauptung.
In ihrem Beweis formulierten sie das Problem um zu einem über Spitzenformen und zeigten eine große-Sieb-Ungleichung für Spitzenformen, welche die Schlüsselrolle in ihrem Beweis spielt.

Kleine Primzahllücken

Ansatz zur Zwillingsvermutung: Zähle “kleine Primzahllücken”

Kleine Primzahllücken

Ansatz zur Zwillingsvermutung: Zähle “kleine Primzahllücken”

Eine *Primzahllücke* ist eine Differenz $p_{n+1} - p_n$ für $n \in \mathbb{N}$, wenn $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ die unendliche Folge der Primzahlen bezeichnet.

Kleine Primzahllücken

Ansatz zur Zwillingsvermutung: Zähle "kleine Primzahllücken"

Eine *Primzahllücke* ist eine Differenz $p_{n+1} - p_n$ für $n \in \mathbb{N}$, wenn $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ die unendliche Folge der Primzahlen bezeichnet.

Wie klein ist die kleinste Primzahllücke, die nachweislich unendlich oft vorkommt, d. h. wie kann

$$\liminf_{n \to \infty} (p_{n+1} - p_n)$$

nach oben abgeschätzt werden?

Kleine Primzahllücken

Ansatz zur Zwillingsvermutung: Zähle "kleine Primzahllücken"

Eine *Primzahllücke* ist eine Differenz $p_{n+1} - p_n$ für $n \in \mathbb{N}$, wenn $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ die unendliche Folge der Primzahlen bezeichnet.

Wie klein ist die kleinste Primzahllücke, die nachweislich unendlich oft vorkommt, d. h. wie kann

$$\liminf_{n \to \infty} (p_{n+1} - p_n)$$

nach oben abgeschätzt werden?

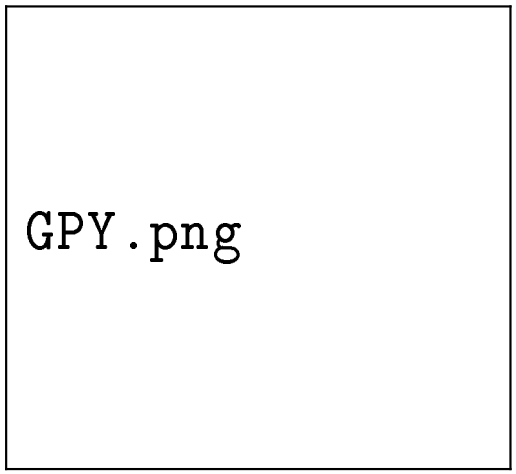
Die Zwillingsvermutung ist genau die Aussage, dass dieser Wert $= 2$ ist.

Der Durchbruch von GPY im Jahr 2005

Laut Primzahlsatz beträgt die Differenz $p_{n+1} - p_n$ *im Mittel* etwa $\log p_n$.

Der Durchbruch von GPY im Jahr 2005

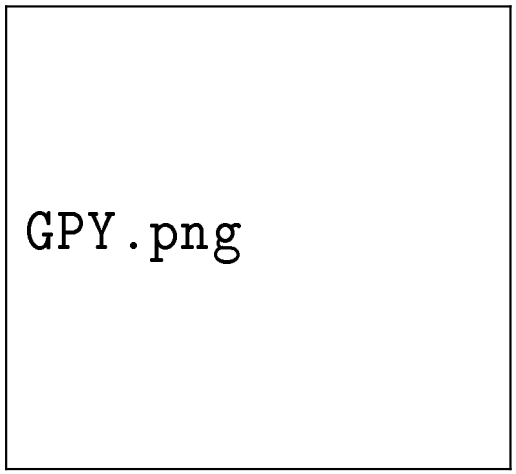
Laut Primzahlsatz beträgt die Differenz $p_{n+1} - p_n$ *im Mittel* etwa $\log p_n$. Tatsächlich ist diese unendlich oft kleiner:



v.r.n.l.: D. Goldston, J. Pintz,
C. Yıldırım (GPY 2005)

Der Durchbruch von GPY im Jahr 2005

Laut Primzahlsatz beträgt die Differenz $p_{n+1} - p_n$ *im Mittel* etwa $\log p_n$. Tatsächlich ist diese unendlich oft kleiner:



v.r.n.l.: D. Goldston, J. Pintz, C. Yıldırım (GPY 2005)

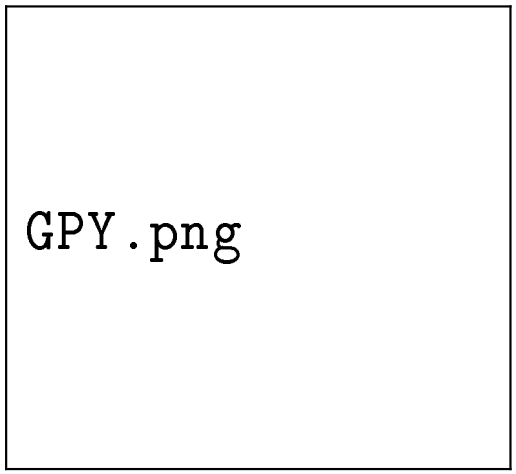
Beweis der *"small gap conjecture"*

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0$$

(sogar unendlich oft kleiner als $\sqrt{\log p_n}(\log\log p_n)^2$)

Der Durchbruch von GPY im Jahr 2005

Laut Primzahlsatz beträgt die Differenz $p_{n+1} - p_n$ *im Mittel* etwa $\log p_n$. Tatsächlich ist diese unendlich oft kleiner:



v.r.n.l.: D. Goldston, J. Pintz, C. Yıldırım (GPY 2005)

Beweis der *"small gap conjecture"*

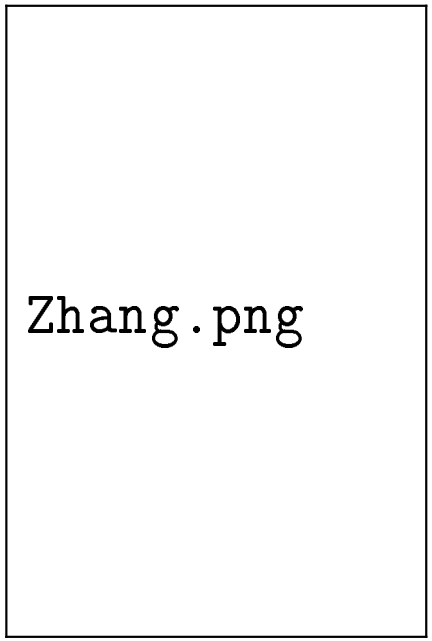
$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0$$

(sogar unendlich oft kleiner als $\sqrt{\log p_n}(\log\log p_n)^2$)

Beweis der *"bounded gap conjecture"* unter Annahme der Elliott–Halberstam-Vermutung:

$$\liminf_{n\to\infty} (p_{n+1} - p_n) \leq 16$$

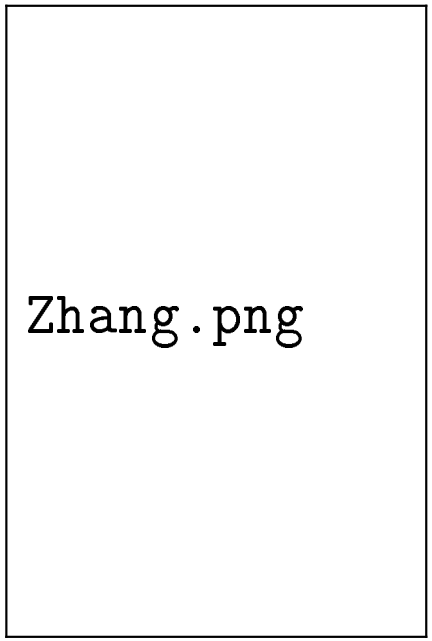
Der Durchbruch im Mai 2013



Y. Zhang

Am 14. Mai 2013 wurde bekannt, dass Y. Zhang die „bounded gap conjecture“ gelöst hat:

Der Durchbruch im Mai 2013



Y. Zhang

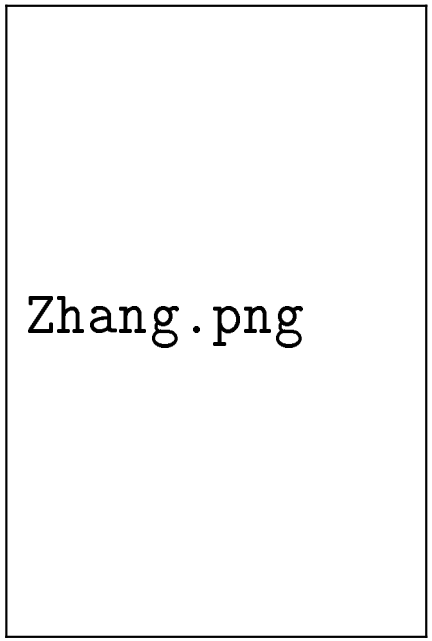
Am 14. Mai 2013 wurde bekannt, dass Y. Zhang die „bounded gap conjecture“ gelöst hat:

Er wies die Existenz einer Konstanten $H > 0$ nach, für die

$$\liminf_{n\to\infty} (p_{n+1} - p_n) \leq H$$

gilt, ganz ohne Annahme einer unbewiesenen Vermutung.

Der Durchbruch im Mai 2013



Y. Zhang

Am 14. Mai 2013 wurde bekannt, dass Y. Zhang die „bounded gap conjecture“ gelöst hat:

Er wies die Existenz einer Konstanten $H > 0$ nach, für die

$$\liminf_{n\to\infty} (p_{n+1} - p_n) \leq H$$

gilt, ganz ohne Annahme einer unbewiesenen Vermutung.

In seinem Beweis leitet er für die Zwillingslückenschranke H den numerischen Wert $H = 70.000.000$ her.

Über Yitang Zhang

Y. Zhang studierte 1978 bis Mitte der 1980er in Beijing.

Über Yitang Zhang

Y. Zhang studierte 1978 bis Mitte der 1980er in Beijing.
Er promovierte 1992 in Purdue.

Über Yitang Zhang

Y. Zhang studierte 1978 bis Mitte der 1980er in Beijing.
Er promovierte 1992 in Purdue.
Er fand im Anschluss keine akademische Anstellung, arbeitete daraufhin in diversen Jobs, u. a. in einem Sandwich-Shop von Subway, einem Motel, als Bote für einen Liefer-Service.

Über Yitang Zhang

Y. Zhang studierte 1978 bis Mitte der 1980er in Beijing.
Er promovierte 1992 in Purdue.
Er fand im Anschluss keine akademische Anstellung, arbeitete daraufhin in diversen Jobs, u. a. in einem Sandwich-Shop von Subway, einem Motel, als Bote für einen Liefer-Service.
1999 fand er eine Lecturer-Stelle an der University of New Hampshire.

Über Yitang Zhang

Y. Zhang studierte 1978 bis Mitte der 1980er in Beijing.
Er promovierte 1992 in Purdue.
Er fand im Anschluss keine akademische Anstellung, arbeitete daraufhin in diversen Jobs, u. a. in einem Sandwich-Shop von Subway, einem Motel, als Bote für einen Liefer-Service.
1999 fand er eine Lecturer-Stelle an der University of New Hampshire.

Er entwickelte ausgefeilte, tiefe Resultate und hatte wichtige Schlüsselideen, die Experten entgangen waren.

Über Yitang Zhang

Y. Zhang studierte 1978 bis Mitte der 1980er in Beijing.
Er promovierte 1992 in Purdue.
Er fand im Anschluss keine akademische Anstellung, arbeitete daraufhin in diversen Jobs, u. a. in einem Sandwich-Shop von Subway, einem Motel, als Bote für einen Liefer-Service.
1999 fand er eine Lecturer-Stelle an der University of New Hampshire.

Er entwickelte ausgefeilte, tiefe Resultate und hatte wichtige Schlüsselideen, die Experten entgangen waren. Seine Arbeit schrieb Zhang so, dass sie nicht gleich abgelehnt werden konnte. Er war zu dem Zeitpunkt 57 Jahre alt.

Über Yitang Zhang

Y. Zhang studierte 1978 bis Mitte der 1980er in Beijing.
Er promovierte 1992 in Purdue.
Er fand im Anschluss keine akademische Anstellung, arbeitete daraufhin in diversen Jobs, u. a. in einem Sandwich-Shop von Subway, einem Motel, als Bote für einen Liefer-Service.
1999 fand er eine Lecturer-Stelle an der University of New Hampshire.

Er entwickelte ausgefeilte, tiefe Resultate und hatte wichtige Schlüsselideen, die Experten entgangen waren. Seine Arbeit schrieb Zhang so, dass sie nicht gleich abgelehnt werden konnte. Er war zu dem Zeitpunkt 57 Jahre alt.
Die Geschichte über Zhang fand ein gewaltiges Medien-Echo, u. a. berichtete am 21. Mai 2013 die New York Times über ihn.

Über Yitang Zhang

Y. Zhang studierte 1978 bis Mitte der 1980er in Beijing.
Er promovierte 1992 in Purdue.
Er fand im Anschluss keine akademische Anstellung, arbeitete daraufhin in diversen Jobs, u. a. in einem Sandwich-Shop von Subway, einem Motel, als Bote für einen Liefer-Service.
1999 fand er eine Lecturer-Stelle an der University of New Hampshire.

Er entwickelte ausgefeilte, tiefe Resultate und hatte wichtige Schlüsselideen, die Experten entgangen waren. Seine Arbeit schrieb Zhang so, dass sie nicht gleich abgelehnt werden konnte. Er war zu dem Zeitpunkt 57 Jahre alt.
Die Geschichte über Zhang fand ein gewaltiges Medien-Echo, u. a. berichtete am 21. Mai 2013 die New York Times über ihn. Zhang erhielt viele Preise für seinen Durchbruch. Heute ist er Professor an seiner Universität in New Hampshire.

Das Polymath-Projekt von Terence Tao

Von T. Tao wurde daraufhin ein Internet-Projekt namens Polymath 8 initiiert, das mehreren Autoren die gemeinsame numerische Verbesserung der Schranke H erlaubte.

Das Polymath-Projekt von Terence Tao

Von T. Tao wurde daraufhin ein Internet-Projekt namens Polymath 8 initiiert, das mehreren Autoren die gemeinsame numerische Verbesserung der Schranke H erlaubte.

Auf der Internet-Webseite des Projekts kann die Entwicklung abgerufen werden. Eine Auswahl:

Datum	Autor	H
14. Mai 2013	Zhang	70.000.000
3. Juni 2013	Tao	285.456
16. Juni 2013	Sutherland	60.744
5. Juli 2013	Engelsma	5.414

Das Polymath-Projekt von Terence Tao

Von T. Tao wurde daraufhin ein Internet-Projekt namens Polymath 8 initiiert, das mehreren Autoren die gemeinsame numerische Verbesserung der Schranke H erlaubte.

Auf der Internet-Webseite des Projekts kann die Entwicklung abgerufen werden. Eine Auswahl:

Datum	Autor	H
14. Mai 2013	Zhang	70.000.000
3. Juni 2013	Tao	285.456
16. Juni 2013	Sutherland	60.744
5. Juli 2013	Engelsma	5.414

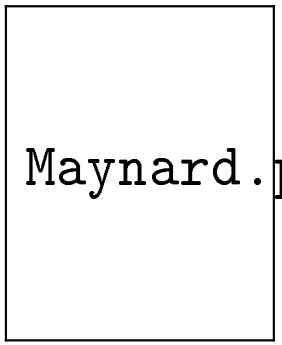
Das Projekt wurde mit $H = 4.680$ abgeschlossen.
Dabei wurden einige Vereinfachungen in Zhangs Beweis erzielt.

Der Durchbruch im November 2013

Im Oktober 2013 haben Terence Tao und James Maynard (unabhängig voneinander) eine Idee zur Verbesserung des GPY-Ansatzes, die die schwierigen Sätze von Zhang umgehen und numerisch überlegen ist.

Der Durchbruch im November 2013

Im Oktober 2013 haben Terence Tao und James Maynard (unabhängig voneinander) eine Idee zur Verbesserung des GPY-Ansatzes, die die schwierigen Sätze von Zhang umgehen und numerisch überlegen ist.

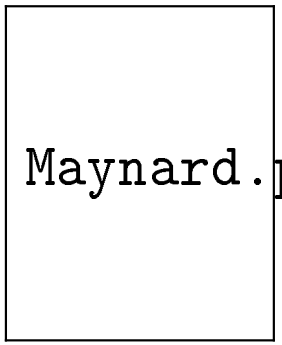


James Maynard

Am 19. November 2013 wurde von James Maynard (damals 26 Jahre alt) eine Arbeit bei arXiv veröffentlicht, in der er die Zwillingslückenschranke von Zhang auf $H = 600$ verbessert.

Der Durchbruch im November 2013

Im Oktober 2013 haben Terence Tao und James Maynard (unabhängig voneinander) eine Idee zur Verbesserung des GPY-Ansatzes, die die schwierigen Sätze von Zhang umgehen und numerisch überlegen ist.



James Maynard

Am 19. November 2013 wurde von James Maynard (damals 26 Jahre alt) eine Arbeit bei arXiv veröffentlicht, in der er die Zwillingslückenschranke von Zhang auf $H = 600$ verbessert.

James Maynard hatte 2009 in Oxford bei R. Heath-Brown promoviert und 2013–2014 in Montréal bei A. Granville geforscht.

Das Projekt Polymath 8b

Das Polymath-Projekt wurde am Tag der Veröffentlichung der Maynard-Arbeit von Terence Tao in die Projekte 8a (das bisherige, was nicht weiter verfolgt wird) und 8b aufgespalten.

Das Projekt Polymath 8b

Das Polymath-Projekt wurde am Tag der Veröffentlichung der Maynard-Arbeit von Terence Tao in die Projekte 8a (das bisherige, was nicht weiter verfolgt wird) und 8b aufgespalten.

Das neue Projekt 8b arbeitete an den weiteren Verbesserungen der Maynard-Methode. Mittlerweile ist so die Zwillingslückenschranke auf $H = 246$ gedrückt worden.

Das Projekt Polymath 8b

Das Polymath-Projekt wurde am Tag der Veröffentlichung der Maynard-Arbeit von Terence Tao in die Projekte 8a (das bisherige, was nicht weiter verfolgt wird) und 8b aufgespalten.

Das neue Projekt 8b arbeitete an den weiteren Verbesserungen der Maynard-Methode. Mittlerweile ist so die Zwillingslückenschranke auf $H = 246$ gedrückt worden.

Unter Annahme der (EH) zeigt die Maynard-Methode $H = 12$, und unter Annahme einer technischen Verallgemeinerung der (EH) kann diese sogar auf $H = 6$ gedrückt werden.

Das Projekt Polymath 8b

Das Polymath-Projekt wurde am Tag der Veröffentlichung der Maynard-Arbeit von Terence Tao in die Projekte 8a (das bisherige, was nicht weiter verfolgt wird) und 8b aufgespalten.

Das neue Projekt 8b arbeitete an den weiteren Verbesserungen der Maynard-Methode. Mittlerweile ist so die Zwillingslückenschranke auf $H = 246$ gedrückt worden.

Unter Annahme der (EH) zeigt die Maynard-Methode $H = 12$, und unter Annahme einer technischen Verallgemeinerung der (EH) kann diese sogar auf $H = 6$ gedrückt werden.

Diese Werte für H sind derzeit die theoretisch besten, die mit den neuen, aktuellen Methoden erreicht werden können.

Zukunft?

Zur Zeit sind keine weitere neue Verbesserungen zu erwarten, es sind wiederum grundlegend neue Ideen erforderlich. Die neuen Methoden von Zhang/Tao/Maynard konnten aber bereits gewinnbringend zur Lösung weiterer Probleme eingesetzt werden.

Zukunft?

Zur Zeit sind keine weitere neue Verbesserungen zu erwarten, es sind wiederum grundlegend neue Ideen erforderlich. Die neuen Methoden von Zhang/Tao/Maynard konnten aber bereits gewinnbringend zur Lösung weiterer Probleme eingesetzt werden.

Im August 2014 gab James Maynard auf arXiv bekannt, dass er das Erdős–Rankin-Problem für große Primzahllücken gelöst hatte. Erdős hatte seinerzeit einen Preis von 10000 US-Dollar für die Lösung des Problems ausgelobt.

Zukunft?

Zur Zeit sind keine weitere neue Verbesserungen zu erwarten, es sind wiederum grundlegend neue Ideen erforderlich. Die neuen Methoden von Zhang/Tao/Maynard konnten aber bereits gewinnbringend zur Lösung weiterer Probleme eingesetzt werden.

Im August 2014 gab James Maynard auf arXiv bekannt, dass er das Erdős–Rankin-Problem für große Primzahllücken gelöst hatte. Erdős hatte seinerzeit einen Preis von 10000 US-Dollar für die Lösung des Problems ausgelobt.

In derselben Woche veröffentlichten Ford, Green, Konyagin, und Tao einen anderen Beweis desselben Problems, aber ebenso wie Maynard mit einer neuen Variante der Tao/Maynard-Methode.

Zukunft?

Zur Zeit sind keine weitere neue Verbesserungen zu erwarten, es sind wiederum grundlegend neue Ideen erforderlich. Die neuen Methoden von Zhang/Tao/Maynard konnten aber bereits gewinnbringend zur Lösung weiterer Probleme eingesetzt werden.

Im August 2014 gab James Maynard auf arXiv bekannt, dass er das Erdős–Rankin-Problem für große Primzahllücken gelöst hatte. Erdős hatte seinerzeit einen Preis von 10000 US-Dollar für die Lösung des Problems ausgelobt.

In derselben Woche veröffentlichten Ford, Green, Konyagin, und Tao einen anderen Beweis desselben Problems, aber ebenso wie Maynard mit einer neuen Variante der Tao/Maynard-Methode.
Satz von Ford-Green-Konyagin-Maynard-Tao [2014]:

$$p_{n+1} - p_n \gg \frac{\log n \ \log\log n \ \log\log\log\log n}{\log\log\log n}$$

(für unendlich viele n)

Vielen Dank!

Literatur:

- A. C. Cojocaru and M. Ram Murty, An Introduction to Sieve Methods and their Applications
- J. Friedlander and H. Iwaniec, Opera de Cribro
- G. Harman, Prime-Detecting Sieves