Primzahlen: vom antiken Griechenland bis in den Computer

Jakob Stix

Institut für Mathematik
Goethe–Universität Frankfurt am Main

28 April 2016

Girls'Day — GU-Frankfurt

Primzahlen

Atome (unteilbar!) der Multiplikation: $1001 = 7 \cdot 11 \cdot 13$

Definition

Eine **Primzahl** ist eine natürliche Zahl $p \geq 2$, die nur als Produkt zweier natürlicher Zahlen geschrieben werden kann, wenn ein Faktor die 1 ist.

$$2, 3, 4 = 2^2, 5, 6 = 2 \cdot 3, 7, 8 = 2^3, 9 = 3^2, 10 = 2 \cdot 5, 11, \ldots$$

$$\ldots, 37, \ldots 101, \ldots, 2017, \ldots, 2^{74.207.281} - 1 \approx 3{\cdot}10^{22.338.617}, \ldots$$

eindeutige Primfaktorzerlegung

- Jede natürliche Zahl hat Primfaktorzerlegung:

$$2016 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 = 2^5 \cdot 3^2 \cdot 7$$

- und zwar eindeutig!
- 1 ist keine Primzahl. Das würde die Eindeutigkeit stören.

17-Jahre-Zikade

Zikaden *Magicicada septendecim* (USA)

17 Jahre Larvenstadium für
nur wenige Wochen als Zikade

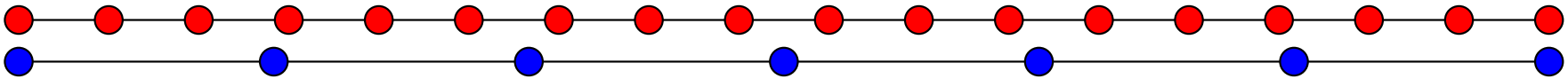
Freßfeinde: z.B. 6-jähriger Rhythmus

$\Longrightarrow$ „treffen sich“ nur alle

$$6 \cdot 17 = 102 \text{ Jahre!}$$

Die Zikade hungert ihre Freßfeinde aus!

(Martin Hauser/
Wikipedia)



Wieviele Primzahlen gibt es?

Unendlich viele!

Satz (Euklid)

Es gibt keine **größte** *Primzahl.*

Beweis.

- Angenommen $2, 3, 5, 7, 11, 13, 17$ ist die Liste aller Primzahlen.
- $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17) + 1$
- N hat Primteiler, aber
- N läßt Rest 1 bei Division durch jede Primzahl der Liste.
- $N = 59 \cdot 509$ hat „neue“ Primzahl als Teiler.

Wieviele Primzahlen gibt es?

Unendlich viele!

Satz (Euklid)

Es gibt keine **größte** *Primzahl.*

Beweis.

- Angenommen $p_1 = 2, p_2 = 3, \ldots, p_n$ ist die Liste aller Primzahlen.
- $N = (2 \cdot 3 \cdot \ldots \cdot p_{n-1} \cdot p_n) + 1$
- N hat Primteiler, aber
- N läßt Rest 1 bei Division durch jede Primzahl der Liste.
- Widerspruch dazu, daß wir bereits alle Primzahlen haben.

Sieb des Eratosthenes

		2	3	4	5	6	7	8	9
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

Sieb des Eratosthenes

		2	3	4	5	6	7	8	9
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

Sieb des Eratosthenes

		2	3		5		7		9
	11		13		15		17		19
	21		23		25		27		29
	31		33		35		37		39
	41		43		45		47		49
	51		53		55		57		59
	61		63		65		67		69
	71		73		75		77		79
	81		83		85		87		89
	91		93		95		97		99

Sieb des Eratosthenes

		2	3		5		7		9
	11		13		15		17		19
	21		23		25		27		29
	31		33		35		37		39
	41		43		45		47		49
	51		53		55		57		59
	61		63		65		67		69
	71		73		75		77		79
	81		83		85		87		89
	91		93		95		97		99

Sieb des Eratosthenes

		2	3		5		7		
	11		13				17		19
			23		25				29
	31				35		37		
	41		43				47		49
			53		55				59
	61				65		67		
	71		73				77		79
			83		85				89
	91				95		97		

Sieb des Eratosthenes

		2	3		5		7		
	11		13				17		19
			23		25				29
	31				35		37		
	41		43				47		49
			53		55				59
	61				65		67		
	71		73				77		79
			83		85				89
	91				95		97		

Sieb des Eratosthenes

		2	3		5		7		
	11		13				17		19
			23						29
	31						37		
	41		43				47		49
			53						59
	61						67		
	71		73				77		79
			83						89
	91						97		

Sieb des Eratosthenes

		2	3		5		7		
	11		13				17		19
			23						29
	31						37		
	41		43				47		49
			53						59
	61						67		
	71		73				77		79
			83						89
	91						97		

Sieb des Eratosthenes

		2	3		5		7		
	11		13				17		19
			23						29
	31						37		
	41		43				47		
			53						59
	61						67		
	71		73						79
			83						89
							97		

Sieb des Eratosthenes

		2	3		5		7		
	11		13				17		19
			23						29
	31						37		
	41		43				47		
			53						59
	61						67		
	71		73						79
			83						89
							97		

Sieb des Eratosthenes

		2	3		5		7		
	11		13				17		19
			23						29
	31						37		
	41		43				47		
			53						59
	61						67		
	71		73						79
			83						89
							97		

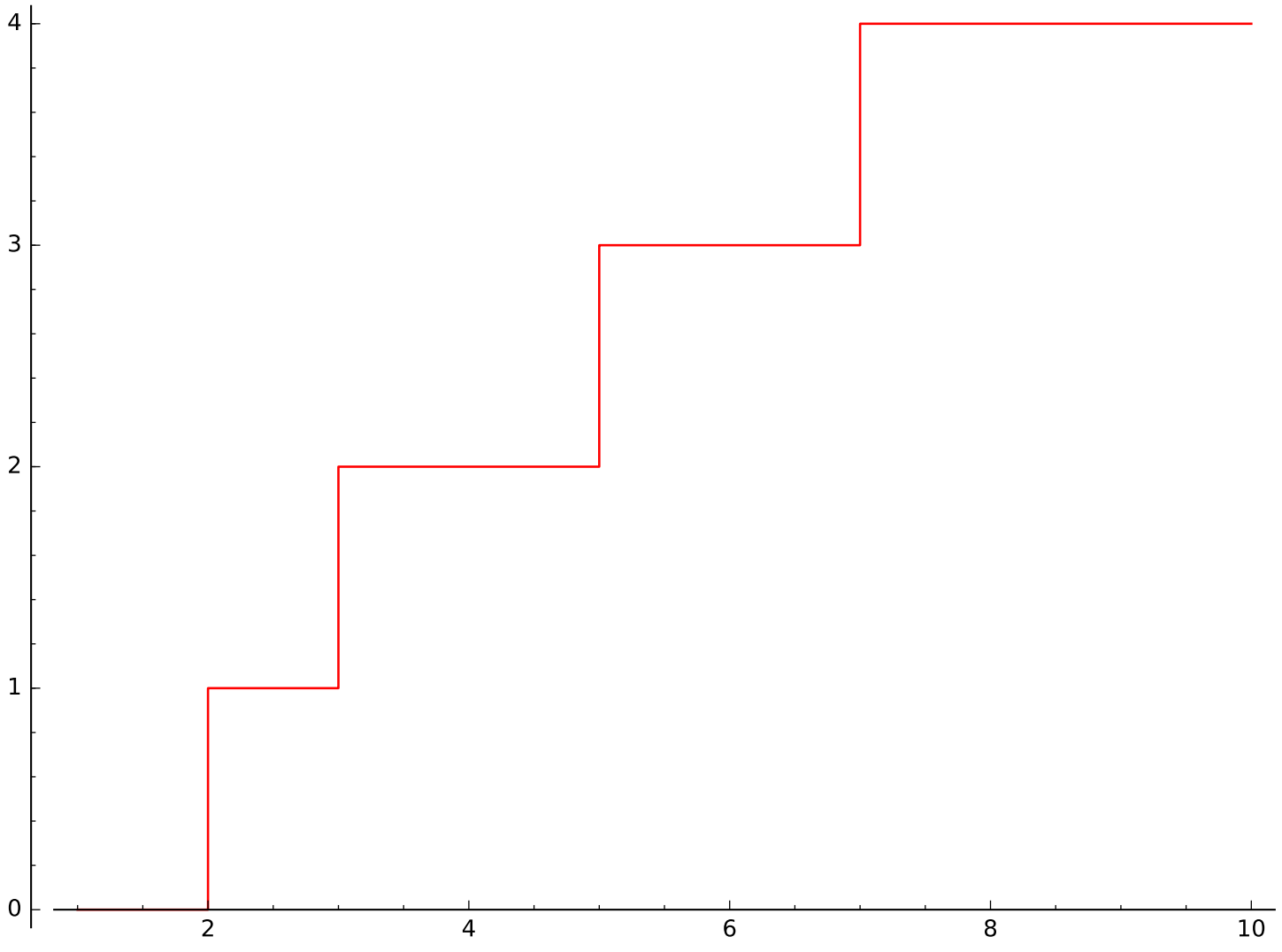
Sieb des Eratosthenes

		2	3		5		7		
	11		13				17		19
			23						29
	31						37		
	41		43				47		
			53						59
	61						67		
	71		73						79
			83						89
							97		

25 Primzahlen unter 100

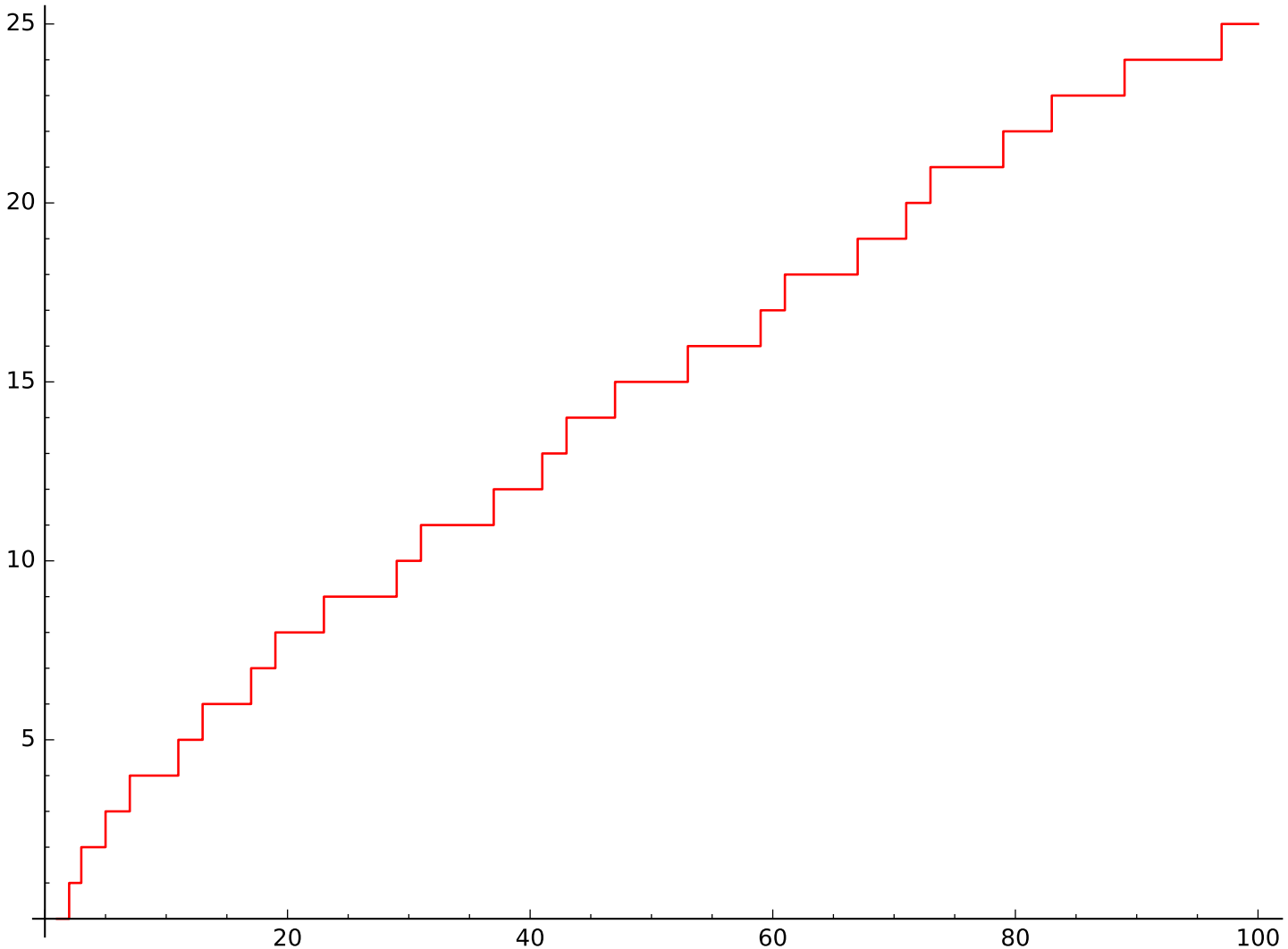
Primzahlverteilung

$\pi(x) :=$ Anzahl der Primzahlen $p \leq x$



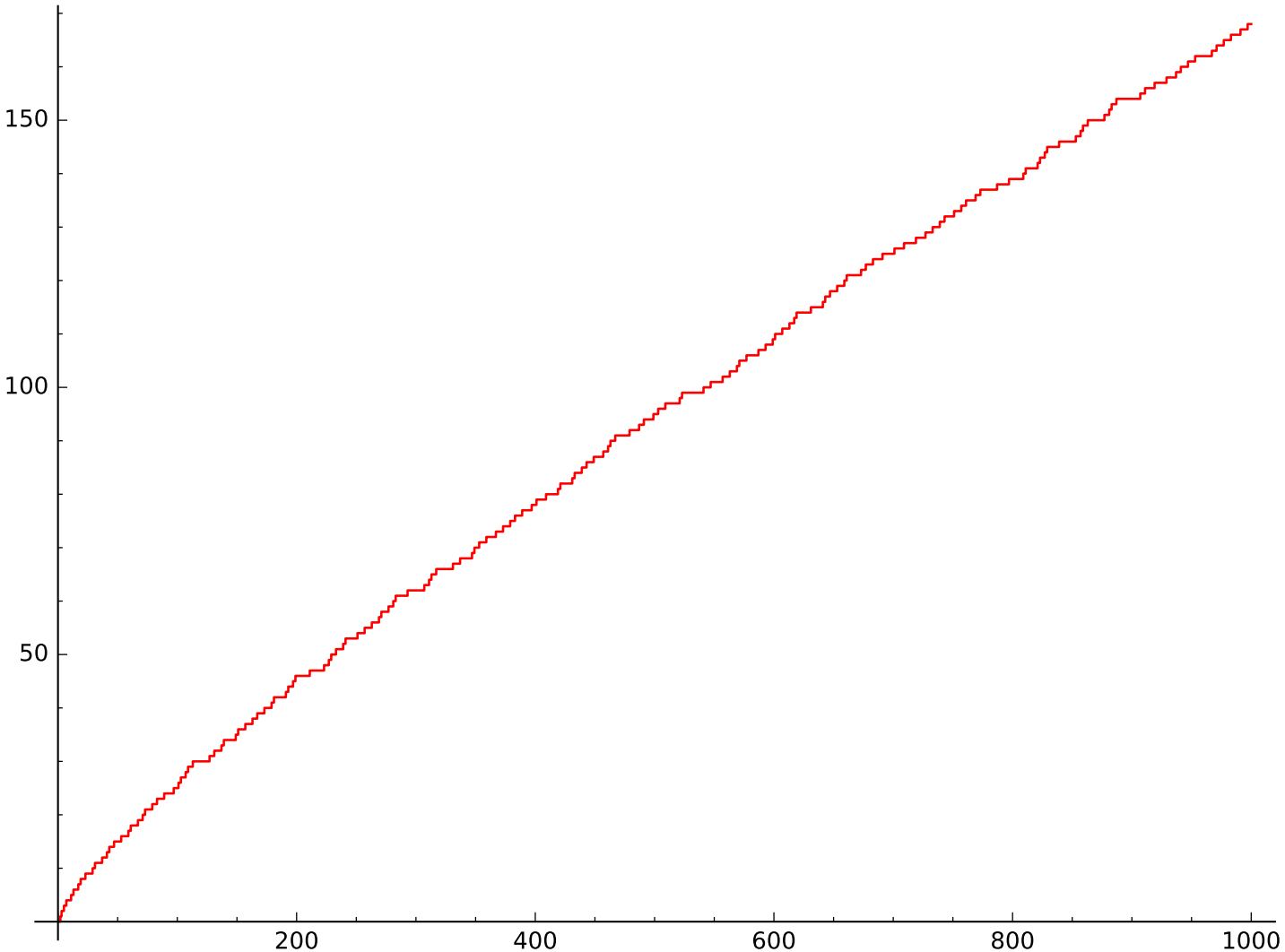
Primzahlverteilung

$\pi(x) :=$ Anzahl der Primzahlen $p \leq x$



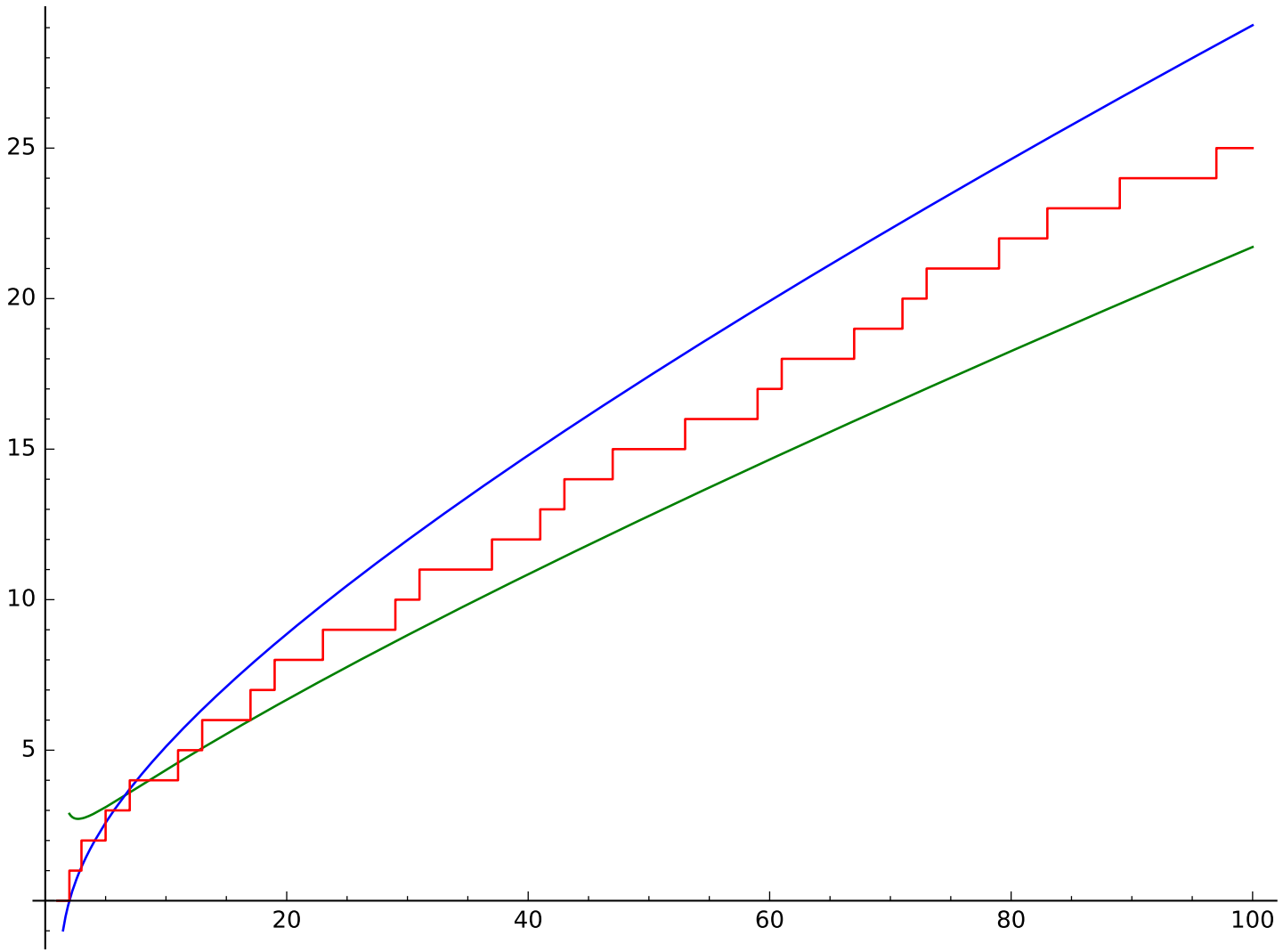
Primzahlverteilung

$\pi(x) :=$ Anzahl der Primzahlen $p \leq x$



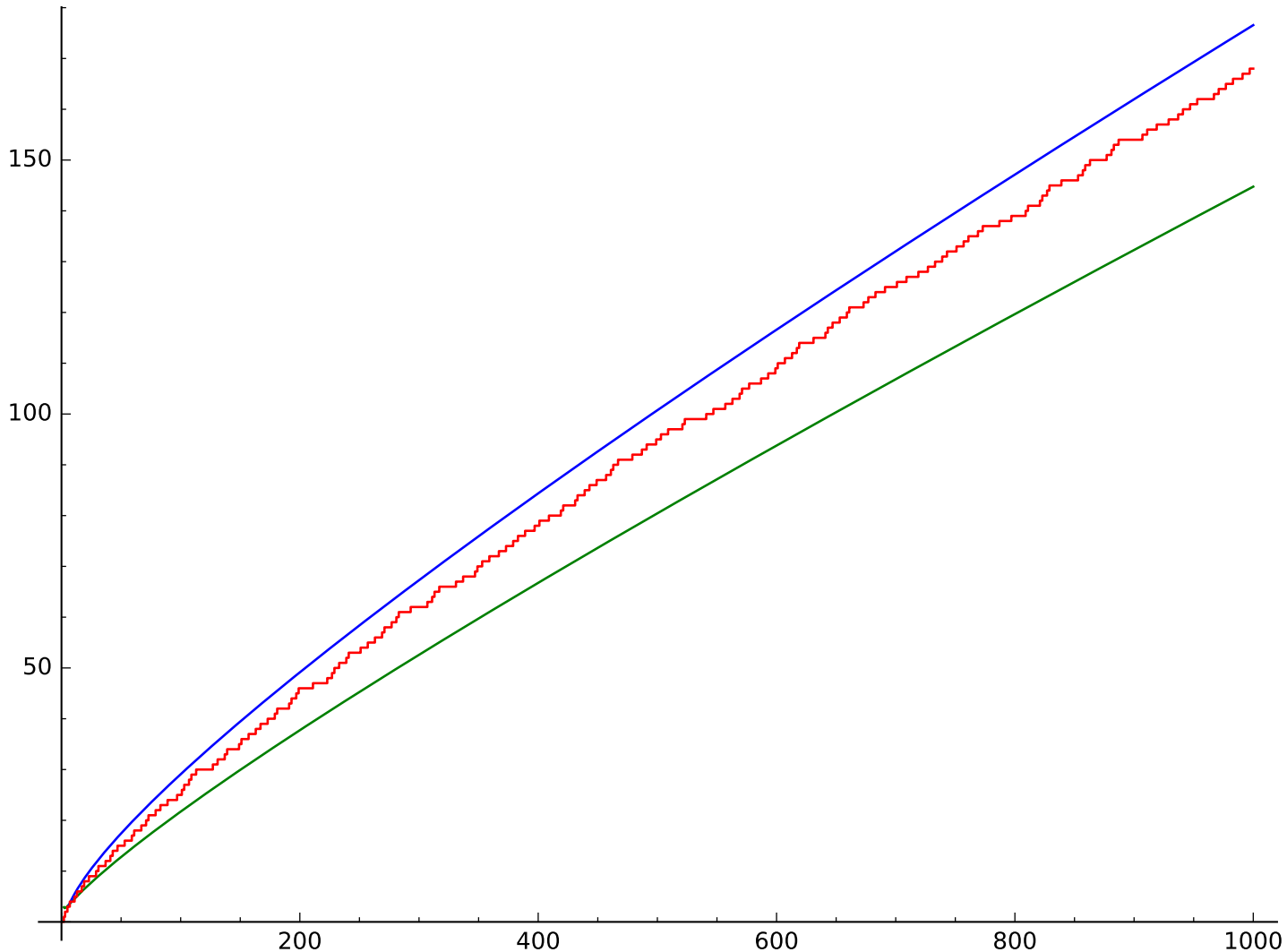
Primzahlsatz (1896)

$$\pi(x) \approx \frac{x}{\ln(x)} \approx \mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$$



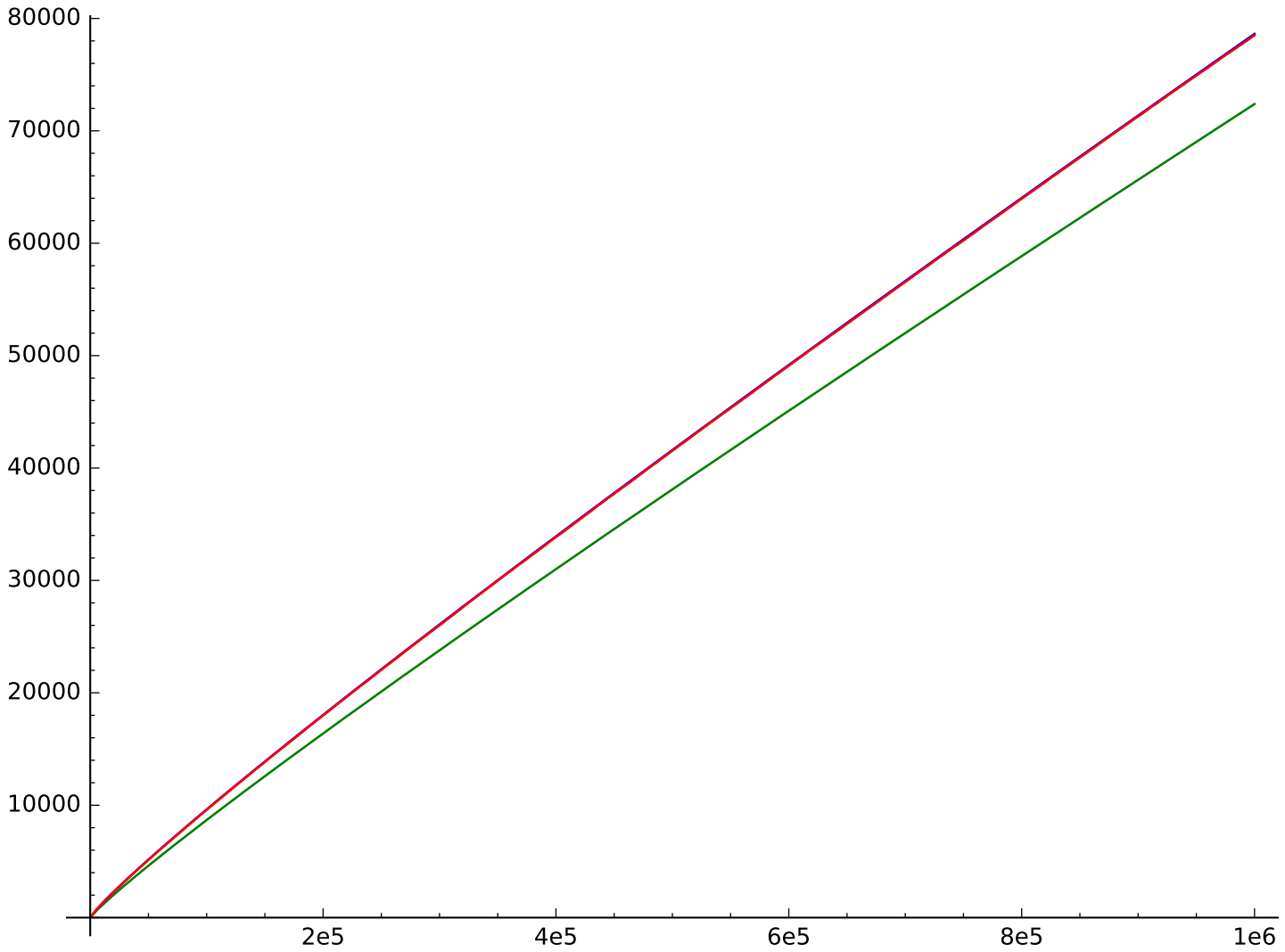
Primzahlsatz (1896)

$$\pi(x) \approx \frac{x}{\ln(x)} \approx \mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$$



Primzahlsatz (1896)

$$\pi(x) \approx \frac{x}{\ln(x)} \approx \mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$$



offene aktuelle Fragen

- **Goldbach**: läßt sich jede gerade natürliche Zahl ≥ 4 als Summe zweier Primzahlen schreiben?
- **Primzahlzwillinge**: gibt es unendlich viele Primzahlzwillinge?
  p und $p+2$ Primzahlen, Beispiel 101, 103
  Y. Zhang, J. Maynard 2014: es gibt unendlich viele Primzahlen p, so daß die nächste $\leq p + 600$.
- **Riemannsche Vermutung:** Fehlerterm beim Primzahlsatz, gibt es $c > 0$ mit

$$|\pi(x) - \mathrm{Li}(x)| \leq c \cdot (\sqrt{x} \cdot \ln(x)) \qquad ?$$

- **abc-Vermutung (Masser, Oesterlé):** Mochizuki ...

Rechnen mit der Uhr

10 Stunden nach 21 Uhr: Reste bei Division durch 12

$$21 + 10 = 31 \equiv 7 \pmod{12}$$

$$9 + 10 \equiv 7 \pmod{12}$$

auf der Uhr alles **modulo** 12

geht auch mit Multiplikation

$$7 \cdot 7 = 49 \equiv 1 \pmod{12}$$

Primzahlen modulo 12

		2	3	4	5	6	7	8	9	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	101	102	103	104	105	106	107
108	109	110	111	112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127	128	129	130	131
132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155
156	157	158	159	160	161	162	163	164	165	166	167
168	169	170	171	172	173	174	175	176	177	178	179

gleichmäßig verteilt auf $\equiv 1$, $\equiv 5$, $\equiv 7$ und $\equiv 11$ modulo 12

Diffie–Hellman Schlüsselaustausch

Wie teile ich ein Geheimnis, wenn alle zuhören?

Wahl einer Primzahl p und eines $a \geq 2$.

	Alice	Lauscher	Bob
1.		p, a öffentlich	
2.	Wahl von x berechnet $S \equiv a^x \pmod{p}$		Wahl von y berechnet $T \equiv a^y \pmod{p}$
3.		S, T öffentlich	
4.	berechnet $G \equiv T^x \pmod{p}$		berechnet $G \equiv S^y \pmod{p}$

gemeinsames Geheimnis G von Alice und Bob:

$$T^x \equiv (a^y)^x \equiv a^{yx} \equiv a^{xy} \equiv (a^x)^y \equiv S^y \pmod{p}$$

Beispiel Schlüsselaustausch

Wahl: $p = 17$ und $a = 3$.

	Alice	Lauscher	Bob
1.		$p = 17,\ a = 3$	
2.	$x = 5$ $3^5 \equiv 5 \pmod{17}$		$y = 3$ $3^3 \equiv 10 \pmod{17}$
3.		$S = 5,\ T = 10$	
4.	$10^5 \equiv 6 \pmod{17}$		$5^3 \equiv 6 \pmod{17}$

Diffie–Hellman Schlüsselaustausch

- Wette: aus p, a, $S \equiv a^x \pmod{p}$ und $T \equiv a^y \pmod{p}$ sind x, y, und vor allem G nur schwer zu berechnen: weil gerechnet $\pmod{p}$.
- Diskreter Logarithmus: „$x = \log_a(S)$“ ist viel langsamer als $S = a^x$.
  Jede bekannte Methode für G nutzt $\log_a$.
- Aktuelle Praxis: Primzahlen p mit > 600 Stellen.
  Primzahlen sicherer als zusammengesetzte Zahlen.

Primzahlen in der Antike

- Euklid
- Eratosthenes

Klassisches zu Primzahlen

- Primzahlsatz
- Offene Fragen

Primzahlen im Computer

- Modulo Arithmetik: Rechnen mit der Uhr
- Verschlüsselung: Diffie-Hellman

Fazit

- es gibt unendlich viele Primzahlen (Antike)
- chaotisch und doch regelmässig: $\pi(x) \approx x/\log(x)$
- offene Fragen, die man verstehen kann: Primzahlzwillinge?
- bedeutende Rolle bei Verschlüsselung, Internetsicherheit