Primzahlen

Highlights aus 2500 Jahren

Prof. Dr. Sönke Rollenske,
Dr. Andreas Lochmann

Philipps Universität Marburg

Was sind Primzahlen?

Definition

Eine natürliche Zahl $p > 1$ heißt Primzahl, falls p nur von 1 und p geteilt wird:

Was sind Primzahlen?

Definition

Eine natürliche Zahl $p > 1$ heißt Primzahl, falls p nur von 1 und p geteilt wird:

$$a \mid p \quad \Rightarrow \quad a = p \text{ oder } a = 1.$$

Was sind Primzahlen?

Definition

Eine natürliche Zahl $p > 1$ heißt Primzahl, falls p nur von 1 und p geteilt wird:

$$a \mid p \quad \Rightarrow \quad a = p \text{ oder } a = 1.$$

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

Fundamentalsatz der Arithmetik

Jede natürliche Zahl $n > 1$ hat eine eindeutige Primfaktorzerlegung, das heißt es gibt eindeutig bestimmte Primzahlen $p_1 \leq p_2 \leq \cdots \leq p_r$, so dass

$$n = p_1 \cdot p_2 \cdots p_r.$$

Fundamentalsatz der Arithmetik

Jede natürliche Zahl $n > 1$ hat eine eindeutige Primfaktorzerlegung, das heißt es gibt eindeutig bestimmte Primzahlen $p_1 \leq p_2 \leq \cdots \leq p_r$, so dass

$$n = p_1 \cdot p_2 \cdots p_r.$$

Beispiele:

100	$2 \cdot 2 \cdot 5 \cdot 5$	105	$3 \cdot 5 \cdot 7$
101	prim	106	$2 \cdot 53$
102	$2 \cdot 3 \cdot 17$	107	prim
104	$2 \cdot 2 \cdot 2 \cdot 13$	108	$2 \cdot 2 \cdot 3 \cdot 3 \cdot 3$

Satz von Euklid

Es gibt unendlich viele Primzahlen.

Beweisidee: Gegeben sei eine endliche Liste von Primzahlen. Erzeuge daraus eine Zahl, die eine neue Primzahl als Faktor enthält.

Beweisidee: Gegeben sei eine endliche Liste von Primzahlen. Erzeuge daraus eine Zahl, die eine neue Primzahl als Faktor enthält.

Verfahren am Beispiel

bekannt	Rechnung	neu
$\{2, 3\}$	$2 \cdot 3 + 1 = 7$	7

Beweisidee: Gegeben sei eine endliche Liste von Primzahlen. Erzeuge daraus eine Zahl, die eine neue Primzahl als Faktor enthält.

Verfahren am Beispiel

bekannt	Rechnung	neu
$\{2, 3\}$	$2 \cdot 3 + 1 = 7$	7
$\{2, 3, 7\}$	$2 \cdot 3 \cdot 7 + 1 = 43$	43

Beweisidee: Gegeben sei eine endliche Liste von Primzahlen. Erzeuge daraus eine Zahl, die eine neue Primzahl als Faktor enthält.

Verfahren am Beispiel

bekannt	Rechnung	neu
$\{2, 3\}$	$2 \cdot 3 + 1 = 7$	7
$\{2, 3, 7\}$	$2 \cdot 3 \cdot 7 + 1 = 43$	43
$\{2, 3, 7, 43\}$	$2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$	$13, 139$

Beweisidee: Gegeben sei eine endliche Liste von Primzahlen. Erzeuge daraus eine Zahl, die eine neue Primzahl als Faktor enthält.

Verfahren am Beispiel

bekannt	Rechnung	neu
$\{2, 3\}$	$2 \cdot 3 + 1 = 7$	7
$\{2, 3, 7\}$	$2 \cdot 3 \cdot 7 + 1 = 43$	43
$\{2, 3, 7, 43\}$	$2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$	$13, 139$

Allgemeiner Fall?

Euklids Beweis: allgemeiner Fall

Gegeben Primzahlen $p_1, \ldots, p_N$, so betrachten wir die Zahl

$$a = p_1 \cdot p_2 \cdots p_N + 1.$$

Euklids Beweis: allgemeiner Fall

Gegeben Primzahlen $p_1, \ldots, p_N$, so betrachten wir die Zahl

$$a = p_1 \cdot p_2 \cdots p_N + 1.$$

Keine der Primzahlen auf unserer Liste teilt a, denn

$$\frac{a}{p_j} = \frac{p_1 \cdot p_2 \cdots p_j \cdots p_N}{p_j} + \frac{1}{p_j}$$

ist keine ganze Zahl.

Euklids Beweis: allgemeiner Fall

Gegeben Primzahlen $p_1, \ldots, p_N$, so betrachten wir die Zahl

$$a = p_1 \cdot p_2 \cdots p_N + 1.$$

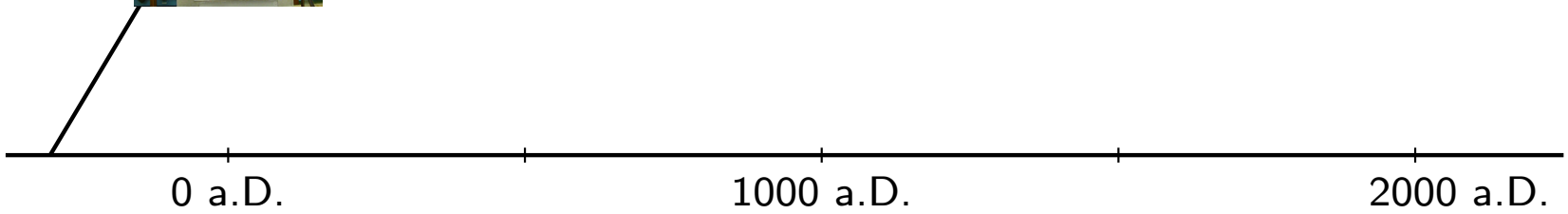
Keine der Primzahlen auf unserer Liste teilt a, denn

$$\frac{a}{p_j} = \frac{p_1 \cdot p_2 \cdots p_j \cdots p_N}{p_j} + \frac{1}{p_j}$$

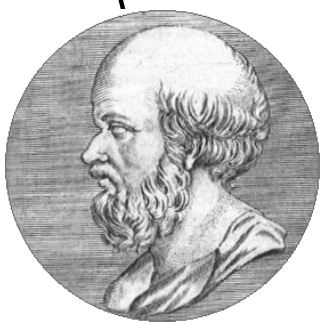
ist keine ganze Zahl.

Also ist jeder Primteiler von a eine weitere Primzahl, die nicht auf unserer Liste steht. Insbesondere kann es nicht nur endlich viele Primzahlen geben.

Euklid (ca. 300 v.Chr.)



Euklid (ca. 300 v.Chr.)



Eratosthenes (ca. 250 v.Chr.)

Wie findet man (kleine) Primzahlen? Das Sieb des Eratosthenes

Um alle Primzahlen zwischen 2 und n zu finden:

1. Mache eine Liste aller Zahlen von 2 bis n.
2. Die kleinste nicht markierte Zahl ist prim: umkringeln!
3. Streiche alle Vielfachen dieser Zahl durch.
4. Wiederhole Schritte 2. und 3. bis alle Zahlen markiert sind.

Wie findet man (kleine) Primzahlen?
Das Sieb des Eratosthenes

Um alle Primzahlen zwischen 2 und n zu finden:

1. Mache eine Liste aller Zahlen von 2 bis n.
2. Die kleinste nicht markierte Zahl ist prim **(Warum?)**: umkringeln!
3. Streiche alle Vielfachen dieser Zahl durch.
4. Wiederhole Schritte 2. und 3. bis alle Zahlen markiert sind.

Knobelaufgabe: Was kann man verbessern?

Wie findet man (kleine) Primzahlen?
Das 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

Wie findet man (kleine) Primzahlen?
Das 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

Wie findet man (kleine) Primzahlen?
Das 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

Wie findet man (kleine) Primzahlen?
Das 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

Wie findet man (kleine) Primzahlen?
Das Sieb des Eratosthenes

	2	3		5	7	
11		13			17	19
		23		25		29
31				35	37	
41		43			47	49

Wie findet man (kleine) Primzahlen?
Das Sieb des Eratosthenes

	2	3		5	7	
11		13			17	19
		23		25		29
31				35	37	
41		43			47	49

Wie findet man (kleine) Primzahlen?
Das Sieb des Eratosthenes

	2	3		5	7	
11		13			17	19
		23				29
31					37	
41		43			47	49

Wie findet man (kleine) Primzahlen?
Das Sieb des Eratosthenes

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49

Wie findet man (kleine) Primzahlen?
Das Sieb des Eratosthenes

	2	3		5	7	
11		13			17	19
		23				29
31					37	
41		43			47	

Wie findet man (kleine) Primzahlen?
Das Sieb des Eratosthenes

		2	3		5		7	
11			13				17		19
			23						29
31							37		
41			43				47		

Wie findet man (kleine) Primzahlen? Das Sieb des Eratosthenes

Um alle Primzahlen zwischen 2 und n zu finden:

1. Mache eine Liste aller Zahlen von 2 bis n.
2. Die kleinste nicht markierte Zahl ist prim: umkringeln!
3. Streiche alle Vielfachen dieser Zahl durch.
4. Wiederhole Schritte 2. und 3. bis alle Zahlen markiert sind.

Wie findet man (kleine) Primzahlen?
Das Sieb des Eratosthenes

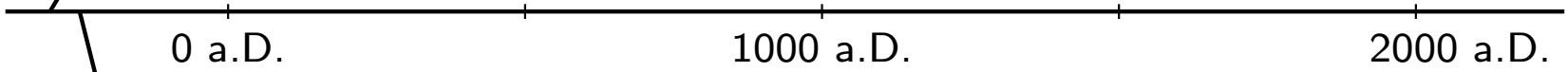
Um alle Primzahlen zwischen 2 und n zu finden:

1. Mache eine Liste aller Zahlen von 2 bis n.
2. Die kleinste nicht markierte Zahl ist prim **(Warum?)**: umkringeln!
3. Streiche alle Vielfachen dieser Zahl durch.
4. Wiederhole Schritte 2. und 3. bis alle Zahlen markiert sind.

Knobelaufgabe: Was kann man verbessern?

Euklid

Eratosthenes




Euklid
Gauß (1777–1855)
0 a.D.
1000 a.D.
2000 a.D.
Eratosthenes

Wie viele Primzahlen gibt es?

Primzahlzählfunktion:

$$\pi(x) \;=\; \text{Anzahl der Primzahlen kleiner als } x$$

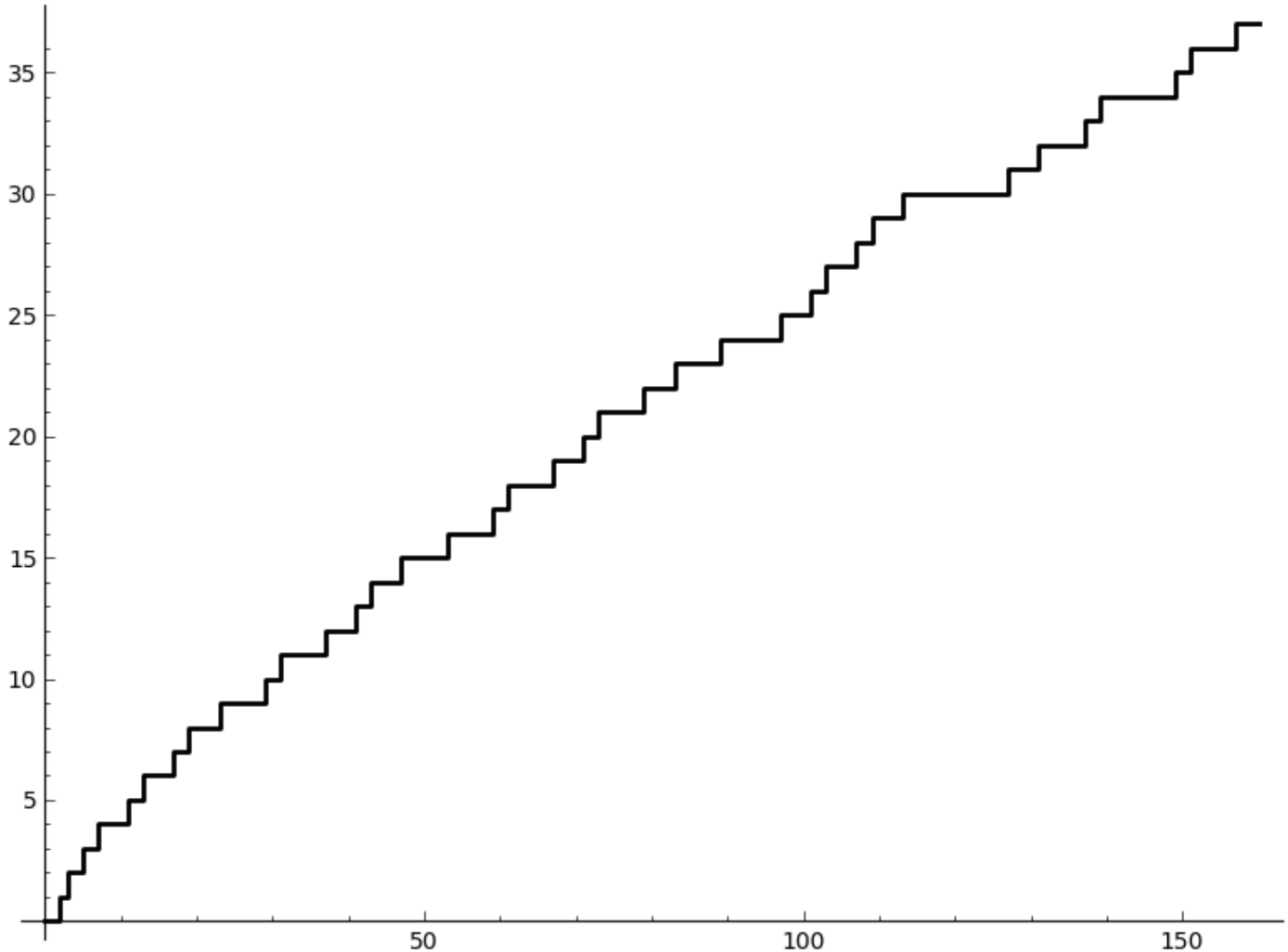
Wie viele Primzahlen gibt es?

Primzahlzählfunktion:

$$\pi(x) \;=\; \text{Anzahl der Primzahlen kleiner als } x$$

x	10	100	1000	10000
$\pi(x)$	4	25	168	1229

Experimente mit $\pi(x)$



Gauß' Vermutung

Die Primzahlzählfunktion $\pi(x)$ verhält sich für große x asymptotisch wie $\frac{x}{\ln(x)}$, das heißt

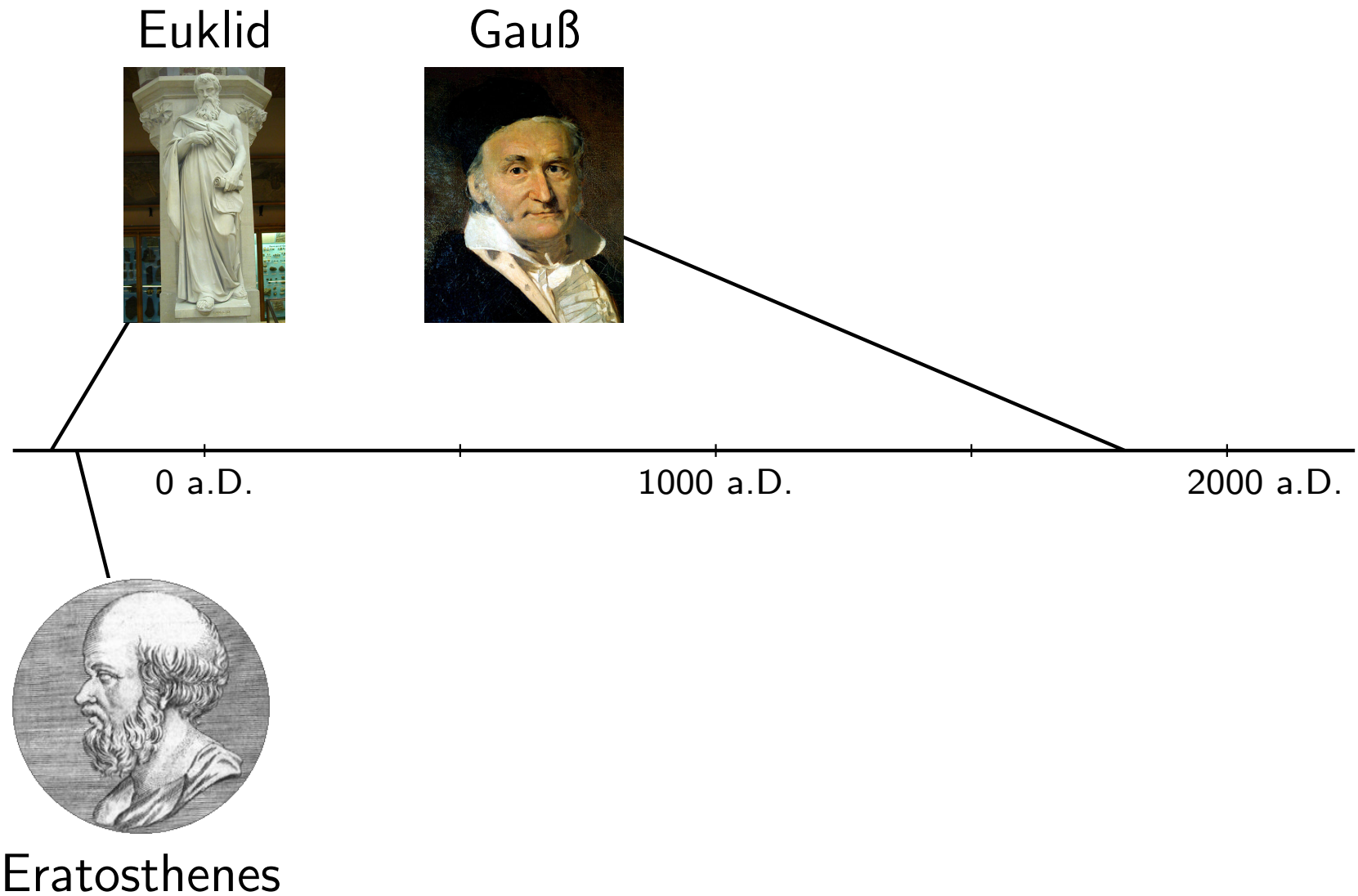
$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

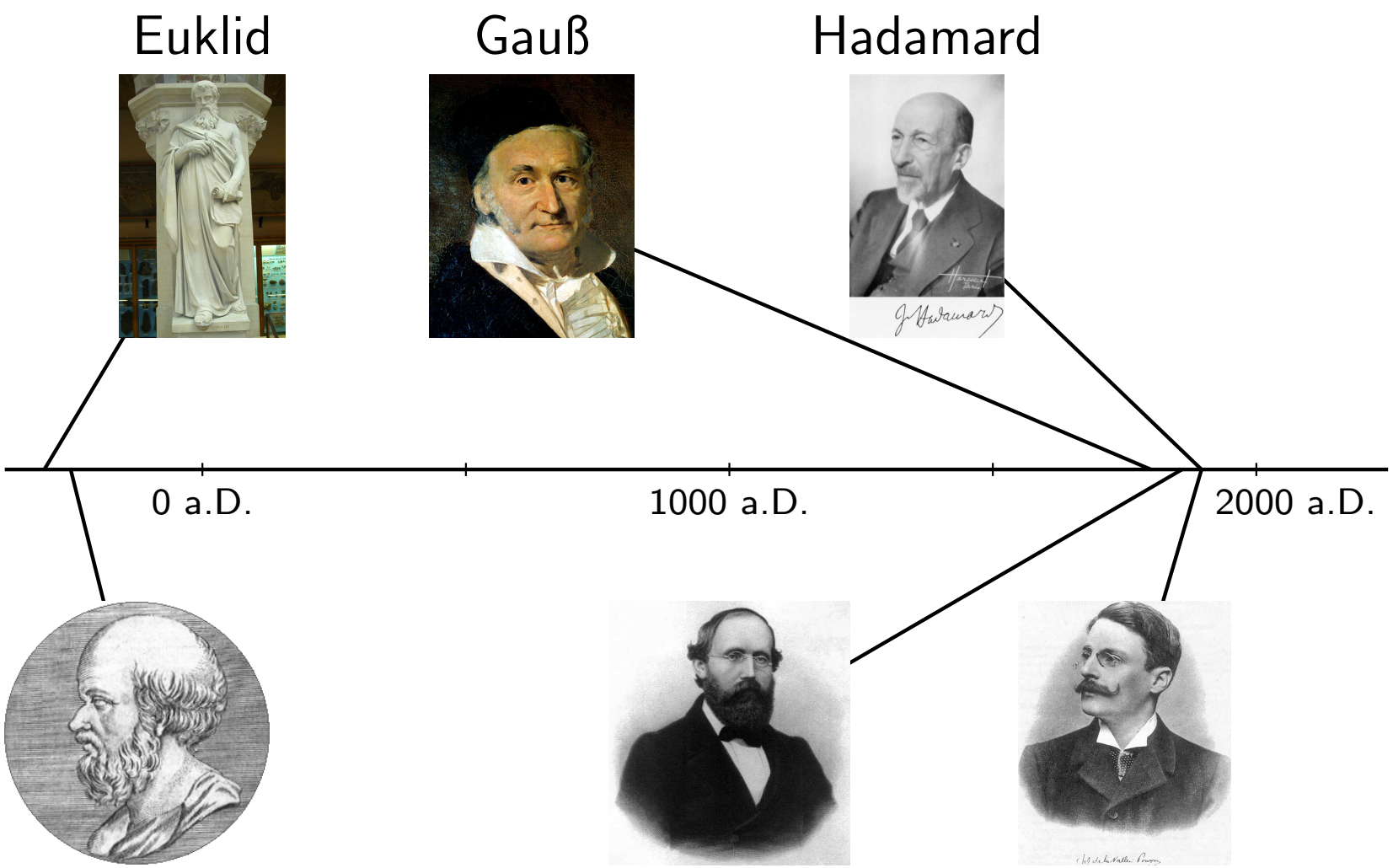
Gauß' Vermutung

Die Primzahlzählfunktion $\pi(x)$ verhält sich für große x asymptotisch wie $\frac{x}{\ln(x)}$, das heißt

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

Frage: Wieviele Primzahlen mit 100 Stellen gibt es ungefähr? Wieviele SD-Karten bräuchte man zu ihrer Speicherung bei 160 TB/kg?


Euklid
Gauß
0 a.D.
1000 a.D.
2000 a.D.
Eratosthenes


Euklid
Gauß
Hadamard
0 a.D.
1000 a.D.
2000 a.D.
Eratosthenes
Riemann
de la Vallée-Poussin

Primzahlsatz

Riemanns Idee (1859): Benutze

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prim}} \frac{1}{1 - p^{-s}}.$$

Für reelle Zahlen s ist dies seit Euler (1735) bekannt, aber benutzt man komplexe Zahlen für s, erhält man neue Einsichten!

Primzahlsatz

Erste Beweise 1896 von

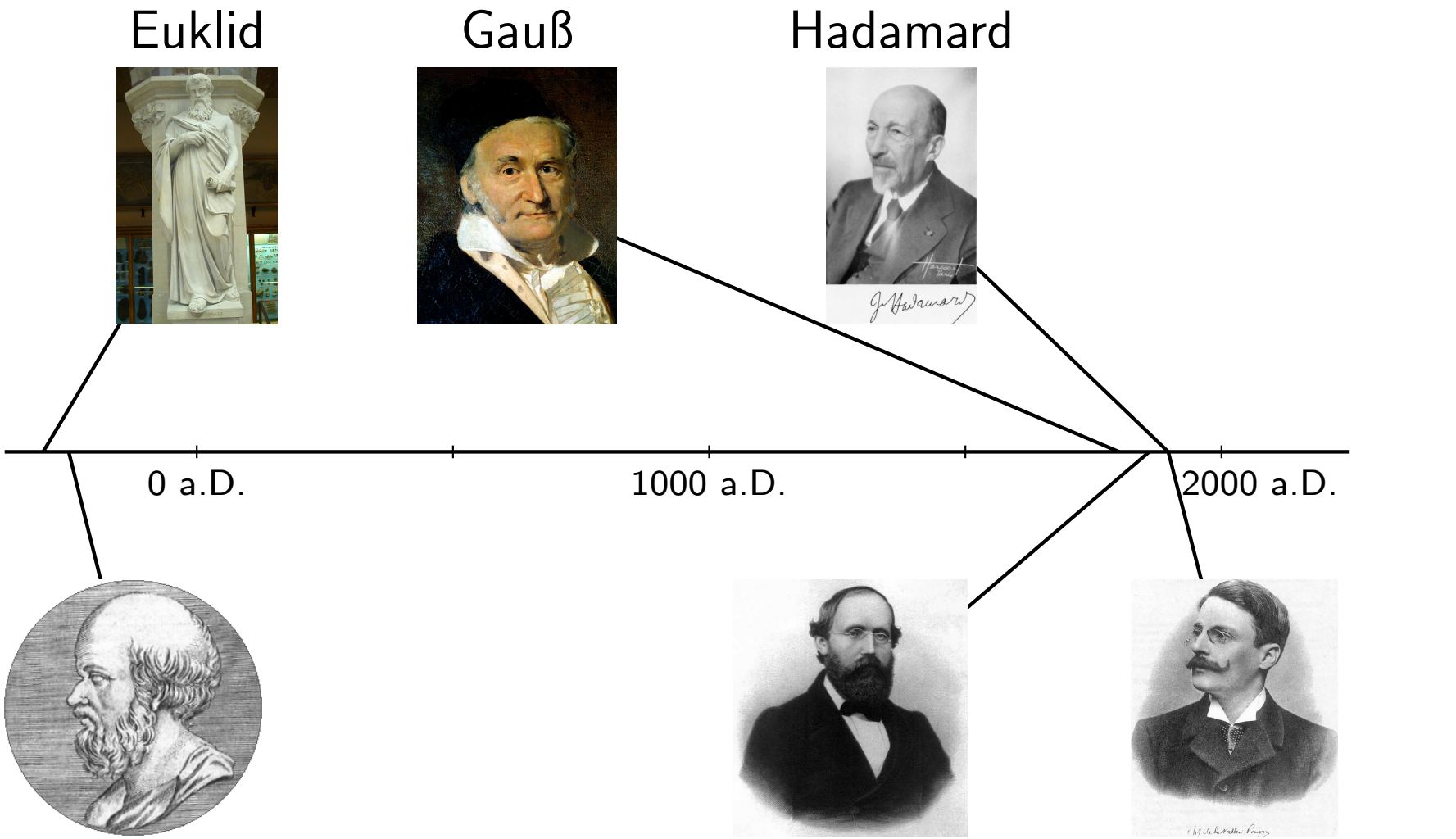
de la Vallée-Poussin &
Hadamard

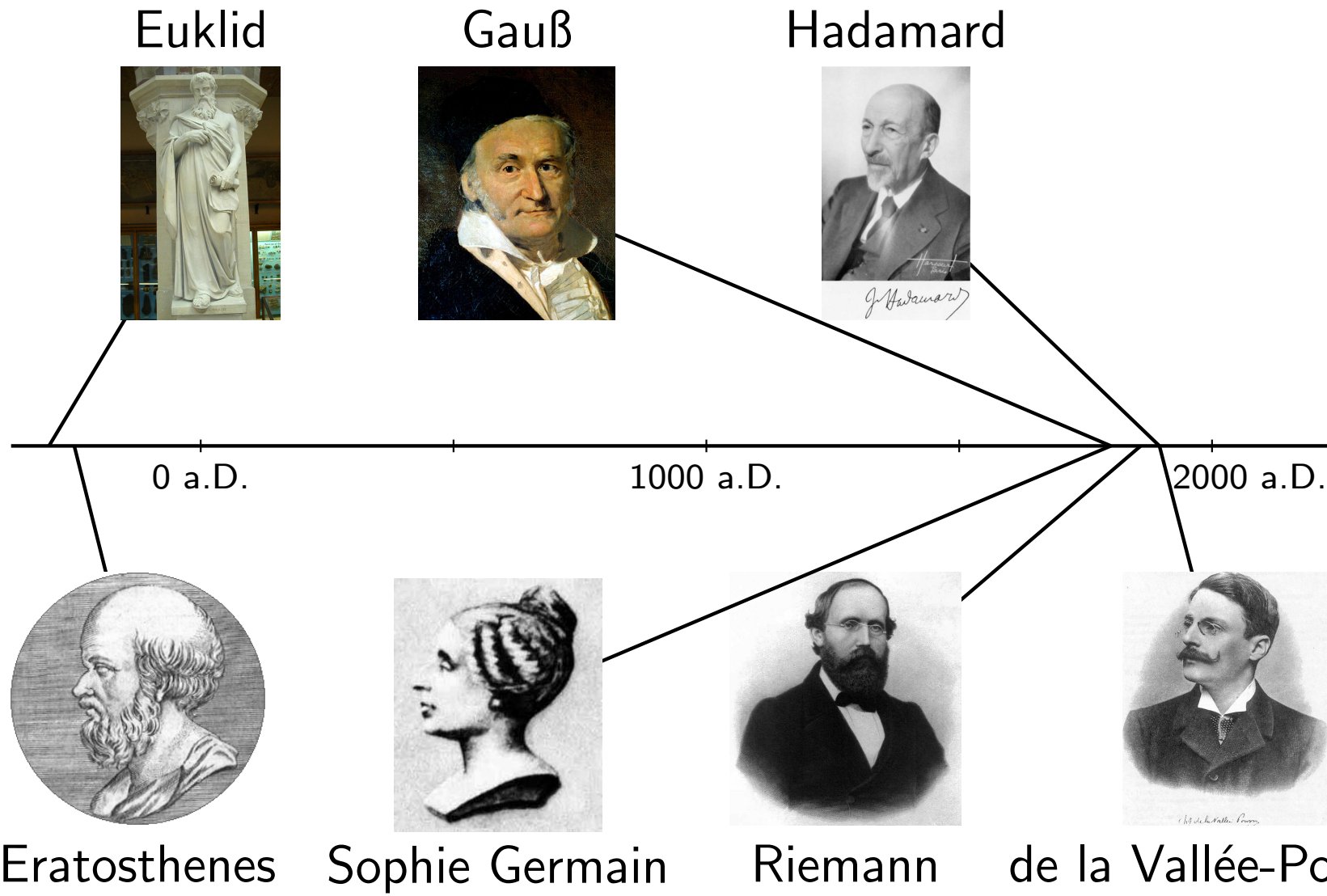
Primzahlsatz

Erste Beweise 1896 von

de la Vallée-Poussin &
Hadamard

Einen präziseren Satz (und 1 Million Dollar vom Clay Institute) erhält man für den Beweis der Riemannschen Vermutung: Ist s eine komplexe Nullstelle der ζ-Funktion, so ist s negativ oder der Realteil von s ist $\frac{1}{2}$.


Euklid
Gauß
Hadamard
0 a.D.
1000 a.D.
2000 a.D.
Eratosthenes
Riemann
de la Vallée-Poussin


Euklid
Gauß
Hadamard
0 a.D.
1000 a.D.
2000 a.D.
Eratosthenes
Sophie Germain
Riemann
de la Vallée-Poussin

Satz von Sophie Germain (Spezialfall; ab 1815)

Sei p eine Primzahl, so dass $2p + 1$ auch prim ist. Dann gibt es keine natürlichen Zahlen a, b, c, so dass

$$a^p + b^p = c^p \quad \text{gilt.}$$

Satz von Sophie Germain (Spezialfall; ab 1815)

Sei p eine Primzahl, so dass $2p + 1$ auch prim ist. Dann gibt es keine natürlichen Zahlen a, b, c, so dass

$$a^p + b^p = c^p \quad \text{gilt.}$$

Vorher gab es nur vereinzelte Resultate zur Fermatschen Vermutung; Germains Methoden bildeten einen neuen Zugang zu diesem alten Problem.

Sophie-Germain-Primzahlen

Eine Primzahl p heißt Sophie-Germain-Primzahl, wenn auch $2p + 1$ prim ist. Die Zahl $2p + 1$ wiederum heißt **sichere Primzahl** (wichtig für moderne Verschlüsselungsverfahren).

Sophie-Germain-Primzahlen

Eine Primzahl p heißt Sophie-Germain-Primzahl, wenn auch $2p + 1$ prim ist. Die Zahl $2p + 1$ wiederum heißt **sichere Primzahl** (wichtig für moderne Verschlüsselungsverfahren).

Welches sind die kleinsten sicheren Primzahlen?

Sophie-Germain-Primzahlen

Eine Primzahl p heißt Sophie-Germain-Primzahl, wenn auch $2p + 1$ prim ist. Die Zahl $2p + 1$ wiederum heißt **sichere Primzahl** (wichtig für moderne Verschlüsselungsverfahren).

Welches sind die kleinsten sicheren Primzahlen?

5 (denn $5 = 2 \cdot 2 + 1$)
7 (denn $7 = 2 \cdot 3 + 1$)
11, 23, 47, 59, 83, ...

Sophie-Germain-Primzahlen

$5 = 2 \cdot 2 + 1$ ist prim.
$11 = 2 \cdot 5 + 1$ ist prim.
$23 = 2 \cdot 11 + 1$ ist prim.
$47 = 2 \cdot 23 + 1$ ist prim.

Sophie-Germain-Primzahlen

$5 = 2 \cdot 2 + 1$ ist prim.
$11 = 2 \cdot 5 + 1$ ist prim.
$23 = 2 \cdot 11 + 1$ ist prim.
$47 = 2 \cdot 23 + 1$ ist prim.

Geht das immer so weiter?

Sophie-Germain-Primzahlen

$5 = 2 \cdot 2 + 1$ ist prim.
$11 = 2 \cdot 5 + 1$ ist prim.
$23 = 2 \cdot 11 + 1$ ist prim.
$47 = 2 \cdot 23 + 1$ ist prim.

Geht das immer so weiter?

Leider nein: $95 = 2 \cdot 47 + 1$ ist nicht prim.

Sophie-Germain-Primzahlen

Gibt es unendlich viele sichere Primzahlen?

Sophie-Germain-Primzahlen

Gibt es unendlich viele sichere Primzahlen?

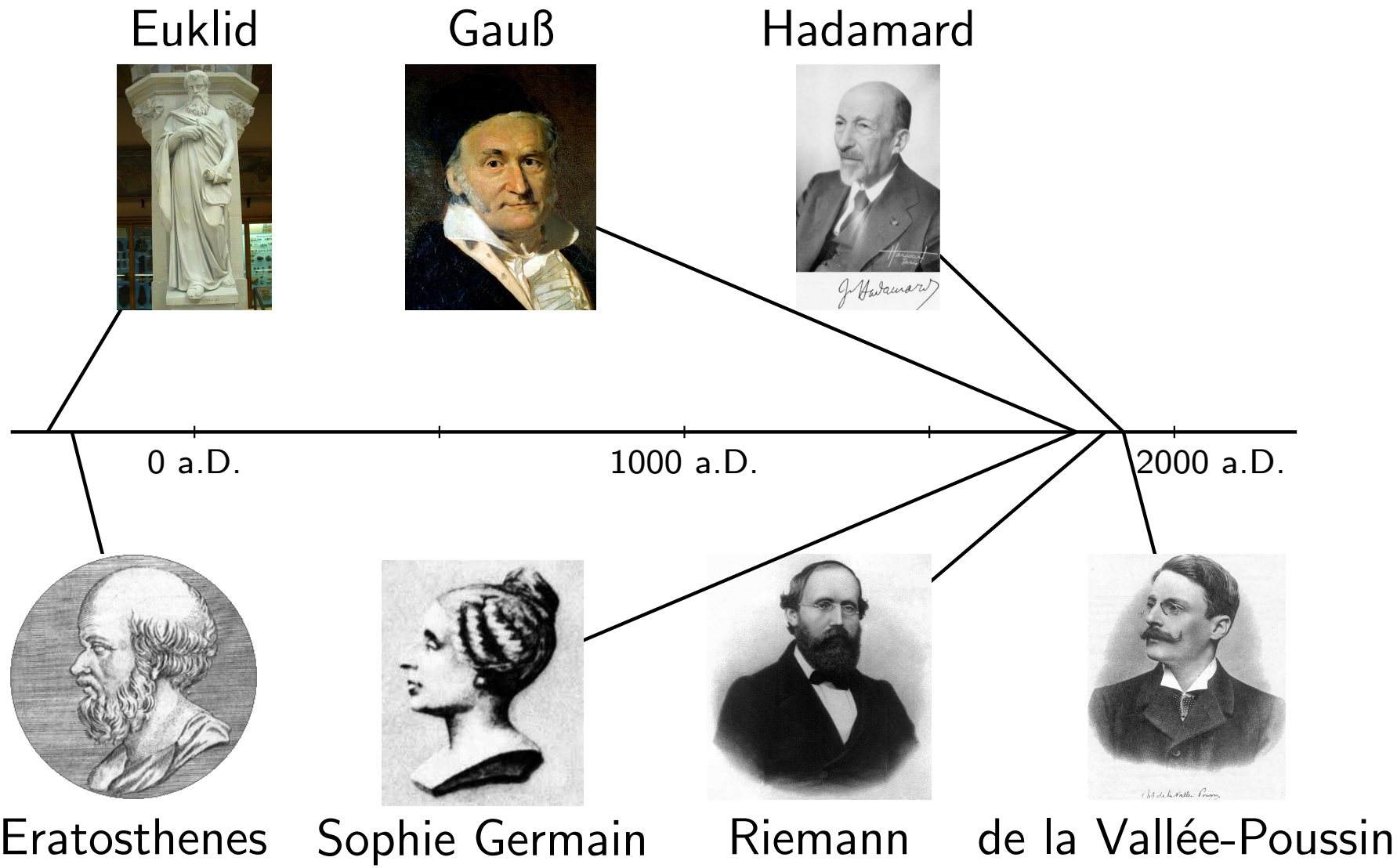
Bis heute unbekannt. Man vermutet, dass es unter den Zahlen 1 bis x ungefähr $\frac{1{,}32 \cdot x}{(\ln x)^2}$ Sophie-Germain-Primzahlen gibt.

Sophie-Germain-Primzahlen

Gibt es unendlich viele sichere Primzahlen?

Bis heute unbekannt. Man vermutet, dass es unter den Zahlen 1 bis x ungefähr $\frac{1{,}32 \cdot x}{(\ln x)^2}$ Sophie-Germain-Primzahlen gibt.

Frage: Wenn man obige Vermutung als wahr annimmt – wieviele sichere Primzahlen mit 100 Stellen gibt es dann ungefähr?


Euklid
Gauß
Hadamard
0 a.D.
1000 a.D.
2000 a.D.
Eratosthenes
Sophie Germain
Riemann
de la Vallée-Poussin

Quellen

Zur Primfaktorzerlegung und dem Beweis des Fundamentalsatzes der Arithmetik siehe Peter Bundschuh: „Einführung in die Zahlentheorie“, Abschnitte 1.1 bis 1.6.

Zum Sieb des Eratosthenes siehe:
`de.wikipedia.org/wiki/Sieb_des_Eratosthenes`

Für einen Beweis des Primzahlsatzes siehe Peter Bundschuh, Abschnitt 7.3 (benötigt fortgeschrittenes mathematisches Grundwissen).

Zum Satz von Sophie Germain siehe die einschlägigen Wikipedia-Artikel und für die Hintergründe Simon Singh: „Fermats letzter Satz“.

Bildquellen

Die Darstellungen von Euklid, Eratosthenes, Gauß, Hadamard, Riemann, de la Vallée-Poussin und Germain sind gemeinfrei, und können via Wikimedia gefunden werden. Details zu einigen Abbildungen:

Euklid: Aus dem Oxford University Museum, Fotografie von Mark A. Wilson.

Gauß: Gauß-Gesellschaft Göttingen e.V., gemalt von C. A. Jensen, Foto: A. Wittmann.

Riemann: Stich von August Weger

Probleme zum Knobeln und Ausarbeiten

(1.1) Wieso funktioniert das Sieb des Eratosthenes, und wie kann man es verbessern/beschleunigen?

(1.2) Wieviele Primzahlen mit 100 Stellen gibt es ungefähr? Wieviele SD-Karten (in Kilogramm, Tonnen oder anderer geeigneter Einheit) bräuchte man zu ihrer Speicherung bei 160 TB/kg?

(1.3) Wieviele *sichere* Primzahlen mit 100 Stellen gibt es ungefähr?