1. Regeln im Unregelmäßigen

1.1. Primzahlen

Natürliche Zahlen sind die Zahlen $1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots$

Eine natürliche Zahl $n > 1$ heißt prim, wenn sie keine Teiler außer 1 und n hat.

Beispiele: die Zahlen $2, 3, 5, 7, 11, 13, 17$ sind prim, nicht prim sind etwa

4 $= 2 \cdot 2$	6 $= 2 \cdot 3$	8 $= 2 \cdot 4$	9 $= 3 \cdot 3$	10 $= 2 \cdot 5$	12 $= 2 \cdot 6$	14 $= 2 \cdot 7$	15 $= 3 \cdot 5$	16 $= 2 \cdot 8$	18 $= 2 \cdot 9$

Mit dem **Sieb des Eratosthenes** (276–194 v. Chr.) kann man Primzahlen finden:

1	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

Man schreibt sich die natürlichen Zahlen auf, so weit man mag (hier bis 160). Die 1 zählt sowieso nicht (nach Definition!). Die erste Primzahl ist $p_1 = 2$, wir können alle anderen geraden Zahlen streichen (im Beispiel ist dies durch Farben codiert).

Die kleinste Zahl, die jetzt übrig bleibt, ist die zweite Primzahl: $p_2 = 3$. Als nächstes streichen wir deswegen alle Vielfachen von 3.

Die kleinste Zahl, die übrig bleibt, ist die dritte Primzahl: $p_3 = 5$.

Diese Verfahren wiederholt man immer wieder:
Hat man die Primzahl p_n gefunden, streicht man aus den bis dahin verbliebenen Zahlen alle Vielfachen von p_n. Die kleinste danach noch übrige Zahl ist die nächste Primzahl: p_{n+1}.

Man kann aufhören zu suchen, wenn man eine Primzahl p_m gefunden hat, deren Quadrat p_m^2 aus der betrachteten Liste fällt (im Beispiel also schon bei $p_6 = 13$ wegen $p_6^2 = 13 \cdot 13 = 169$). Jede der dann noch verbliebenen Zahlen muss prim sein (sonst wäre sie teilbar durch eine Primzahl p, für diesen müsste $p \geq p_m$ gelten, und nach Division durch p bliebe eine Zahl kleiner als p_m — also hätte diese Zahl wegen eines Primteilers kleiner als p_m schon gestrichen werden müssen).

Eine etwas größere Liste von Primzahlen (vgl. z. B. RIBENBOIM 1991):

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	101	103	107
109	113	127	131	137	139	149	151	157	163	167	173	179	181
191	193	197	199	211	223	227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503	509	521
523	541	547	557	563	569	571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659	661	673	677	683	691	701
709	719	727	733	739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863	877	881	883	887
907	911	919	929	937	941	947	953	967	971	977	983	991	997
1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069	1087	1091
1093	1097	1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187	1193
1201	1213	1217	1223	1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373	1381	1399	1409	1423
1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493
1499	1511	1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601

? Wann hört das auf? ?

1.2. Es gibt unendlich viele Primzahlen

Wir wollen — wie bereits EUKLID um 300 v. Chr. (Buch IX, §20) — nachweisen, dass die Reihe der Primzahlen nicht endet.

Dazu nummerieren wir die Primzahlen (der Reihe nach, wie z. B. das Sieb des Eratosthenes sie liefert), also

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ p_6 = 13,\ p_7 = 17,\ p_8 = 19,\ p_9 = 23,\ \ldots$$

Um zu zeigen, dass es zu jeder vorgegebenen Primzahl noch eine größere gibt, betrachten wir eine (beliebige) Primzahl p_n und bilden

$$Z_n := (p_1 \cdot p_2 \cdots p_n) + 1$$

Teilt man Z_n durch p_1, p_2, …, so bleibt jedes Mal der Rest 1. Also ist Z_n durch keine der ersten n Primzahlen teilbar.

Auch wenn Z_n selbst nicht prim ist, muss doch wenigstens ein Primteiler von Z_n existieren, der nicht in $\{p_1, p_2, \ldots, p_n\}$ enthalten ist!

Beispiel: Für $n = 3$ erhalten wir zu $\{p_1, p_2, p_3\} = \{2, 3, 5\}$ die Zahl $Z_3 = (2{\cdot}3{\cdot}5){+}1 = 31$, und damit die neue Primzahl 31 $(= p_6)$.

Für $n = 4$ ergibt sich $Z_4 = (2 \cdot 3 \cdot 5 \cdot 7) + 1 = 211$, ebenfalls eine Primzahl (nämlich p_{47}).

Auch für $n = 5$ erhalten wir mit $Z_5 = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) + 1 = 2311\,(= p_{344})$ eine Primzahl.

Aber: für $n = 6$ ergibt sich $Z_6 = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) + 1 = 30031 = 59 * 509\ (= p_{17} \cdot p_{97})$.

In keinem dieser Fälle erhält man die „nächst gelegene“ Primzahl:
es werden jedes Mal einige Primzahlen übersprungen!

Für die alten Griechen war es ein philosophisches Tabu, einer Menge von Objekten aktual Unendlichkeit zuzuschreiben. Dies hat aber die Mathematiker nicht abgehalten, das Phänomen präzise zu benennen: Die Menge der Primzahlen ist jedenfalls nicht endlich!

In anderer Form taucht diese Frage in einem Grundlagenproblem der modernen Mathematik wieder auf: Kann man überhaupt widerspruchsfrei von unendlichen Mengen sprechen? (Man vergleiche etwa das Russellsche Paradox!)

Dieses Problem darf durch die axiomatische Mengenlehre als gelöst angesehen werden. Wer sich in solche Fragen vertiefen will, konsultiere etwa Meschkowski 1973.

1.3. Gibt es auch unendlich viele Primzahl-Zwillinge?

In der Liste der Primzahlen fällt auf, dass es wenigstens anfangs häufiger vorkommt, dass zwei auf einander folgende Primzahlen gerade den Abstand 2 haben.

Später scheint das seltener zu werden.

Bis heute ist — trotz intensiver Bemühungen einer ganzen Reihe von Mathematikern — ungeklärt, ob es unendlich viele solcher Primzahl-Zwillinge (also Paare von Primzahlen (p, q) mit $q = p + 2$) gibt!
Im Jahr 1990 schienen die größten bekannten Primzahlzwillinge die beiden Paare

$$(1706595 \cdot 2^{11235} - 1\,,\ 1706595 \cdot 2^{11235} + 1) \text{ und } (571305 \cdot 2^{7701} - 1\,,\ 571305 \cdot 2^{7701} + 1)$$

zu sein, vgl. Ribenboim 1991 p.147. Im Jahr 2002 lag der Rekord bei dem Paar

$$(33218925 \cdot 2^{169690} - 1\,,\ 33218925 \cdot 2^{169690} + 1)\,,$$ diese Zahlen haben 51090 Stellen!

Neuere Rekorde findet man auf `www.utm.edu/research/primes/largest.html`.

In der oben angegebenen Liste sind die Zwillinge farblich markiert (p orange, q rot — mit einer Ausnahme).

1.4. Es gibt beliebig große Lücken in der Reihe der Primzahlen

Obwohl es unendlich viele Primzahlen gibt, sind diese doch eher dünn gesät: Das Verfahren von Eratosthenes siebt ganz gewaltig!

Wir wollen zeigen, dass es tatsächlich sehr große Lücken gibt.

Beispiel: Wir betrachten wieder $Z_3 := (2 \cdot 3 \cdot 5) + 1 = 31$.
Es ist $Z_3 + 1 = 32$ durch 2 teilbar,
$Z_3 + 2 = 33$ durch 3 teilbar,
$Z_3 + 3 = 34$ durch 2 teilbar,
und $Z_3 + 4 = 35$ durch 5 teilbar:
damit sind die 4 Zahlen, die auf Z_3 folgen, alle nicht prim.

Das ist nicht *sehr* überraschend, aber wir fangen auch erst klein an.

Beispiel: Wir betrachten $Z_4 := (2 \cdot 3 \cdot 5 \cdot 7) + 1 = 211$.
Es ist $Z_4 + 1 = 212$ durch 2 teilbar,
$Z_4 + 2 = 213$ durch 3 teilbar,
$Z_4 + 3 = 214$ durch 2 teilbar,
$Z_4 + 4 = 215$ durch 5 teilbar,
$Z_4 + 5 = 216$ durch 2 teilbar,
und $Z_4 + 6 = 217$ durch 7 teilbar:
das ist schon eine Folge von 6 Zahlen, die alle nicht prim sind.

Beispiel: Wir betrachten $Z_5 := (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) + 1 = 2311$.
Es ist $Z_5 + 1 = 2312$ durch 2 teilbar,
$Z_5 + 2 = 2313$ durch 3 teilbar,
$Z_5 + 3 = 2314$ durch 2 teilbar,
$Z_5 + 4 = 2315$ durch 5 teilbar,
$Z_5 + 5 = 2316$ durch 2 teilbar,
$Z_5 + 6 = 2317$ durch 7 teilbar,
$Z_5 + 7 = 2318$ durch 2 teilbar,
$Z_5 + 8 = 2319$ durch 3 teilbar,
$Z_5 + 9 = 2320$ durch 2 teilbar,
und $Z_5 + 10 = 2321$ durch 11 teilbar:
wir erhalten eine Folge von 10 Zahlen, die alle nicht prim sind.

Den Beispielen liegt eine allgemeine Konstruktion zu Grunde:

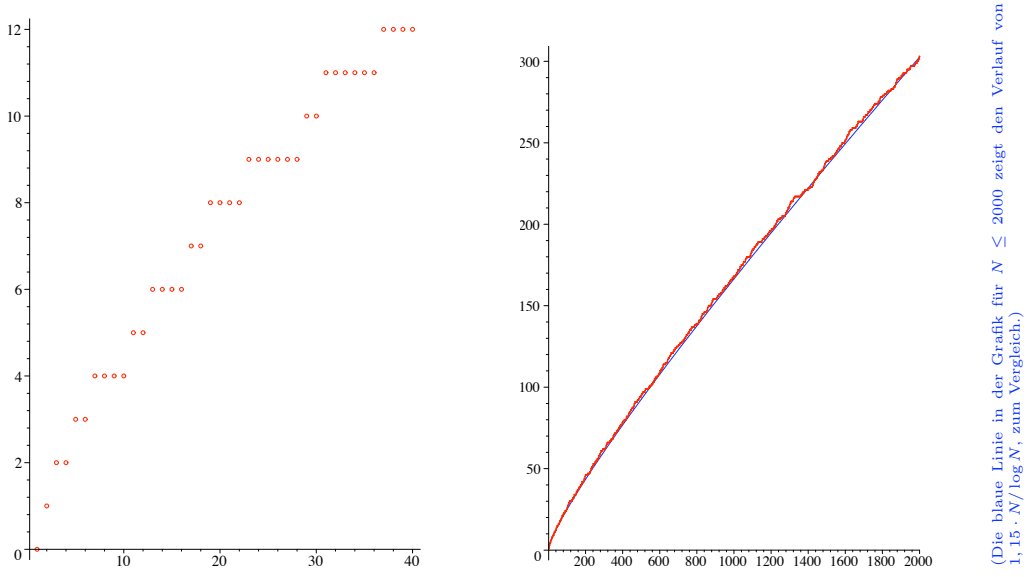
Beispiel: Wir betrachten jetzt allgemein $Z_n := (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n) + 1$.
Für jede natürliche Zahl k zwischen 1 und $p_n - 1$ ist $1+k$ teilbar durch eine der Primzahlen $2, 3, 5, 7 \ldots p_n$. Damit ist aber auch $Z_n + k = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n) + 1 + k$ durch eben diese Primzahl teilbar, und also nicht prim!
Wir erhalten eine Folge von $p_n - 1$ Zahlen, die alle nicht prim sind.

Damit haben wir, wie angekündigt, nachgewiesen:

Es gibt beliebig große Lücken in der Reihe der Primzahlen.

Präziser: Zu jeder Schranke N gibt es eine Lücke, die mindestens die Länge N hat.
Man muss nur n so groß wählen, dass die Primzahl p_n größer als N ist —
und das geht, weil es unendlich viele Primzahlen gibt!

Mathematisch interessant (aber viel tiefer als die hier vorgestellten Überlegungen) sind Fragen nach der Verteilung der Primzahlen: Es wurde hier beispielsweise bewiesen, dass die Anzahl $\pi(N)$ der Primzahlen unterhalb N sich im Großen so verhält wie $N/\log(N)$.



Erste Skizzen des Verlaufs von $\pi(N)$ sieht man hier für $N \leq 40$ bzw. $N \leq 2000$.
Das eigentliche Problem ist damit kaum angekratzt: Obwohl die rechte Grafik schon recht regelmäßig aussieht, sagen uns endlich viele Stichproben *nichts* über die weitere Verteilung! Dies führt uns hier zu weit, vgl. z. B. LeVeque 1959.

Damit Sie heute Nacht nicht schlecht träumen:
Lesen Sie vor dem Einschlafen die „dritte Nacht“ in Enzensberger 1997.