Prof. Dr. Manfred Lehn[1]

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

Immer noch mysteriös: Primzahlen !

Liebe Schülerinnen und Schüler[2],

ich werde häufig gefragt, wenn die Leute hören, dass ich Mathematiker bin, was es denn in der Mathematik überhaupt noch zu forschen gibt. „Die Zahlen, mit denen man im täglichen Leben zu tun hat, und die paar Rechenregeln, die man dafür braucht, die sind doch schon alle gefunden,“ sagen die Leute. Das liegt natürlich daran, dass sich am Einmaleins wirklich nichts geändert hat, seit die Menschen vor vielen Tausend Jahren gelernt haben, wie man multipliziert.

Es gibt aber viele schwierige mathematische Probleme zu lösen, wenn man Satelliten auf die richtige Flugbahn ins Weltall schicken will, damit hinterher das GPS-System im Navigationsgerät im Auto auch richtig funktioniert, oder wenn die Funksignale eines Handys so verschlüsselt werden müssen, dass sie gegen Verrauschen und Störungen geschützt sind und man klar und deutlich telefonieren kann.

Aber alle diese schwierigen Probleme, für die man an der Universität studieren muss, damit man sie überhaupt verstehen kann, sind viel einfacher als zwei Probleme, über die ich heute etwas erzählen möchte. Das Schöne an diesen Problemen ist, dass sie ganz leicht zu erklären sind, aber kein Mensch weiß, wie man sie lösen soll. Und vielleicht sind ja Einige unter Euch, die eines Tages das Problem knacken und damit richtig berühmt werden.

Die Probleme, von denen ich heute spreche, haben alle mit Primzahlen zu tun, also

[1] Institut für Mathematik, Johannes Gutenberg-Universität Mainz, www.mathematik.uni-mainz.de/lehn

[2] Vortrag im Rahmen der Regionalsiegerehrung im Junior-Wettbewerb Mathematik ohne Grenzen für die Klassenstufen 5 und 6 am 16. Mai 2012, Schott AG Mainz

mit Zahlen wie
$$2, 3, 5, 7, 11, \dots .$$
Ihr wisst bestimmt, was Primzahlen sind, aber ich will es noch einmal wiederholen, sozusagen als Lockerungsübung zum Warmmachen für das, was wir noch vorhaben. Die Zahl 90 können wir in ein Produkt zerlegen:
$$90 = 9 \cdot 10.$$
Und wir können sowohl die 9 wie die 10 weiterzerlegen, also
$$9 = 3 \cdot 3 \qquad \text{und} \qquad 10 = 2 \cdot 5.$$
Also zusammen
$$90 = 9 \cdot 10 = 3 \cdot 3 \cdot 2 \cdot 5,$$
oder etwas schöner geordnet
$$90 = 2 \cdot 3 \cdot 3 \cdot 5.$$
Aber dann ist Schluss, weiter geht es nicht. Die Zahlen 2, 3, 5 kann man nicht weiter in kleinere Zahlen zerlegen. Solche Zahlen nennt man Primzahlen. Genauer: Eine Zahl ist eine Primzahl, wenn sie größer als 1 ist und keine anderen Teiler als 1 und sich selbst hat. Jede Zahl ist dann entweder selbst eine Primzahl oder lässt sich als Produkt von kleineren Primzahlen schreiben. Und wenn man die auftretenden Primzahlen auch noch der Größe nach ordnet, gibt es sogar nur eine einzige Möglichkeit dafür. Zum Beispiel hat man
$$\begin{array}{rcl} 23 & = & \text{Primzahl} \\ 24 & = & 2 \cdot 2 \cdot 2 \cdot 3 \\ 25 & = & 5 \cdot 5 \end{array}$$
oder mit ein paar größeren Zahlen
$$\begin{array}{rcl} 99 & = & 3 \cdot 3 \cdot 11 \\ 100 & = & 2 \cdot 2 \cdot 5 \cdot 5 \\ 101 & = & \text{Primzahl} \\ 102 & = & 2 \cdot 3 \cdot 17 \\ 103 & = & \text{Primzahl} \end{array}$$
Die Zahl 1 wollen wir übrigens keine Primzahl nennen, weil wir sonst $5 = 1 \cdot 5 = 1 \cdot 1 \cdot 5$ usw. schreiben könnten, und es gäbe plötzlich viele Zerlegungen, die sich aber doch eigentlich gar nicht wesentlich unterscheiden.

Wir fangen vorne an: Die ersten Primzahlen heißen

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31, \quad 37, \ldots$$

Wieviele Primzahlen gibt es eigentlich? Wir können ja mal zählen: Zwischen 1 und 10 gibt es 4 Primzahlen, nämlich 2, 3, 5 und 7. Und zwischen 1 und 100? Das ist schon eine richtige Fleißarbeit und ziemlich mühselig. Hier ist eine Tabelle der Zahlen von 1 bis 100. Die Primzahlen habe ich fett und etwas größer gedruckt, damit man sie leichter zählen kann.

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

Heraus kommt 25. Und zwischen 1 und 1000? Ich gebe zu, so richtig Lust, das mit dem Bleistift auszurechnen, habe ich auch nicht. Wenn man den Computer zu Hilfe nimmt, findet man 168 Primzahlen zwischen 1 und 1000. Und der Computer ächzt auch nicht, wenn ich nach den Primzahlen zwischen 1 und 10.000 frage. Die Antwort ist 1.229. Ich schreibe die Zahlen mal in eine Tabelle, damit wir sie leichter überblicken können:

alle Zahlen	10	100	1.000	10.000	100.000	1.000.000	10.000.000
Primzahlen	4	25	168	1.229	9.592	78.498	664.579

Wir können daraus zweierlei lernen. Anscheinend gibt es immer mehr Primzahlen, sie scheinen jedenfalls nicht aufzuhören. Andererseits nimmt der Anteil der Primzahlen immer mehr ab. So sind 40% aller Zahlen kleiner gleich 10 Primzahlen, bis 100 sind es aber nur noch 25%, und bis zu einer Million nur noch rund 8%. Heutzutage kann man mit dem Computer - und mit viel Mathematik, die man braucht, um den Computer zu programmieren, - auch ganz schnell große Primzahlen produzieren. Zum Beispiel braucht mein Laptop weniger als 1 Sekunde, um die folgende Primzahl zu finden, die 57 Stellen hat!

$$234.058.234.589.459.872.430.598.724.359.349.587.343.948.573.984.573.948.949,$$

Wie groß können denn Primzahlen eigentlich werden? Geht die Reihe der Primzahlen unendlich weiter? Oder kann es passieren, dass es irgendwann einmal eine größte aller Primzahlen gibt und danach kommen keine weiteren mehr?

Da kann uns der Computer natürlich nicht weiterhelfen. Denn egal, wie weit und wie lange der Computer rechnet, wir wissen ja nie, was danach kommt. Selbst wenn uns der Computer eine Primzahl ausrechnen würde, die so groß ist wie das ganze Vermögen von Dagobert Duck, sagen wir 500 Phantastrilliarden, und wenn dann lange nichts mehr kommt und wir die Rechnung enttäuscht abbrechen, könnte niemand sagen, ob wir wirklich die größte Primzahl gefunden haben oder ob danach nicht doch noch eine größere kommt. Wie ist es also: Gibt es unendlich viele Primzahlen oder gibt es eine größte Primzahl?

Diese Frage ist tatsächlich einfacher als sie aussieht, und das Problem wurde schon vor fast 2.300 Jahren gelöst, und zwar ganz ohne Computer, von einem klugen Mathematiker namens Euklid, der in der Stadt Alexandria in Ägypten gelebt hat.

Euklid[3] (ca. 360 - 280 v. Chr.)

Euklid hat sich nämlich Folgendes überlegt: Wenn ich Primzahlen 2, 3, 5 und 7 nehme, miteinander multipliziere und 1 addiere:

$$2 \cdot 3 \cdot 5 \cdot 7 + 1,$$

dann ist die Zahl sicher nicht durch 2 teilbar, sondern ungerade. Aber sie lässt sich auch nicht durch 3 teilen, sondern lässt den Rest 1 übrig. Und dasselbe passiert bei 5 und bei 7. Also ist das Ergebnis entweder selbst eine Primzahl, oder die Primzahlen, die bei der Zerlegung vorkommen, sind jedenfalls nicht 2, 3, 5 oder 7, sondern irgendwelche neue Primzahlen, die wir vorher nicht hatten. Tatsächlich kommt

$$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

heraus, und das ist eine Primzahl. Und jetzt sagt Euklid: Es muss unendlich viele Primzahlen geben, denn wenn wir wirklich eine größte Primzahl hätten - und weil wir sie nicht kennen, schreibe ich einmal den Buchstaben p dafür - dann könnten wir ja alle Primzahlen, angefangen von 2, 3 usw. bis hinauf zu p aufmultiplizieren und 1 addieren. Das Ergebnis

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p \quad + 1$$

wäre natürlich riesig. Praktisch könnten wir das gar nicht ausrechnen. Wahrscheinlich gäbe es auf der ganzen Welt nicht genug Papier, um die Zahl überhaupt hinzuschreiben. Aber wir können uns zumindest vorstellen, wir könnten es tun. Was wissen wir

[3]Wir wissen sehr wenig Biographisches über Euklid, schon gar nicht, wie er ausgesehen hat. Die Zeichnung ist also ein neuzeitliches Phanthasieprodukt. Bildquelle: Wikipedia

dann über das Ergebnis? Es ist nicht durch 2 teilbar, auch nicht durch 3 oder 5 oder p, sondern würde jedesmal den Rest 1 lassen. Es ist durch überhaupt keine bekannte Primzahl teilbar. Also müssen in der Zerlegung dieser riesigen Zahl neue Primzahlen vorkommen, die größer als die Zahl p sind. Und das, obwohl wir doch angenommen hatten, p wäre die größte Primzahl. Das kann ja wohl nicht sein. Der Fehler war, dass wir angenommen hatten, es gäbe eine größte Primzahl. Wenn sich nun herausstellt, dass das Unsinn ist, bleibt nur noch die umgekehrte Möglichkeit, dass es wirklich unendlich viele Primzahlen gibt! Ein kluger Mann, der Herr Euklid.

Dieses Problem ist also gelöst. Wir können uns zurücklehnen und zufrieden sagen: Wir sind ganz sicher, dass es unendlich viele Primzahlen gibt, dank dem Herrn aus Ägypten. Aber ich hatte ja zu Beginn versprochen, auch über zwei Probleme zu sprechen, die noch ungelöst sind. Hier ist das erste:

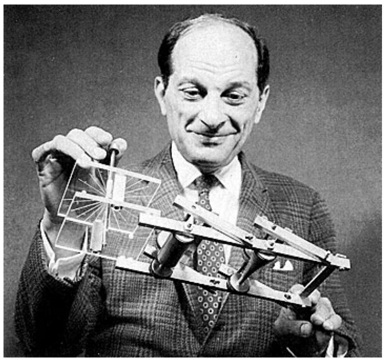
Manchmal passiert es, dass zwei Primzahlen dicht hintereinander folgen, wie zum Beispiel $5, 7$, oder $11, 13$ oder $59, 61$ oder $10.007, 10.009$. Zwei solche Primzahlen nennt man Primzahlzwillinge[4]. Die sind natürlich viel seltener als Primzahlen. Wir können wieder unsere Rechenkiste anwerfen und den Computer fragen, wieviele solcher Zwillinge es gibt. Hier ist die Antwort. Bis zur angegebenen Grenze gibt es jeweils so viele Primzahlzwillinge, wie in der zweiten Zeile angegeben:

alle Zahlen	10	100	1.000	10.000	100.000	1.000.000	10.000.000
Zwillinge	2	8	35	205	1.224	8.169	58.980

Das sind zwar deutlich weniger als Primzahlen, aber die Zahl scheint doch auch klar anzusteigen. Wir können also wieder fragen: Hören die Primzahlzwillinge auf oder gibt es unendlich viele Primzahlzwillinge? Diese Frage ist nun allerdings völlig offen. Viele kluge Mathematikerinnen und Mathematiker haben sich darüber seit mehr als 100 Jahren den Kopf zerbrochen, aber bisher ist noch niemand auf die rettende Idee gekommen. Mit dem Computer kann man nach immer größeren Primzahlzwillingen suchen. Das größte bekannte Primzahlzwillingspaar zum jetzigen Zeitpunkt[5] ist $3.756.801.695.685 \cdot 2^{666.669} \pm 1$. Das sind riesige Zahlen mit über 200.000 Stellen. Sie zu finden, verlangt selbst mit allerschnellsten Computern und einer sehr durchdachten Programmierung wochen- und möglicherweise monatelanges Rechnen. Und für unser Problem nützt es uns eigentlich gar nichts. Und wie uns Euklid gezeigt hat, ist ein kluger Einfall mehr wert als sture Rechnerei. Also bleibt die Frage: Gibt es unendlich viele Primzahlzwillinge? Wär das nicht eine Frage für Euch?

[4]Man könnte die Zahlen 3, 5, 7 Primzahltrillinge nennen. Gibt es noch andere? Die Antwort ist nein! Aber warum?

[5]Stand April 2012. Die Primzahlzwillinge wurden von Timothy Winslow am 25. Dezember 2011 nach zweieinhalbjähriger Suche, an der sich 20.344 Personen mit ihren Computern beteiligt hatten, gefunden.



Stanislaw Ulam[6] (1909 - 1984)

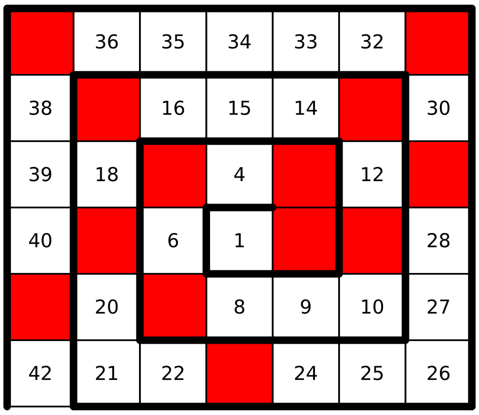
Als letztes möchte ich noch eine Geschichte erzählen, die zu einem sehr merkwürdigen Problem führt. Vielleicht ist das Problem sogar weit wichtiger und interessanter als die Frage nach den Primzahlzwillingen. Im letzten Jahrhundert lebte ein polnisch-amerikanischer Mathematiker names Stanisław Ulam, der an vielen wichtigen mathematischen Theorien gearbeitet hat.

Einmal war er auf einer Konferenz und musste sich viele Vorträge von anderen Mathematikern anhören. Manche davon waren sehr interessant, manche waren eher etwas langweilig. Ein bisschen wie in der Schule.

Bei einem dieser Vorträge fing er an, auf seinem Rechenkästchenpapier alle Zahlen in einer Spirale hinzuschreiben. Also vielleicht so:

37	36	35	34	33	32	31
38	17	16	15	14	13	30
39	18	5	4	3	12	29
40	19	6	1	2	11	28
41	20	7	8	9	10	27
42	21	22	23	24	25	26

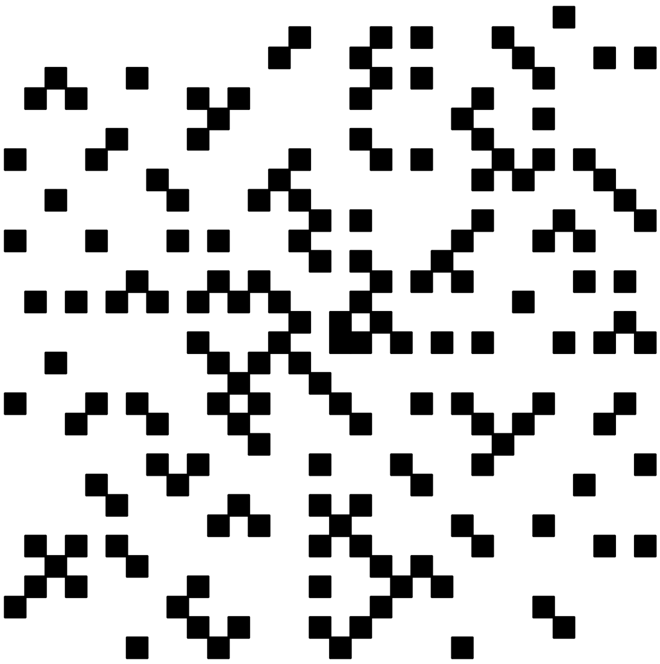
Dann begann er, vor sich hin träumend, der Reihe nach alle Kästchen, in denen Primzahlen stehen, auszumalen.



Und weil der Vortrag wirklich so richtig zum Gähnen langweilig war und Ulam nicht so unhöflich sein wollte und den Saal verlassen, machte er die Spirale immer länger und immer länger. Er war ein fixer Rechner und konnte im Kopf schnell entscheiden, ob eine Zahl eine Primzahl war oder nicht.

Nach 1000 Zahlen kam so etwas heraus:

[6]Bildquelle: http://www-history.mcs.st-and.ac.uk/PictDisplay/Ulam.html

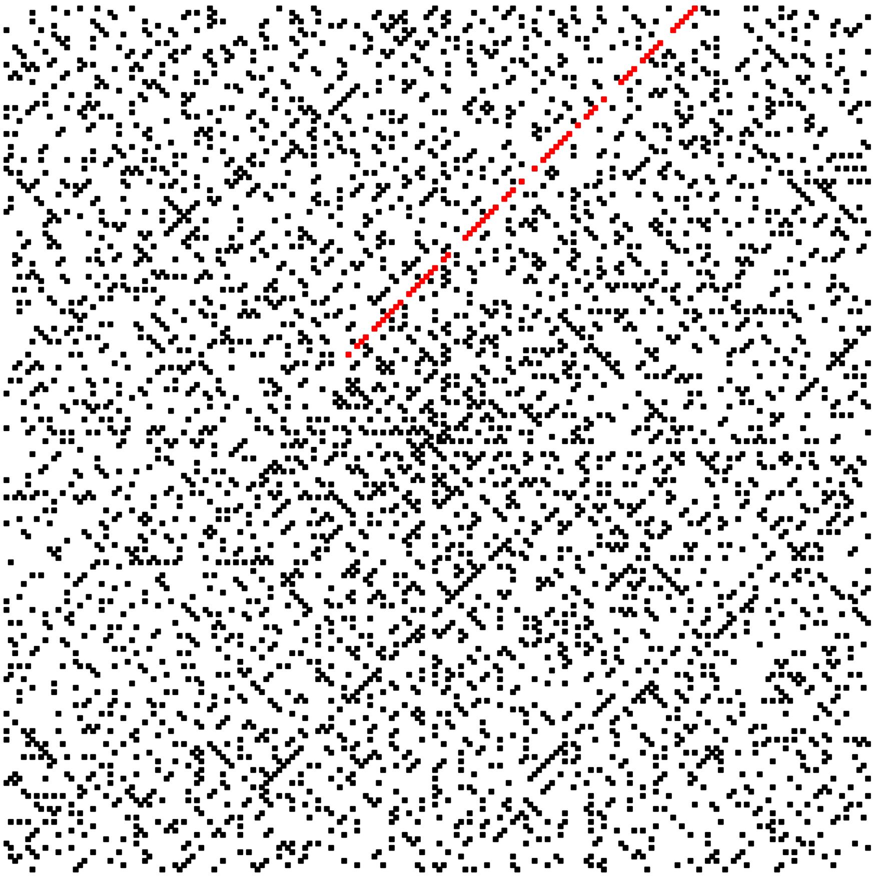


Ich habe die Zahlen weggelassen, damit wir die Übersicht behalten, und auch die störenden Linien. Das Muster hat Ulam gefallen. Und als er wieder zurück in seinem Institut war, hat er mit einem Computer noch weiter gerechnet. Das war in den 60er Jahren des letzten Jahrhunderts, und damals waren Computer bei weitem noch nicht so weit entwickelt wie heute. Ulam konnte auch das Ergebnis nicht einfach ausdrucken, wie ich es gemacht habe, sondern hat mit einem Fotoapparat ein Bild von einer Tafel mit unzähligen kleinen Glühbirnchen abfotografiert. Jedenfalls kommt das folgende Bild[7] heraus, wenn man die ersten 40.000 Zahlen nimmt. Manchmal nennt man dieses Bild auch Ulams Tischdecke.

Das Interessante an diesem Bild ist, dass man plötzlich ganz ungewöhnliche Muster sieht. Zum Beispiel schräge Linien und Diagonalen, auf denen ganz viele schwarze Punkte liegen. Es gibt sogar Geraden, auf den fast nur schwarze Punkte zu liegen scheinen. Aber schwarze Punkte bedeuten doch Primzahlen! Das Bild deutet also darauf hin, dass es irgendwelche Gesetzmäßigkeiten bei der Verteilung der Primzahlen gibt[8]. Aber niemand versteht das Bild. Woher kommen die dunklen Geraden? Welches Geheimnis über Primzahlen verbirgt sich dahinter, das wir nicht kennen?

[7] auf der folgenden Seite

[8] Schon der schweizer Mathematiker Leonhard Euler hat im 18. Jahrhundert die Entdeckung gemacht, dass die Formel $n^2 - n + 41$ nur Primzahlen produziert, wenn man der Reihe nach $n = 1, 2, \ldots, 40$ einsetzt. Für $n = 41$ erhält man natürlich 41^2, also sicher keine Primzahl. Aber selbst, wenn man bis $n = 100$ geht, finden sich unter diesen Zahlen immer noch 86 Primzahlen, und auch für die Obergrenze $n = 1000$ ist mehr als die Hälfte aller Zahlen eine Primzahl!



Ulams Tischdecke

Als die Mathematiker anfingen, über Primzahlen nachzudenken, war das alles Spielerei. Spannend und interessant, aber ein schönes Spiel. Inzwischen brauchen wir Primzahlen und Wissen über Primzahlen an sehr vielen Stellen, wenn wir Geldgeschäfte, aber auch e-mail und Telefongespräche sicher machen und gegen Unbefugte schützen wollen. Denn unsere Theorien über Primzahlen fließen direkt in die sogenannte kryptographische Forschung, also die Forschung von den Verschlüsselungstechnologien, ein. Aber wenn man solche Probleme, wie die, die ich Euch heute erzählt habe, lösen will, reicht es nicht, über mögliche Anwendungen zu spekulieren, sondern man muss sich auf das Spiel einlassen und spielen und rechnen, nachdenken und knobeln.

Mainz, 24. April 2012.