

Von einigen mathematischen Sätzen läßt sich zeigen, daß sie wahr sind, qua Beweis, von anderen, daß sie falsch sind. Es läßt sich darüber hinaus zeigen, erstaunlicherweise, daß es in jeder (halbwegs anspruchsvollen) Axiomatisierung der Mathematik Sätze gibt, die unentscheidbar sind, die sich weder beweisen noch widerlegen lassen.

Ein bekanntes Beispiel für einen unentscheidbaren Satz ist das Auswahlaxiom innerhalb des axiomatischen Systems von Zermelo-Fraenkel (ZF) [wenn hier im folgenden von ZF oder ZFC die Rede ist, dann soll dieses Axiomensystem immer in Verbindung mit einem bestimmten System logischen Schließens gedacht sein, denn ZF selbst braucht zusätzlich eine Logik als Antrieb, um Sätze ableiten zu können]. Es läßt sich beweisen, daß sich das Auswahlaxiom aus den Axiomen von ZF weder beweisen noch widerlegen läßt. Freilich gibt es für diesen Sachverhalt auch viele andere Beispiele (wir können aus ZF andere Axiome streichen und dann zeigen, daß sich die gestrichenen Axiome nicht aus dem verbleibenden Rest ableiten lassen), und in einer solchen Situation können wir das Beispiel eliminieren, indem wir es in den Korpus der Axiome mit aufnehmen (In ZFC, dem Axiomensystem ZF plus Auswahlaxiom, ist das Auswahlaxiom natürlich trivial beweisbar).

Jedenfalls, wenn wir einen (in einer bestimmten Axiomatisierung) unentscheidbaren Satz haben, dann kann es sein, daß wir wenigstens beweisen können, daß der Satz unentscheidbar ist.

Stellen wir uns aber nun einen Satz  $F$  vor, der eine bestimmte Existenzaussage macht. Ein Beispiel wäre etwa Fermats letzter Satz, der behauptet, daß die Gleichung  $a^n + b^n = c^n$  für  $n > 2$  und  $a, b, c > 0$  keine ganzzahligen Lösungen besitzt. Dieser Satz ist natürlich nicht unentscheidbar (da er inzwischen bewiesen ist), aber wir können uns für einen Moment vorstellen, er sei unentscheidbar, das heißt, es gäbe in einer bestimmten Axiomatisierung der Mathematik, etwa ZF, keine Möglichkeit, diesen Satz zu beweisen oder zu widerlegen. In diesem Fall würde das bedeuten, daß dieser Satz wahr sein muß. Denn wenn er nicht widerlegt werden kann, dann bedeutet das, daß es nicht möglich ist,  $n, a, b$  und  $c$  zu finden, die den Satz zu widerlegen, das heißt, es gibt keine solchen Zahlen, das heißt, der Satz ist wahr. Wenn wir uns vorstellen, der Satz  $F$  würde die Existenz eines  $n$  mit der Eigenschaft  $E(n)$  behaupten. Wenn  $F$  unentscheidbar ist, dann bedeutet das, daß  $F$  falsch ist (denn gäbe es ein solches  $n$ , dann wäre  $F$  beweisbar wahr).

Wenn ein solches  $F$  unentscheidbar ist, dann kann es auch nicht möglich sein, die Unentscheidbarkeit von  $F$  innerhalb des entsprechenden Systems zu beweisen. Denn wir haben uns ja bereits überlegt, daß aus der Unentscheidbarkeit von  $F$  die Falschheit von  $F$  folgt (beziehungsweise folgt bei einer negierten Existenzaussage, wie bei Fermats Satz, aus der Unentscheidbarkeit die Gültigkeit des Satzes).

Werden wir ein bißchen formalistischer: sei  $E(n)$  eine Aussage über die natürliche Zahl  $n$ , und die Gültigkeit von  $E(n)$  sei leicht nachzuprüfen (Beispiel:  $E(n) =$  „ $n$  läßt sich schreiben als  $2^m 3^a 5^b 7^c$ , und es gilt  $a^m + b^m = c^m$ , und  $n$  läßt sich durch 840 teilen“). Sei  $F_0$  die Aussage  $\exists n: E(n)$ . Sei außerdem  $F_{n+1}$  die Aussage, daß  $F_n$  in ZFC unentscheidbar ist (da es in ZFC nicht direkt möglich ist, über Aussagen von ZFC zu sprechen, erfordern diese Aussagen einen gewissen technischen Aufwand, um sie codiert dennoch in ZFC ausdrücken zu können, aber die Details können wir uns ersparen).

Wir wollen außerdem annehmen, daß  $F_0$  unentscheidbar ist. Es folgt daraus, daß  $F_0$  falsch ist, und  $F_1$  wahr. Wäre  $F_1$  entscheidbar, dann müßte  $F_1$  gültig sein (wenn wir optimistischerweise davon ausgehen, daß wir nur gültige Sätze beweisen können), aus der Gültigkeit von  $F_1$  läßt sich aber die Falschheit von  $F_0$  ableiten. Also folgt, daß auch  $F_1$  unentscheidbar sein muß.

Nehmen wir an, daß  $F_n$  unentscheidbar ist (und ebenso  $F_{n-1}$ ). Dann ist  $F_{n+1}$  wahr. Nehmen wir an,  $F_{n+1}$  sei entscheidbar. Dann ist (wiederum Widerspruchsfreiheit vorausgesetzt)  $F_{n+1}$  beweisbar. Dann aber ist auch  $F_n$  beweisbar. Denn  $F_n$  behauptet ja gerade,  $F_{n-1}$  sei unentscheidbar. Wäre  $F_n$  falsch, dann müßte  $F_{n-1}$  beweisbar sein. Dann aber wäre  $F_n$  beweisbar falsch, und ebenso  $F_{n+1}$ . Da  $F_n$  nicht falsch sein kann, muß es wahr sein, damit ist die Wahrheit von  $F_n$  bewiesen,  $F_{n+1}$  damit falsch, im Widerspruch zur Voraussetzung. Wenn  $F_n$  und  $F_{n-1}$  unentscheidbar sind, dann auch  $F_{n+1}$ .

In gewisser Weise sind also Sätze der Form  $\exists n:E(n)$  beziehungsweise  $\neg\exists n:E(n)$  (mit leicht entscheidbarem  $E(n)$ ), wenn sie unentscheidbar sind, nicht einfach nur unentscheidbar, sondern böartig unentscheidbar, da auch die Unentscheidbarkeit sich nicht mit gewöhnlichen Mitteln beweisen läßt.

Wenn das so ist, wie kann es dann sein, daß die Unentscheidbarkeit des Auswahlaxioms beweisbar ist? Denn alle Sätze außer den völlig elementaren beginnen doch entweder mit einem  $\exists$  oder einem  $\neg\exists$  und sind insofern mit unserem böartig unentscheidbaren Satz  $F$  vergleichbar, oder? Müßte dann nicht auch das Auswahlaxiom böartig unentscheidbar sein?

Der Beweis der Unentscheidbarkeit des Auswahlaxioms wird gewöhnlich nicht in ZF selbst geführt (was außerordentlich mühsam wäre), so daß ein Teil unserer obigen Argumentation für  $F$  gar nicht anwendbar ist, aber das ist nicht der wesentliche Unterschied. Wesentlich für unsere Argumentation ist, daß unsere Beispiele beziehungsweise Gegenbeispiele eindeutig und leicht zu durchschauen sind und keinerlei Mühe bereiten. Wir können gemütlich nach und nach jedes  $n$  prüfen, und ob  $E(n)$  gilt oder nicht gilt, erfordert selbst wieder keinerlei Beweise, sondern ist mechanisch nachzuprüfen.

In gewisser Weise gilt tatsächlich für das Auswahlaxiom etwas analoges wie im Fall des Satzes  $F$ . In ZF gibt es nämlich besondere Mengen einer Klasse  $K$  von konstruierbaren Mengen, und diese Klasse ist ein Modell (und zwar das kleinste Modell) für die Klasse aller Mengen, also ein Modell für ZF. Aus den Axiomen von ZF läßt sich nicht beweisen, daß es neben den Mengen in  $K$  noch weitere Mengen gibt, ebensowenig, wie diese Behauptung sich widerlegen läßt. Für die Mengen in  $K$  läßt sich mehr oder weniger leicht überprüfen, ob für irgendwelche Konstrukte aus diesen Mengen das Auswahlaxiom gilt oder nicht gilt. Und innerhalb dieser Klasse ist das Auswahlaxiom auch nicht unentscheidbar: wäre es unentscheidbar, dann würde das bedeuten, daß wir kein Gegenbeispiel konstruieren können, was aber wiederum zur Folge haben muß, daß es eben kein Gegenbeispiel gibt und wir tatsächlich wissen, daß es innerhalb von  $K$  kein Gegenbeispiel gibt. Innerhalb von  $K$  ist das Auswahlaxiom beweisbar wahr, und  $K$  stellt deshalb ein Modell von ZF dar, in dem das Auswahlaxiom gilt (Das Modell beweist die Unwiderlegbarkeit des Auswahlaxioms). Der umgekehrte Fall, die Unbeweisbarkeit des Auswahlaxioms zu zeigen, ist sehr viel schwieriger (und gelang auch erst viel später), weil es keine einfachen Modelle von ZF gibt, in denen das Auswahlaxiom beweisbar falsch ist. Außerhalb von  $K$  könnte es Gegenbeispiele geben, die aber so bizarr sind, daß wir nicht mit dem Finger darauf deuten können, aber innerhalb des

Bereiches, in dem jedes Gegenbeispiel ein konkretes Gegenbeispiel ist, haben wir eine Situation analog zum Satz F, für den jedes Gegenbeispiel ein konkretes Gegenbeispiel ist. Falls wir als Gegenbeispiele zum Auswahlaxiom nur tatsächlich konstruierbare Gegenbeispiele, quasi Gegenbeispiele „zum Anfassen“ zulassen, dann ist das Auswahlaxiom nicht unentscheidbar, sondern wahr. Etwas ähnliches gilt für die Kontinuumshypothese, bei der es um die Frage geht, ob sich zwischen die Kardinalzahlen  $\aleph_0$  und  $2^{\aleph_0}$  noch weitere Kardinalzahlen tummeln oder nicht: die Frage ist unentscheidbar (und es ist möglich, daß es in diesem Intervall sehr, sehr viele Kardinalzahlen gibt), aber es ist klar (oder jedenfalls beweisbar), daß uns im täglichen Leben niemals konkrete Gegenbeispiele begegnen werden (nichtsdestotrotz scheint der Konsens allerdings inzwischen eher in die Richtung zu gehen, daß die Kontinuumshypothese besser falsch sein sollte).

Damit ist die Situation in der Zahlentheorie freilich eine andere als in der Mengenlehre. In der Mengenlehre tauchen ständig Gebilde auf, die mehr oder weniger hypothetischen Charakter haben und von denen durchaus unklar ist, ob es tatsächlich Beispiele für diese Gebilde gibt. Sätze über „schwach unerreichbare Kardinalzahlen“ (die nur die unterste Stufe einer Hierarchie wolkenreicher Zahlengötter sind) sind nun einmal nicht von der Art, daß sie sich ebenso nachrechnen lassen wie  $5 + 7$ . Die Welt der natürlichen Zahlen dagegen ist zwar auch ein unüberschaubarer Ort, aber aus ganz anderen Gründen. Es ist daher zu befürchten, daß unentscheidbare Sätze der Zahlentheorie oftmals böseartig unentscheidbare Sätze sind. Es versteht sich, daß ich kein „echtes“ Beispiel eines böseartig unentscheidbaren Satzes angeben kann; Gödels unentscheidbarer Satz für die Principia Mathematica Und Verwandte Systeme allerdings ist vom Typ eines böseartig unentscheidbaren Satz.

Das gilt natürlich nicht für eine Betrachtung von außerhalb des Systems. Von außen betrachtet, ist Gödels unentscheidbare Satz nicht unentscheidbar, sondern wahr, und dementsprechend ist auch der Satz, der seine Unentscheidbarkeit behauptet, für uns nicht unentscheidbar, sondern wahr, und so weiter für die ganze Hierarchie der böseartigen unentscheidbaren wahren Sätze, die Gödels Satz nach sich zieht.

Das aber ist nicht wirklich ein Trost. Denn wenn es auch noch vergleichsweise einfach ist, gegenüber Gödels für die Principia unentscheidbarem Satz einen Standpunkt außerhalb der Principia anzunehmen, so gilt dies doch nicht ebenso für die gewöhnliche Arithmetik.

Stellen wir uns noch einmal vor, Fermats Satz sei innerhalb einer bestimmten Axiomatisierung der Mathematik ein unentscheidbarer Satz, etwa innerhalb von ZF. Selbstverständlich gibt es andere Axiomatisierungen, für die Fermats Satz nicht unentscheidbar ist, etwa für die Axiome ZF+Fermat, also die Axiome von ZF mit einem zusätzlichen Axiom, das gerade der Fermatsche Satz ist. Wir würden uns dann aber kaum auf den Standpunkt stellen können „in bestimmten unglücklichen Axiomatisierungen ist dieser Satz unentscheidbar, macht nichts, wir müssen eben nur mit den geeigneten Axiomen beginnen“. Denn es scheint doch klar, daß alle „vernünftigen“ Axiomatisierungen der Arithmetik (und damit indirekt der ganzen Mathematik) letztlich alle gleich sind, also inhaltlich das gleiche liefern, und daß, wenn eine „vernünftige“ Axiomatisierung A den Beweis des inhaltlich nichttrivialen Satzes F nicht erlaubt, daß dann die Axiomatisierung A+F keine vernünftige Alternative darstellt. Zumal ja die allermeisten Mathematiker überhaupt keine Formalisierung verwenden, und unsere Besorgnis dem Fall gilt, daß ein bestimmter Satz F nicht in dieser oder jener speziellen Formalisierung unentscheidbar ist, sondern daß er in der gewöhnlichen informellen Mathematik unentscheidbar ist. Zwar ist es möglich (und geschieht auch

ständig), die gewöhnliche Mathematik und ihren Formalismus zu erweitern, zu verändern oder einen Metastandpunkt einzunehmen, freilich sind nicht mehr alle denkbaren Erweiterungen und Modifikationen derart, daß wir sie als Mathematik bezeichnen möchten, und es könnte sein, daß jeder Form dessen, was wir als Mathematik bezeichnen, ein gemeinsames Gerüst zugrunde liegt und daß der fragliche Satz  $F$  in keiner dieser Formen entscheidbar ist.

Der Fermatsche Satz mußte in den obigen Abschnitten als Beispiel erhalten, weil er sehr bekannt und sehr einfach ist, obwohl er nun inzwischen entschieden ist. Es bleiben genug Sätze übrig, die noch nicht entschieden sind und von denen denkbar ist, daß sie böartig unentscheidbare Sätze sind. Ein besonders frappantes Beispiel möchte ich (um der Leserin wohlige Schauer des Entsetzens über den Rücken zu jagen bei der Vorstellung, es könne sich um böartig unentscheidbare Sätze handeln) noch kurz vorstellen.

Im Grunde ist es (um Hardy zu wiederholen) sehr einfach, Vermutungen auszusprechen, die zu beweisen oder zu widerlegen dann ungeheuer schwer ist. Insbesondere in der Zahlentheorie scheint es besonders einfach, einfach formulierte Vermutungen zu finden, die sich hartnäckig allen Lösungsversuchen widersetzen. Letztlich ist das Verhältnis zwischen Addition und Multiplikation (die lediglich eine verschlungene Form der Addition ist) nicht richtig verstanden und durchdrungen. Bezüglich der Addition sind die natürlichen Zahlen ein harmloses Gebilde, das sich, ausgehend von der 0, durch beharrliches Addieren der 1 erzeugen läßt. Bezüglich der Multiplikation handelt es sich um ein etwas komplizierteres Gebilde mit einer unendlichen Basis, in dem jede Zahl größer Null sich darstellen läßt als  $\prod_{p \in P} p^{a_i}$ , wobei  $P$  die Menge der Primzahlen ist und nur endlich viele Koeffizienten von Null verschieden, aber letztlich ist auch dieses Gebilde, für sich betrachtet, nicht übermäßig kompliziert. Wirklich kompliziert ist, daß die Basis der multiplikativen Zusammensetzung der Zahlen, die Primzahlen, so schief und schräg innerhalb der natürlichen Zahlen liegen, wie sie sich durch fortgesetzte Addition der 1 ergeben. Sofort stellen sich mehr oder weniger schwierige Fragen, die wir längst nicht alle beantworten können, etwa die harmlose Frage, ob es unendlich viele Primzahlzwillinge gibt, also Primzahlenpaare mit der Differenz 2. Auch Fragen derart, wie wir Potenzen von bestimmten Zahlen summieren können, um bestimmte andere Zahlen zu erhalten, wie Fermats Satz oder die Goldbachvermutung, entstehen aus dieser Verwirrung.

Um das verschlungene Verhältnis von Addition und Multiplikation zu entwinden, liegt es nahe, die Menge der Teiler einer Zahl zu betrachten, und der Begriff des Teilers dürfte eine der ältesten mathematischen Begriffsbildungen sein. Unabhängig voneinander wurde in verschiedenen Kulturen die Entdeckung gemacht, daß es bestimmte Zahlen gibt, die gerade die Summe ihrer echten Teiler sind (eine Zahl ist ihr eigener Teiler, wenn sie nicht gerade die Null ist, aber da dieses Teilbarkeitsverhältnis so trivial ist, gilt dieser Teiler als minderwertig, also unecht), wie zum Beispiel  $1 + 2 + 3 = 6$ , oder  $1 + 2 + 4 + 7 + 14 = 28$ . Zahlen mit dieser Eigenschaft heißen „perfekt“. Es liegt nahe, zu fragen, ob es unendlich viele solcher perfekten Zahlen gibt, wie sie sich charakterisieren lassen oder wie sie sich systematisch erzeugen lassen. Eine weitere sehr naheliegende und wohl auch sehr alte Frage ist, ob es auch ungerade perfekte Zahlen gibt.

Nun ist es nicht so, daß wir inzwischen, seit den archaischen Tagen, an denen diese Fragen das erste Mal gestellt wurden, nicht einiges herausgefunden hätten. Wir wissen beispielweise folgendes: wenn  $p$  eine Primzahl ist und  $2^p - 1$  ebenfalls eine Primzahl ist (in welchem Fall sie „Mersen-

ne-Primzahl“ heißt), dann ist  $2^{p-1}(2^p - 1)$  eine perfekte Zahl. Wir wissen auch, daß alle geraden perfekten Zahlen von dieser Form sind, wir wissen, daß 191561942608236107294793378084303638130997321548169216 eine perfekte Zahl ist, wir kennen perfekte Zahlen mit 8107892 Ziffern, die ich hier allerdings nicht hinschreiben möchte, weil das ein Konvolut im Bibelformat ergäbe, allerdings kennen wir erst 39 gerade perfekte Zahlen und wissen nicht, ob es unendlich viele davon gibt. Ein wenig wissen wir auch über ungerade perfekte Zahlen: sollte es denn tatsächlich eine geben, dann hat sie mindestens 29 Primfaktoren, davon mindestens acht verschiedene, wenigstens einer davon ist größer als  $10^{20}$  und die Zahl selbst größer als  $10^{300}$ . Ob es denn aber eine gibt, wissen wir nicht. Das heißt, grob gesagt, dreitausend Jahre Forschung haben uns nicht weiter gebracht, als die Frage „Wie viele perfekte Zahlen gibt es?“ durch die Frage „Wie viele gerade und wie viele ungerade perfekten Zahlen gibt es?“ zu ersetzen.

Es gibt ebenso viele perfekte Zahlen wie Mersenne-Primzahlen, aber wir wissen nicht, ob es unendlich viele Mersenne-Primzahlen gibt. Derartige Fragen lassen sich leicht vervielfältigen: sei  $M_1(p) = 2^p - 1$ ,  $M_{n+1}(p) = M(M_n(p))$ . Wie viele Primzahlen gibt es, so daß  $M_2(p)$  prim ist? Was ist das größte  $n$ , so daß es eine Primzahl  $p$  gibt, so daß  $M_n(p)$  prim ist? Selbst eine einfache Frage (die sich im Prinzip mechanisch beantworten lassen sollte, wenn die Antwort nicht gerade „unendlich“ lautet) wie die, welches das kleinste  $n$  ist, so daß  $M_n(2)$  nicht prim ist, stößt an die Grenzen unserer Rechenkapazität: die Antwort ist  $\geq 5$ , aber ob  $M_5(2)$  prim ist, ist schwer zu sagen, da  $M_5(2)$  bereits mehr als  $10^{38}$  Ziffern hat.

In unseren Überlegungen haben wir ein realistisches Modell der Mathematik zugrunde gelegt („realistisch“ nicht in dem Sinne, daß es die Realität besonders realistisch wiedergeben würde, sondern im Sinne von platonisch, die mathematischen Entitäten als Realien auffassend, im Gegensatz zu „konstruktivistisch“). Wir gingen davon aus, daß es ein Beispiel  $n$  mit der Eigenschaft  $E(n)$  entweder gibt oder nicht gibt, unabhängig davon, was wir darüber wissen, unter Verwendung des Satzes vom ausgeschlossenen Dritten, die Menge der natürlichen Zahlen als ein selbstständiges, von uns Menschen unabhängiges Ding auffassend. Ich überlasse es der Leserin als Übung, sich zu überlegen, was sich ergibt, wenn wir auf diese Voraussetzung verzichten.

---

17.9.2002

---

Heute wird Selene 256 Tage alt. Das ist eine Fermatsche Zweierpotenz, also eine Zweierpotenz, deren Exponent selbst wieder eine Zweierpotenz ist. Die nächste derartige Zahl ist 65536, das entspricht etwas mehr als 179 Jahren.

---

Ein kleiner Nachtrag zu den Mersenne-Primzahlen, im Lichte des Konstruktivismus:

Wir definieren:

$$M_0(n) = n$$

$$M_1(n) = 2^n - 1$$

$$M_{k+1} = M_1(M_k(n))$$

Falls  $n$  und  $M_1(n)$  Primzahlen sind, dann ist  $M_1(n)$  gerade eine Mersenne-Primzahl. Zu beachten ist, daß, wenn  $M_k(n)$  keine Primzahl ist, daß dann auch  $M_{k+1}(n)$  keine Primzahl ist (die erste zusammengesetzte Zahl sorgt dafür, daß die Iteration von da an nur noch zusammengesetzte Zahlen liefert). [Beweis gefällig? Sei  $n = mk$ . Dann läßt sich  $2^{km} - 1$  zerlegen in  $2^m - 1$  und  $2^{m(k-1)} + 2^{m(k-2)} + \dots + 2^m + 1$ .]

Sei ferner  $P$  die Menge der Primzahlen. Dann definieren wir

$$m(n) = |\{k \mid M_k(n) \in P\}|$$

also die Anzahl der Zahlen  $k$ , für die  $M_k(n)$  eine Primzahl ist. Für eine zusammengesetzte Zahl  $n$  ist  $m(n)$  gerade 0, für eine Primzahl mindestens 1, für eine Primzahl, für die  $M_1(n)$  eine Mersenne-Primzahl liefert, ist  $m(n)$  mindestens 2. Es ist denkbar, daß es Zahlen gibt, für die  $m(n)$  den Wert  $\infty$  liefert, aber daran wollen wir uns nicht stören (in solchen Fällen könnten wir  $m(n)$  den Wert  $-1$  zuordnen, wenn wir eine Abbildung  $\mathbf{N} \rightarrow \mathbf{N}$  verwenden möchte, aber dieser Aufwand scheint mir übertrieben). Wir können fragen, wie groß  $m(n)$  maximal werden kann, also nach dem Wert von  $\sup_k \{\exists j: k = m(j)\}$ , aber die Frage nach diesem Wert ist schwer zu beantworten, ich weiß nicht einmal, ob dieser Wert endlich oder unendlich ist. Eine andere Frage ist die, ob die Folge  $\sum_{i>0} \frac{m(i)}{i}$  konvergiert; jedenfalls wird sie größer als 5.

Hier die ersten 32 Werte der Funktion:

0	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
0	0	$\geq 4$	$\geq 3$	0	3	0	$\geq 2$	0	0	0	1	0	2	0	0	0	2	0	2	0	0	0	1	0	0	0	0	0	1	0	2

Wir definieren nun eine weitere Zahl:

$$m = \min_n \{m(n) = \sup_k \{\exists j: k = m(j)\}\}$$

Wir wissen nicht, wie groß  $m$  ist. Es ist denkbar und noch nicht einmal unplausibel, daß  $m$  den Wert 2 annimmt. Es dürfte nicht ganz einfach sein, den Wert von  $m$  zu bestimmen. Schlimmer noch: es ist denkbar, daß  $m$  überhaupt nicht existiert. Das ist dann möglich, wenn zwar  $m(n)$  jede beliebige Schranke übersteigt, so daß  $\sup_k \{\exists j: k = m(j)\} = \infty$ , es aber kein  $m$  gibt, so daß  $M_k(m)$  für beliebiges  $k$  prim ist

Insgesamt scheint die Existenz von  $m$  plausibler als die Nichtexistenz. Darüber hinaus scheint es plausibel, anzunehmen, daß  $\sup_k \{\exists j: k = m(j)\}$  endlich ist. Das liegt daran, daß es für größere Zahlen immer schwieriger wird, prim zu sein, so daß es immer schwieriger werden dürfte, lange Ketten von Zahlen zu finden, die Mersenne-Primzahlen ergeben. Zwar haben wir unendlich viele Versuche zur Verfügung, unsere Chancen werden aber auch immer schlechter.

Die Chance, daß eine Zahl  $n$  eine Primzahl ist, ist von der Größenordnung  $\ln^{-1}n$ . Damit  $m(n) \geq 2$  gilt, muß auch  $M_1(n)$  prim sein, mit einer Wahrscheinlichkeit von  $\ln^{-1}(2^n - 1)$ . Eine Abschätzung der Wahrscheinlichkeit, daß  $m(n) \geq r$  ist, ergibt  $\prod_{i \in [0, r]} \ln^{-1}(M_i(n))$ , und für größere Werte von  $n$  und  $r$

wird diese Zahl sehr schnell sehr klein (und die Summe über alle  $n$  konvergiert). Es ist daher nicht unvernünftig, zu vermuten, daß  $m(2) = 4$  und  $m = 2$  (ein ähnlich primitives Argument legt nahe, daß es unendlich viele Mersenne-Primzahlen gibt, aber nur endlich viele Zahlen  $n$ , für die  $M_2(n)$  eine Primzahl ist). Aber letztlich wissen wir das nicht sicher. Es könnte sein, daß unsere Wahrscheinlichkeitsüberlegungen zwar an sich richtig sind, daß aber durch einen sehr, sehr unwahrscheinlichen Zufall eben doch etwas anderes der Fall ist. Oder aber die Wahrscheinlichkeiten mehrere Zahlen, prim zu sein, ist eben nicht unabhängig, wenn diese Zahlen in der Relation stehen, das  $M_0(n)$ ,  $M_1(n)$ ,  $M_2(n)$ , ... einer Zahl  $n$  zu sein (siehe auch die übernächste Skizze).

Nehmen wir an,  $m$  existiert. In welchem Sinn können wir sagen, daß  $m$  existiert? Von einem streng monistisch-materialistischen Standpunkt aus existiert natürlich noch nicht einmal die Zahl 2, allenfalls ließe sich sagen, bestimmte menschliche Tätigkeiten seien derart, daß in ihr die-und-die Schriftzeichen und Laute das-und-das bewirken. Vom realistischen Standpunkt aus fühlen wir uns bedrängt, uns  $m$  als eine Art undurchsichtiger Schachtel zu denken, die vielleicht leer ist, vielleicht aber auch die Zahl 2 enthält oder die Zahl  $2^{13466917} - 1$  oder sonst eine Zahl. Jedenfalls existiert, vom realistischen Standpunkt aus, der Inhalt der Schachtel  $m$ , mag er auch das Nichts sein, unabhängig davon, ob wir Menschen in die Schachtel hinein geschaut haben oder nicht. Von einem etwas anspruchsvolleren Standpunkt aus existiert noch nicht einmal die Funktion  $m(\cdot)$ , da wir ja kein Verfahren angegeben haben, das es erlauben würde,  $m(\cdot)$  zu berechnen. Allerdings sind wir durchaus imstande (wie die obige Tabelle zeigt), eine ganze Reihe von Werten von  $m(\cdot)$  zu berechnen. Wir könnten also versucht sein zu sagen,  $m(\cdot)$  sei definiert und berechenbar auf jenen Werten  $n$ , die  $m(n) < \infty$  liefern. Möglicherweise aber (und die Überlegung des vorangegangenen Abschnitts läßt diese Möglichkeit sogar als wahrscheinlich erscheinen) gilt sogar für  $\forall n \in \mathbb{N}: m(n) < \infty$ , so daß  $m$  für sämtliche Werte definiert und berechenbar wäre. Wir hätten dann eine Funktion, für die jeder Funktionswert wohldefiniert und berechenbar ist, von der wir das aber nicht wissen. In welchem Sinn können wir dann sagen, daß  $m(\cdot)$  existiert?

Wenn  $m(n)$  für alle  $n$  endlich ist, dann läßt sich  $m(\cdot)$  durch eine simple Turingmaschine berechnen. Falls sogar das Supremum aller  $m(n)$  endlich ist (beispielsweise gleich 4), dann können wir sogar Zeitschranken angeben, innerhalb derer die Turingmaschine ihre Antwort liefert (Mersenne-Zahlen daraufhin zu testen, ob sie Primzahlen sind, ist sogar vergleichsweise einfach, ärgerlich ist lediglich, daß  $M_4(n)$  die Tendenz hat, um einiges größer als  $n$  auszufallen). Für die orthodoxe Rekursionstheorie wäre  $m(\cdot)$  dann eine langweilige Funktion. Nehmen wir aber an, die Endlichkeit von  $m(n)$  für alle  $n$  ließe sich nicht beweisen (wobei diese Unentscheidbarkeit nicht einmal bössartig im Sinne der gestrigen Skizze zu sein braucht; denn für ein gegebenes  $n$  braucht es kein einfaches Verfahren zu geben, von dem wir wissen, daß es abbricht, mit dem wir entscheiden können, ob  $n$  das Gegenbeispiel mit  $m(n) = \infty$  ist). Wir könnten zwar für jedes konkrete  $n$  den Wert von  $m(n)$  bestimmen, wir könnten aber nicht zeigen, daß wir für jedes  $n$  den Wert von  $m(n)$  bestimmen können.  $m(\cdot)$  bliebe zu einer schattenhaften und ein wenig zweifelhaften Existenz verurteilt.

---

Nachtrag, als Warnung für hoffnungsvolle Anfänger: plausibel klingende Wahrscheinlichkeitsargumente für zahlentheoretische Vermutungen lassen sich leicht finden und können leicht in die Irre führen. Wenn wir etwa davon ausgehen, daß bei einem Zahlenpaar  $n$  und  $n + 1$  beide Zahlen mit einer Wahrscheinlichkeit von  $\ln^{-1}n$  prim sind, dann können wir „beweisen“, daß es „wahrscheinlich“ unendlich viele derartige Paare gibt, bei denen beide Zahlen prim sind. Tatsächlich aber ist es so, daß entweder  $n$  oder  $n + 1$  gerade ist. Falls also  $n$  eine Primzahl ist, dann ist  $n + 1$  entweder die Zahl drei, oder  $n + 1$  ist eben nicht prim. Es gibt also keineswegs unendlich viele benachbarte Primzahlpaare, sondern bloß ein einziges. Insofern ist oben auch keineswegs bewiesen, daß „wahrscheinlich“ (was auch immer dieses Wort hier bedeuten mag) unendlich viele Primzahlen der Form  $M_1(n)$ , aber nur endlich viele der Form  $M_2(n)$  existieren. Eine Zahl der Form  $M_2(n)$  scheint „doppelt so gute Chancen“ zu haben, prim zu sein, als eine beliebige Zahl, da  $M_2(n)$  ungerade ist und somit nicht zu der Hälfte der Zahlen gehört, die von vorneherein nicht prim sein können, weil sie durch zwei teilbar sind. Wenn wir nicht gründlicher über diese Fragen nachgedacht haben, können wir nicht sicher sein, daß es nicht aufgrund ähnlicher, aber komplizierterer und verborgenerer Beziehungen doch bloß endlich viele Primzahlen der Form  $M_1(n)$  oder doch unendlich viele Primzahlen der Form  $M_2(n)$  (allerdings schwerlich beides gleichzeitig) gibt.

---

18.9.2002

Jan Thor