Zahlentheorie – Über Größe und Teilbarkeit

Christian Bernert, 4. Oktober 2020

Einleitung

In diesem Skript geht es um die folgende sehr nützliche Tatsache aus der Zahlentheorie:

Trick: Ist d eine natürliche Zahl und $n \neq 0$ eine ganze Zahl mit $d \mid n$, so folgt $d \leq |n|$.

!!!Warnung!!! Die Bedingung $n \neq 0$ sollte hier nicht übersehen werden.

Wir wollen dieses Prinzip nun an einigen Aufgaben illustrieren.

Eine Aufgabe aus der Bundesrunde

Wir beginnen mit einer einfachen Aufgabe aus der Bundesrunde, die einige von euch sicherlich noch gut kennen.

Aufgabe 1: Man bestimme alle positiven ganzen Zahlen n, für die eine positive ganze Zahl d mit der Eigenschaft existiert, dass n durch d teilbar ist sowie $n^2 + d^2$ durch $d^2n + 1$ teilbar ist.

Wenn ihr die Aufgabe noch nicht kennt, versucht sie erst einmal selbst zu lösen, bevor ihr weiterlest.

Wie gehen wir bei einer solchen Aufgabe vor? Wir haben zwei Bedingungen, nämlich $d \mid n$ und $d^2n + 1 \mid n^2 + d^2$. Indem wir eine neue Variable einführen, können wir eine der Bedingungen loswerden. Wir schreiben also $n = d \cdot k$. Dann suchen wir ganze Zahlen d und k mit

$$d^3k + 1 \mid d^2k^2 + d^2.$$

An dieser Stelle könnten wir schon unseren Trick benutzen und erhalten

$$d^3k + 1 \leq d^2k^2 + d^2,$$

da beide Seiten positiv sind. Dies ist allerdings, wie man sich leicht überzeugt, noch keine besonders starke Einschränkung. Die Strategie ist es also, die Teilbarkeitsbeziehung vor der Anwendung des Tricks so zu manipulieren, dass die Zahl auf der rechten Seite möglichst klein ist, sodass die Anwendung des Fakts ein möglichst starkes Resultat liefert. Eine sehr nützliche Beobachtung ist hier, das sich $d^2k^2+d^2$ faktorisieren lässt zu $d^2(k^2+1)$. Da $d^3k + 1$ offensichtlich teilerfremd zu d ist, folgt also sogar $d^3k + 1 \mid k^2 + 1$.

Würden wir jetzt den Trick anwenden, erhielten wir $d^3k + 1 \leq k^2 + 1$ oder äquivalent $k \geq d^3$. Dies ist schon interessant, aber immer noch nicht genug.
Stattdessen ziehen wir noch einmal $d^3k + 1$ ab und erhalten

$$d^3k + 1 \mid k^2 - d^3k.$$

Der Vorteil ist nun, dass sich die rechte Seite wieder faktorisieren lässt als $k(k - d^3)$. Da auch k teilerfremd zu $d^3k + 1$ ist, folgt sofort

$$d^3k + 1 \mid k - d^3.$$

Wegen $k \geq d^3$ ist die rechte Seite nicht negativ, sie ist aber offensichtlich kleiner als k und damit auch kleiner als d^3k+1. Nach Anwendung des Tricks ist also die einzige verbliebene Möglichkeit $k = d^3$ und somit $n = d^4$. Damit ist die Aufgabe im Wesentlichen gelöst. □

Eine Aufgabe aus der Chinesischen Mädchenolympiade

Nachdem wir jetzt aufgewärmt sind, versuchen wir eine etwas härtere Nuss zu knacken.

Aufgabe 2: Es seien p und q Primzahlen mit $p < q$. Zeige

$$\mathrm{ggT}(p! - 1, q! - 1) \leq p^{p/3}.$$

Wir versuchen zunächst den merkwürdigen Ausdruck $p^{p/3}$ auf der rechten Seite zu ignorieren und eine möglichst gute Schranke für die linke Seite zu finden. Dazu bezeichnen wir diese mit d. Es ist also d ein Teiler von $p! - 1$ und von $q! - 1$.

Mit unserem Fakt folgt sofort $d < q!$. An dieser Stelle lohnt es sich etwas über die Größe von Fakultäten nachzudenken. Einige von euch kennen vielleicht die **Stirlingsche Formel**, die besagt, dass für große n asymptotisch

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

gilt, wobei die Notation bedeutet, dass der Quotient der beiden Seiten für $n \to \infty$ gegen 1 geht. Wer es ganz genau wissen möchte, kann versuchen sich die für alle $n > 0$ exakte Abschätzung

$$1 < e^{1/(12n+1)} < \frac{n!}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} < e^{1/(12n)} < 1 + \frac{1}{11n}$$

zu merken. In der Praxis sind allerdings die „offensichtlichen“ Abschätzungen

$$n^{\frac{n}{2}} \leq n! \leq n^n$$

für $n \geq 1$ oft gut genug.

Übung 1: Überzeuge dich davon, dass die behaupteten Ungleichungen offensichtlich sind. (Tipp für die untere Schranke: Betrachte $k(n + 1 - k)$.)

Die Stirlingsche Formel kann man sich dann in der weniger präzisen Form merken, dass $n!$ „im Wesentlichen“ so groß ist wie $\left(\frac{n}{e}\right)^n$ liegt, was bedeutet, dass die triviale obere Schranke n^n gar nicht so schlecht ist.

Wir kommen nun zurück zur chinesischen Aufgabe und verwenden die triviale obere Schranke, um

$$d < q! \leq q^q < p^q < p^p$$

zu erhalten (mit dem Wissen im Hinterkopf, dass dies nicht wesentlich verbessert werden kann). Damit haben wir die Aufgabe immerhin bereits gelöst, falls $q \leq \frac{p}{3}$ ist.
Falls q allerdings wesentlich größer ist, müssen wir uns eine neue Idee überlegen. Die Strategie ist es nun, möglichst kleine Vielfache von d zu „erzeugen“, aus denen wir neue Schranken ableiten können.
Dazu ist es nützlich, die Bedingung zu $p! \equiv 1 \mod d$ und $q! \equiv 1 \mod d$ umzuschreiben. Hier sehen wir bereits eine Möglichkeit: Wegen $p > q$ ist auch $\frac{p!}{q!}$ eine ganze Zahl und es gilt $\frac{p!}{q!} \equiv 1 \mod d$ und wegen $p! > q!$ folgt dann sofort

$$d \leq \frac{p!}{q!} - 1 < \frac{p!}{q!}.$$

Kombinieren wir dies mit unserer vorherigen Abschätzung $d < q!$ folgt sofort $d^2 < p! < p^p$ und somit $d < p^{p/2}$. Dies ist allerdings noch ein Stück entfernt von der Behauptung.

Man hätte auch die Abschätzung

$$d < \frac{p!}{q!} = p(p-1)\dots(q+1) < p^{p-q}$$

verwenden können, was die Behauptung für $q \geq \frac{2p}{3}$ zeigt. Auch hier bleibt allerdings der Bereich $\frac{p}{3} < q < \frac{2p}{3}$ übrig.

Wie können wir unser Argument noch optimieren? Eine natürliche Idee ist es, $\frac{p!}{(q!)^2}$ zu betrachten. Für $p \geq 2q$ ist dies ein Vielfaches von $\frac{(2q)!}{(q)!^2} = \binom{2q}{q}$, also eine ganze Zahl und wie zuvor folgt dann

$$\frac{p!}{(q!)^2} \equiv 1 \mod d$$

und somit

$$d < \frac{p!}{(q!)^2},$$

falls $p \geq 2q$ ist. Kombiniert mit $d < q!$ erhalten wir wiederum $d^3 < p! < p^p$, also $d < p^{p/3}$ wie gewünscht. Es bleibt allerdings immer noch der Bereich $\frac{p}{2} < q < \frac{2p}{3}$ übrig. Hier benötigen wir noch einen weiteren Trick:
Dazu betrachten wir die schon gezeigten Tatsachen $d \mid q! - 1$ und $d \mid \frac{p!}{q!} - 1$. Wie in der ersten Aufgabe können wir diese nun kombinieren zu

$$d \mid q! - \frac{p!}{q!}.$$

Der Vorteil ist, dass nun die Einsen verschwunden sind und wir einen gemeinsamen Faktor der beiden Zahlen herausziehen können. Tatsächlich wissen wir, dass beide Zahlen durch $(p-q)!$ teilbar sind und d zu $p!$ und damit auch zu $(p-q)!$ teilerfremd ist, also folgt sogar

$$d \mid \frac{q!}{(p-q)!} - \frac{p!}{q!(p-q)!} = \frac{q!}{(p-q)!} - \binom{p}{q}.$$

Nun wollen wir wieder unseren Trick anwenden, allerdings ist zunächst nicht vollkommen klar, ob die rechte Seite positiv oder negativ ist. Sie kann zumindest nicht Null sein (dann würde unser Trick gar nichts aussagen), denn $\binom{p}{q}$ ist durch p teilbar, $\frac{q!}{(p-q)!}$ jedoch nicht.[1] Damit folgt jetzt sicherlich

$$d < \max\left(\frac{q!}{(p-q)!}, \binom{p}{q}\right).$$

Dabei ist

$$\frac{q!}{(p-q)!} = q(q-1)\dots(p-q+1) < q^{2q-p} < p^{2q-p} < p^{p/3}$$

wegen $q < \frac{2p}{3}$ und andererseits

$$\binom{p}{q} < \sum_k \binom{p}{k} = 2^p < p^{p/3},$$

falls $p > 8$ ist. Die Fälle mit $p < 8$ kann man schließlich leicht per Hand überprüfen. □

[1] Hier benutzen wir, dass p eine Primzahl ist!

Eine Aufgabe aus der IMO

In der letzten Aufgabe haben wir gelernt, mit Fakultäten und Binomialkoeffizienten umzugehen. Aus der Abschätzung $\binom{p}{q} < 2^p$ sieht man schön, dass Binomialkoeffizienten in einem gewissen Sinne „viel kleiner“ sind als Fakultäten, was sie zusammen mit der Tatsache, dass sie ganze Zahlen sind[2], zu einem sehr mächtigen Hilfsmittel macht, welches wir im nächsten Abschnitt noch nutzen wollen. Zunächst wollen wir aber noch eine andere Aufgabe mit Fakultäten lösen, bei der wir noch eine neue Perspektive kennenlernen.

Aufgabe 3: Finde alle Paare (k, n) positiver ganzer Zahlen mit

$$k! = (2^n - 1)(2^n - 2)(2^n - 4)\dots(2^n - 2^{n-1}).$$

Wir haben soeben gelernt, wie wir die Größe der linken Seite nach oben und nach unten abschätzen können. Auch für die rechte Seite fällt uns sicherlich eine Möglichkeit ein, obere und untere Schranken zu gewinnen. Da es sich aber bei n und k um zwei unabhängige Variablen handelt, werden wir damit alleine keinen Widerspruch erhalten können.

Stattdessen benutzen wir wiederum Teilbarkeit, um eine Größenabschätzung zu erhalten, allerdings auf eine andere Weise als zuvor.

Suchen wir große Teiler einer der beiden Seiten, so springt ins Auge, dass die rechte Seite sehr oft durch 2 teilbar ist. Genauer gesagt ist der Faktor $2^n - 2^m$ für $m < n$ genau m-mal durch 2 teilbar, die rechte Seite (und damit auch die linke Seite) ist also durch

$$2^1 \cdot 2^2 \cdot 2^3 \cdots 2^{n-1} = 2^{\frac{n(n-1)}{2}}$$

teilbar. Nun folgt also

$$2^{\frac{n(n-1)}{2}} \mid k!.$$

Eine billige Anwendung unseres Tricks wäre hier keine gute Idee, denn wir können viel mehr darüber aussagen, wie oft $k!$ durch 2 teilbar ist. Unter den k Faktoren $1, 2, \dots, k$ im Produkt sind nämlich genau $\left\lfloor \frac{k}{2} \right\rfloor$ gerade Zahlen, genau $\left\lfloor \frac{k}{4} \right\rfloor$ Vielfache von 4, genau $\left\lfloor \frac{k}{8} \right\rfloor$ Vielfache von 8 etc. Damit folgt, dass $k!$ genau

$$\nu_2(k!) = \left\lfloor \frac{k}{2} \right\rfloor + \left\lfloor \frac{k}{4} \right\rfloor + \left\lfloor \frac{k}{8} \right\rfloor + \dots$$

Mal durch 2 teilbar ist. Hier ist die rechte Seite sicherlich kleiner als $\frac{k}{2} + \frac{k}{4} + \frac{k}{8} + \dots = k$, also ergibt sich $k > \frac{n(n-1)}{2}$. Jetzt kombinieren wir dies mit der Größenabschätzung der beiden Seiten und erhalten

$$2^{n^2} > k! > \left(\frac{n(n-1)}{2}\right)^{\frac{n(n-1)}{4}}.$$

Nach Vereinfachen wird dies zu

$$16^n > \left(\frac{n(n-1)}{2}\right)^{n-1}$$

und man sieht leicht, dass dies für halbwegs große n einen Widerspruch ergibt. Die übrigen kleinen Werte von n müssen dann noch durchprobiert werden.[3] □

[2] Die Tatsache, dass dies aus der kombinatorischen Interpretation folgt, sollte man nicht unterschätzen!

[3] Es ist ein typisches Phänomen dieser Lösungsmethode, dass sie nur für hinreichend große Werte der Variablen funktioniert und einige kleine Fälle gesondert betrachtet werden müssen. Es lohnt sich dann zumeist, eine möglichst gute Abschätzung zu erreichen, um die Anzahl dieser kleinen Fälle zu begrenzen.

Wie viele Primzahlen gibt es?

Blöde Frage, natürlich unendlich viele. Das wusste schon Euklid. Aber wenn wir mit $\pi(N)$ die Anzahl der Primzahlen bis N bezeichnen, können wir dann etwas über das Wachstum der Funktion $\pi(N)$ aussagen, wenn N größer wird? Gauß hat ohne Taschenrechner und Computer große Tabellen von Primzahlen ausgerechnet und ist darüber auf die Vermutung

$$\pi(N) \sim \frac{N}{\log N}$$

gekommen (hier ist $\log N$ der natürliche Logarithmus). Dieser sogenannte *Primzahlsatz* ist aber sehr schwierig und wurde erst 1896 – also mehr als hundert Jahre nach Gauß – bewiesen.

Für einige Olympiadeaufgaben ist es nützlich, zu wissen, wie groß $\pi(N)$ ungefähr ist. Dann darf dieser Primzahlsatz durchaus zitiert werden, wie bei der Stirlingschen Formel genügen aber oft auch einfachere Abschätzungen, mit denen wir uns hier beschäftigen wollen.

Da es nicht einmal vollkommen offensichtlich ist, dass es unendlich viele Primzahlen gibt, müssen wir hier allerdings natürlicherweise etwas härter arbeiten, um ein interessantes Ergebnis zu erhalten.

Der Trick ist es wiederum, Binomialkoeffizienten zu betrachten, und zwar einen speziellen, nämlich $\binom{2N}{N}$. Wir wissen, dass dieser eine ganze Zahl ist und können auch etwas über die Größe aussagen.

Übung 2: Zeige

$$\frac{4^N}{2N} \leq \binom{2N}{N} < 4^N.$$

(Tipp: Betrachte die $2N$-te Zeile im Pascalschen Dreieck.)

Andererseits können wir etwas über die Primteiler von $\binom{2N}{N}$ aussagen. Jede Primzahl $N < p \leq 2N$ kommt nämlich mindestens einmal darin vor. Also folgt

$$\prod_{N<p\leq 2N} p < 4^N.$$

Hier ist jeder Faktor auf der linken Seite mindestens N und es gibt genau $\pi(2N) - \pi(N)$ Faktoren, also folgt

$$N^{\pi(2N)-\pi(N)} < 4^N.$$

Damit folgt

$$\pi(2N) - \pi(N) < (\log 4) \cdot \frac{N}{\log N}.$$

Zwischen N und $2N$ gibt es also höchstens $\log 4 \cdot \frac{N}{\log N}$ Primzahlen. Mit ein wenig Rechenaufwand lässt sich daraus nun leicht mit Induktion die Abschätzung

$$\pi(N) < 2 \cdot \frac{N}{\log N}$$

für $N \geq 2$ zeigen. Bis auf den Faktor 2 ist dies also genau die richtige Größenordnung. [4]

[4] Im Prinzip kann man in diesem Argument die Konstante 2 durch jede Konstante $c > \log 4$ ersetzen, allerdings muss man umso mehr kleine Werte von N per Hand überprüfen, je kleiner man c wählt.

Wollen wir auch eine untere Schranke für $\pi(N)$ erhalten, müssen wir alle Primteiler von $\binom{2N}{N}$ berücksichtigen. Dazu kommen wir noch einmal auf die obige Bestimmung von $\nu_2(n!)$ zurück, also der exakten Zweierpotenz, die $n!$ teilt.

Übung 3: Erweitere das Argument von oben zur Formel von Legendre: Die Zahl $n!$ ist genau

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

Mal durch p teilbar.

Übung 4: Folgere aus der Formel von Legendre, dass $p^{\nu_p(\binom{2N}{N})} \leq 2N$ für alle Primzahlen p gilt.

Aus Übung 4 folgt nun wie oben

$$\frac{4^N}{2N} \leq \binom{2N}{N} = \prod_{p \leq 2N} p^{\nu_p(\binom{2N}{N})} \leq (2N)^{\pi(2N)}$$

und damit

$$\pi(2N) \geq \log 4 \cdot \frac{N}{\log 2N} - 1 = \log 2 \cdot \frac{2N}{\log 2N} - 1$$

und damit

$$\pi(N) \geq \log 2 \cdot \frac{N}{\log N} - 2.$$

Wir fassen also zusammen, dass für $N \geq 2$ stets

$$\log 2 \cdot \frac{N}{\log N} - 2 \leq \pi(N) < 2 \cdot \frac{N}{\log N}$$

gilt. Für praktische Anwendungen genügt es oft auch schon zu wissen, dass es *irgendwelche* Konstanten $c_1, c_2 > 0$ gibt mit

$$c_1 \cdot \frac{N}{\log N} < \pi(N) < c_2 \cdot \frac{N}{\log N}.$$

Diese Argumente kommen übrigens im Wesentlichen vom russischen Mathematiker Tschebyschow, der Mitte des 19. Jahrhunderts eine Verfeinerung dieser Ideen benutzte um zu zeigen, dass es zwischen N und $2N$ stets eine Primzahl gibt. Kannst du das auch?

* * *

Vielleicht sehen einige Argumente in diesem Skript sehr kompliziert aus und du hast das Gefühl, dass sie nur aus langen und nicht besonders eleganten Rechnungen bestehen?

Versuche, noch einmal von vorne zu lesen, aber diesmal alle Rechnungen zu ignorieren und nur die *entscheidenden Ideen* zu verstehen. In den meisten Lösungen sind das nur sehr wenige, manchmal vielleicht sogar nur eine.
Versuche zu verstehen, wie man auf diese Idee kommt und warum sie so hilfreich für diese Aufgabe ist. Das Ziel sollte sein, irgendwann sagen zu können:

- Ich habe eine bestimmte Idee, was man bei dieser Aufgabe tun kann.
- Ich habe ein Bauchgefühl, was mir sagt, dass der Rest der Lösung jetzt „nur noch“ eine Rechnung sein sollte.
- Ich fühle mich in der Lage, diese Rechnung auch alleine durchzuführen.