Die Teiler von $x^n - y^n$ und $x^n + y^n$

Christian Bernert, 28. Oktober 2021

Einleitung

In diesem Brief geht es um zwei wichtige Aussagen über die Teiler von Zahlen der Form $x^n - y^n$ und $x^n + y^n$, das sogenannte *Exponentenlemma* und den *Satz von Zsigmondy*.

1 Das Exponentenlemma

Wir beginnen mit einer einfachen Aufgabe aus dem Bundeswettbewerb Mathematik 2014:

Aufgabe: Zeige, dass für alle positiven ganzen Zahlen n die Zahl $2^{3^n} + 1$ durch 3^{n+1} teilbar ist.

Lösung: Aufgrund der Struktur der Aufgabe bietet es sich an, vollständige Induktion anzuwenden, wobei der Induktionsanfang für $n = 1$ trivial ist. Im Induktionsschritt ist nun die Beobachtung

$$2^{3^{n+1}} + 1 = (2^{3^n})^3 + 1 = (2^{3^n} + 1)((2^{3^n})^2 - 2^{3^n} + 1)$$

entscheidend. Nach Induktionsvoraussetzung ist der erste Faktor durch 3^{n+1} teilbar. Insbesondere ist $2^{3^n} \equiv -1 \mod 3$, somit ist der zweite Faktor ebenfalls durch 3 teilbar und die gesamte rechte Seite ist sogar durch 3^{n+2} teilbar. Das war zu zeigen. □

Eine natürliche Frage ist, ob das Ergebnis bestmöglich ist, ob also $2^{3^n} + 1$ nie durch 3^{n+2} teilbar ist. Dazu genügt es im Induktionsschritt zu untersuchen, ob der zweite Faktor durch 9 teilbar sein kann. Da allerdings nach Voraussetzung sogar $2^{3^n} \equiv -1 \mod 9$ gilt, ist der zweite Faktor $\equiv 3 \mod 9$ und somit nicht durch 9 teilbar. In jedem Schritt kommt also genau ein Faktor 3 hinzu. Wir notieren dieses Ergebnis als $3^{n+1} \| 2^{3^n} + 1$, wobei die Notation $p^k \| m$ bedeutet, dass m durch p^k nicht jedoch durch p^{k+1} teilbar ist.
Eine andere Schreibweise ist $k = v_p(m)$. Die Zahl $v_p(m)$ gibt also an, wie oft eine Zahl m durch p teilbar ist. Dies wird auch *p-adische Bewertung* genannt.
Wir haben also gezeigt: $v_3(2^{3^n} + 1) = n + 1$.

Wir setzen unsere Untersuchungen mit einer weiteren Aufgabe fort:

Aufgabe: Finde alle natürlichen Zahlen n mit

$$3^n \mid 5^n + 1.$$

Lösung: Ist n gerade, so ist $5^n + 1$ sicherlich überhaupt nicht durch 3 teilbar, also muss n ungerade sein. Ausprobieren kleiner Werte zeigt, dass dies für $n = 1$ in Ordnung ist, für $n = 3$ jedoch nicht. Tatsächlich liegt es nahe, dass für die allermeisten Werte von n die Zahl $5^n + 1$ nicht besonders oft durch 3 teilbar sein kann.
Doch wie oft ist sie durch 3 teilbar? Können wir $v_3(5^n + 1)$ bestimmen?
Wörtlich das gleiche Argument wie bei der letzten Aufgabe zeigt $v_3(5^{3^m} + 1) = m + 1$. Ist n also eine (halbwegs große) Dreierpotenz, so ist $5^n + 1$ deutlich seltener als n-mal durch 3 teilbar. Doch was, wenn n keine Dreierpotenz ist?

Als anderen Extremfall betrachten wir die Möglichkeit, dass n überhaupt nicht durch 3 teilbar ist. Dann ist

$$5^n + 1 = 6 \cdot (5^{n-1} - 5^{n-2} + 5^{n-3} - \cdots + 1),$$

wobei wir die Faktorisierung

$$x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + x^{n-3} - \cdots + 1)$$

für ungerade n benutzt haben. Betrachten wir den zweiten Faktor modulo 3, so ist dieser

$$(-1)^{n-1} - (-1)^{n-2} + (-1)^{n-3} - \cdots + 1 \equiv 1 + 1 + 1 + \cdots + 1 \equiv n \mod 3,$$

also nach Annahme nicht durch 3 teilbar.
Ist also n (ungerade und) selbst nicht durch 3 teilbar, so haben wir $v_3(5^n+1) = 1$ bewiesen. Wir können nun die Ergebnisse aus den beiden Extremfällen kombinieren: Schreiben wir $n = 3^k \cdot r$ mit $3 \nmid r$, so folgt wie in der ersten Aufgabe $v_3(5^n + 1) = v_3(5^r + 1) + k = k + 1$, also

$$v_3(5^n + 1) = v_3(n) + 1$$

für alle ungeraden Zahlen n. Damit lässt sich nun leicht unsere Aufgabe lösen: Wäre n eine Lösung, müsste ja $v_3(5^n + 1) \geq n$ gelten, also $v_3(n) + 1 \geq n$, d.h. $3^{n-1} \mid n$ und insbesondere $3^{n-1} \leq n$. Nun ist es aber leicht per Induktion zu zeigen, dass für $n \geq 2$ stets $n < 3^{n-1}$ gilt, es ist also $n = 1$ tatsächlich die einzige Lösung der Aufgabe. □

* * *

Wir wollen die eben entwickelten Ideen nun in einem etwas allgemeineren Rahmen ausführen und kommen damit zum bereits versprochenen

Exponenten-Lemma für $p > 2$: Sei $p > 2$ eine Primzahl.
Ist n eine natürliche Zahl und sind a, b ganze Zahlen mit $p \mid a - b$, aber $p \nmid a, b$, dann ist

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

Ist n ungerade und sind a, b ganze Zahlen mit $p \mid a + b$, aber $p \nmid a, b$, dann ist

$$v_p(a^n + b^n) = v_p(a + b) + v_p(n).$$

Beweis: Die zweite Aussage folgt sofort aus der ersten, indem wir b durch $-b$ ersetzen. Um die erste Aussage zu beweisen, genügt es die Fälle $n = p$ und $p \nmid n$ zu zeigen, denn dann können wir wieder $n = p^k \cdot r$ mit $p \nmid r$ schreiben und erhalten

$$v_p(a^n - b^n) = v_p(a^{p^{k-1}r} - b^{p^{k-1}r}) + 1 = \cdots = v_p(a^r - b^r) + k = v_p(a-b) + k = v_p(a-b) + v_p(n)$$

wie gewünscht.

Wir nehmen also zunächst $p \nmid n$ an und beginnen mit der Faktorisierung

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}).$$

Aus der Annahme $p \mid a - b$ folgt $a \equiv b \mod p$. Die zweite Klammer ist modulo p also kongruent zu $a^{n-1} + a^{n-1} + \cdots + a^{n-1} \equiv na^{n-1}$, also nach Annahme nicht durch p teilbar. Damit folgt sofort $v_p(a^n - b^n) = v_p(a - b)$ wie behauptet.

Wir nehmen nun $n = p$ an und müssen $v_p(a^p - b^p) = v_p(a-b)+1$ zeigen. Aus der gleichen Überlegung wie im ersten Fall folgt, dass dies äquivalent dazu ist, dass

$$N := a^{p-1} + a^{p-2}b + \cdots + b^{p-1}$$

genau einmal durch p teilbar ist. Wie oben folgt auch, dass N modulo p kongruent zu pa^{p-1} ist und damit durch p teilbar ist. Wir müssen also nur noch zeigen, dass N nicht durch p^2 teilbar ist.
In der vorigen Aufgabe wussten wir sogar $a \equiv b \mod p^2$, dann folgt sofort $N \equiv pa^{p-1} \mod p^2$ und wir wären fertig. Allerdings ist dies nicht als Voraussetzung gegeben und ist auch als Annahme nicht nötig. Stattdessen schreiben wir $b = a + pc$ und beachten, dass aus dem Binomischen Lehrsatz sofort

$$b^k \equiv (a+pc)^k \equiv a^k + ka^{k-1}pc \mod p^2$$

folgt, da alle weiteren Summanden im Binomischen Lehrsatz einen Faktor p^2 enthalten. Damit folgt nun

$$N \equiv \sum_{k=0}^{p-1} b^k a^{p-1-k} \equiv pa^{p-1} + pa^{p-2} \cdot \sum_{k=0}^{p-1} k \mod p^2.$$

Nun ist die Annahme $p > 2$ entscheidend, denn dann ist die hintere Summe $\frac{p(p-1)}{2}$ durch p teilbar und es folgt in der Tat $N \equiv pa^{p-1} \mod p^2$ und damit $p^2 \nmid N$. □

Auch für $p = 2$ gibt es ein Exponenten-Lemma, dieses sieht lediglich etwas anders aus:

Exponenten-Lemma für $p = 2$:
Sei n eine natürliche Zahl und a, b ungerade ganze Zahlen.
Ist n gerade, so ist

$$v_2(a^n - b^n) = v_2(a^2 - b^2) + v_2(n) - 1.$$

Ist n ungerade, so ist

$$v_2(a^n - b^n) = v_2(a - b)$$

und

$$v_2(a^n + b^n) = v_2(a + b).$$

Beweis: Fast alles kann von oben kopiert werden, denn wir haben ja nur im letzten Schritt die Annahme $p > 2$ benutzt. Im Fall $n = 2$ können wir tatsächlich nicht $v_2(a^2 - b^2)$ durch $v_2(a - b)$ ausdrücken, denn es kann durchaus sein, dass $v_2(a - b) = 1$ gilt, aber $v_2(a + b)$ und damit $v_2(a^2 - b^2)$ beliebig groß wird, etwa für $a = 2^k - 1, b = 1$.
Dies ist der Grund, warum auf der rechten Seite jetzt $v_2(a^2 - b^2) - 1$ und nicht $v_2(a - b)$ stehen muss. Mit dieser Umformulierung haben wir aber den Beweis schon gefunden, denn dann ist $a^2 - b^2$ sogar durch 4 teilbar und für $a \equiv b \mod p^2$ hatten wir im Fall $n = p$ oben bereits einen Beweis, der auch für $p = 2$ funktioniert. Natürlich können wir diesen auch leicht noch einmal explizit für $p = 2$ aufschreiben: Sind a und b ungerade und ist $a - b$ durch 4 teilbar, so ist $a + b$ gerade, aber nicht durch 4 teilbar und somit

$$a^2 - b^2 = (a - b)(a + b)$$

genau einmal mehr durch 2 teilbar als $a - b$. □

Typischerweise ist das Exponentenlemma nützlich um zu zeigen, dass eine Zahl der Form $x^n - y^n$ oder $x^n + y^n$ nicht allzu oft durch eine bestimmte Primzahl teilbar sein kann.

WARNUNG: Bei der Anwendung des Exponentenlemmas sollte die Bedingung $p \mid x-y$ nicht vergessen werden. Über Primteiler von $x^n - y^n$, die nicht bereits $x - y$ teilen, lässt sich mit dem Exponentenlemma nichts aussagen, egal wie oft n durch diese Primzahl teilbar ist.

Übung: Finde alle natürlichen Zahlen n mit $2^n \mid 3^n - 1$.

Zur Illustration, wie mächtig das Exponentenlemma ist, sei noch die folgende Aufgabe besprochen. Der interessierte Leser möge sich überlegen, wie die Aufgabe ohne die eben besprochene Technik zu lösen ist.

Aufgabe: Finde alle natürlichen Zahlen n, für die es eine natürliche Zahl $k > 1$ sowie teilerfremde natürliche Zahlen x und y gibt mit

$$3^n = x^k + y^k.$$

Lösung: Für gerade k steht rechts eine Summe von zwei Quadraten. Diese kann nur dann durch 3 teilbar sein, wenn x und y schon durch 3 teilbar sind – was ausgeschlossen wurde. Somit muss k ungerade sein. Dann ist

$$3^n = x^k + y^k = (x+y)(x^{k-1} - x^{k-2}y + \cdots + y^{k-1}),$$

also muss auch $x + y = 3^m$ eine Dreierpotenz sein. Insbesondere ist die Bedingung des Exponentenlemmas mit $p = 3$ erfüllt, denn x und y sind beide nicht durch 3 teilbar, aber $x + y$ ist durch 3 teilbar. Also folgt

$$n = v_3(x^k + y^k) = v_3(x+y) + v_3(k) = m + v_3(k).$$

Wir erwarten nun eigentlich, dass $x+y$ deutlich kleiner als x^k+y^k und damit m deutlich kleiner als n ist. Dann müsste aber $v_3(k)$ und damit auch k sehr groß sein, was hoffentlich zu einem Widerspruch führen sollte.
Diese Überlegung müssen wir nun noch präzise machen. Nach Annahme soll

$$\frac{x^k + y^k}{x+y} = 3^{v_3(k)}$$

gelten. Wird nun ohne Einschränkung der Allgemeinheit $x \geq y$ angenommen, so folgt aber

$$3^{v_3(k)} \geq \frac{x^k}{x+y} \geq \frac{x^k}{2x} = \frac{x^{k-1}}{2}.$$

Ist $x \geq 4$, so folgt bereits

$$3^{v_3(k)} \geq \frac{1}{2} \cdot 4^{k-1} > 3^{k-2},$$

also $v_3(k) \geq k-2$ und damit $3^{k-2} \mid k$. Nun ist es wie in einer ähnlichen Situation oben leicht zu sehen, dass dies nur für $k = 3$ passieren kann. Hier wird die Ungleichung aber zu $3 \geq \frac{16}{2}$, was auch falsch ist.
Somit folgt $x < 4$ und damit $x = 2$ und $y = 1$, also $3^n = 2^k + 1$ und $v_3(k) = n - 1$, also

$$3^n > 2^k \geq 2^{3^{n-1}}.$$

Hier überzeugt man sich wiederum leicht, dass diese Ungleichung für alle $n \geq 3$ falsch wird.
Es bleiben also nur die Fälle $n = 1$ und $n = 2$, wobei wir nur für $n = 2$ tatsächlich eine Lösung (nämlich $k = 3$, $x = 2, y = 1$) erhalten. □

2 Der Satz von Zsigmondy

Wir haben bereits davor gewarnt, dass das Exponentenlemma nichts über Primteiler von $x^n - y^n$ aussagt, die nicht schon $x - y$ teilen. Tatsächlich gibt es aber eine mächtige und sehr nützliche Aussage, die etwas über solche *primitiven* Primteiler von $x^n - y^n$ oder $x^n + y^n$ aussagt.
Dabei heißt ein Primteiler von $x^n - y^n$ (bzw. $x^n + y^n$) *primitiv*, wenn es kein Primteiler einer Zahl $x^k - y^k$ (bzw. $x^k + y^k$) für ein $1 \leq k < n$ ist. Es gilt der

Satz von Zsigmondy: Sind $a > b > 0$ ganze Zahlen und $n \geq 2$ eine natürliche Zahl, dann hat $a^n - b^n$ einen primitiven Primteiler bis auf in den folgenden Fällen:
1) $n = 2$ und $a + b$ ist eine Zweierpotenz.
2) $n = 6, a = 2, b = 1$.
Analog hat $a^n + b^n$ stets einen primitiven Primteiler bis auf im folgenden Fall:
3) $n = 3, a = 2, b = 1$.

Diese etwas merkwürdigen Sonderfälle machen den Satz leider weniger elegant als man ihn vielleicht gerne hätte. Leider ist die Wahrheit nun einmal so. Der Satz von Zsigmondy darf durchaus in Olympiaden zitiert werden (und kann dort eine mächtige Waffe sein, wie wir gleich noch sehen werden), allerdings ist es dann wichtig auch wirklich die genauen Bedingungen und insbesondere alle Sonderfälle zu kennen, da diese oftmals genau die einzigen Lösungen zur Aufgabe „ausspucken“.

Zur Illustration wenden wir den Satz von Zsigmondy auf die vorige Aufgabe an:
Ist $3^n = x^k + y^k$, so hat $x^k + y^k$ keinen primitiven Primteiler, also müssen wir im einzigen Sonderfall 3) sein und es muss $k = 3, x = 2, y = 1$ sein. Fertig! □

Da wir bei dieser Lösung so viel Platz gespart haben, bleibt sogar noch genug Raum, um die Aufgabe N4 von der kurzen Liste der IMO 2000 zu erledigen:

Aufgabe: Finde alle Tripel (a, m, n) natürlicher Zahlen mit $a^m + 1 \mid (a + 1)^n$.

Lösung: Insbesondere ist jeder Primteiler von $a^m + 1$ bereits ein Primteiler von $a + 1$. Nach Zsigmondy ist dies nur für $a = 1$ oder $m = 1$ oder $a = 2, m = 3$ möglich. Wir erhalten also die Lösungen $(1, m, n), (a, 1, n)$ und $(2, 3, k + 1)$. Fertig! □

Natürlich haben wir den Satz von Zsigmondy noch nicht bewiesen – und werden dies auch hier nicht tun. Wie man aus der Form der Sonderfälle bereits erahnen kann, gibt es keinen besonders eleganten Beweis. Allerdings ist der Beweis auch nicht furchtbar kompliziert. Er benutzt einige elementare Eigenschaften von Kreisteilungspolynomen und das Exponentenlemma. Die daraus resultierenden Ungleichungen müssen dann sorgfältig umgeformt werden. Wer die Details lesen möchte, dem sei der Artikel von Bart Michels unter https://www.math.univ-paris13.fr/~michels/files/zsigmondy_en.pdf empfohlen (auf Englisch).

Zum Abschluss sei nur noch kurz erwähnt, dass der Teil für $x^n + y^n$ leicht aus dem Teil für $x^n - y^n$ folgt: Nach der Version für $x^n - y^n$ hat nämlich $x^{2n} - y^{2n}$ einen primitiven Primteiler, außer im Fall $x = 2, y = 1, n = 3$. Dieser kann also nicht $x^n - y^n$ teilen, muss daher $x^n + y^n$ teilen. Er kann auch kein $x^k + y^k$ teilen, denn sonst würde er auch $x^{2k} - y^{2k}$ teilen. Fertig! □