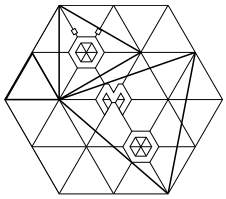

MATHEMATIK macht FREU(N)DE

52. Österreichische Mathematik-Olympiade

Kurs für Internationale „Mathematik macht Freu(n)de“ – Aufgabenblatt für den 7. November 2020

Ablauf

Dieses Aufgabenblatt wurde von Karl Grill zusammengestellt.

Wir freuen uns auf deine Fragen und Lösungsvorschläge per E-Mail.

Am 3. November 2020 wird das Blatt mit Tipps zur Lösung ausgewählter Aufgaben ergänzt. Karl Grill bespricht die Aufgaben mit euch im virtuellen Olympiade-Kurs am 7. November 2020 von 13:15–15:00 Uhr. Kurz darauf ergänzen wir das Blatt um ausgewählte Lösungsvorschläge und Angaben zu den Quellen der Aufgaben.

Schreibe uns, wenn du bei den virtuellen Kursen dabei sein möchtest. Du bist jederzeit willkommen!

Primzahlen und Quadrate

Einführung

Primzahlen

Eine klassische Beweistechnik ist der indirekte Beweis: es wird das Gegenteil dessen behauptet, das gezeigt werden soll, und zu einem Widerspruch geführt. Das Ur-Beispiel ist Euklids Beweis dafür, dass unendlich viele Primzahlen existieren: angenommen, es gäbe nur endlich viele Primzahlen, sagen wir $p_1, \dots, p_n$. Dann ist $a = p_1 p_2 \dots p_n + 1$ größer als 1, daher gibt es eine Primzahl, die a teilt, aber keine der endlichen vielen Primzahlen $p_1, \dots, p_n$ teilt a, und wir haben unseren Widerspruch.
Primzahlen sind bekanntlich Zahlen, die nur sich selbst und 1 als Teiler haben. Es sollte auch bekannt sein, dass in allgemeineren Betrachtungen (andere Ringe als $\mathbb{Z}$) solche Elemente “irreduzibel” heißen, und dass Primelemente durch die Beziehung $p|ab \Rightarrow p|a$ oder $p|b$ charakterisiert werden. In den natürlichen/ganzen Zahlen (und allgemeiner in Euklidischen Ringen) wird das als Lemma von Euklid bewiesen (mit der klassischen Definition einer Primzahl; in modernen Begriffen besagt dieses Lemma, dass in diesen Ringen jedes irreduzible Element prim ist).
Für manche Anwendungen (klassisches Beispiel sind pythagoräische Tripel, also ganzzahlige Lösungen der Gleichung $a^2 + b^2 = c^2$) sind Primzahlen von Interesse, die in einer gewissen Restklasse zu einem Modul m liegen. Die Vermutung liegt nahe, dass in jeder teilerfremden Restklasse unendlich viele Primzahlen liegen. Das hat Dirichlet in allgemeiner Form bewiesen, und auch, dass in einem sehr viel präziseren Sinn in jeder Restklasse “gleich viele” Primzahlen liegen. Für gewisse Restklassen können “euklidische” Beweise geführt werden. Einige einfache Beispiele kommen in den Aufgaben.
Auch schon Euklid war bekannt: Jede ganze Zahl x hat eine eindeutige Primzahlzerlegung der Form

$$x = e \prod_{i=1}^{l} p_i^{\nu_i}$$

mit $e = \pm 1$, Primzahlen $p_1 < p_2 < \dots < p_l$ und positiven ganzzahligen Exponenten ν_i.
Für eine beliebige Primzahl p soll $\nu_p(x)$ die größte nichtnegative Zahl sein, für die p^ν in x enthalten ist.
Auch in der Modulo-Arithmetik kann man quadratische Gleichungen betrachten. Der erste Schritt ist der, sich zu überlegen, wie die “Quadratzahlen” aussehen:

Definition 1. m sei eine natürliche Zahl. Die zu m teilerfremde Zahl (bzw. Restklasse) x heißt quadratischer Rest modulo m, wenn es ein y gibt mit

$$x \equiv y^2 \pmod{m}.$$

Quadratische Reste

Über quadratische Reste wird Irfan Glogic im Jänner vortragen, hier soll einstweilen nur so viel gesagt werden:

Satz 1. p sei eine ungerade Primzahl. Dann ist $x \not\equiv 0 \pmod{p}$ genau dann quadratischer Rest modulo p, wenn

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Wir brauchen hier nur die einfachere Hälfte: ist x quadratischer Rest, also $x \equiv y^2 \pmod{p}$, dann ist

$$x^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1 \pmod{p}$$

nach dem Satz von Fermat.
Insbesondere gilt: wenn -1 quadratischer Rest modulo p ist, dann ist $p \equiv 1 \pmod{4}$. Das kann natürlich auch im Licht der Ordnungen gesehen werden: aus $y^2 \equiv -1 \pmod{p}$ folgt, dass die Ordnung von y modulo p 4 ist, und diese ist ein Teiler von $p-1$.

Aufgaben

Aufgabe 1. Zeige, dass es unendlich viele Primzahlen $\equiv 3 \pmod{4}$ gibt.

Aufgabe 2. Zeige, dass es unendlich viele Primzahlen $\equiv 2 \pmod{3}$ gibt.

Aufgabe 3. Zeige, dass es unendlich viele Primzahlen $\equiv 1 \pmod{4}$ gibt.

Aufgabe 4. Der Satz von Wilson sagt, dass

$$(p-1)! \equiv -1 \pmod{p}$$

genau dann gilt, wenn p eine Primzahl ist. Wenn p eine ungerade Primzahl ist, was kann man dann über

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}$$

sagen?

Aufgabe 5. Zwischendurch zur Abwechslung ein Beispiel, bei dem es nicht um Primzahlen geht (außer der kleinsten), aber dafür können wir eine klassische Beweistechnik üben:
k und n seien positive ganze Zahlen. Dann gibt es k (nicht notwendig verschiedene) positive ganze Zahlen $m_1, \ldots, m_k$ mit

$$1 + \frac{2^k - 1}{n} = \left(1 + \frac{1}{m_1}\right) \ldots \left(1 + \frac{1}{m_k}\right).$$

Aufgabe 6. $k > 2$ und n seien ganze Zahlen und $a_1, \ldots, a_k$ verschiedene ganze Zahlen aus der Menge $\{1, \ldots, n\}$ mit der Eigenschaft, dass $a_i(a_{i+1} - 1)$ für alle $i = 1, \ldots, k-1$ durch n teilbar ist. Zeige, dass $a_k(a_1 - 1)$ nicht durch n teilbar ist.

Aufgabe 7. $n > 2$ sei eine ganze Zahl. Zeige: wenn $P(k) = k^2 + k + n$ für alle ganzzahligen k mit $0 \leq k \leq \sqrt{3n}$ eine Primzahl ist, dann auch für alle $k = 0, \ldots, n-2$.

Tipps zu ausgewählten Aufgaben

Aufgabe 1. Kann man den Beweis von Euklid so modifizieren, dass die neu gefundene Primzahl Rest 3 hat?

Aufgabe 3. Quadratische Reste.

Aufgabe 4. Teile $(p-1)!$ in zwei Produkte.

Aufgabe 5. Die linke Seite ist

$$\frac{n+2^k-1}{n},$$

auf der rechten Seite steht ein Faktor

$$\frac{m_1+1}{m_1}.$$

Man könnte versuchen, entweder die beiden Zähler oder die beiden Nenner gleichzusetzen.

Aufgabe 6. Indirekt: p sei ein Primteiler von n. Wenn $a_k(a_1-1)$ durch n teilbar ist, dann ist entweder a_k oder a_1-1 durch p teilbar. Wenn a_1-1 durch p teilbar ist, was gilt dann für a_2 etc.? Wie viele verschiedene Reste können die a_i modulo n haben?

Aufgabe 7. Indirekt: k_0 sei das kleinste k, für das $P(k)$ zusammengesetzt ist, p der kleinste Primteiler von $P(k_0)$. Zeige

$$k_0 \leq \frac{p-1}{2}$$

und

$$P(k_0) \geq p^2.$$

Lösungsvorschläge zu ausgewählten Aufgaben

Lösungsvorschläge von Karl Grill, bearbeitet vom MmF-Team

Aufgabe 1.

Wir setzen im Beweis von Euklid

$$a = 4p_1p_2 \dots p_n - 1 \equiv 3 \pmod 4,$$

und dass kann nicht nur Primfaktoren $\equiv 1 \pmod 4$ enthalten.

Aufgabe 3.

Wir lehnen uns wieder an Euklid an und setzen diesmal

$$a = \prod_{i=1}^{n} p_i^2 + 1.$$

Jeder Primteiler p von a hat jetzt die Eigenschaft, dass -1 quadratischer Rest modulo p ist, also ist $p \equiv 1 \pmod 4$.

Aufgabe 4.

$$-1 \equiv (p-1)! = \left(\frac{p-1}{2}\right)! \prod_{i=\frac{p+1}{2}}^{p-1} i = \left(\frac{p-1}{2}\right)! \prod_{i=1}^{\frac{p-1}{2}} (p-i) \equiv \left(\frac{p-1}{2}\right)! \prod_{i=1}^{\frac{p-1}{2}} (-i) = \left(\left(\frac{p-1}{2}\right)!\right)^2 (-1)^{\frac{p-1}{2}}.$$

Daher ist für $p \equiv 1 \pmod 4$

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p,$$

und -1 quadratischer Rest, für $p \equiv 3 \pmod 4$

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod p,$$

also

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod p,$$

und es scheint keine einfache Regel zu geben, wann da $+$ oder $-$ steht.

Aufgabe 5.

Für $k = 1$ ist alles klar, also soll ab sofort $k > 1$ sein, und wir führen einen Induktionsbeweis (nach k). Wenn n ungerade ist, $n = 2n' - 1$, dann funktioniert $m_1 = n = 2n' - 1$:

$$\frac{n + 2^k - 1}{n} = \frac{m_1 + 1}{m_1} \frac{2n' + 2^k - 2}{2n'} = \frac{m_1 + 1}{m_1} \frac{n' + 2^{k-1} - 1}{n'},$$

und auf den zweiten Faktor können wir die Induktionsvoraussetzung anwenden.
Wenn $n = 2n'$ gerade ist, setzen wir $m_1 = n + 2^k - 2 = 2n' + 2^k - 2$:

$$\frac{n + 2^k - 1}{n} = \frac{m_1 + 1}{m_1} \frac{2n' + 2^k - 2}{2n'} = \frac{m_1 + 1}{m_1} \frac{n' + 2^{k-1} - 1}{n'},$$

ganz wie vorhin.

Aufgabe 6.

Also p sei ein Primteiler von p. Wir nehmen an, dass $a_k(a_1 - 1)$ durch n teilbar ist, also auch durch p, und es muss also entweder $a_1 - 1$ oder a_k durch p teilbar sein. Im ersten Fall ist $a_1 \equiv 1 \pmod{p}$ nicht durch p teilbar, und weil $a_1(a_2 - 1)$ durch $p^{\nu_p(n)}$ teilbar ist, muss $a_2 - 1$ durch $p^{\nu_p(n)}$ teilbar sein. Dieses Argument kann jetzt schrittweise fortgesetzt werden, und ergibt, dass $a_i \equiv 1 \pmod{p^{\nu_p(n)}}$ für $i = 3, \ldots, k$ und schlieslich auch wieder für $i = 1$ gelten muss. Im zweiten Fall ergibt sich analog

$$a_{k-1} \equiv a_{k-2} \equiv \cdots \equiv a_1 \equiv a_k \equiv 0 \pmod{p^{\nu_p(n)}};$$

in jedem Fall haben alle a_i bezüglich jeder Primzahlpotenz, die n teilt, denselben Rest, und nach dem chinesischen Restsatz haben sie denselben Rest modulo n, also müssen sie alle übereinstimmen weil sie ja nur Werte zwischen 1 und n annehmen dürfen, in eklatantem Widerspruch zu den Voraussetzungen.

Aufgabe 7.

Wie im Hinweis: $P(k)$ soll für ein $k \leq n - 2$ zusammengesetzt sein. k_0 sei das kleinste k, für das $P(k)$ zusammengesetzt ist, p der kleinste Primteiler von $P(k_0)$. $P(k_0)$ enthält mindestens noch einen Primteiler $\geq p$, also gilt

$$p^2 \leq P(k_0) < P(n-1) = n^2,$$

also $p < n$.
Es muss $k_0 \leq p - 1$ gelten, sonst wäre $0 \leq k_0 - p < k_0$. und weil

$$P(k_0 - p) \equiv P(k_0) \equiv 0 \pmod{p}$$

und $P(k_0 - p) \geq n > p$, wäre auch $P(k_0 - p)$ zusammengesetzt, im Widerspruch zur Minimalität von k_0. Ebenso muss $k_0 \leq \frac{p-1}{2}$ gelten, sonst wäre $p - 1 - k_0 < k_0$. und weil

$$P(p - 1 - k_0) \equiv P(k_0) \equiv 0 \pmod{p},$$

wäre auch $P(p - 1 - k_0)$ zusammengesetzt. Damit haben wir

$$p^2 \leq P(k_0) \leq P(\frac{p-1}{2}) = \frac{p^2 - 1}{4} + n,$$

und daher

$$p \leq \sqrt{\frac{4n - 1}{3}} \leq 2\sqrt{\frac{n}{3}},$$

und

$$k_0 \leq \frac{p}{2} \leq \sqrt{\frac{n}{3}}.$$

Wenn also $P(k)$ für irgendein $k < n - 1$ zusammengesetzt ist, dann gibt es ein $k_0 \leq \sqrt{n/3}$, für das dasselbe gilt. Das war zu beweisen.

Diese Polynome sind für die Fälle $n = 17$ und $n = 41$ berühmte Beispiele für "Primzahlpolynome", das sind Polynome, die für viele ganzzahlige Werte des Arguments Primzahlen als Wert liefern. Die Fälle $n = 2$, $n = 3$, $n = 5$ und $n = 11$ fallen auch noch in diese Kategorie. Damit hat es sich leider auch schon: man kann zeigen, dass diese Zahlen alle Möglichkeiten sind, bei denen für alle $k < n-1$ Primzahlen herauskommen. Das schmälert natürlich die Nützlichkeit dieses ansonsten sehr netten Satzes.

Quellenangaben zu den Aufgaben

Aufgabe 1.

Alle diese Aussagen über Primzahlen zählen mehr oder weniger zur mathematischen Folklore; in der einen oder anderen Form finden sie sich in vielen Einführungstexten zur Zahlentheorie, allerdings oft nur in Nebensätzen oder Andeutungen. Explizit gefunden habe ich sie in Hlawka und Schoissengeier [3], und Remmert [4]. Dickson's "History of the Theory of numbers" [2] listet einige Resultate von diesem Zuschnitt auf.

Aufgabe 2.

Folklore.

Aufgabe 3.

Darf auch als Folklore gelten.

Aufgabe 4.

Auch dieser Satz ist Folklore und zum Beispiel auch im (englischen) Wikipedia-Artikel zum Satz von Wilson aufgeführt. Im Buch von Remmert [4] wird er auch erwähnt.

Aufgabe 5.

IMO 2013 auf dem IMO-Server[1], übersetzt und bearbeitet von Karl Grill und vom MmF-Team

Aufgabe 6.

IMO 2009 auf dem IMO-Server[1], übersetzt und bearbeitet von Karl Grill und vom MmF-Team

Aufgabe 7.

IMO 1987 auf dem IMO-Server[1], übersetzt und bearbeitet von Karl Grill und vom MmF-Team

Literatur

[1] Internationale Mathematik-Olympiade. `https://www.imo-official.org/problems.aspx`. Alle IMO - Angaben und die meisten IMO-Shortlists vergangener Jahre (aufgerufen am 10.11.2020).

[2] L.E. Dickson. *History of the Theory of Numbers: Divisibility and primality.* Carnegie Institution of Washington publication. Stechert, 1934.

[3] E. Hlawka and J. Schoissengeier. *Zahlentheorie: eine Einführung.* Vorlesungen über Mathematik. Manz, 1979.

[4] R. Remmert and P. Ullrich. *Elementare Zahlentheorie.* vieweg studium; Grundkurs Mathematik. Birkhäuser Basel, 2013.