Georg Keller
Kantonsschule Schaffhausen, georg.keller@kanti.sh.ch

Erstaunliche Teilbarkeitseigenschaft gewisser Produkt- resp. Potenzsummen

Teil 2

Einleitung

Im 1. Teil [1] dieser kleinen Bulletin-Beitragsreihe formulierten wir den

Satz: Für alle $n \in \mathbb{N}, n \geq 3$, gilt:

- n ist prim $\Leftrightarrow$ für alle $1 \leq k \leq (n-2)$ ist $\sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n-1} i_1 \cdot i_2 \cdots i_k$ teilbar durch n (1)
- n ist prim $\Leftrightarrow$ für alle $1 \leq k \leq (n-2)$ ist $\sum_{i=1}^{n-1} i^k$ teilbar durch n (2)

und bewiesen die Richtigkeit von (1). Das Ziel des vorliegenden zweiten und letzten Teils ist ein Beweis von (2). Bevor wir aber mit diesem Beweis beginnen können, müssen wir noch einige algebraische Vorbereitungen treffen. Dazu könnten wir auf die in [1] vorgenommene algebraische Vorbereitung für den Beweis von (1) verweisen und diese soweit als nötig ergänzen; zwecks möglichst einfacher Lesbarkeit des vorliegenden Bulletin-Beitrags verzichten wir aber auf diesen Verweis auf [1] und legen die später benötigten, lehrbuchmässigen algebraischen Grundlagen vollständig, wenn auch ohne Beweise, dar.

Algebraische Vorbereitung für den Beweis von (2)

Mit $\mathbb{Z}_n := \{0, 1, 2, \ldots, (n-1)\}$ bezeichnen wir die Menge der Restklassen modulo $n \in \mathbb{N}$ und mit $\mathbb{Z}_n^+ := \{1, 2, \ldots, (n-1)\}$ die Menge der positiven Restklassen modulo n. Den trivialen Fall $n = 1$ mit $\mathbb{Z}_1 = \{0\}$ und $\mathbb{Z}_1^+ = \emptyset$ ausklammernd, beschränken wir uns im Folgenden auf den Fall $n \geq 2$. Im wichtigen Spezialfall, wo n eine Primzahl ist, werden wir (wenn sinnvoll möglich) jeweils p statt n schreiben, z.B. also $\mathbb{Z}_p$ statt $\mathbb{Z}_n$. Und der Kürze halber werden wir statt $a \equiv b \pmod{n}$ nur $a =_n b$ schreiben.

Mit der üblichen Addition und Multiplikation (und wie erwähnt für $n \geq 2$) wird $\mathbb{Z}_n$ ein kommutativer Ring mit Eins, $\mathbb{Z}_p$ ein endlicher Körper und $\mathbb{Z}_p^+$ eine multiplikative kommutative Gruppe. Eine berühmte, in $\mathbb{Z}_p^+$ geltende Tatsache ist der Kleine Satz von Fermat: $a^{p-1} =_p 1$, für alle $a \in \mathbb{Z}_p^+$. Ausserdem ist $\mathbb{Z}_p^+$ eine zyklische Gruppe, d.h. es gibt ein Element $w \in \mathbb{Z}_p^+$, sodass $\mathbb{Z}_p^+ = \{w, w^2 \bmod p, w^3 \bmod p, \ldots, w^{p-1} \bmod p\}$ ist (wobei, wie erwähnt, $w^{p-1} \bmod p = 1$ ist); w heisst erzeugendes Element von $\mathbb{Z}_p^+$.

Für $n \in \mathbb{N}$ ist die Eulersche Phi-Funktion als $\varphi(n) := |\{a \mid a \in \{1,2,\ldots,n\}, ggT(a,n) = 1\}|$ definiert. Wenn wir die Primfaktorzerlegung von n in der Form $n = \prod_{q|n} q^{k_q}$, q = prim, schreiben (wobei für $n = 1$ das Produkt über die leere Indexmenge gebildet und daher wie üblich als die Zahl 1 definiert ist), kann $\varphi(n)$ so berechnet werden:

$$\varphi(n) = \prod_{q|n} q^{k_q - 1}(q-1) \tag{3}$$

Und der den Kleinen Satz von Fermat von $\mathbb{Z}_p^+$ auf $\mathbb{Z}_n^+$ verallgemeinernde Satz von Euler besagt:

$$a^{\varphi(n)} =_n 1 \quad , \quad \forall a \in \mathbb{Z}_n^+ \text{ mit } ggT(a,n) = 1 \tag{4}$$

Beweis von (2)

„⇒“ Es sei also n eine beliebige Primzahl $p \geq 3$. Und w sei ein erzeugendes Element von $\mathbb{Z}_p^+$. Dann ist $\{i \mid 1 \leq i \leq (p-1)\} = \{w^j \bmod p \mid 1 \leq j \leq (p-1)\}$, und daher kann die zu untersuchende Potenzsumme $\sum_{i=1}^{p-1} i^k$ modulo p wie folgt umgeschrieben werden:

$$\sum_{i=1}^{p-1} i^k = \sum_{j=1}^{p-1} (w^j \bmod p)^k =_p \sum_{j=1}^{p-1} (w^k \bmod p)^j \tag{5}$$

Mit der Abkürzung $y := w^k \bmod p$ erfüllt die in (5) auftretende Summe $S := \sum_{j=1}^{p-1} y^j$ die Gleichung

$$S \cdot (y-1) = y^p - y \quad . \tag{6}$$

Weil w ein erzeugendes Element und $1 \leq k \leq (p-2)$ ist, ist $2 \leq y \leq (p-1)$; daher liegt der in (6) auftretende Faktor $(y-1)$ in $\mathbb{Z}_p^+$, hat also in $\mathbb{Z}_p$ ein Inverses $(y-1)^{-1}$, und aufgrund des Kleinen Satzes von Fermat ist $y^p - y =_p 0$. Damit erhalten wir

$$\sum_{i=1}^{p-1} i^k =_p S =_p (y^p - y) \cdot (y-1)^{-1} =_p 0 \quad . \quad \blacksquare$$

Anmerkungen:

- Für den Spezialfall k = ungerade gibt es noch einen viel direkteren Beweis von (2): Es ist ja $(p-1) =_p -1$, $(p-2) =_p -2$, etc.; daher folgt, dass

$$\begin{aligned} \sum_{i=1}^{p-1} i^k &= 1^k + 2^k + \cdots + (p-2)^k + (p-1)^k \\ &=_p 1^k + 2^k + \cdots + (-2)^k + (-1)^k \end{aligned}$$

  ist. Weil p ungerade ist, hat diese Summe eine gerade Anzahl Summanden, welche sich – weil auch k ungerade ist – paarweise aufheben.

- (2) „⇒“ kann auch als Folgerung aus (1) „⇒“ verstanden werden. Und das geht so: Zuerst beweist man für $m \in \mathbb{N}$ und $1 \leq k \leq m$ die folgende Zerlegung gewisser symmetrischer Polynome in den Variablen z_i, $1 \leq i \leq m$:

$$\begin{aligned} \sum_{1 \leq i \leq m} z_i^k = &\left(\sum_{1 \leq i \leq m} z_i^{k-1}\right) \cdot \left(\sum_{1 \leq i \leq m} z_i\right) \\ &- \left(\sum_{1 \leq i \leq m} z_i^{k-2}\right) \cdot \left(\sum_{1 \leq i_1 < i_2 \leq m} z_{i_1} \cdot z_{i_2}\right) \\ &+ \left(\sum_{1 \leq i \leq m} z_i^{k-3}\right) \cdot \left(\sum_{1 \leq i_1 < i_2 < i_3 \leq m} z_{i_1} \cdot z_{i_2} \cdot z_{i_3}\right) \\ &- \cdots + \cdots \\ &+ (-1)^k \cdot \left(\sum_{1 \leq i \leq m} z_i^1\right) \cdot \left(\sum_{1 \leq i_1 < i_2 < \cdots < i_{k-1} \leq m} z_{i_1} \cdot z_{i_2} \cdots z_{i_{k-1}}\right) \\ &+ (-1)^{k+1} \cdot k \cdot \left(\sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq m} z_{i_1} \cdot z_{i_2} \cdots z_{i_k}\right) \end{aligned} \tag{7}$$

  Und jetzt setzen wir in (7) $m := p-1$, $z_i := i$, schränken k auf $1 \leq k \leq (p-2)$ ein, rechnen beide Seiten von (7) modulo p und verwenden auf der rechten Seite von (7) die Aussage (1) „⇒“, woraus wir (2) „⇒“ erhalten.

„⇐“ • n ist also eine beliebige natürliche Zahl mit $n \geq 3$. Unsere Beweisstrategie ist: Wir wollen zeigen, dass für *zusammengesetztes* n mindestens die Potenzsumme $\sum_{i=1}^{n-1} i^k$ mit $k := \varphi(n)$ *nicht* durch n teilbar ist. Weil der dabei auftretende Exponent k die Bedingung $1 \leq k \leq (n-2)$ erfüllt – da definitionsgemäss $\varphi(n) \geq 1$ und, für zusammengesetztes $n \geq 3$, ebenfalls $\leq (n-2)$ ist – werden wir damit (2) „⇐“ bewiesen haben.

- Es sei also n eine beliebige *zusammengesetzte* Zahl mit $n \geq 3$. Mit p einen der Primfaktoren von n bezeichnend und mit p^j seine höchste in n auftretende Potenz, schreiben wir die Primfaktorzerlegung von n in der Form

$$n = p^j \cdot Q \quad \text{mit} \quad Q := \begin{cases} \text{restl. Primpotenzen} \ , & \text{für } j = 1 \\ \text{restl. Primpotenzen oder } 1 \ , & \text{für } j \geq 2 \end{cases} . \tag{8}$$

  Gemäss (3) und (8) kann $\varphi(n)$ wie folgt dargestellt werden:

$$\varphi(n) = p^{j-1}(p-1) \cdot \begin{cases} \prod_{q|Q} q^{k_q - 1}(q-1) \ , & \text{für } Q \neq 1 \\ 1 \ , & \text{für } Q = 1 \end{cases} = \varphi\left(p^j\right) \cdot \varphi(Q) \tag{9}$$

- Wie erwähnt, wollen wir nachweisen, dass $\sum_{i=1}^{n-1} i^{\varphi(n)} \neq_n 0$ ist; wir werden dies erreichen, indem wir zeigen, dass $\sum_{i=1}^{n-1} i^{\varphi(n)} \neq_{p^j} 0$ ist. Dazu schreiben wir zuerst die Summe $\sum_{i=1}^{n-1} i^{\varphi(n)}$ für später etwas bequemer als $\sum_{a \in \mathbb{Z}_n^+} a^{\varphi(n)}$ und zerlegen diese in zwei geeignet gewählte Teilsummen:

$$\sum_{i=1}^{n-1} i^{\varphi(n)} = \sum_{a \in \mathbb{Z}_n^+} a^{\varphi(n)} =_{p^j} \left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)=1}} a^{\varphi(n)} \right) \bmod p^j \tag{10}$$

$$+ \left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1}} a^{\varphi(n)} \right) \bmod p^j \tag{11}$$

  - Auswertung der Teilsumme (10): Dank (4) können wir für jedes $a \in \mathbb{Z}_n^+$ mit $ggT(a,n) = 1$ den Term $a^{\varphi(n)}$ als $a^{\varphi(n)} = 1 + n \cdot \mathbb{Z}$ schreiben; und weil ja $n \bmod p^j = 0$ ist, erhalten wir

$$\left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)=1}} a^{\varphi(n)} \right) =_{p^j} \left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)=1}} (1 + n \cdot \mathbb{Z}) \right) =_{p^j} \left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)=1}} 1 \right) =_{p^j} \varphi(n) \quad . \tag{12}$$

  - Auswertung der Teilsumme (11): Wir teilen die Summanden von (11) in zwei Gruppen auf bezüglich des Primfaktors p von n :

$$\left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1}} a^{\varphi(n)} \right) =_{p^j} \left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p \mid a}} a^{\varphi(n)} \right) \bmod p^j \tag{13}$$

$$+ \left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p \nmid a}} a^{\varphi(n)} \right) \bmod p^j \tag{14}$$

    - Auswertung der Teil-Teilsumme (13): Weil die 3. Summationsbedingung $p|a$ die 2. Summationsbedingung impliziert, muss Letztere gar nicht mehr beachtet werden. Und weil jedes $a \in \mathbb{Z}_n^+$ mit $p|a$ die Form $a = p \cdot b$, $b \in \mathbb{N}$, hat, schreiben wir zuerst (13) als

$$\left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p \mid a}} a^{\varphi(n)} \right) =_{p^j} \left(p^{\varphi(n)} \bmod p^j \right) \cdot \left(\sum_{\text{gewisse } b \in \mathbb{N}} b^{\varphi(n)} \right)$$

$$\overset{(9)}{=}_{p^j} \left(p^{\varphi(p^j)} \bmod p^j \right)^{\varphi(Q)} \cdot \left(\sum_{\text{gewisse } b \in \mathbb{N}} b^{\varphi(n)} \right) \tag{15}$$

Jetzt werten wir den ersten Faktor von (15) aus. Dazu beobachten wir Folgendes [2]: Für alle $p \geq 2$ und $j \geq 1$ sind die Zahlen $p^1 - 1, p^2 - 1, p^3 - 1, \ldots, p^j - 1$ insgesamt j unterschiedliche Elemente der Zahlenmenge $\{1, 2, \ldots, p^j\}$, und sie alle sind teilerfremd zu p^j, d.h. $ggT(p^i - 1, p^j) = 1$, für $1 \leq i \leq j$. Daher ist $\varphi(p^j) \geq j$, und entsprechend gilt

$$p^{\varphi(p^j)} \bmod p^j = 0 \quad . \tag{16}$$

Gemäss (15), (16) erhalten wir also

$$\left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p \mid a}} a^{\varphi(n)} \right) =_{p^j} 0 \quad . \tag{17}$$

- Auswertung der Teil-Teilsumme (14): Erstens schreiben wir

$$\left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p \nmid a}} a^{\varphi(n)} \right) \overset{(9)}{\equiv}_{p^j} \left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p \nmid a}} \left((a \bmod p^j)^{\varphi(p^j)} \bmod p^j \right)^{\varphi(Q)} \right) \tag{18}$$

und bemerken zweitens, dass wegen der Summationsbedingung $p \nmid a$ nicht nur $(a \bmod p^j) \in \mathbb{Z}_{p^j}^+$ gilt, sondern auch $p \nmid (a \bmod p^j)$ und deswegen $ggT((a \bmod p^j), p^j) = 1$. Via Satz von Euler können wir (18) daher wie folgt fortsetzen:

$$=_{p^j} \left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p \nmid a}} 1^{\varphi(Q)} \right) =_{p^j} \left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p \nmid a}} 1 \right) \tag{19}$$

Jetzt berechnen wir die in (19) auftretende Summe:

$$\left(\sum_{\substack{a \in \mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p \nmid a}} 1 \right) = |\{a \in \mathbb{Z}_n^+ \mid ggT(a,n) > 1 \ , \ p \nmid a\}|$$

$$= |\{a \in \mathbb{Z}_n^+ \mid ggT(a,n) > 1\}| - |\{a \in \mathbb{Z}_n^+ \mid ggT(a,n) > 1 \ , \ p|a\}|$$

und wiederum die dank $p|a$ automatisch erfüllte Bedingung $ggT(a,n) > 1$ weglassend:

$$= [\, |\{a \in \mathbb{Z}_n^+\}| - |\{a \in \mathbb{Z}_n^+ \mid ggT(a,n) = 1\}| \,] - |\{a \in \mathbb{Z}_n^+ \mid p|a\}|$$

$$\overset{(8)}{=} [\, (n-1) - \varphi(n) \,] - \left|\{p \cdot 1, \ p \cdot 2, \ p \cdot 3, \ldots, p \cdot (p^{j-1} \cdot Q - 1)\}\right|$$

(beachte, dass für alle zulässigen p, j, Q die Zahl $(p^{j-1} \cdot Q - 1) \geq 1$ ist)

$$= (n-1) - \varphi(n) - (p^{j-1} \cdot Q - 1) = n - \varphi(n) - p^{j-1} \cdot Q \tag{20}$$

womit wir sehen:

$$\left(\sum_{\substack{a\in\mathbb{Z}_n^+ \\ ggT(a,n)>1 \\ p\nmid a}} a^{\varphi(n)} \right) \overset{(19,20)}{\equiv}_{p^j} n-\varphi(n)-p^{j-1}\cdot Q \qquad (21)$$

(10)-(14) und (17), (21) zusammenfassend, erhalten wir schliesslich das in Aussicht gestellte Resultat:

$$\sum_{i=1}^{n-1} i^{\varphi(n)} =_{p^j} \left[\varphi(n)+n-\varphi(n)-p^{j-1}\cdot Q\right] =_{p^j} \left[-p^{j-1}\cdot Q\right] \neq_{p^j} 0 \quad \blacksquare$$

Anmerkung: Für die Richtigkeit der Behauptung „$\sum_{i=1}^{n-1} i^k$ ist teilbar durch $n \geq 3$, für alle $1 \leq k \leq (n-2) \Rightarrow n \notin 2\mathbb{N}$“, was ja eine Teilaussage von (2) ist, gibt's einen sehr viel kürzeren Beweis: Wegen $(n-1) =_n -1$, $(n-2) =_n -2$, etc., erhalten wir für $n \in 2\mathbb{N}$, $n \geq 3$, und für $k = 1$: $\sum_{i=1}^{n-1} i^1 =_n 1+2+\cdots+\left(\frac{n}{2}-1\right)+\left(\frac{n}{2}\right)+\left(-\left(\frac{n}{2}-1\right)\right)+\cdots+(-2)+(-1) =_n \frac{n}{2} \neq_n 0$.

Ergänzung

Es gibt jahrhundertealte Formeln, um die Potenzsumme $\sum_{i=1}^{n-1} i^k$ als explizite Funktion von n auszudrücken, so z.B. die Faulhabersche Formel [3] $\sum_{i=1}^{n-1} i^k = \frac{1}{k+1}\sum_{j=0}^{k}\binom{k+1}{j} B_j\, n^{k+1-j}$, wobei $k, n \in \mathbb{N}$ und die B_j die Bernoulli-Zahlen erster Art ($B_3 = B_5 = B_7 = B_9 = \ldots = 0$; $B_0 = 1$, $B_1 = \frac{-1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = \frac{-1}{30}$, $B_6 = \frac{1}{42}$, ...) sind. Damit kann der Quotienten $\frac{\sum_{i=1}^{n-1} i^k}{n}$ als $\frac{1}{k+1}\sum_{j=0}^{k}\binom{k+1}{j} B_j\, n^{k-j}$ geschrieben werden. Diese Schreibweise legt zwar weder die Vermutung noch eine Beweisidee dafür nahe, dass, wie oben gezeigt, $\frac{\sum_{i=1}^{n-1} i^k}{n}$ für primes $n \geq 3$ und alle $1 \leq k \leq (n-2)$ eine natürliche Zahl ist, für nicht-primes n und gewisse k hingegen nicht. Aber sie zeigt, dass die Bernoulli-Zahlen erster Art, genauer gesagt die spezielle Summe $\frac{1}{k+1}\sum_{j=0}^{k}\binom{k+1}{j} B_j\, n^{k-j}$, diese wohl kaum erwartete, bemerkenswerte Eigenschaft besitzen.

Referenzen

[1] G. Keller: Erstaunliche Teilbarkeitseigenschaft gewisser Produkt- resp. Potenzsummen - Teil 1. VSMP-Bulletin 155 (2024), S. 48

[2] Die hier präsentierte Begründung, dass $\varphi(p^j) \geq j$ ist, verdanke ich Dr. Jonas Gloor, Gymnasium Oberwil. Sie ist weniger abstrakt, kürzer und einfacher als meine ursprüngliche Begründung.

[3] https://de.wikipedia.org/wiki/Faulhabersche_Formel (31.01.23)