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

Erstaunliche Teilbarkeitseigenschaft gewisser Produkt- resp. Potenzsummen

(Teil 1)

Einleitung

Vor etwa einem Jahr liess ich mich beim Lesen der ersten Seiten des Buches „Combinatorial Geometry“ [1] dazu anregen, mir einige wesentliche algebraische Eigenschaften von $\mathbb{Z}_n$ nicht nur wieder einmal vor Augen zu führen, sondern - im Sinne einer sportlichen Herausforderung - auch deren Richtigkeit zu beweisen, und zwar möglichst ohne Beizug von Hilfsmitteln. Damit nahm ich natürlich in Kauf, ggf. auf ineffiziente, nicht standardmässig begangene Wege durch $\mathbb{Z}_n$ zu gelangen. Genau auf diese Weise aber stiess ich auf die folgende, unerwartete Teilbarkeitseigenschaft gewisser Produkt- und Potenzsummen:

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)

Dieser Satz war in meinem mathematischen Umfeld unbekannt, und auch eine (zugegebenermassen nicht allzu intensive) Literaturrecherche förderte keine entsprechende Publikation zutage. Weil es vielleicht Bulletin-Leser gibt, die an (1) interessiert sind, wird in diesem Bulletin-Beitrag - nach einer algebraischen Vorbereitung - ein kurzer Beweis von (1) dargelegt. An (2) Interessierte müssen sich noch etwas gedulden, denn der Beweis von (2) - bei welchem die Beweisrichtung „$\Leftarrow$“ etwas aufwendiger ist - wird aus Platzgründen erst in einem späteren, separaten Bulletin-Beitrag erscheinen.

Algebraische Vorbereitung für den Beweis von (1)

Im Hinblick auf den Beweis von (1) listen wir in diesem Abschnitt einige lehrbuchmässige, elementare algebraische Aspekte von $\mathbb{Z}_n$ auf, jeweils ohne Beweis.

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 $a \in \mathbb{Z}_p^+$.

Mit $\mathbb{Z}_n[X]$ bezeichnen wir den Polynomring über $\mathbb{Z}_n$, d.h. den Ring der Polynome $P(X) = \sum_{j=0}^{r} c_j X^j$ mit $c_j \in \mathbb{Z}_n$ und $c_r \neq 0$ (ausser beim Null-Polynom mit $r = c_r = 0$), wobei die Polynomaddition, -multiplikation und -auswertung als Rechenoperationen in $\mathbb{Z}_n$, d.h. mod n, definiert sind, ohne dies aber schreiberisch

speziell kenntlich zu machen. c_r ist der sogenannte Leitkoeffizient von P, und $\deg(P) := r$. In $\mathbb{Z}_p[X]$ gilt u.a.:

- Falls ein Polynom $P \in \mathbb{Z}_p[X]$ mit $r \equiv \deg(P) \geq 1$ und Leitkoeffizient c_r genau r unterschiedliche Nullstellen $x_1, x_2, ..., x_r \in \mathbb{Z}_p$ hat, so ist $P(X) = c_r \cdot (X - x_1) \cdot (X - x_2) \cdots (X - x_r)$. (3)

- Es seien $P_1, P_2 \in \mathbb{Z}_p[X]$ mit $\deg(P_{1,2}) \leq p - 1$. Falls $P_1(x) = P_2(x)$, für alle $x \in \mathbb{Z}_p$, stimmen die Koeffizienten von P_1 mit denjenigen von P_2 überein. (4)

  (Anmerkung: Die Bedingung $\deg(P_{1,2}) \leq p - 1$ ist wesentlich, denn andernfalls gibt's aufgrund des Kleinen Satzes von Fermat Gegenbeispiele zu (4), so z.B. $P_1(X) = X^p$ und $P_2(X) = X$.)

Beweis von (1)

„⇒" Es sei also n eine beliebige Primzahl $p \geq 3$. Wir betrachten das Polynom $X^{p-1} + ((-1) \bmod p) \in \mathbb{Z}_p[X]$, wobei wir der Einfachheit halber ab jetzt das explizite „mod p" weglassen und nur noch $X^{p-1} - 1$ schreiben (und damit keinen Fehler begehen, denn in $\mathbb{Z}_p[X]$ sind ja alle Rechenoperationen sowieso nur modulo p gemeint). $X^{p-1} - 1$ hat den Grad $(p - 1) \geq 2$, den Leitkoeffizienten 1 und, aufgrund des Kleinen Satzes von Fermat, in $\mathbb{Z}_p$ die $p - 1$ unterschiedlichen Nullstellen 1, 2, 3, ..., $(p - 1)$. Gemäss (3) kann unser Polynom wie folgt in Linearfaktoren zerlegt werden:

$$X^{p-1} - 1 = (X - 1) \cdot (X - 2) \cdots \big(X - (p - 1)\big) \tag{5}$$

Auf der rechten Seite von (5) lösen wir die Klammern auf und erhalten

$$\begin{aligned} &X^{p-1} - 1 \\ &= X^{p-1} + \sum_{k=1}^{p-2} X^{p-1-k} \cdot \Big[(-1)^k \cdot \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq p-1} i_1 \cdot i_2 \cdots i_k\Big] + (-1)^{p-1} \cdot (p - 1)! \end{aligned} \tag{6}$$

Die linke Seite von (6) $P_1(X)$ nennend und die rechte Seite $P_2(X)$, mit $\deg\big(P_{1,2}\big) = p - 1$, besagt (6), dass $P_1(x) = P_2(x)$ ist, $\forall x \in \mathbb{Z}_p$; gemäss (4) stimmen daher die (wie erwähnt mod p zu verstehenden) Koeffizienten von P_1 mit denjenigen von P_2 überein, insbesondere gilt also (1). ■

Anmerkungen:

- Den obigen Koeffizientenvergleich auch noch für die Koeffizienten von X^0 durchführend, erhalten wir die ergänzende Aussage $(-1)^{p-1} \cdot (p - 1)! =_p - 1$, d.h., weil $p - 1$ eine gerade Zahl ist, die Aussage $(p - 1)! =_p - 1$, was (bis auf die Einschränkung $p \geq 3$) die eine Hälfte des Satzes von Wilson [2] ist.

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

  $$\sum_{1 \leq i_1 \leq p-1} i_1 =_p 1 + 2 + \cdots + \left(\tfrac{p-1}{2}\right) + \left(-\tfrac{p-1}{2}\right) + \cdots + (-2) + (-1) = 0$$

  ist. Und für $k \geq 3$ schreiben wir zuerst die Summe $\sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq p-1} i_1 \cdot i_2 \cdots i_k$ kompakter als $\sum_{\vec{i} \in M} \prod_{j=1}^{k} i_j$, mit $M := \{(i_1, i_2, \ldots, i_k) \mid 1 \leq i_1 < i_2 < \cdots < i_k \leq p - 1\}$. Die Menge M ist die disjunkte Vereinigung der Mengen $M_1 := \{\vec{i} \in M \,\big|\, i_{\frac{k+1}{2}} \leq \frac{p-1}{2}\}$ und $M_2 := \{\vec{i} \in M \,\big|\, i_{\frac{k+1}{2}} > \frac{p-1}{2}\}$. Die Abbildung $S: M_1 \to M_2$ und umgekehrt mit $S(\vec{i}) := ((p - i_k), (p - i_{k-1}), \ldots, (p - i_2), (p - i_1))$ ist, wegen $S^2(\vec{i}) = \vec{i}$, eine bijektive Abbildung $M_1 \leftrightarrow M_2$, und daher gilt:

  $$\sum_{\vec{i} \in M} \prod_{j=1}^{k} i_j = \sum_{\vec{i} \in M_1} \prod_{j=1}^{k} i_j + \sum_{\vec{i} \in M_2} \prod_{j=1}^{k} i_j = \sum_{\vec{i} \in M_1} \Big[\prod_{j=1}^{k} i_j + \prod_{j=1}^{k} \big(S(\vec{i})\big)_j\Big] \tag{7}$$

Anhand von $\prod_{j=1}^{k}\left(S(\vec{i})\right)_j = \prod_{j=1}^{k}(p - i_j) =_p (-1)^k \cdot \prod_{j=1}^{k} i_j$ erhalten wir via (7)

$$\sum_{1\le i_1<i_2<\cdots<i_k\le p-1} i_1 \cdot i_2 \cdots i_k =_p \sum_{\vec{i}\in M_1}\left[\prod_{j=1}^{k} i_j + (-1)^k \cdot \prod_{j=1}^{k} i_j\right] \quad ,$$

wobei $\prod_{j=1}^{k} i_j + (-1)^k \cdot \prod_{j=1}^{k} i_j = 0$ ist, weil k ungerade ist.

„⇐“ • n ist also eine beliebige natürliche Zahl mit $n \ge 3$, welche die in (1) genannte Voraussetzung für die Beweisrichtung „⇐“ erfüllt. Wir betrachten das folgende Polynom $Q \in \mathbb{Z}_n[X]$:

$$Q(X) := \sum_{k=1}^{n-2} X^{n-1-k} \cdot \left[\left((-1)^k \cdot \sum_{1\le i_1<i_2<\cdots<i_k\le n-1} i_1 \cdot i_2 \cdots i_k\right) \bmod n\right] \qquad (8)$$

Wiederum das explizite „mod n“ nebenwirkungsfrei weglassend und inspiriert durch (5), (6) schreiben wir (8) wie folgt um:

$$Q(X) = (X-1)\cdot(X-2)\cdots\left(X-(n-1)\right) - X^{n-1} - (-1)^{n-1}\cdot(n-1)! \qquad (9)$$

Gemäss der in (1) genannten Voraussetzung und (8) ist $Q(x) = 0$, $\forall x \in \mathbb{Z}_n$. Insbesondere ist also $Q(1) = 0$, was via (9) mit $x = 1$ zu $0 =_n 0 - 1^{n-1} - (-1)^{n-1}\cdot(n-1)!$ führt, d.h. zur Aussage, dass diejenigen n , welche die in (1) genannte Voraussetzung erfüllen, die folgende Eigenschaft besitzen:

$$(n-1)! =_n (-1)^n \qquad (10)$$

• Jetzt zeigen wir noch, dass alle *zusammengesetzten* Zahlen $n \in \mathbb{N}$, $n \ge 3$, die spezielle Eigenschaft (10) *nicht* besitzen, d.h. n muss prim sein, womit unser Beweis beendet sein wird: Wie in [2] gezeigt, kann man z.B. für alle zusammengesetzten Zahlen $n \in \mathbb{N}$, $n \ge 3$, den Term $(n-1)!$ mod n in einfacher Weise direkt berechnen, wobei man jeweils ein Resultat erhält, welches offensichtlich nicht mit (10) übereinstimmt:

- Falls $n = 4$ ist: Dann ist $(n-1)! = 6$, und daher ist $(n-1)! =_n 2$.
- Falls $n \ge 6$ ist:
  - Wenn $n \ne$ Quadratzahl : Weil n weder prim noch eine Quadratzahl ist, gibt es zwei Zahlen $n_1 < n_2$ in $\mathbb{Z}_n^+$ mit $n_1 \cdot n_2 = n$. n_1, n_2 sind sicherlich zwei der insgesamt $n-1$ Faktoren des Produktes $(n-1)!$, d.h. das Produkt $(n-1)!$ ist ein Vielfaches von $n_1 \cdot n_2 = n$, d.h. $(n-1)! =_n 0$.
  - Wenn $n =$ Quadratzahl : Dann gibt es eine Zahl $q \in \mathbb{Z}_n^+$ mit $q^2 = n$. Weil $n > 4$ ist, ist $q > 2$ und daher $2q < q \cdot q = n$, d.h. auch $2q \in \mathbb{Z}_n^+$. Daher treten die zwei Zahlen q und $2q$ als Faktoren im Produkt $(n-1)!$ auf, welches damit ein Vielfaches ist von $q^2 = n$, d.h. $(n-1)! =_n 0$. ■

Anmerkung: Wir weisen noch darauf hin, dass es für die Richtigkeit der Behauptung

$$\left.\begin{array}{l}\sum_{1\le i_1<i_2<\cdots<i_k\le n-1} i_1 \cdot i_2 \cdots i_k \text{ ist teilbar durch } n \ , \\ \text{für alle } 1 \le k \le (n-2) \ , \text{ wobei } n \ge 3\end{array}\right\} \Rightarrow \ n \notin 2\mathbb{N} \quad ,$$

welche ja eine Teilaussage von (1) ist, einen viel direkteren Beweis gibt: Wegen $(n-1) =_n -1$, $(n-2) =_n -2$, etc., können wir für $n \in 2\mathbb{N}$, $n \ge 3$, und für $k = 1$ die Summe $\sum_{1\le i_1<i_2<\cdots<i_k\le n-1} i_1 \cdot i_2 \cdots i_k$ bequem mod n berechnen und erkennen, dass diese Summe sicherlich nicht durch n teilbar ist:

$$\sum_{1\le i_1\le n-1} i_1 =_n 1 + 2 + \cdots + \left(\tfrac{n}{2}-1\right) + \left(\tfrac{n}{2}\right) + \left(-\left(\tfrac{n}{2}-1\right)\right) + \cdots + (-2) + (-1) =_n \tfrac{n}{2} \ne_n 0$$

Ergänzungen

- Die gemäss (1), (2) berechneten Summenwerte sind ja, sofern $n \geq 3$ eine Primzahl p ist, durch p teilbar. Zur Illustration listen wir für die vier kleinsten Primzahlen $p \geq 3$ und die dazugehörenden k $(1 \leq k \leq (p-2))$ die entsprechenden, durch p teilbaren Summenwerte auf:

p	**k**	Produktsummen aus (1): $\sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq p-1} i_1 \cdot i_2 \cdots i_k$	Potenzsummen aus (2): $\sum_{i=1}^{p-1} i^k$
3	1	3	3
5	1	10	10
	2	35	30
	3	50	100
7	1	21	21
	2	175	91
	3	735	441
	4	1624	2275
	5	1764	12‘201
11	1	55	55
	2	1320	385
	3	18‘150	3025
	4	157‘773	25‘333
	5	902‘055	220‘825
	6	3‘416‘930	1‘978‘405
	7	8‘409‘500	18‘080‘425
	8	12‘753‘576	167‘731‘333
	9	10‘628‘640	1‘574‘304‘985

- Z.B. bei gewissen kryptologischen Anwendungen der Zahlentheorie ist es von Interesse, möglichst effizient bestimmen zu können, ob eine vorliegende ungerade Zahl n prim ist. Es scheint, als ob es nach wie vor keine deterministischen Primzahltests gibt, welche in der Praxis den besten probabilistischen Tests den Rang ablaufen können. Anhand der Teilbarkeitseigenschaften (1), (2) könnten natürlich entsprechende deterministische resp. probabilistische Primzahltests formuliert werden. Aber die deterministischen Versionen wären noch ineffizienter als die Probedivision und daher keine Konkurrenz zu den bestehenden Primzahltests, und numerische Experimente suggerieren, dass Ähnliches wahrscheinlich auch für die probabilistischen Versionen gilt.

- In (1) findet ja der Sonderfall $k = n - 1$ keine Erwähnung. Für diesen Wert von k ist offensichtlich $\sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n-1} i_1 \cdot i_2 \cdots i_k = (n-1)!$, und daher gilt gemäss Satz von Wilson [2]: n ist prim $\Leftrightarrow \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n-1} i_1 \cdot i_2 \cdots i_k =_n -1$.

- In (2) wurden die Fälle $k = 0$ und $k \geq n - 1$ nicht thematisiert. Nun, für primes n und für alle $k \geq 0$ kann man rasch einsehen, dass $\sum_{i=1}^{p-1} i^k \bmod p$ periodisch ist in k , denn es gilt: Gemäss dem Kleinen Satz von Fermat ist $\sum_{i=1}^{p-1} i^0 =_p \sum_{i=1}^{p-1} i^{p-1} =_p \sum_{i=1}^{p-1} i^{2(p-1)} =_p \cdots =_p -1$, und via (2) und Kleiner Satz von Fermat erhält man $\sum_{i=1}^{p-1} i^k =_p 0$, für die übrigen Werte von k .

Referenzen

[1] J. Pach, P.K. Agarwal: Combinatorial Geometry. Wiley-Interscience Series in Discrete Mathematics and Optimization (1995)
[2] John Wilson (1741 – 1793); https://de.wikipedia.org/wiki/Satz_von_Wilson (28.01.23)