WOLFGANG K. SEILER
Tel. 2515

B6, B4.18

21. Oktober 2020

4. Übungsblatt Algebra

Aufgabe 1: *(5 Punkte)*
Finden Sie mit dem Sieb des ERATOSTHENES und eventuell zusätzlichen Divisionen ohne Computerhilfe alle Primzahlen p mit $1320 \leq p \leq 1340$!

Lösung: 1320 ist durch zwei, drei (Quersumme sechs) und fünf teilbar; also streichen wir ausgehend von 1320 jede zweite, dritte *bzw.* fünfte Zahl; übrig bleiben 1321, 1327, 1331, 1333, 1337 und 1339. Bei der Division durch sieben hat 1320 den Rest vier, also streichen wir ausgehend von 1323 jede siebte Zahl; nur 1337 wird neu gestrichen. Elf ist ein Teiler von 1320, also wird $1331 = 1320 + 11$ gestrichen. Da 1300 durch 13 teilbar ist, ist 1326 die erste durch 13 teilbare Zahl im Suchintervall; neu gestrichen wird $1326 + 13 = 1339$. Übrig bleiben 1321 und 1327. Wenn diese nicht prim sind, haben Sie einen Primteiler der kleiner ist als $\sqrt{1327} \approx 36{,}4$; wir müssen also noch die Primzahlen $17, 19, 23, 29$ und 31 überprüfen. Keine teilt eine der beiden Zahlen; somit sind sie prim.

Aufgabe 2: *(4 Punkte)*

a) Ein Mathematiklehrer, der immer gerne Dreiecksgeometrie unterrichtet hat, möchte zur Feier seines Geburtstags die Kerzen (eine für jedes Lebensjahr) so auf ausgewählten Geburtstagstorten verteilen, daß sie auf jeder Torte in Form eines Dreiecks einer festen Kantenlänge n angeordnet sind. Ein solches Dreieck beginnt mit einer Kerze als oberer Ecke, darunter kommt eine Reihe aus zwei Kerzen, dann eine aus drei, und so weiter, bis zur unteren Kante aus n Kerzen. Leider geht das für kein n auf: Bei $n = 5$ etwa muß er die übrig gebliebenen fünf Kerzen auf der letzten Torte in Form eines Zweierquadrats mit zusätzlichem Mittelpunkt anordnen, und bei $n = 7$ bleiben noch Kerzen für ein 3×3 Quadrat auf der letzten Torte übrig. Wie alt wird er?

Lösung: Die Anzahl der Kerzen für ein Dreieck mit Kantenlänge n ist die Summe der ersten n natürlichen Zahlen, also $\frac{1}{2}n(n+1)$. Für $n = 5$ ist dies 15, für $n = 7$ ist es 28. Das Alter x erfüllt also die beiden Kongruenzen

$$x \equiv 5 \bmod 15 \quad \text{und} \quad x \equiv 3^2 = 9 \bmod 28\,.$$

Wir wenden den erweiterten EUKLIDischen Algorithmus an auf 28 und 15:

$$\begin{aligned} 28 : 15 = 1 \text{ Rest } 13 &\Longrightarrow 13 = 28 - 15 \\ 15 : 13 = 1 \text{ Rest } 2 &\Longrightarrow 2 = 15 - (28 - 15) = 2 \cdot 15 - 28 \\ 13 : 2 = 6 \text{ Rest } 1 &\Longrightarrow 1 = 13 - 6 \cdot 2(28 - 15) - 6 \cdot (2 \cdot 15 - 28) = 7 \cdot 28 - 13 \cdot 15\,. \end{aligned}$$

Also ist $7 \cdot 28 = 196$ kongruent Null modulo 28 und kongruent eins modulo 15, während $-13 \cdot 15 = -195$ durch 15 teilbar ist und kongruent eins modulo 28. Somit ist

$$x = 196 \cdot 5 - 195 \cdot 9 = -775$$

eine Lösung.

Da niemand seinen –775-ten Geburtstag feiert, ist das noch nicht die gesuchte Lösung. Das Ergebnis ist modulo $15 \cdot 28 = 420$ bestimmt; um ein positives Alter zu erreichen, müssen wir dies mindestens zweimal addieren. $-775 + 840 = 65$, also feiert er seinen 65. Geburtstag, denn er wird garantiert nicht 485 Jahre alt.

b) Wie viele Torten braucht er bei $n = 5$ und bei $n = 7$ jeweils, um alle Kerzen unterzubringen?

Lösung: $65 = 4 \cdot 15 + 5 = 2 \cdot 28 + 9$. Er braucht also fünf beziehungsweise drei Torten.

Aufgabe 3: *(3 Punkte)*
Zeigen Sie ohne Verwendung des kleinen Satzes von Fermat, daß für jede Primzahl p gilt

$$(a_1 + \cdots + a_r)^p \equiv a_1^p + \cdots + a_r^p \quad \text{für alle } a_1, \ldots, a_r \in \mathbb{Z}\,!$$

Lösung: Beweis durch Induktion nach r. Der Induktionsanfang $r = 1$ ist trivial; sei also $r \geq 2$. Mit $a = a_1 + \cdots a_{r-1}$ ist dann

$$(a + a_r)^p = a^p + \binom{p}{1} a^{p-1} a_r + \binom{p}{2} a^{p-2} a_r^2 + \cdots + \frac{p}{p-2} a^2 a_r^{p-2} + \binom{p}{p-1} a a_r^{p-1} + a_r^p\,.$$

Für $1 \leq i \leq p-1$ ist

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$$

durch p teilbar, da der Zähler, nicht aber der Nenner durch p teilbar ist. Daher ist

$$(a_1 + \cdots + a_r)^p = (a + a_r)^p \equiv a^p + a_r^p \equiv a_1^p + \cdots + a_{r-1}^p + a_r^p \bmod p$$

nach Induktionsannahme.

Aufgabe 4: *(5 Punkte)*
$p = 561 = 3 \cdot 11 \cdot 17$ ist keine Primzahl. Zeigen Sie, daß trotzdem $a^{p-1} \equiv 1 \bmod p$ gilt für alle zu p teilerfremden ganzen Zahlen a!
Hinweis: Betrachten Sie a^{p-1} modulo 3, 11 und 17!

Lösung: $p-1 = 560$ ist ein Vielfaches von $3-1 = 2$, von $11-1 = 10$ und von $17-1 = 16$. Ein zu p teilerfremdes a ist natürlich auch teilerfremd zu den Primteilern 3, 11 und 17 von p; nach dem kleinen Satz von FERMAT ist daher $a^{q-1} \equiv 1 \bmod q$ für $q \in \{3, 11, 17\}$. Da $p-1$ ein Vielfaches von $q-1$ ist, gilt auch in allen drei Fällen $a^{p-1} \equiv 1 \bmod q$; also ist $a^{p-1} - 1$ durch 3, 11 und 17 teilbar. Da die drei Zahlen paarweise teilerfremd sind, ist die Zahl auch durch $3 \cdot 11 \cdot 17 = p$ teilbar; also ist $a^{p-1} \equiv 1 \bmod p$ für alle zu p teilerfremden ganzen Zahlen a.

Aufgabe 5: *(3 Punkte)*
Finden sie eine natürliche Zahl d mit der Eigenschaft, daß die Abbildung

$$\begin{cases} \{0,1,\dots 100\} \to \{0,1,\dots,100\} \\ x \mapsto x^d \bmod 101 \end{cases} \quad \text{invers ist zu} \quad \begin{cases} \{0,1,\dots 100\} \to \{0,1,\dots,100\} \\ x \mapsto x^9 \bmod 101 \end{cases} !$$

Lösung: 101 ist eine Primzahl, denn sie ist offensichtlicht nicht durch $2, 3$ oder 5 teilbar, $100 : 7 = 14$ Rest 2, und $11^2 > 101$. Somit ist nach dem kleinen Satz von FERMAT $x^{100} \equiv 1 \bmod 101$ für alle nicht durch 101 teilbaren x, und $x^{n\cdot 100+1} \equiv x \bmod 101$ für alle x. d muß daher so gewählt werden, daß $9d \equiv 1 \bmod 100$ ist. Anwendung des erweiterten EUKLIDischen Algorithmus auf neun und hundert führt schon in der ersten Division zum Erfolg:

$$100 : 9 = 11 \text{ Rest } 1 \Longrightarrow 1 = 100 - 11 \cdot 9$$

Leider ist der Koeffizient -11 von neun negativ; daher müssen wir noch die Gleichung $-9 \cdot 100 + 100 \cdot 9 = 0$ addieren und erhalten

$$1 = -8 \cdot 100 + 89 \cdot 9 \Longrightarrow 89 \cdot 9 \equiv 1 \bmod 100\,.$$

Somit ist $d = 89$.