Wolfgang K. Seiler
Tel. 2515

A5, C201

13. Juni 2014

Modulklausur Zahlentheorie

• • • **Schreiben Sie bitte auf jedes Blatt Ihren Namen!** • • •

Aufgabe 1: (*5 Punkte*)

Die *Paarquersumme* einer natürlichen Zahl n wird berechnet, indem man die Zahl von rechts her in Gruppen aus zwei Ziffern aufteilt und die entstehenden zweistelligen Zahlen addiert; die Paarquersumme von 12345 ist also $45 + 23 + 1 = 68$.

a) Zeigen Sie, daß n genau dann durch elf teilbar ist, wenn seine Paarquersumme durch elf teilbar ist.

b) Ist jede natürliche Zahl n modulo elf kongruent zu ihrer Paarquersumme?

Lösung: Ist $n = \sum_{i=0}^{r} a_i \cdot 100^i$ mit $0 \le a_i \le 99$, so ist $\sum_{i=0}^{r} a_i$ die Paarquersumme. Da $100 \equiv 1 \bmod 11$, sind die beiden Zahlen kongruent modulo elf, insbesondere ist also n genau dann durch elf teilbar, wenn dies für die Paarquersumme der Fall ist.

c) Welchen Rest hat die Zahl 2718281828459045 bei der Division durch elf?

Lösung: Sie ist modulo elf kongruent zu ihrer Paarquersumme $45+90+45+28+18+28+18+27 = 299$; diese wiederum hat Paarquersumme 101, und diese hat Paarquersumme zwei. Somit hat 2718281828459045 bei der Division durch elf den Rest zwei.

Aufgabe 2: (*6 Punkte*)

Für ein *public viewing* zur Fußballweltmeisterschaft möchte ein Choreograph zum Auftakt Statisten in Fußballtrikots in die Arena einmarschieren lassen. Wenn er sie in Elferreihen marschieren läßt, bleiben in der letzten Reihe acht übrig, allerdings ist der Zug dann zu lang. Deshalb ordnet er sie in Fünfundzwanzigerreihen an; jetzt bleiben in der letzten Reihe sieben übrig.

a) Finden Sie eine untere Schranke für die Anzahl der Statisten!

Lösung: Über die Anzahl N der Statisten wissen wir, daß einerseits $N \equiv 8 \bmod 11$ und andererseits $N \equiv 7 \bmod 25$. Um beides über den chinesischen Restesatz kombinieren zu können, müssen wir zunächst den ggT von 11 und 25 als Linearkombination darstellen:

$$\begin{aligned} 25 : 11 = 2 \quad \text{Rest } 3 &\Longrightarrow 3 = 25 - 2 \cdot 11 \\ 11 : 3 = 3 \quad \text{Rest } 2 &\Longrightarrow 2 = 11 - 3 \cdot (25 - 2 \cdot 11) = 7 \cdot 11 - 3 \cdot 25 \\ 3 : 2 = 1 \quad \text{Rest } 1 &\Longrightarrow 1 = (25 - 2 \cdot 11) - (7 \cdot 11 - 3 \cdot 25) = 4 \cdot 25 - 9 \cdot 11 \end{aligned}$$

Somit ist

$$4 \cdot 25 = 100 \equiv \begin{cases} 1 \bmod 11 \\ 0 \bmod 25 \end{cases} \quad \text{und} \quad -9 \cdot 11 = -99 \equiv \begin{cases} 0 \bmod 11 \\ 1 \bmod 25 \end{cases},$$

also ist

$$100 \cdot 8 - 99 \cdot 7 = 107 \equiv \begin{cases} 8 \bmod 11 \\ 7 \bmod 25 \end{cases}.$$

N ist über die obigen beiden Kongruenzen modulo $11 \cdot 25 = 275$ eindeutig bestimmt; die kleinste positive Lösung ist daher gerade 107.

b) Welche anderen Anzahlen wären auch noch möglich?

Lösung: Alle Zahlen der Form $107 + k \cdot 275$ mit $k \in \mathbb{N}_0$.

Aufgabe 3: *(8 Punkte)*

a) Berechnen Sie im Körper $\mathbb{F}_{29}$ die Elemente

$$x_1 = 2 - 5^2, \qquad x_2 = 26 \cdot 27, \qquad x_3 = \frac{5}{27} \quad \text{und} \quad x_4 = 28! = \prod_{i=1}^{28} i$$

Lösung: In $\mathbb{F}_{29}$ ist $x_1 = 2 - 25 = -23 = 6$ und $x_2 = 26 \cdot 27 = (-3) \cdot (-2) = 6$.
Zur Berechnung von x_3 müssen wir zunächst über den erweiterten EUKLIDischen Algorithmus das multiplikative Inverse von 27 bestimmen:

$$\begin{aligned} 29 : 27 = 1 \quad \text{Rest } 2 &\Longrightarrow 2 = 29 - 27 \\ 27 : 2 = 13 \quad \text{Rest } 1 &\Longrightarrow 1 = 27 - 13 \cdot (29 - 27) = 14 \cdot 27 - 13 \cdot 29 \end{aligned}$$

Somit ist $14 \cdot 27 \equiv 1 \bmod 29$; im Körper $\mathbb{F}_{29}$ ist also $x_3 = 5/27 = 5 \cdot 14 = 70 = 12$. Zur Probe können wir noch nachrechnen, daß in der Tat $12 \cdot 27 = 12 \cdot (-2) = -24 = 5$ ist.
x_4 schließlich hat nach der WILSONschen Kongruenz den Wert $-1 = 28$.

b) Zeigen Sie, daß die Zwei und die Drei primitive Wurzeln modulo 29 sind, nicht aber die Sechs.

Lösung: $29 - 1 = 28 = 2^2 \cdot 7$; ein Element a ist also genau dann eine primitive Wurzel, wenn $a^{28} \equiv 1 \bmod 29$ ist, aber a^4 und a^{14} modulo 29 beide von eins verschieden sind.
$2^4 = 16$ ist offensichtlich nicht kongruent zu eins. $2^5 = 32 \equiv 3 \bmod 29$, und damit ist $2^{10} \equiv 9 \bmod 29$ und $2^{14} \equiv 9 \cdot 16 = 144 = 5 \cdot 29 - 1 \equiv -1 \bmod 29$. Damit ist $2^{28} \equiv 1 \bmod 29$ und alle Bedingungen an eine primitive Wurzel sind erfüllt.
$3^3 = 27 \equiv -2 \bmod 29$; also ist $3^4 \equiv -6 \bmod 29$. Weiter ist $3^{12} = (-2)^4 = 16 \bmod 29$, also $3^{14} \equiv 9 \cdot 16 \equiv -1 \bmod 29$. Auch hier sind alle Bedingungen an eine primitive Wurzel erfüllt.
$6^{14} = 2^{14} \cdot 3^{14} = (-1) \cdot (-1) = 1$; die Sechs hat somit höchstens die Ordnung 14 und kann daher keine primitive Wurzel sein.

c) Geben Sie zu jeder möglichen Ordnung eines Elements von $\mathbb{F}_{29}^{\times}$ ein Element an, das exakt diese Ordnung hat!

Lösung: Möglich sind alle Teiler von 28, also 1, 2, 4, 7, 14 und 28. Wie wir aus *b)* wissen, haben 2 und 3 beide die Ordnung 28, ihre Quadrate 4 und 9 haben also Ordnung 14 und $4^2 = 16$ hat die Ordnung sieben. $2^7 = 128 = 12$ hat die Ordnung vier, $-1 = 28$ die Ordnung zwei, und nur die Eins hat Ordnung eins.

Aufgabe 4: *(8 Punkte)*

J sei eine Jahreszahl und $1900 < J < 2072$.

a) Zeigen Sie: Im Jahr $J + 4$ hat sich der Wochentag, auf den der 1. Januar fällt, gegenüber dem Jahr J um fünf verschoben.

Lösung: Da das Jahr 2000 ein Schaltjahr war, ist im fraglichen Zeitraum jedes vierte Jahr ein Schaltjahr; unter den Jahren J bis $J+3$ gibt es daher genau ein Schaltjahr. Nach einem

gewöhnlichen Jahr verschiebt sich der Wochentag des ersten Januars wegen $365 \equiv 1 \bmod 7$ um eins, nach einem Schaltjahr um zwei, insgesamt also um $3 \cdot 1 + 2 = 5$.

b) J' sei das erste Jahr nach J, in dem jedes Datum auf den gleichen Wochentag fällt wie im Jahr J. Zeigen Sie;

$$J' = \begin{cases} J + 28 & \text{falls } J \equiv 0 \bmod 4 \\ J + 6 & \text{falls } J \equiv 1 \bmod 4 \\ J + 11 & \text{sonst} \end{cases}$$

Lösung: Ist $J \equiv 0 \bmod 4$, so ist J ein Schaltjahr; damit muß auch J' eines sein. Die Differenz $J' - J$ ist daher durch vier teilbar. Im Jahr $J + 4k$ hat sich der Wochentag des ersten Januars nach *a)* um $5k$ verschoben; wenn wir gleiche Wochentage wollen, muß dies ein Vielfaches von sieben sein. Die erste Möglichkeit ist $k = 7$, d.h. $J' = J + 28$.

Ist $J \equiv 1 \bmod 4$, so haben wir nach *a)* im Jahr J+4 einen um fünf Wochentage verschobenen ersten Januar; da $J + 4$ und $J + 5$ beide keine Schaltjahre sind, haben wir im Jahr $J + 6$ erstmalig eine Verschiebung um sieben Wochentage, d.h. $J' = J + 6$.

Ist $J \equiv 2 \bmod 4$, so folgt wie im Falle $J \equiv 1 \bmod 4$, daß der erste Januar $J + 6$ auf den gleichen Wochentag fällt wie der erste Januar im Jahr J. Wegen $J \equiv 2 \bmod 4$ ist $J + 6$ aber ein Schaltjahr, d.h. ab dem 29. Februar stimmen die Wochentage nicht mehr überein. Im Jahr $J + 7$ ist der erste Januar zwei Wochentage später als im Jahr J; vier Jahre später, im Jahr $J + 11$ sind wir nach *a)* noch einmal fünf Tage weiter, also wieder beim gleichen Wochentag wie im Jahr J. Da $J + 11 \equiv 1 \bmod 4$, ist dies kein Schaltjahr.

Ist schließlich $J \equiv 3 \bmod 4$, so sind wir im Jahr J+6 nicht sieben, sondern acht Wochentage weiter, da $J + 5$ ein Schaltjahr war. Im Jahr $J + 7$ sind wir wie im vorigen Fall neun *bzw.* zwei Tage weiter, und da $J + 11 \equiv 2 \bmod 4$, folgt wie dort, daß im Jahr $J + 11$ alle Daten auf die gleichen Wochentage fallen wie im Jahr J.

c) Warum sind diese Formeln falsch für $J = 1900$ und $J = 2072$?

Lösung: 1900 war kein Schaltjahr, 1928 aber doch; entsprechend ist 2072 ein Schaltjahr, 2100 aber nicht.In beiden Fällen können daher die Wochentage des Jahres J nicht alle mit denen des Jahres $J + 28$ übereinstimmen.

Aufgabe 5: *(6 Punkte)*

a) Wie läßt sich bei RSA mit öffentlichem Exponenten $e = 5$ und Modul $N = pq$ ein privater Exponent d ohne EUKLIDischen Algorithmus aus e und einem gemeinsamen Vielfachen m von $p - 1$ und $q - 1$ berechnen?

Lösung: Wir suchen positive ganze Zahlen d und k, für die $1 = de - km$ ist. Zu dieser Gleichung können wir beliebige Vielfache der Gleichung $0 = m \cdot e - e \cdot m$ addieren; daher kann $1 \leq k < e$ erreicht werden. Für jedes Lösungspaar (d, k) ist $d = (1 + km)/e$. Wir müssen für $e = 5$ daher nur probieren, für welchen der Werte $k = 1, 2, 3, 4$ obiger Ausdruck ein ganzzahliges d liefert.

b) Finden Sie für das RSA-System mit $p = 409$, $q = 523$ und $e = 5$ einen möglichst kleinen privaten Exponenten d !

Lösung: $p - 1 = 408 = 2^3 \cdot 3 \cdot 17$ und $q - 1 = 522 = 2 \cdot 3^2 \cdot 29$; das kleinste gemeinsame Vielfache von $p - 1$ und $q - 1$ ist daher $m = 2^3 \cdot 3^2 \cdot 17 \cdot 29 = 35496$. Die Gleichung $1 = de - km$ läßt sich auflösen zu $d = (1 + km)/5$ mit $1 \leq k < 5$. Dies ist ganzzahlig,

wenn die Zahl im Zähler auf null oder fünf endet, wenn also km auf neun oder vier endet. Da m gerade ist, ist die Neun nicht möglich; für $k = 4$ erhalten wir die Vier und

$$d = \frac{1 + 4 \cdot 35496}{5} = \frac{141985}{5} = 28397\,.$$

c) Warum ist es hier nicht möglich, den öffentlichen Exponenten $e = 3$ zu nehmen?

Lösung: e muß teilerfremd sein zu $p - 1$ und zu $q - 1$; hier sind aber beide Zahlen durch drei teilbar.

Aufgabe 6: (*10 Punkte*)

a) Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{10}$!

Lösung: Da $3^2 < 10 < 4^2$, ist der ganzzahlige Anteil drei.

$$\frac{1}{\sqrt{10} - 3} = \frac{\sqrt{10} + 3}{10 - 3^2} = 3 + \sqrt{10}$$

hat dementsprechend den ganzzahligen Anteil sechs, und $3 + \sqrt{10} - 6 = \sqrt{10} - 3$, d.h. ab hier wiederholt sich die Rechnung und auch alle weiteren Koeffizienten sind sechs. Die gesuchte Kettenbruchentwicklung ist daher

$$\sqrt{10} = [3; \overline{6}] = 3 + \cfrac{1}{6 + \cfrac{1}{6 + \ddots}}\,.$$

b) Finden Sie einen Näherungsbruch für $\sqrt{10}$ mit möglichst kleinem Nenner, der sich höchstens um 10^{-3} von $\sqrt{10}$ unterscheidet!

Lösung: Die ersten Konvergenten der gerade berechneten Kettenbruchentwicklung sind

$$3, \qquad 3 + \frac{1}{6} = \frac{19}{6} \quad \text{und} \quad 3 + \frac{1}{6 + \frac{1}{6}} = 3 + \frac{1}{\frac{37}{6}} = 3\frac{6}{37} = \frac{117}{37}$$

Der letzte dieser Brüche hat Nenner 37; da $37^2 > 1000$, hat er einen kleineren Approximationsfehler als 10^{-3}.

c) Finden Sie eine ganzzahlige Lösung der Gleichung $x^2 - 10y^2 = 1$!

Lösung: Wir können die Nenner und Zähler der Konvergenten der Kettenbruchentwicklung durchprobieren:

$$3^2 - 10 \cdot 1^2 = -1, \qquad 19^2 - 10 \cdot 6^2 = 1$$

Somit ist $x = 19, y = 6$ eine Lösung.

d) Konstruieren Sie aus der Lösung von *c)* ein Element der Norm eins aus $\mathbb{Q}[\sqrt{10}]$!

Lösung: Die Norm von $x + y\sqrt{10}$ ist $(x + y\sqrt{10})(x - y\sqrt{10}) = x^2 - 10y^2$; daher ist $19 + 6\sqrt{10}$ ein solches Element.

e) Konstruieren Sie über das Quadrat dieses Elements eine weitere Lösung der Gleichung $x^2 - 10y^2 = 1$!

Lösung: $\left(19 + 6\sqrt{10}\right)^2 = 361 + 228\sqrt{10} + 10 \cdot 36 = 721 + 228\sqrt{10}$ hat ebenfalls die Norm eins; daher ist $721^2 - 10 \cdot 228^2 = 1$.

Aufgabe 7: *(8 Punkte)*

a) Bestimmen Sie im Ring $\mathbb{Z} \oplus \mathbb{Z}i$ der Gaussschen Zahlen die Primzerlegung der Zahl $15i$!

Lösung: i ist eine Einheit, und in $\mathbb{Z}$ ist $15 = 3 \cdot 5$. Da Primzahlen kongruent drei modulo vier auch in $\mathbb{Z} \oplus \mathbb{Z}i$ irreduzibel bleiben, ist die Drei irreduzibel; $5 \equiv 1 \bmod 4$ läßt sich weiter zerlegen: Wegen $2^2 + 1^2 = 5$ ist $5 = (2+i)(2-i) = (1+2i)(1-2i)$. Somit ist beispielsweise

$$15i = i \cdot 3 \cdot (2+i)(2-i) = 3 \cdot (2+i)(1+2i)\,.$$

b) Finden Sie alle ganzzahligen Lösungen der Gleichung $x^2 + y^2 = 15$!

Lösung: Da 15 die Primzahl drei nur einmal enthält (oder auch weil $15 \equiv 3 \bmod 4$) gibt es keine Lösungen.

c) Berechnen Sie in $\mathbb{Z} \oplus \mathbb{Z}i$ den ggT von $1 + 5i$ und $2 + 8i$!

Lösung:

$$\frac{2+8i}{1+5i} = \frac{(2+8i)(1-5i)}{26} = \frac{42-2i}{26} = \frac{21}{13} - \frac{1}{13}i$$

hat 2 als nächstgelegene Zahl aus $\mathbb{Z} \oplus \mathbb{Z}i$; wir können also setzen

$$(2+8i) : (1+5i) = 2 \quad \text{Rest } -2i\,.$$

Im nächsten Schritt ist

$$\frac{1+5i}{-2i} = \frac{-5+i}{2} = -\frac{5}{2} + \frac{i}{2}\,;$$

eine der nächstgelegenen Zahlen aus $\mathbb{Z} \oplus \mathbb{Z}i$ ist -2, d.h.

$$(1+5i) : (-2i) = -2 \quad \text{Rest } 1+i\,.$$

Da $\dfrac{-2i}{1+i} = -1 - i$ in $\mathbb{Z} \oplus \mathbb{Z}i$ liegt, ist der ggT gleich $1 + i$.

d) Zeigen Sie: $\mathrm{ggT}(a + ib, a - ib) = \mathrm{ggT}(a, b)$ für alle $a + ib \in \mathbb{Z} \oplus \mathbb{Z}i$

Lösung: Natürlich teilt jeder gemeinsame Teiler von a und b auch $a \pm bi$, also auch deren ggT. Umgekehrt teilt jeder gemeinsame Teiler von $a \pm bi$ auch deren Summe $2a$ sowie die Differenz $2bi$, ist also bis auf Einheiten eine natürliche Zahl. Diese kann $a + bi$ aber nur dann teilen, wenn sie sowohl a als auch b teilt.

Aufgabe 8: *(8 Punkte)*

Welche der folgenden Kongruenzen sind lösbar:

a) $x^2 \equiv 4 \bmod 12345$

Lösung: Da die Gleichung $x^2 = 4$ über $\mathbb{Z}$ lösbar ist (mit $x = \pm 2a$), ist sie erst recht modulo jeder natürlichen Zahl m lösbar.

b) $x^2 \equiv 5 \bmod 23$

Lösung: Nach dem quadratischen Reziprozitätsgesetz ist, da $5 \equiv 1 \bmod 4$ ist,

$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1\,,$$

denn modulo drei sind nur null und eins Quadrate. Somit ist die Kongruenz nicht lösbar.

c) $x^2 \equiv 5 \bmod 21$

Lösung: Da $21 = 3 \cdot 7$ keine Primzahl ist, können wir hier nicht einfach das JACOBI-Symbol ausrechnen und nach dessen Wert entscheiden. Nach dem chinesischen Restesatz ist die Gleichung genau dann modulo 21 lösbar, wenn sie modulo drei und modulo sieben lösbar ist. Modulo drei wird sie aber zur unlösbaren Gleichung $x^2 \equiv 2 \bmod 3$; also ist auch die Ausgangsgleichung nicht lösbar.

d) Finden Sie die kleinste ungerade Primzahl p, für die die Kongruenz $x^2 \equiv p \bmod 127$ lösbar ist! (127 ist prim.)

Lösung: Hier können wir wieder das LEGENDRE-Symbol ausrechnen; da $127 \equiv 3 \bmod 4$ und $3 \equiv 3 \bmod 4$ ist

$$\left(\frac{3}{127}\right) = -\left(\frac{127}{3}\right) = -\left(\frac{1}{3}\right) = -1\,,$$

denn die Eins ist natürlich ein quadratischer Rest modulo drei. Für $p = 3$ gibt es somit keine Lösung.
Für $p = 5$ ist

$$\left(\frac{5}{127}\right) = \left(\frac{127}{5}\right) = \left(\frac{2}{5}\right) = -1\,,$$

denn modulo fünf sind nur $0, 1$ und 4 Quadrate.
Für $p = 7$ erhalten wir

$$\left(\frac{7}{127}\right) = -\left(\frac{127}{7}\right) = -\left(\frac{1}{7}\right) = -1\,,$$

und für $p = 11$ schließlich

$$\left(\frac{11}{127}\right) = -\left(\frac{127}{11}\right) = -\left(\frac{6}{11}\right) = -\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)\,.$$

Dabei ist

$$\left(\frac{2}{11}\right) = (-1)^{(11^2-1)/8} = (-1)^{15} = -1$$

und

$$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1\,.$$

Somit ist

$$\left(\frac{11}{127}\right) = -\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = 1\,,$$

$p = 11$ ist also die kleinste ungerade Primzahl, für die die Kongruenz lösbar ist.