Wolfgang K. Seiler
Tel. 2515

A5, C201

25. August 2014

Modulklausur Zahlentheorie

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

Aufgabe 1: (*5 Punkte*)

Die *alternierende Quersumme* einer natürlichen Zahl n wird berechnet, indem man ihre Dezimalziffern, ausgehend von der niedrigsten, abwechselnd positiv und negativ nimmt und diese Zahlen aufaddiert; die alternierende Quersumme von 12345 ist demnach also $5-4+3-2+1=3$.

a) Zeigen Sie, daß eine natürliche Zahl n genau dann durch elf teilbar ist, wenn ihre alternierende Quersumme durch elf teilbar ist!

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

Lösung: Ist $n=\sum_{i=0}^{r} a_i \cdot 10^i$ mit $0 \le a_i \le 9$, so ist die alternierenden Quersumme gleich $\sum_{i=0}^{r}(-1)^i a_i$. Da $10 \equiv -1 \bmod 11$, sind die beiden Zahlen kongruent modulo elf, insbesondere ist also n genau dann durch elf teilbar, wenn dies für die alternierende Quersumme der Fall ist.

c) Wie verhält es sich mit *a)* und *b),* wenn man bei der Berechnung der *alternierenden Quersumme* mit der höchsten Dezimalziffer anfängt?

Lösung: Bei gerader Stellenzahl ändert sich nichts an der alternierenden Quersumme, andernfalls ändert sich das Vorzeichen, so daß zwar *a)* weiterhin gilt, nicht aber *b).*

d) Welchen Rest hat die Zahl $n=3141592654$ bei der Division durch elf?

Lösung: Nach *b)* ist $n \equiv 4-5+6-2+9-5+1-4+1-3=2 \bmod 11$, hat also bei der Division durch elf den Rest zwei.

Aufgabe 2: (*6 Punkte*)

a) Wie viele Elemente hat die prime Restklassengruppe $(\mathbb{Z}/19800)^\times$?
(Hinweis: Die alternierende Quersumme von 19800 ist null.)

Lösung: Da die alternierende Quersumme von 19800 null ist, ist die Zahl durch elf teilbar:

$$19800 = 11 \cdot 1800 = 11 \cdot 18 \cdot 100 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11\,.$$

Die Gruppenordnung ist daher

$$\varphi(19800) = \varphi(2^3)\cdot\varphi(3^2)\cdot\varphi(5^2)\cdot\varphi(11) = (8-4)\cdot(9-3)\cdot(25-5)\cdot(11-1) = 4\cdot6\cdot20\cdot10 = 4800\,.$$

b) $n=4704977$ ist ein Produkt zweier Primzahlen, und $\varphi(n)=4700160$. Bestimmen Sie die Primzerlegung von n ausgehend von diesen Informationen!

Lösung: $n=pq=4704977$ und $\varphi(n)=(p-1)(q-1)=n-(p+q)+1=4700160$. Somit ist $p+q=n+1-\varphi(n)=4704978-4700160=4818$ und

$$(x-p)(x-q) = x^2-4818+4704977\,.$$

p und q sind also die Nullstellen dieser quadratischen Gleichung. Wir können sie umschreiben als

$$(x-2409)^2 = 2409^2 - 4704977 = 5803281 - 4704977 = 1098304 = 1048^2\,;$$

p und q sind also 2409 ± 1048, d.h. 1361 und 3457.

c) Bestimmen Sie den kleinsten Exponenten r, für den $a^r \equiv 1 \bmod n$ gilt für alle zu n teilerfremden ganzen Zahlen a!

Lösung: $a^{p-1} \equiv 1 \bmod p$ für alle zu p teilerfremden a, und $a^{q-1} \equiv 1 \bmod q$ für alle zu q teilerfremden a. Ist r ein gemeinsames Vielfaches von $p-1$ und $q-1$, ist daher auch $a^r \equiv 1$ für alle zu $n = pq$ teilerfremden a. Da

$$p - 1 = 1360 = 2^4 \cdot 5 \cdot 17 \quad \text{und} \quad q - 1 = 2^7 \cdot 3^3\,,$$

haben $p-1$ und $q-1$ den ggT $2^4 = 16$ und somit das kleinste gemeinsame Vielfache

$$r = \frac{(p-1)(q-1)}{16} = \frac{\varphi(n)}{16} = 293760\,.$$

Aufgabe 3: *(9 Punkte)*

a) Berechnen Sie im Körper $\mathbb{F}_{31}$ die Elemente

$$x_1 = 5 - 3^2, \qquad x_2 = 2^5, \qquad x_3 = 2^{2014}, \qquad x_4 = \frac{3}{25} \quad \text{und} \quad x_5 = 29! = \prod_{i=1}^{29} i$$

Lösung: In $\mathbb{F}_{31}$ ist $x_1 = 5 - 9 = -4 = 27$ und $x_2 = 2^5 = 32 = 1$. Da $2014 \equiv 4 \bmod 5$ folgt, daß $x_3 = 2^4 = 16$ ist.
Zur Berechnung von x_4 müssen wir zunächst über den erweiterten EUKLIDischen Algorithmus das multiplikative Inverse von 25 bestimmen:

$$\begin{aligned} 31 : 25 = 1 \quad \text{Rest } 6 &\Longrightarrow 6 = 31 - 25 \\ 25 : 6 = 4 \quad \text{Rest } 1 &\Longrightarrow 1 = 25 - 4 \cdot (31 - 25) = 5 \cdot 25 - 4 \cdot 31 \end{aligned}$$

Somit ist $5 \cdot 25 \equiv 1 \bmod 31$; im Körper $\mathbb{F}_{31}$ ist also $x_4 = 3/25 = 3 \cdot 5 = 15$. Zur Probe können wir noch nachrechnen, daß in der Tat $15 \cdot 25 = 15 \cdot (-6) = -90 = 3 - 3 \cdot 31$ ist.
Für x_5 schließlich verwenden wir am besten die WILSONsche Kongruenz. Sie besagt, daß $x_5 \cdot 30 = \prod_{i=1}^{30} i = -1$ ist. In $\mathbb{F}_{31}$ ist $30 = -1$, also ist $-x_5 = -1$ und $x_5 = 1$.

b) Bestimmen Sie die kleinste natürliche Zahl, die eine primitive Wurzel modulo 31 ist!

Lösung: Die Eins kommt natürlich nicht in Frage, genauso wenig die Zwei, denn wie wir aus *a)* wissen, ist $2^5 \equiv 1 \bmod 31$.
Die Ordnung von $(\mathbb{Z}/31)^\times$ ist $30 = 2 \cdot 3 \cdot 5$; ein Element x hat also genau dann die Ordnung 30, wenn x^6, x^{10} und x^{15} allesamt von eins verschieden sind.
Für $x = 3$ ist $x^2 = 9$, $x^4 = 9^2 = 19$, $x^5 = 3 \cdot 19 = 26$, $x^6 = 3 \cdot 26 = 16 \neq 1$, und auch $x^{10} = 26^2 = (-5)^2 = 25$ und $x^{15} = 25 \cdot 26 = (-6) \cdot (-5) = 30 = -1$ sind beide von eins verschieden. Somit ist x^{30} die erste Dreierpotenz, die in $\mathbb{F}_{31}$ gleich eins ist; die Drei ist also eine primitive Wurzel.

c) Geben Sie zu jeder möglichen Ordnung eines Elements von $\mathbb{F}_{31}^\times$ ein Element an, das exakt diese Ordnung hat!

Lösung: Möglich sind alle Teiler von 30, also 1, 2, 3, 5, 6, 10, 15 und 30. Wie wir aus *b)* wissen, hat 3 die Ordnung 30, ihr Quadrat 9 hat also Ordnung 15 und $3^3 = 27$ hat die Ordnung zehn. Die Zwei hat nach *a)* Ordnung fünf. $3^5 = 9 \cdot 27 = 9 \cdot (-4) = -36 = -5 = 26$ hat die Ordnung sechs, sein Quadrat $26^2 = (-5)^2 = 25$ hat die Ordnung drei, $-1 = 30$ die Ordnung zwei, und nur die Eins hat Ordnung eins.

Aufgabe 4: (*4 Punkte*)

a) Der (wenn auch vielleicht nicht unter Bachelorstudenten) bekannte Mathematiker MAXIM KONTSEVICH feiert heute seinen fünfzigsten Geburtstag. An welchem Wochentag wurde er geboren?

Lösung: Heute ist Montag, der 25. August 2014; geboren wurde er also am 25. August des Schaltjahrs 1964, allerdings nach dem 29. Februar. Daher liegt der Wochentag seines ersten Geburtstag nur einen Tag hinter dem seiner Geburt. Schaltjahre, die den Wochentag um zwei verschieben, sind nur die zwischen 1968 und 2012. Da auch 2000 ein Schaltjahr war, sind das 12 Stück. Insgesamt verschob sich also der Wochentag seit seiner Geburt um $50 + 12 = 62 \equiv 6 \bmod 7$. Da heute Montag ist, wurde er also an einem Dienstag geboren.

b) Der ehemalige indische Premierminister MORAJI DESAI wurde am 29. Februar 1896 geboren und starb am 10. April 1995. Wie oft konnte er seinen Geburtstag an einem 29. Februar feiern? (1896 war er natürlich noch zu jung zum Feiern.)

Lösung: Da 1900 nach dem gregorianischen Kalender kein Schaltjahr ist, mußte er damals seine Feier auf einen anderen Tag verlegen; am 29. Februar konnte er nur in den Schaltjahren von 1904 bis 1992 feiern, also 23 Mal.

Aufgabe 5: (*8 Punkte*)

a) Die Zahl $N = 98587$ hat keinen Primteiler, der wesentlich kleiner ist als ihre Quadratwurzel. Bestimmen Sie ihre Primzerlegung!

Lösung: Wenn kein Primfaktor wesentlich kleiner ist als die Quadratwurzel, kann es nur zwei Primfaktoren geben, die sich beide nicht stark von der Quadratwurzel und damit auch voneinander unterscheiden. Daher ist das Verfahren von FERMAT zu empfehlen: $98587 + 1 = 98588$ und $98587 + 2^2 = 98591$ sind keine Quadratzahlen, aber

$$98587 + 3^2 = 98596 = 314^2 .$$

Somit ist $98587 = 314^2 - 3^2 = (314 - 3)(314 + 3) = 311 \cdot 317$.

b) Welche Zahlen $1 < e < 10$ kommen als öffentliche Exponenten für ein RSA-System mit Modul N in Frage?

Lösung: $311 - 1 = 310 = 2 \cdot 5 \cdot 31$ und $317 - 1 = 316 = 2^2 \cdot 79$; daher darf e durch keine der Primzahlen $2, 5, 31$ und 79 teilbar sein. Im angegebenen Bereich trifft dies zu auf die Exponenten $3, 7$ und 9.

c) Bestimmen Sie für den öffentlichen Exponenten $e = 19$ einen möglichst kleinen privaten Exponenten!

Lösung: 310 und 316 haben nur die Zwei als gemeinsamen Primfaktor; ihr kleinstes gemeinsames Vielfaches ist daher $\frac{1}{2} \cdot 310 \cdot 316 = 48980$. Wir wenden den erweiterten

EUKLIDischen Algorithmus an auf diese Zahl und $e = 19$:

$$\begin{aligned} 48980 : 19 = 2577 \quad \text{Rest } 17 &\Longrightarrow 17 = 48980 - 2577 \cdot 19 \\ 19 : 17 = 1 \quad \text{Rest } 2 &\Longrightarrow 2 = 19 - (48980 - 2577 \cdot 19) = 2578 \cdot 19 - 48980 \\ 17 : 2 = 8 \quad \text{Rest } 1 &\Longrightarrow 1 = (48980 - 2577 \cdot 19) - 8 \cdot (2578 \cdot 19 - 48980) = 9 \cdot 48980 - 23201 \cdot 19 \end{aligned}$$

Da der Faktor vor 19 negativ ist, addieren wir das kgV und erhalten

$$d = 48980 - 23201 = 25779\,.$$

d) Wie viele Multiplikationen modulo N sind notwendig, um eine Nachricht in diesem System mit $e = 19$ zu verschlüsseln?

Lösung: $19 = 16 + 2 + 1$; zur Bestimmung von $m^e \bmod N$ berechnet man daher zweckmäßigerweise durch sukzessive Quadrierung modulo N die Zahlen $m^2 \bmod N$, $m^4 \bmod N$, $m^8 \bmod N$ und $m^{16} \bmod N$; dann ist $m^{19} \bmod N = m^{16} \cdot m^2 \cdot m \bmod N$. Benötigt werden also vier Quadrierungen und zwei sonstige Multiplikationen modulo N, insgesamt sechs Multiplikationen.

Aufgabe 6: (*10 Punkte*)

a) Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{5}$!

Lösung: Da $2^2 < 5 < 3^2$, ist der ganzzahlige Anteil zwei.

$$\frac{1}{\sqrt{5} - 2} = \frac{\sqrt{5} + 2}{5 - 2^2} = 2 + \sqrt{5}$$

hat dementsprechend den ganzzahligen Anteil vier, und $2 + \sqrt{2} - 4 = \sqrt{5} - 2$, d.h. ab hier wiederholt sich die Rechnung und auch alle weiteren Koeffizienten sind vier. Die gesuchte Kettenbruchentwicklung ist daher

$$\sqrt{5} = [2; \overline{4}] = 2 + \cfrac{1}{4 + \cfrac{1}{4 + \ddots}}\,.$$

b) Finden Sie einen Näherungsbruch für $\sqrt{5}$ mit möglichst kleinem Nenner, der sich höchstens um 10^{-2} von $\sqrt{5}$ unterscheidet!

Lösung: Die ersten Konvergenten der gerade berechneten Kettenbruchentwicklung sind

$$2, \qquad 2 + \frac{1}{4} = \frac{9}{4} \quad \text{und} \quad 2 + \cfrac{1}{4 + \cfrac{1}{4}} = 2 + \frac{1}{\frac{17}{4}} = 2\frac{4}{17} = \frac{38}{17}$$

Der letzte dieser Brüche hat Nenner 17; da $17^2 > 10^2 = 100$, hat er einen kleineren Approximationsfehler als 10^{-2}.

c) Finden Sie eine ganzzahlige Lösung der Gleichung $x^2 - 5y^2 = 1$!

Lösung: Wir können die Nenner und Zähler der Konvergenten der Kettenbruchentwicklung durchprobieren: $2^2 - 5 \cdot 1^2 = -1$, aber $9^2 - 5 \cdot 4^2 = 1$. Somit ist $x = 9, y = 4$ eine Lösung.

d) In der Kettenbruchentwicklung der reellen Zahl x seien alle Koeffizienten gleich der natürlichen Zahl a, d.h.

$$x = [\overline{a}] = a + \cfrac{1}{a + \cfrac{1}{a + \ddots}} .$$

Bestimmen Sie x!

Lösung: x erfüllt die Gleichung $x = a + \frac{1}{x}$; Multiplikation mit x macht daraus $x^2 = ax + 1$ oder $(x - \frac{a}{2})^2 = 1 + \frac{a^2}{4}$. Somit ist x eine der beiden Zahlen $\frac{a}{2} \pm \sqrt{1 + \frac{a^2}{4}}$. Da der Ausdruck unter der Wurzel größer ist als das Quadrat von $\frac{a}{2}$, liefert das Minuszeichen eine negative Zahl, während x wegen $a \in \mathbb{N}$ positiv sein muß. Daher ist $x = \frac{a}{2} + \sqrt{1 + \frac{a^2}{4}}$.

e) Was erhalten Sie speziell für $a = 4$?

Lösung: $x = 2 + \sqrt{1+4} = 2 + \sqrt{5}$, ganz in Übereinstimmung mit *a)*.

Aufgabe 7: (*8 Punkte*)

a) Zeigen Sie, ausgehend von der Kongruenz $20206^2 \equiv 1 \bmod 54329$, daß $p = 54329$ keine Primzahl sein kann!

Lösung: Wäre p eine Primzahl, so wäre $\mathbb{Z}/p$ ein Körper, und dort hätte die quadratische Gleichung $x^2 = 1$ nur die beiden Lösungen $x = 1$ und $x = -1 = p - 1$. Da 20206 eine weitere Lösung ist, kann p nicht prim sein.

b) Wie lassen sich aus obiger Gleichung zwei nichttriviale Faktoren von p bestimmen? (Die Faktoren müssen nicht berechnet werden.)

Lösung: $20206^2 - 1 = 20205 \times 20207$ ist durch p teilbar, teilt aber keinen der beiden Faktoren. Daher sind $\mathrm{ggT}(20205, p)$ und $\mathrm{ggT}(20207, p)$ nichttriviale Faktoren.
($\mathrm{ggT}(20205, p) = 449$ ist prim und $\mathrm{ggT}(20207, p) = 121 = 11^2$.)

c) Führen Sie für p sowohl den FERMAT-Test als auch den Test von MILLER und RABIN für die Basis $a = 20206$ durch! Sie können dabei neben der Kongruenz aus *a)* auch noch benutzen, daß $p - 1 = 8 \times 6791$ ist und $a^{6791} \equiv a \bmod p$.

Lösung: Wegen $p - 1 = 8 \times 6791$ ist $2^3 = 8$ die maximale Zweierpotenz, durch die $p - 1$ teilbar ist. Für den Test von MILLER und RABIN muß zunächst $a^{6791} \equiv a \bmod p$ berechnet werden; das Quadrat davon ist modulo p gleich eins. Somit hat p den Test von MILLER und RABIN nicht bestanden. Da aber bereits $a^{2 \cdot 6791} \equiv a^2 \equiv 1 \bmod p$ ist, muß erst recht $a^{p-1} \equiv 1 \bmod p$ sein, so daß der FERMAT-Test die Zusammengesetztheit von p nicht erkennt.

Aufgabe 8: (*10 Punkte*)

Untersuchen Sie, welche der folgenden Kongruenzen lösbar sind, und bestimmen Sie gegebenenfalls eine Lösung:

a) $x^2 \equiv 7 \bmod 31$

Lösung: Da 31 eine Primzahl ist, können wir das über das LEGENDRE-Symbol entscheiden. Nach dem quadratischen Reziprozitätsgesetz gilt, da $7 \equiv 31 \equiv 3 \bmod 4$ ist,

$$\left(\frac{7}{31}\right) = -\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1 ,$$

denn die Eins ist natürlich ein Quadrat modulo drei. Somit ist die Kongruenz lösbar.
Da $31 \equiv 3 \bmod 4$ ist und $\frac{31+1}{4} = 8$, wissen wir, daß dann $7^8 \bmod 31$ eine Lösung sein muß. $7^2 \bmod 31 = 18$, $7^4 \equiv 18^2 = 324 \equiv 14 \bmod 31$ und $7^8 \equiv 14^2 = 196 \equiv 10 \bmod 31$. In der Tat ist $10^2 = 100 = 3 \cdot 31 + 7$.

b) $x^2 \equiv 11 \bmod 35$

Lösung: Da $35 = 5{\cdot}7$ 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 35 lösbar, wenn sie modulo fünf und modulo sieben lösbar ist. Modulo fünf wird sie zur Gleichung $x^2 \equiv 11 \bmod 5$ oder äquivalent $x^2 \equiv 1 \bmod 5$. Die ist natürlich lösbar, z.B. mit $x = 1$. Modulo sieben erhalten wir $x^2 \equiv 11 \equiv 4 \bmod 7$, auch das ist lösbar, z.B. mit $x = 2$. Somit ist auch die Ausgangsgleichung lösbar; wir erhalten eine Lösung, wenn wir nach dem chinesischen Restesatz ein x konstruieren mit $x \equiv 1 \bmod 5$ und $x \equiv 2 \bmod 7$. Der EUKLIDische Algorithmus, angewandt auf sieben und fünf gibt uns

$$\begin{aligned} 7 : 5 = 1 \quad \text{Rest } 2 &\Longrightarrow 2 = 7 - 5 \\ 5 : 2 = 2 \quad \text{Rest } 1 &\Longrightarrow 1 = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7 \end{aligned}$$

Somit ist

$$3 \cdot 5 = 15 \equiv \begin{cases} 1 \bmod 7 \\ 0 \bmod 5 \end{cases} \quad \text{und} \quad -14 \equiv \begin{cases} 0 \bmod 7 \\ 1 \bmod 5 \end{cases}.$$

Die Zahl $15{\cdot}2 - 14{\cdot}1 = 16$ ist daher kongruent eins modulo fünf und kongruent zwei modulo sieben und damit eine Lösung. In der Tat ist $16^2 = 256 = 7{\cdot}35 + 11$, d.h. $16^2 \equiv 11 \bmod 35$.

c) $x^2 \equiv 13 \bmod 37$

Lösung: 37 ist prim und kongruent eins modulo vier; nach dem quadratischen Reziprozitätsgesetz ist

$$\left(\frac{13}{37}\right) = \left(\frac{37}{13}\right) = \left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = (-1)^{(11^2-1)/8} = (-1)^{15} = -1\,.$$

Somit ist diese Kongruenz nicht lösbar.

d) Die natürliche Zahl n sei kongruent sieben modulo acht. Zeigen sie, daß n nicht als Summe dreier Quadratzahlen geschrieben werden kann! *(Hinweis: Betrachten Sie die Quadrate modulo acht!)*

Lösung: Quadrate modulo acht sind $0^2 = 0$, $1^2 = 7^2 = 1$, $2^2 = 6^2 = 4$ und $3^2 = 5^2 = 1$, also $0, 1$ und 4. Wäre $n = x^2 + y^2 + z^2$, so wäre modulo acht daher sieben eine Summe aus drei Summanden, die allesamt $0, 1$ oder 4 sein müssen. Offensichtlich muß es genau eine Vier geben. aber die restliche Drei läßt sich nicht als Summe von zwei Summanden aus $\{0, 1\}$ darstellen.