Wolfgang K. Seiler
Tel. 2515

A5, C201

31. August 2018

Modulklausur Zahlentheorie

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

Aufgabe 1: (*5 Punkte*)

a) a und b seien beliebige ganze Zahlen. Zeigen Sie, daß $10a + b$ genau dann durch sieben teilbar ist, wenn $a - 2b$ durch sieben teilbar ist.

Lösung: Ist $a - 2b$ durch sieben teilbar, so ist $a \equiv 2b \bmod 7$, also

$$10a + b \equiv 20b + b = 21b \equiv 0 \bmod 7\,.$$

Ist umgekehrt $10a + b$ durch sieben teilbar, so ist $b \equiv -10a \bmod 7$, also

$$a - 2b \equiv a + 20a = 21a \equiv 0 \bmod 7\,.$$

b) Gilt auch allgemeiner, daß $10a + b \equiv a - 2b \bmod 7$ für alle $a, b \in \mathbb{Z}$?

Lösung: Nein; schon für $a = b = 1$ sind $10a + b = 11$ und $a - 2b = -1$ nicht kongruent modulo sieben.

c) Wenden Sie *a)* mehrfach an um ohne Divisionen zu entscheiden, ob 12345 durch sieben teilbar ist!

Lösung: 12345 ist genau dann durch sieben teilbar, wenn $1234 - 2 \cdot 5 = 1224$ durch sieben teilbar ist. Dies wiederum ist genau dann durch sieben teilbar, wenn $122 - 2 \cdot 4 = 114$ durch sieben teilbar ist, was genau dann der Fall ist, wenn $11 - 2 \cdot 4 = 3$ durch sieben teilbar ist. Letzteres ist offensichtlich nicht der Fall.

Aufgabe 2: (*7 Punkte*)

a) Im August 2345 werden an der Rhineckar School of Commerce die Klausuren für den Studiengang Wirtschaftsmathematik geschrieben. Alle Studenten des dritten Studienjahrs sind pflichtangemeldet für die Klausuren Wirtschaftsalgebra, Wirtschaftsgeometrie und Wirtschaftszahlentheorie. Im Hörsaal werden die Studenten jeweils in der Reihenfolge ihres Eintreffens auf die zur Verfügung stehenden Plätze verteilt, so daß alle Reihen außer der letzten voll besetzt sind. In der letzten Reihe sitzt bei jeder Klausur genau ein Student.

Wirtschaftsalgebra wird in einem Hörsaal geschrieben, in dem unter Klausurbedingungen sieben Studenten in eine Reihe passen; elf Studenten sind nicht erschienen.

Wirtschaftsgeometrie wird in einem Hörsaal geschrieben, in dem neun Studenten in eine Reihe passen; zehn Studenten sind nicht erschienen.

Im Hörsaal für die Wirtschaftszahlentheorie passen nur fünf Studenten in eine Reihe; hier sind neun Studenten nicht erschienen.

Insgesamt sind 444 Studenten im Studiengang Wirtschaftsmathematik eingeschrieben, von denen natürlich weniger als die Hälfte im dritten Studienjahr sind. Wie viele Studenten sind im dritten Studienjahr?

Lösung: x sei die gesuchte Anzahl der Studenten im dritten Studienjahr. Dann ist

$$x-11 \equiv 1 \bmod 7\,, \quad x-10 \equiv 1 \bmod 9 \quad \text{und} \quad x-9 \equiv 1 \bmod 5\,,$$

also

$$x \equiv 12 \equiv 5 \bmod 7\,,\ x \equiv 11 \equiv 2 \bmod 9 \quad \text{und} \quad x \equiv 10 \equiv 0 \bmod 5\,.$$

Da sieben und neun teilerfremd sind, kann aus den ersten beiden Kongruenzen nach dem chinesischen Restesatz die Restklasse von x modulo $7 \cdot 9 = 63$ bestimmt werden: Der erweiterte EUKLIDische Algorithmus liefert

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

Somit ist

$$4 \cdot 7 = 28 \equiv \begin{cases} 0 & \bmod 7 \\ 1 & \bmod 9 \end{cases} \quad \text{und} \quad -3 \cdot 9 = -27 \equiv \begin{cases} 1 & \bmod 7 \\ 0 & \bmod 9 \end{cases},$$

also ist

$$28 \cdot 2 - 27 \cdot 5 = -79 \equiv \begin{cases} 5 & \bmod 7 \\ 2 & \bmod 9 \end{cases},$$

und damit $x \equiv -79 \equiv -16 \equiv 47 \bmod 63$.

Um noch die Kongruenz modulo fünf ins Spiel zu bringen, könnten wir den erweiterten EUKLIDischen Algorithmus auf 63 und 5 anwenden; einfacher ist es aber, nach einer Zahl k zu suchen derart, daß $47+63k$ durch fünf teilbar ist. Dies ist offensichtlich bereits für $k = 1$ der Fall, also ist $x \equiv 47 + 63 = 110 \bmod 315$. Da weniger als 222 Studenten im dritten Studienjahr sind, studieren dort also 110 Studenten.

b) Die Klausur in Wirtschaftszahlentheorie wird am letzten Freitag im August geschrieben. Welches Datum ist das?

Lösung: Falls der 31. August ein Donnerstag ist, fällt der letzte Freitag im August auf den 25. August; dies ist also der frühestmögliche Termin. Im Jahr 2345 fällt er auf den Wochentag mit der Nummer

$$\begin{aligned} &2344 + \left[\frac{2344}{4}\right] - \left[\frac{2344}{100}\right] + \left[\frac{2344}{400}\right] + 31 + 28 + 31 + 30 + 31 + 30 + 31 + 25 \bmod 7 \\ &\quad = 2344 + 586 - 23 + 5 + 237 \bmod 7 = 3149 \bmod 7 = 6\,, \end{aligned}$$

ist also ein Samstag. Der darauffolgende Freitag ist der $25 + 6 = 31$. August, wie dieses Jahr.

Aufgabe 3: *(6 Punkte)*

Bestimmen Sie alle ganzzahligen Lösungen des linearen Gleichungssystems

$$x + 2y + 3z = 101 \quad \text{und} \quad 2x - 7y + 8z = 102\,!$$

Lösung: Nach der ersten Gleichung ist $x = 101-2y-3z$; Einsetzen in die zweite Gleichung ergibt $202-11y+2z = 102$ oder $11y-2z = 100$. Der ggT von elf und zwei ist $1 = 11-5\cdot 2$, also ist $100 = 11 \cdot 100 - 2 \cdot 500$. Weiter ist $11 \cdot 2 - 2 \cdot 11$ die kleinstmögliche Darstellung der Null als zwei und elf, also ist die allgemeine Lösung $y = 100 + 2k$ und $z = 500 + 11k$ mit $k \in \mathbb{Z}$. Daraus folgt dann noch $x = 101 - 2y - 3z = -1599 - 37k$.

Einfacher wird es, wenn wir $k = j - 50$ setzen; dann ist

$$y = 2j, \quad z = -50 + 11j \quad \text{und} \quad x = 251 - 37j\,.$$

b) Bestimmen Sie alle Lösungen mit $x, y, z \in \mathbb{N}$!

Lösung: $y \in \mathbb{N}$ ist äquivalent zu $j \in \mathbb{N}$, und damit z in $\mathbb{N}$ liegt, muß sogar $j \geq 5$ sein. $x = 251 - 37j$ ist positiv für $j \leq 6$, also kommen nur $j = 5$ und $j = 6$ in Frage. Die entsprechenden Lösungstripel sind $x = 66, y = 10, z = 5$ und $x = 29, y = 12, z = 16$.

Aufgabe 4: *(8 Punkte)*

a) Berechnen Sie im Körper $\mathbb{F}_{97}$ die Elemente

$$x_1 = 10^2 + 11^2 + 12^2, \qquad x_2 = 31 \cdot 32 \quad \text{und} \quad x_3 = \frac{20}{33}$$

Lösung: In $\mathbb{F}_{97}$ ist $10^2 = 100 = 3$, $11^2 = 121 = 24$ und $12^2 = 144 = 47$, also ist $x_1 = 3 + 24 + 47 = 74$.
$31 \cdot 32 = 992 \equiv 22 \bmod 97$; also ist $x_2 = 22$.
Zur Berechnung von x_3 müssen wir zunächst über den erweiterten EUKLIDischen Algorithmus das multiplikative Inverse von 33 bestimmen:

$$\begin{aligned} 97 : 33 = 2 \text{ Rest } 31 &\Longrightarrow 31 = 97 - 2 \cdot 33 \\ 33 : 31 = 1 \text{ Rest } 2 &\Longrightarrow 2 = 33 - 31 = 33 - (97 - 2 \cdot 33) = 3 \cdot 33 - 97 \\ 31 : 2 = 15 \text{ Rest } 1 &\Longrightarrow 1 = 31 - 2 \cdot 15 = (97 - 2 \cdot 33) - 15 \cdot (3 \cdot 33 - 97) = 16 \cdot 97 - 47 \cdot 33 \end{aligned}$$

Das multiplikative Inverse von 33 in $\mathbb{F}_{97}$ ist also $-47 = 50$, und

$$x_3 = \frac{20}{33} = 20 \cdot 50 = 1000 = 30\,.$$

Zur Probe können wir noch nachrechnen, daß in der Tat $30 \cdot 33 = 990 \equiv 20 \bmod 97$ ist.

b) Im Körper $\mathbb{F}_{103}$ hat die Zwei die Ordnung 51. (Das müssen Sie nicht beweisen.) Zeigen Sie: Wenn es ein Element $x \in \mathbb{F}_{103}$ gibt mit $x^2 = 2$, so ist entweder x oder $-x$ eine primitive Wurzel.

Lösung: Die geraden Potenzen von x und von $-x$ sind genau die Potenzen von zwei; davon gibt es 51 verschiedene. Somit haben beide mindestens die Ordnung 51. Da die Ordnung nach dem kleinen Satz von FERMAT ein Teiler von 102 sein muß, ist sie entweder 102 oder 51. Hat x die Ordnung 102, so ist x eine primitive Wurzel. Andernfalls hat x die Ordnung 51 und $(-x)^{51} = (-1)^{51} \cdot x^{51} = -1$; also hat $-x$ die Ordnung 102 und ist primitive Wurzel.

c) Geben Sie eine Formel an, mit der man ein x mit $x^2 = 2$ in $\mathbb{F}_{103}$ bestimmen kann – sofern ein solches x existiert.

Lösung: $103 \equiv 3 \bmod 4$; falls es ein solches x gibt, ist daher auch $y = 2^{104/4} = 2^{26}$ eine Lösung, denn nach dem kleinen Satz von FERMAT ist $y^2 = 2^{52} = 2^{51} \cdot 2 = 2$ in $\mathbb{F}_{103}$.
(Hier ist $2^{26} = 38$; 38 hat die Ordnung 51, aber $-38 = 65$ ist primitive Wurzel.)

d) Nun sei p eine beliebige Primzahl. Bestimmen Sie in Abhängigkeit von p die drei Elemente

$$S = \sum_{x \in \mathbb{F}_p} x\,, \qquad P_1 = \prod_{x \in \mathbb{F}_p} x \quad \text{und} \quad P_2 = \prod_{x \in \mathbb{F}_p^\times} x\,!$$

Lösung: Für $p = 2$ ist $S = 0+1 = 1$; für $p \neq 2$ ist p ungerade, d.h. für jedes $x \neq 0$ aus $\mathbb{F}_p$ ist $-x \neq x$. In der Summe aller Elemente treten also die von Null verschiedenen Elemente in Paaren additiv inverser Elemente auf, so daß die Summe gleich Null ist.

Da $0 \in \mathbb{F}_p$, ist natürlich $P_1 = 0$ für alle p.

Für P_2 verwenden wir die WILSONsche Kongruenz, wonach $(p-1)! = \prod_{i=1}^{p-1} i \equiv -1 \bmod p$ ist; somit ist $P_2 = -1$ für alle p. (Für $p = 2$ ist natürlich $-1 = 1$, so daß man hier kürzer auch $P_2 = 1$ schreiben könnte.)

Aufgabe 5: (*11 Punkte*)

a) Zerlegen Sie die Zahl $N = 37!$ in ihre Primfaktoren!

Lösung: Von den Zahlen zwischen eins und 37 sind die Hälfte durch zwei teilbar, jede vierte sogar durch vier, jede achte durch acht und so weiter; die Primzahl zwei hat in der Primzerlegung also den Exponenten

$$\sum_{i=1}^{\infty} \left[\frac{37}{2^i}\right] = 18 + 9 + 4 + 2 + 1 = 34\,.$$

Für die Drei erhalten wir entsprechend

$$\sum_{i=1}^{\infty} \left[\frac{37}{3^i}\right] = 12 + 4 + 1 = 17\,,$$

für die Fünf

$$\left[\frac{37}{5}\right] + \left[\frac{37}{25}\right] = 7 + 1 = 8\,.$$

Alle übrigen Primzahlen p können in einer Zahl kleiner oder gleich 37 höchstens in der ersten Potenz auftreten; die Anzahl der durch p teilbaren Zahlen und damit der Exponent von p in der Primzerlegung von N ist also $[37/p]$. Für $19 \leq p \leq 37$ ist das eins; für $p = 7$ erhalten wir fünf, für $p = 11$ drei und für $p = 13$ oder 17 ist es zwei. Somit ist

$$N = 2^{34} \cdot 3^{17} \cdot 5^8 \cdot 7^5 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37\,.$$

b) Zeigen Sie: Ist $N + i$ eine Primzahl, so muß $\mathrm{ggT}(i, N) = 1$ sein.

Lösung: Der ggT ist ein Teiler von $N+i$; falls er ungleich eins ist, kann $N+i$ daher nicht prim sein.

c) Man kann zeigen, daß $P = N + 1$ prim ist. Q sei die nächstgrößere Primzahl. Geben Sie eine möglichst gute untere Schranke für $Q - P$ an!

Lösung: Wir suchen ein $i \geq 2$, das teilerfremd zu N ist, also keinen Primteiler kleiner oder gleich 37 hat. Das kleinste soche i ist die nächste Primzahl nach 37, also 41. Somit ist $N+41 = P+40$ die kleinste Zahl, von der wir nicht offensichtlich ausschließen können, daß sie prim ist. Wir wissen somit, daß $Q - P \geq 40$ sein muß. (Tatsächlich ist $N+41$ nicht prim und $Q - P = 126$.)

d) Entscheiden Sie für jede der drei Zahlen $r = 31, 41, 64$, ob es in $(\mathbb{Z}/P)^\times$ Elemente der Ordnung r gibt, und bestimmen Sie gegebenenfalls deren Anzahl!

Lösung: Da P prim ist, ist $(\mathbb{Z}/P)^\times$ eine zyklische Gruppe der Ordnung $P - 1 = N = 37!$; g sei ein Erzeugendes dieser Gruppe. Für jeden Teiler d von N erzeugt dann $g^{N/d}$ eine

Gruppe der Ordnung d; es gibt also Elemente der Ordnung d. Da die Ordnung eines jeden Elements die Gruppenordnung teilen muß, gibt es somit genau dann Elemente der Ordnung d, wenn d Teiler von N ist. Dies ist bei 31 und $64 = 2^6$ der Fall, nicht aber bei 41.

Die Elemente der Ordnung d sind im Körper $\mathbb{Z}/P$ Lösungen der Gleichung $x^d = 1$; da eine Polynomgleichung in einem Körper höchstens so viele Lösungen haben kann, wie ihr Grad angibt, gibt es höchstens d. Diese haben aber nicht alle die Ordnung d; die Ordnung könnte auch ein Teiler von d sein.

$r = 31$ ist eine Primzahl; eine Lösung der Gleichung $x^{31} = 1$ hat also entweder die Ordnung 31 oder eins; letzteres ist nur für $x = 1$ der Fall. Somit gibt es 30 Elemente der Ordnung 31.

$r = 64$ ist eine Zweierpotenz; eine Lösung der Gleichung $x^{64} = 1$ hat also Zweipotenzordnung. Alle x, deren Ordnung kleiner als 64 ist, sind Lösungen von $x^{32} = 1$; wegen $x^{64} - 1 = (x^{32} + 1)(x^{32} - 1)$ sind die Elemente der Ordnung 64 die 32 Nullstellen von $x^{32} = -1$; es gibt also 32 solche Elemente.

(Alternativ könnte man auch benutzen, daß $\varphi(31) = 30$) und $\varphi(64) = 32$ ist.)

e) Hat die Kongruenz $x^2 \equiv 3 \bmod 37$ ganzzahlige Lösungen?

Lösung: Da 37 eine Primzahl ist, gilt dies genau dann, wenn das LEGENDRE-Symbol $\left(\frac{3}{37}\right) = 1$ ist. Da $37 \equiv 1 \bmod 4$ ist, gilt nach dem quadratischen Reziprozitätsgesetz

$$\left(\frac{3}{37}\right) = \left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1\,,$$

denn eins ist natürlich ein quadratischer Rest modulo drei. Somit ist die Kongruenz lösbar.

f) Hat die Kongruenz $x^2 \equiv 3 \bmod 185$ ganzzahlige Lösungen? ($185 = 5 \cdot 37$.)

Lösung: Dies ist genau dann der Fall, wenn die entsprechenden Kongruenzen modulo fünf und modulo 37 lösbar sind. Nach der vorigen Teilaufgabe klappt es für 37, aber $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$, da zwei kein quadratischer Rest modulo drei ist. Somit ist die Kongruenz nicht lösbar.

Aufgabe 6: *(7 Punkte)*

a) Die Zahl $N = 17\,690\,411$ ist Produkt zweier ungefähr gleich großer Primzahlen. Bestimmen Sie diese!

Lösung: In dieser Situation bietet sich das Verfahren von FERMAT an, d.h. wir suchen ein i, für das $N + i^2$ eine Quadratzahl ist. Für $i = 0, 1, 2, 3, 4$ ist $\sqrt{N + i^2}$ keine ganze Zahl, aber

$$N + 5^2 = 17\,690\,436 = 4206^2\,.$$

Somit ist $N = 4206^2 - 5^2 = (4206 - 5)(4206 - 5) = 4201 \cdot 4211$

b) Wenn wir alle Empfehlungen bezüglich der Größe der Parameter ignorieren, können wir N als RSA-Modul verwenden. Bestimmen Sie den kleinstmöglichen Exponenten, mit dem das funktioniert!

Lösung: e muß teilerfremd sein zu $p - 1 = 4200 = 42 \cdot 100 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$ und zu $q - 1 = 4210$. Damit muß e insbesondere ungerade sein und darf auch nicht durch drei, fünf oder sieben teilbar sein; die kleinste zu $p - 1$ teilerfremde Zahl ist also elf. Elf ist auch teilerfremd zu $q - 1 = 4210$, denn sonst wäre 421 durch elf teilbar und damit auch

$440 - 421 = 19$, was offensichtlich nicht der Fall ist. Somit ist $e = 11$ der kleinstmögliche öffentliche Exponent.

c) Finden Sie dazu einen möglichst kleinen privaten Exponenten d!

Lösung: $p-1$ und $q-1$ sind beide durch zehn teilbar, und das ist auch ihr ggT, denn zwei Zahlen mit Differenz zehn können keinen größeren ggT haben. Das kleinste gemeinsame Vielfache von $p-1$ und $q-1$ ist daher

$$\lambda = \frac{(p-1)(q-1)}{10} = 4200 \cdot 421 = 1\,768\,200\,.$$

Wir müssen eins als Linearkombination aus dieser Zahl und elf ausdrücken, also den erweiterten EUKLIDischen Algorithmus anwenden:

$$\begin{aligned} 1\,768\,200 : 11 = 160\,745 \text{ Rest } 5 &\Longrightarrow 5 = 1\,768\,200 - 11 \cdot 160\,745 \\ 11 : 5 = 2 \text{ Rest } 1 &\Longrightarrow 1 = 11 - 2 \cdot (1\,768\,200 - 11 \cdot 160\,745) = 321\,491 \cdot 11 - 2 \cdot 1\,768\,200\,. \end{aligned}$$

Somit können wir $d = 321\,491$ wählen.

Aufgabe 7: *(6 Punkte)*

a) Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{26}$!

Lösung: Da $5^2 < 10 < 6^2$, ist der ganzzahlige Anteil fünf; der Kehrwert der Differenz ist

$$\frac{1}{\sqrt{26}-5} = \frac{\sqrt{26}+5}{26-5^2} = 5 + \sqrt{26}$$

und hat ganzzahligen Anteil zehn. Den Kehrwert der Differenz ist

$$\frac{1}{\sqrt{26}-5} = \frac{\sqrt{26}+5}{26-5^2} = 5 + \sqrt{26}\,,$$

wie im vorigen Schritt. Also ist die Kettenbruchentwicklung ab hier periodisch:

$$\sqrt{26} = 5 + \cfrac{1}{10 + \cfrac{1}{10 + \cfrac{1}{10 + \cdots}}}\,.$$

b) Finden Sie eine ganzzahlige Lösung der Gleichung $x^2 - 26y^2 = 1$ sowie eine der Gleichung $x^2 - 26y^2 = -1$!

Lösung: Aus $x^2 - 26y^2 = \pm 1$ folgt

$$\left(\frac{x}{y}\right)^2 - 26 = \left(\frac{x}{y} - \sqrt{26}\right)\left(\frac{x}{y} + \sqrt{26}\right) = \pm\frac{1}{y^2} \Longrightarrow \frac{x}{y} - \sqrt{26} = \pm\frac{1}{y^2\left(\frac{x}{y} + \sqrt{26}\right)}\,.$$

Wegen $\left(\frac{x}{y}\right)^2 > 1$ ist $\frac{x}{y} > \sqrt{26}$, also ist der Nenner rechts insbesondere größer als $2y^2$, und damit muß x/y nach LEGENDRE eine Konvergente der Kettenbruchentwicklung von $\sqrt{26}$ sein.

Wir müssen also die Nenner und Zähler der Konvergenten der Kettenbruchentwicklung durchprobieren. $5 = \frac{5}{1}$ liefert $5^2 - 26 \cdot 1^2 = -1$, löst also die zweite Gleichung. Die nächste Konvergente ist $5\frac{1}{10} = \frac{51}{10}$, und $51^2 - 26 \cdot 10^2 = 1$. Somit ist $x = 51, y = 10$ eine Lösung der ersten Gleichung.

c) Finden Sie einen Näherungsbruch mit möglichst kleinem Nenner, der sich höchstens um 10^{-4} von $\sqrt{26}$ unterscheidet! Beweisen Sie diese Schranke, ohne die Dezimaldarstellung von $\sqrt{26}$ zu verwenden!

Lösung: Die besten Näherungen sind die Konvergenten der Kettenbruchentwicklung; ist p/q eine solche Konvergente, so ist der Betrag der Abweichung kleiner als $1/q^2$. Für eine Abweichung von höchstens 10^{-4} brauchen wir also eine Konvergente mit Nenner mindestens hundert. Bei den beiden in *b)* berechneten Konvergenten ist das noch nicht der Fall; wir müssen also die nächste Berechnen. Diese ist $5\frac{10}{101} = \frac{515}{101}$, und die löst unser Problem.

Aufgabe 8: (*10 Punkte*)

a) Zeigen Sie: Jedes Element $x \in \mathbb{Z} \oplus \mathbb{Z}i$, dem Ring der Gaussschen Zahlen, mit primer Norm ist irreduzibel.

Lösung: Angenommen, $x = yz$ läßt sich als Produkt zweier Gaussscher Zahlen schreiben. Wegen der Multiplikativität der Norm ist dann $N(x) = N(y)N(z)$, und da $N(x)$ eine Primzahl ist, muß damit entweder $N(y)$ oder $N(z)$ gleich eins sein. Damit ist in jeder Produktdarstellung $x = yz$ einer der beiden Faktoren eine Einheit, d.h. x ist irreduzibel.

b) Zerlegen Sie $85i$ im Ring $\mathbb{Z} \oplus \mathbb{Z}i$ in ein Produkt irreduzibler Element!

Lösung: $85 = 5 \cdot 17$ ist ein Produkt zweier Primzahlen kongruent eins modulo vier, beide lassen sich also weiter zerlegen. Wegen $5 = 2^2 + 1^2$ und $17 = 4^2 + 1^2$ ist

$$5 = (2+i)(2-i) = (1+2i)(1-2i) \quad \text{und} \quad 17 = (4+i)(4-i) = (1+4i)(1-4i)\,.$$

Somit ist $85i$ beispielsweise das Produkt

$$85i = (2+i)(2-i)(4+i)(4+i)i\,.$$

Außer dem Faktor i sind alle Faktoren irreduzibel, denn $N(2 \pm i) = 5$ und $N(4 \pm i) = 5$ sind Primzahlen. Die Einheit i können wir in irgendeinen der übrigen Faktoren hineinziehen, ohne etwas an dessen Irreduzibilität zu ändern, z.B. in den ersten. Damit ist

$$85i = (2i-1)(2-i)(4+i)(4-1)\,.$$

c) Finden Sie, ausgehend von *b)*, alle Darstellungen von 85 als Summe zweier Quadrate!

Lösung: Da 85 Produkt zweier Primzahlen kongruent eins modulo vier ist, gibt es bis auf Reihenfolge zwei solche Darstellungen. In der Zerlegung $85 = (2+i)(2-i)(4+i)(4-i)$ können wir einmal die Faktoren mit plus zusammenfassen zu

$$85 = \big((2+i)(4+i)\big)\big((2-i)(4-i)\big) = (7+6i)(7+6i) = 7^2 + 6^2$$

oder wir fassen Faktoren mit verschiedenem Zeichen zusammen:

$$85 = \big((2+i)(4-i)\big)\big((2-i)(4+i)\big) = (9+2i)(9-2i) = 9^2 + 2^2\,.$$

d) Bestimmen Sie alle Elemente der Norm 85 in $\mathbb{Z} \oplus \mathbb{Z}i$!

Lösung: Die Norm von $a + bi$ ist $a^2 + b^2$; nach *c)* ist das genau für die Zahlen $\pm 7 \pm 6i$ und $\pm 6 \pm 7i$, $\pm 9 \pm 2i$ und $\pm 2 \pm 9i$ gleich 85.

e) Leiten Sie aus dem Ergebnis von *d)* eine Darstellung von π als Linearkombination geeigneter Arkustangenswerte ab!

Lösung: Auf dem Kreis mit Radius $\sqrt{85}$ um den Nullpunkt O liegen die Punkte

$$P_1 = (9,2), \quad P_2 = (7,6), \quad P_3 = (6,7), \quad P_4 = (2,9)$$

sowie noch $P_0 = \left(\sqrt{85}, 0\right)$ und $P_5 = \left(0, \sqrt{85}\right)$. Alles ist symmetrisch zur ersten Winkelhalbierenden, d.h.

$$< OP_0P_1 = < OP_4P_5 \quad \text{und} \quad < OP_1P_2 = < OP_3P_4 \,.$$

Damit ist

$$\frac{\pi}{2} = < OP_0P_5 = 2 < OP_0P_1 + 2 < OP_1P_2 + < OP_2P3 \,,$$

also

$$\pi = 4 < OP_0P_1 + 4 < OP_1P_2 + 2 + < OP_2P3 \,.$$

Projizieren wir P_1 senkrecht auf die Gerade OP_0, erhalten wir einen Punkt $P_1' = (9,0)$, der zusammen mit O und P_1 ein rechtwinkliges Dreieck bildet. Die Gegenkathete $\overline{P_1'P_1}$ des Winkels bei O hat die Länge zwei, die Ankathete Länge neun, also ist

$$\tan < OP_0P_1 = \frac{2}{9} \quad \text{und} \quad < OP_0P_1 = \arctan \frac{2}{9} \,.$$

Für die übrigen Winkel müssen wir den Satz vom Innenwinkel anwenden, um rechtwinklige Dreiecke zu bekommen: Bezeichnet Q_i den an der y-Achse gespiegelten Punkt P_i, so ist

$$< OP_iP_{i+1} = 2 < Q_iP_iP_{i+1} \,.$$

Bezeichnet P_i' den auf die Gerade Q_iP_i projizierten Punkt P_{i+1}, so ist $\triangle Q_iP_i'P_{i+1}$ ein rechtwinkliges Dreieck, dessen Winkel bei Q_i wir berechnen können.
Für $i = 1$ ist $P_1 = (9,2)$, also $Q_1 = (-9,2)$, und die Projektion von $P_2 = (7,6)$ auf die Gerade Q_1P_1 ist $P_1' = (7,2)$. Die Gegenkathete $P_1'P_2$ hat somit die Länge $6 - 2 = 4$, und für die Ankathete erhalten wir $9 + 7 = 16$. Somit ist

$$\tan < Q_1P_1'P_2 = \frac{4}{16} = \frac{1}{4} \quad \text{und} \quad < OP_1P_2 = 2 < Q_1P_1'P_2 = 2 \arctan \frac{1}{4} \,.$$

Entsprechend haben wir für $i = 2$ die Punkte $P_2 = (7,6)$ und $P_3 = (6,7)$; hier ist also $Q_2 = (-7,6)$ und $P_2' = (6,6)$. Die Ankathete hat somit Länge eins und die Gegenkathete Länge dreizehn, d.h.

$$\tan < Q_2P_2'P_3 = \frac{1}{13} \quad \text{und} \quad < OP_2P_3 = 2 < Q_2P_2'P_3 = 2 \arctan \frac{1}{13} \,.$$

Einsetzen in die obige Formel führt auf das Ergebnis

$$\pi = 4 \arctan \frac{2}{9} + 8 \arctan \frac{1}{4} + 4 \arctan \frac{1}{13} \,.$$