Klausur zur Elementaren Zahlentheorie
Sommersemester 2017
04.08.2017, 14:30 - 16:30 Uhr

Bergische Universität Wuppertal
PD Dr. Thorsten Weist
Dr. Martin Bender

Bitte tragen Sie die folgenden Daten leserlich und in Blockschrift ein:

Name	Vorname	Matrikelnummer
Geburtsort	Geburtsdatum	Studiengang

Aufgabe	1	2	3	4	5	6	7	8	$\sum$	Note
Max. Punktzahl	4	4	4	4	3	3	3	3	28	
erreichte Punktzahl										

Es gelten die Notationen aus der Vorlesung. Alle Beweis- und Rechenschritte müssen erläutert werden.

Aufgabe 1

a) Für welche Zahlen $a \in \mathbb{Z}$ ist die Kongruenz

$$ax \equiv 5 \bmod 12$$

lösbar?

b) Geben Sie die Lösungsmenge des folgenden Systems von simultanen Kongruenzen an:

$$x \equiv 2 \bmod 11$$
$$x \equiv 2 \bmod 12$$
$$5x \equiv 2 \bmod 13$$

a) Die Kongruenz ist genau dann lösbar, wenn $\mathrm{ggT}(a, 12) \mid 5$, also genau dann, wenn a und 12 teilerfremd sind, da 5 kein Teiler von 12 ist; also für $a \in \mathbb{Z}$, so dass $[a]_{12} \in \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$.

b) Die dritte Kongruenz ist äquivalent zu $x \equiv 3 \bmod 13$. Mit dem Algorithmus aus der Vorlesung erhält man die Lösungsmenge $926 + 1716\mathbb{Z}$.

Aufgabe 2

a) Ist die Gleichung $x^2 = [-20]_{31}$ im Ring $\mathbb{Z}/31\mathbb{Z}$ lösbar?

b) Ist die Gleichung $x^2 = [42]_{47}$ im Ring $\mathbb{Z}/47\mathbb{Z}$ lösbar?

c) Zeigen Sie, dass

$$\left(\frac{-2}{p}\right) = 1$$

für alle Primzahlen $p \in \mathbb{P}$ mit $p \equiv 1 \bmod 32$.

a,b) Man rechnet mit den Sätzen aus der Vorlesung nach, dass

$$\left(\frac{-20}{31}\right) = \left(\frac{11}{31}\right) = -1 \text{ und } \left(\frac{42}{47}\right) = 1,$$

was zeigt, dass die erste Kongruenz nicht lösbar ist und die zweite lösbar.

c) Da $p \equiv 1 \bmod 32$ nach Voraussetzung, folgt $p \equiv 1 \bmod 4$ und $p \equiv 1 \bmod 8$. Somit folgt aus den Ergänzungssätzen des QRP, dass

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$$

und somit die Behauptung.

Aufgabe 3

Geben Sie Primfaktorzerlegungen von $a = 15$ und $b = 9 + 18i$ in $\mathbb{Z}[i]$ an und bestimmen Sie einen größten gemeinsamen Teiler von a und b in $\mathbb{Z}[i]$.

Es gilt $15 = 3{\cdot}5 = 3{\cdot}(1{+}2i){\cdot}(1{-}2i)$. Da $3 \equiv 3 \bmod 4$, ist 3 prim in $\mathbb{Z}[i]$ und da $N(1{+}2i) = N(1{-}2i) = 5 \in \mathbb{P}$, sind auch die anderen beiden Faktoren prim. Somit ist das eine Primfaktorzerlegung von 15. Weiter gilt $(9{+}18i) = 3^2(1+2i)$. Damit ist das mit dem gleichen Argument eine Primfaktorzerlegung von $9 + 18i$. An den Zerlegungen kann man auch ablesen, dass $3(1 + 2i)$ ein ggT ist. Alternativ kann man den euklidischen Algorithmus benutzen.

Aufgabe 4

Betrachten Sie die Gruppe $G = (\mathbb{Z}/13\mathbb{Z})^*$.

a) Bestimmen Sie alle Primitivwurzeln von G.

b) Bestimmen Sie alle Elemente der Ordnungen 4 und 5 in G.

a) Man rechnet nach, dass $[2]_{13}$ eine Primitivwurzel ist. Aus der Vorlesung folgt

$$\operatorname{ord}([2]_{13}^k) = \frac{\operatorname{ord}([2]_{13})}{\operatorname{ggT}((\operatorname{ord}([2]_{13}), k)}.$$

Damit erhält man, dass $[2]_{13}^5 = [6]_{13}$, $[2]_{13}^{11} = [7]_{13}$ und $[2]_{13}^7 = [11]_{13}$ die weiteren Primitivwurzeln sind. Außerdem folgt mit der Formel, dass es keine Elemente der Ordnung der 5 gibt und dass $[8]_{13}$ und $[5]_{13}$ die Ordnung 4 haben.

Aufgabe 5

Zeigen Sie, dass für alle Primzahlen $p, q \in \mathbb{Z}$, wobei $p \neq q$, gilt, dass

$$[p^{q-1} + q^{p-1}]_{pq} = [1]_{pq} \text{ in } \mathbb{Z}/pq\mathbb{Z}.$$

Es ist zu zeigen, dass $pq \mid p^{q-1} + q^{p-1} - 1$. Da $p \neq q$ erhält man aus dem kleinen Satz von Fermat, dass $[p^{q-1}]_q = [1]_q$ und $[q^{p-1}]_p = [1]_p$ und somit $q \mid p^{q-1} - 1$ und $p \mid q^{p-1} - 1$. Außerdem gilt offenbar $p \mid p^{q-1}$ und $q \mid q^{p-1}$ und somit $p \mid p^{q-1} + q^{p-1} - 1$ und $q \mid p^{q-1} + q^{p-1} - 1$. Da $\operatorname{ggT}(p, q) = 1$, folgt damit die Behauptung.

Aufgabe 6

a) Sei $a \in \mathbb{Z}$ beliebig. Zeigen Sie, dass die Gleichung $x^2 + y^2 = 11a^2$ keine Lösung in $\mathbb{Z}$ hat.

b) Zeigen Sie mithilfe von a), dass $x^2 + y^2 = 11$ keine Lösung in $\mathbb{Q}$ hat.

a) Der Faktor 11 kommt in der Primfaktorzerlegung von $11a^2$ mit ungeradem Exponenten vor. Da $11 \equiv 3 \bmod 4$, kann $11a^2$ nach einem Satz aus der Vorlesung nicht als Summe von zwei Quadraten geschrieben werden.

b) Wäre $x = \frac{x_1}{x_2}$, $y = \frac{y_1}{y_2}$ mit $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ eine rationale Lösung, so würde folgen, dass

$$(y_2x_1)^2 + (x_2y_1)^2 = y_2^2x_1^2 + x_2^2y_1^2 = 11x_2^2y_2^2 = 11(x_2y_2)^2$$

mit $(y_2x_1), (x_2y_1), (x_2y_2) \in \mathbb{Z}$ im Widerspruch zum ersten Teil.

Aufgabe 7

Zeigen Sie, dass für alle ganzen Zahlen n und für $x = 2, 3, 5$ gilt, dass $x \mid n^5 - n$. Folgern Sie, dass $30 \mid n^5 - n$ für alle ganzen Zahlen n.

Es gilt

$$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n - 1)n(n + 1)(n^2 + 1).$$

Da also drei aufeinanderfolgende Zahlen $n - 1, n, n + 1$ als Faktoren auftreten, folgt $2, 3 \mid n^5 - n$. Da nach Satz von Euler-Fermat gilt, dass $[n^5]_5 = [n]_5$ für alle ganzen Zahlen n, folgt $5 \mid n^5 - n$. Da 2, 3 und 5 paarweise teilerfremd sind, folgt damit $2 \cdot 3 \cdot 5 = 30 \mid n^5 - n$.

Aufgabe 8

Beweisen oder widerlegen Sie folgende Aussagen:

a) Gilt $\mathrm{ggT}(x, 6) = 1$ für eine ganze Zahl x, so folgt $x \equiv \pm 1 \bmod 6$.

b) Für alle ganzen Zahlen $x \geq 1$ gilt, dass $\sum_{i=0}^{n-1} x^i \mid x^n - 1$.

c) Gilt $p = 4q + 1$ für zwei ungerade Primzahlen p, q, so ist die Kongruenz $x^2 \equiv 2 \bmod p$ lösbar für alle $x \in \mathbb{Z}$.

Die erste Aussage ist wahr, da aus $\mathrm{ggT}(x, 6) = 1$ folgt, dass $x = 6k \pm 1$ für ein $k \in \mathbb{Z}$ und somit $x \equiv \pm 1 \bmod 6$.

Auch die zweite Aussage ist wahr, da

$$x^n - 1 = (x - 1)(\sum_{i=0}^{n-1} x^i)$$

für alle ganzen Zahlen x.

Die dritte Aussage ist falsch, da für $q = 3$ bzw. $p = 13$ gilt, dass $\left(\frac{2}{13}\right) = -1$, da $13 \equiv 5 \bmod 8$.