Routine-Zettel 2

1. Bestimme mit dem Euklid'schen Algorithmus den größten gemeinsamen Teiler von 11 917 und 12 053.

2. Bestimme mit dem Euklid'schen Algorithmus eine Bézout-Gleichung für den größten gemeinsamen Teiler von 13 und 23.

3. Wie zeigt man mit dem Sieb des Eratosthenes, dass 151 eine Primzahl ist? (Anzugeben sind die Primzahlen, die man schon kennen muss.)

4. Gesucht ist x mit

$$\begin{aligned} x &\equiv 2 \mod 17, \\ x &\equiv 3 \mod 19, \\ x &\equiv 4 \mod 23. \end{aligned}$$

Verwende dabei die folgenden Bézout-schen Gleichungen:

$$\begin{aligned} 1 &= 180 \cdot 17 + (-7) \cdot 19 \cdot 23 \\ 1 &= (-144) \cdot 19 + 7 \cdot 17 \cdot 23 \\ 1 &= (-14) \cdot 23 + 1 \cdot 17 \cdot 19. \end{aligned}$$

5. Wir betrachten den Polynomring $\mathbb{Z}[X]$ in einer Variablen X. Zeige: Das Polynom $X^2 - 1$ teilt das Polynom $X^{2n} - 1$

6. Zeige: Für jedes $a \in \mathbb{Z}$ gilt $a^{193} \equiv a \mod 195$.

7. Welche Elemente im Ring $\mathbb{Z}/323$ sind nilpotent? Welche Elemente sind Nullteiler? Anmerkung: $(323 = 17 \cdot 19)$

8. Man gebe alle invertierbaren Elemente in $\mathbb{Z}/15$ an.

9. Man zeige, dass 3 eine Primitivwurzel modulo 7 ist.

10. Man zeige, dass 2 keine Primitivwurzel modulo 7 ist.

11. Welche Struktur hat die Gruppe $(\mathbb{Z}/32)^*$?

12. Welche Struktur hat die Gruppe $(\mathbb{Z}/315)^*$?

Hinweis zu den Aufgaben 11 und 12: Gesucht sind Zahlen $t_1, \ldots, t_r$, so dass die jeweilige Gruppe isomorph zu $C_{t_1} \times \cdots \times C_{t_r}$ ist.

13. Zeige: Die Gruppe $(\mathbb{Z}/17, +) \times (\mathbb{Z}/19, +)$ ist zyklisch.

1. Use the Euclidean algorithm in order to determine the greatest common divisor of 11 917 und 12 053.

2. Use the Euclidean algorithm in order to exhibit a Bézout equation for the greatest common divisor of 13 and 23.

3. What has one to do in order to show that 151 is a prime (using the sieve of Eratosthenes)? (We ask for the set of primes which already have been known.)

4. Determine x with

$$\begin{aligned} x &\equiv 2 \mod 17, \\ x &\equiv 3 \mod 19, \\ x &\equiv 4 \mod 23. \end{aligned}$$

using the following Bézout equations:

$$\begin{aligned} 1 &= 180 \cdot 17 + (-7) \cdot 19 \cdot 23 \\ 1 &= (-144) \cdot 19 + 7 \cdot 17 \cdot 23 \\ 1 &= (-14) \cdot 23 + 1 \cdot 17 \cdot 19. \end{aligned}$$

5. Consider the polynomial ring $\mathbb{Z}[X]$ in the variable X. Show that $X^2 - 1$ divides $X^{2n} - 1$

6. Show: Every $a \in \mathbb{Z}$ satisfies $a^{193} \equiv a \mod 195$.

7. Which elements of the ring $\mathbb{Z}/323$ are nilpotent? Which elements are zero-divisors? Note: $(323 = 17 \cdot 19)$

8. List all the invertible elements of $\mathbb{Z}/15$.

9. Show that 3 is a primitive root modulo 7.

10. Show that 2 is not a primitive root modulo 7.

11. Determine the structure of the group $(\mathbb{Z}/32)^*$.

12. Determine the structure of the group $(\mathbb{Z}/315)^*$.

Remark for 11 and 12: We ask for numbers $t_1, \ldots, t_r$, such that the corresponding group is isomorphic to $C_{t_1} \times \cdots \times C_{t_r}$.

13. Show: The group $(\mathbb{Z}/17, +) \times (\mathbb{Z}/19, +)$ is cyclic.