# Proseminar Algebra 1
# WS 2012/13

## 10. und 11. Dezember 2012

52) Erläutern Sie den Chinesischen Restsatz für ganze Zahlen.
Drei Sender $S$, $T$, $U$ senden über eine gemeinsame Leitung. Die Zeit zwischen den ausgesandten Impulsen beträgt für $S$ fünf Sekunden, für $T$ acht Sekunden und für $U$ elf Sekunden. $T$ beginnt drei Sekunden nach $S$, $U$ sieben Sekunden nach $T$ zu senden. Die Leitung kann zugleich höchstens zwei Impulse übertragen. Wann ist sie überlastet?

53) Berechnen Sie alle Zahlen $x \in \mathbb{Z}$ mit

$$x \equiv 14 \; mod \; 4 \; , \quad x \equiv 2 \; mod \; 7 \; , \quad x \equiv -3 \; mod \; 15$$

und alle Zahlen $y \in \mathbb{Z}$ mit

$$y \equiv 13 \; mod \; 4 \; , \quad y \equiv -11 \; mod \; 7 \; , \quad y \equiv -1 \; mod \; 15 \; .$$

54) Erläutern Sie den Chinesischen Restsatz für Polynome.
Berechnen Sie ein Polynom $f \in \mathbb{Q}[x]$ minimalen Grades so, dass

$$f - (x-7) \text{ ein Vielfaches von } x^2 + 2x + 2,$$

$$f - (x^2 - 2x + 1) \text{ ein Vielfaches von } (x+1)^3$$

und

$$f - (x-2) \text{ ein Vielfaches von } (x-1)^2$$

ist.

55) Berechnen Sie eine Zahl $a \in \mathbb{Z}$ mit der Eigenschaft

$$\overline{a}^{13} = \overline{447} \in \mathbb{Z}_{667} \ .$$

Wieviele positive ganze Zahlen sind kleiner als $11^2 \cdot 17^2 = 34969$ und teilerfremd zu dieser Zahl?

56) Erläutern Sie das RSA-Verfahren zur Verschlüsselung von Nachrichten.
Die Zahlen p:= 104 723 und q:=104 659 sind Primzahlen (Sie können das in Maple mit dem Befehl isprime(104723) nachprüfen), ihr Produkt ist n:=10 960 204 457. Die Zahl e:=343 hat keine gemeinsamen Teiler mit (p-1)(q-1).
Verwenden Sie Maple, um den Text *algebra* mit dem RSA-Verfahren (bezüglich e und n) zu verschlüsseln (dabei ist $a = 0$, $b = 1$, ..., $z = 25$).

57) Was ist ein Isomorphismus von Ringen?
Zeigen Sie, dass die Ringe $\mathbb{Z}_{476}$ und $\mathbb{Z}_{17} \times \mathbb{Z}_4 \times \mathbb{Z}_7$ isomorph sind. Es sei

$$f : \mathbb{Z}_{476} \longrightarrow \mathbb{Z}_{17} \times \mathbb{Z}_4 \times \mathbb{Z}_7, \bar{n} \longmapsto (\bar{n}, \bar{n}, \bar{n})$$

Berechnen Sie $\bar{b}, \bar{c} \in \mathbb{Z}_{476}$ so, dass $f(\bar{b}) = (\overline{15}, \bar{3}, \bar{1})$ und $f(\bar{c}) = (\overline{19}, \bar{1}, \overline{-4})$ ist.
Finden Sie $x, y, z \in \mathbb{Z}_{476} \setminus \{\bar{0}\}$ so, dass

$$x^2 = x,\ y^2 = y,\ z^2 = z\ ,\ xy = yz = xz = \bar{0}$$

ist.