5. Übung zur Diskreten Mathematik

Aufgaben für den 5.11.2013

26. (a) Für $a, b, a', b', m \in \mathbb{Z}$ und $m > 0$, beweisen Sie, dass aus $a \equiv a' \bmod m$ und $b \equiv b' \mod m$ die Aussage $a + b \equiv a' + b' \bmod m$ folgt.

    (b) Für $a, b, m_1, m_2 \in \mathbb{Z}$, $m_1, m_2 > 0$ beweisen Sie:

$$a \equiv b \bmod m_i \text{ für alle } i = 1, 2 \Longleftrightarrow a \equiv b \bmod \mathrm{kgV}(m_1, m_2).$$

27. Beweisen Sie die Kürzungsregel für $a, b, c, m \in \mathbb{Z}$, $m > 0$:

$$ac \equiv bc \bmod m \Longleftrightarrow a \equiv b \bmod \frac{m}{\mathrm{ggT}(c, m)}.$$

28. Zeigen Sie: (a) Für $a_1, \ldots, a_n, c \in \mathbb{Z}$, nicht alle a_i gleich 0, ist die diophantische Gleichung

$$a_1 X_1 + \ldots + a_n X_n = c \tag{1}$$

    genau dann in $\mathbb{Z}$ lösbar, wenn $\mathrm{ggT}(a_1, \ldots, a_n)$ ein Teiler von c ist. (Die Gleichung (1) heißt in $\mathbb{Z}$ lösbar, falls es $x_1, \ldots, x_n \in \mathbb{Z}$ gibt, so dass $a_1 x_1 + \ldots + a_n x_n = c$.)

    (b) Sei $d = \mathrm{ggT}(a_1, a_2)$ ein Teiler von c, dann ist im Fall $n = 2$ die Lösungsmenge von (1) gleich

$$\{(x_1, x_2) + t(\frac{a_2}{d}, -\frac{a_1}{d}) \mid t \in \mathbb{Z}\},$$

    wobei $(x_1, x_2) \in \mathbb{Z} \times \mathbb{Z}$ eine beliebige Lösung von (1) ist.

29. Berechnen Sie die letzten beiden Stellen in der Dezimaldarstellung von

$$7^{(7^{(7^7)})} - 7^{(7^7)}.$$

30. Zeigen Sie, dass die Gleichung $X^2 + 7Y^9 + 1 = 0$ keine Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ besitzt. Hinweis: Betrachten Sie diese Gleichung modulo 7.

Zusatzaufgaben:

1. Sei F_n die n-te Fermatsche Zahl. Geben Sie eine Abschätzung für die Anzahl der Stellen in Dezimaldarstellung von F_n an. Berechnen Sie (a) die letzte (b) die letzten zwei (c) die letzten drei Stellen von F_{73}.

   Hinweis: Wie berechnet man F_{n+1} aus F_n? Geben Sie eine Abschätzung wievielstellig n^2 ist, wenn n eine k-stellige Zahl ist, $k \in \mathbb{N}$.

2. Der erweiterte Euklidische Algorithmus vereinfacht die Berechnung der Koeffizienten in der Bézout'schen Identität. Zu ganzen Zahlen $a > b > 0$ wollen wir $x, y \in \mathbb{Z}$ bestimmen, so dass $xa + yb = \mathrm{ggT}(a, b)$ ist. Wir wissen bereits, dass $\mathrm{ggT}(a, b)$ der letzte nichtverschwindende Rest im Euklidischen Algorithmus ist. Setzen wir

$r_1 = a$, $r_2 = b$, dann bestimmen wir im Euklidischen Algorithmus für $n \geq 3$ Zahlen $q_n, r_n \in \mathbb{Z}$, $0 \leq r_n < r_{n-1}$, so dass

$$r_{n-2} = q_n r_{n-1} + r_n.$$

Nun drücken wir r_n sofort als $x_n a + y_n b$ aus. Daher ist $x_1 = 1$, $y_1 = 0$, $x_2 = 0$ und $y_2 = 1$. Für $n \geq 3$ finden Sie eine Darstellung von x_n in x_{n-1} und x_{n-2} und eine Darstellung von y_n in y_{n-1} und y_{n-2}. Falls $r_N = 0$ und $r_{N-1} \neq 0$, dann ist $\mathrm{ggT}(a, b) = r_{N-1} = x_{N-1}a + y_{N-1}b$.

Dieses Verfahren kann man in einer Tabelle wie folgt anordnen:

i	q_i	r_i	x_i	y_i
1		a	1	0
2		b	0	1
3	q_3	r_3	x_3	y_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$N-1$	q_{N-1}	r_{N-1}	x_{N-1}	y_{N-1}
N	q_N	0		