Übungen zur Vorlesung
Elliptische Kurven und Kryptographie

1. Veranstaltungswoche, ohne Abgabe, nur zur Besprechung

13.04.2015

PD Dr. K. Halupczok
Dipl.–Math. A. Juhas

SoSe 2015

Übung 1:

Sei $g \in \mathbb{N} \setminus \{1\}$. Dann besitzt jedes $n \in \mathbb{N}$ die eindeutige Gestalt

$$n = \sum_{i=0}^{k} c_i g^i, \text{ mit } c_i \in \{0, \dots, g-1\}, \ k \in \mathbb{N}_0.$$

Man schreibt auch $n = c_k c_{k-1} \dots c_{0(g)}$. Häufige Darstellungen sind binär ($g = 2$), dezimal ($g = 10$) und hexadezimal ($g = 16$).

(a) Finden Sie für $2015_{(10)}$ die binäre und hexadezimale Darstellung.

(b) Zeigen Sie $(11_{(g)})^3 = 1331_{(g)}$ für $g \geq 4$.

Übung 2:

Seien $a, b, c, m, x, y \in \mathbb{Z}$. Wir schreiben $a \mid b :\Longleftrightarrow b = ka$ für ein $k \in \mathbb{Z}$. Es gelten folgende Teilbarkeitsregeln.

(i) $a \mid b,\ b \mid c \Longrightarrow a \mid c$

(ii) $a \mid b,\ a \mid c \Longrightarrow a \mid bx + cy$

(iii) $a \mid b, b \mid a \Longrightarrow a = \pm b$,

(iv) $a \mid b \Longleftrightarrow am \mid bm$, falls $m \neq 0$.

Eine natürliche Zahl $p > 1$ heißt Primzahl, falls p und 1 die einzigen positiven Teiler sind. Jedes $n > 1$ hat eine eindeutige Darstellung

$$n = \prod_{i=1}^{r} p_i^{e_i}, \text{ mit } 2 \leq p_1 < p_2 < \dots < p_r, \ e_i \in \mathbb{N}.$$

(a) Seien p, q, r paarweise verschiedene Primzahlen. Berechnen Sie kgV und ggT der Zahlen $p^5 q^2$ und $p^3 q^3 r$.

(b) Bezeichne $\omega(n)$ die Anzahl der verschiedenen Primteiler von $n \in \mathbb{N}$. Zeigen Sie

$$\lim_{N \to \infty} \frac{\frac{1}{N} \sum_{n=1}^{N} \omega(n)}{\log \log N} = 1.$$

Demnach haben die $n \leq N$ im Mittel nur etwa $\log \log N$ verschiedene Primteiler. Darüber hinaus kann man zeigen, dass $\omega(n) \approx \log \log n$ für die meisten n gilt. Für $n \approx 10^8$ gilt also typischerweise $\omega(n) = 3$.
Hinweis zu (b): Es gilt

$$\sum_{p \leq N} \frac{1}{p} = \log \log N + R(N) \text{ mit } \lim_{N \to \infty} \frac{R(N)}{\log \log N} = 0.$$

Übung 3:

Ein zahlentheoretischer Zaubertrick: Der Zauberkünstler verbindet sich die Augen und bittet den Zuschauer eine siebenstellige ganze Zahl z_1 seiner Wahl aufzuschreiben, danach eine weitere ganze Zahl z_2, die durch eine beliebige Permutation der Ziffern von z_1 hervorgeht, und letztendlich die Differenz $z_1 - z_2$ zu bilden. Von diesem Ergebnis soll nun der Zuschauer eine frei gewählte Ziffer $\neq 9$ wegstreichen und dem Zauberkünstler die verbleibenden Ziffern vorlesen. Dieser nennt daraufhin die weggestrichene Ziffer. Wie konnte dies dem Zauberer gelingen? Beweisen Sie eine Erklärung des Tricks.