Aufgaben zu Kongruenzen und zu Ordnungen von Elementen

(1) Seien $a, m \in \mathbb{Z}$, $\underset{u}{ggT}(a,m) = 1$. Zeigen Sie: $\exists k \in \mathbb{Z}, 1 \leq k \leq \phi(m)$, so daß $a^k \equiv 1 \pmod m$.

Notation: $\operatorname{ord}_m(a)$ ist der kleinste positive k mit $a^k \equiv 1 \pmod m$.
(wie in der Vorlesung, aber wir notieren auch m)

(2) (a) Berechnen Sie die Reste der folgenden Zahlen bei Division durch 7:
$10^0, 10^1, 10^2, 10^3, 10^4, 10^5$

(b) Prüfen Sie nach: $\frac{1}{7} = 0.\overline{142857}$ ($\overline{\ }$ steht für periodisch fortzusetzen)

$\frac{2}{7} = 0.\overline{285714}$

$\frac{3}{7} = 0.\overline{428571}$

$\frac{4}{7} = 0.\overline{571428}$

$\frac{5}{7} = ?$

$\frac{6}{7} = ?$

Fällt Ihnen etwas auf?

Fällt Ihnen noch etwas auf?

(c) Zeigen Sie: $\frac{10^6 - 1}{7} \in \mathbb{Z}$. Berechnen Sie den Wert und folgern Sie:

$$\frac{1}{7} = 0.142857 + \frac{0.142857}{10^6} + \frac{1}{10^{12}} \cdot \frac{1}{7} = 0.\overline{142857}$$

Berechnen Sie damit auch $\frac{10}{7}$ und $\frac{3}{7}$ sowie $\frac{2}{7} = \frac{10^2}{7} - \underbrace{\left[\frac{10^2}{7}\right]}_{\substack{\text{ganzzahliger Teil} = \\ \text{größte ganze Zahl} \\ \leq \frac{10^2}{7}}}$

und zeigen Sie: $\frac{10^4}{7} = 1428 + \frac{4}{7}$,

wobei nach dem Dezimalpunkt $\frac{e}{7}$ steht,

wobei e der kleinste positive Rest von 10^4 modulo 7 ist.

Analog für k statt 4.

(d) Beweisen Sie: Sei $m \in \mathbb{Z}$ mit $(m,10)=1$ und $1 \leq a < m$. Dann ist die Dezimalentwicklung von $\frac{a}{m}$ ab irgendeiner Stelle periodisch mit Periode der Länge $\mathrm{ord}_m(10)$. Wenn $(a,m)=1$ ist das die minimale Periodenlänge.

(3) (a) Zeigen Sie für $(a,m)=1$ mit $a, m \in \mathbb{Z}$, $m \geq 1$, und $n \in \mathbb{Z}$:

$$a^n \equiv 1 \pmod{m} \Leftrightarrow \mathrm{ord}_m(a) \mid n$$

(b) Sei p prim, $a \in \mathbb{Z}$, $p \nmid a$. Zeigen Sie: $\mathrm{ord}_p(a) \mid p-1$.

(c) Folgern Sie den Kleinen Satz von Fermat.

(d) Sei p prim und q ein Primteiler von 2^p-1. Zeigen Sie: $\mathrm{ord}_q(2)=p$. Folgern Sie daraus: Es gibt unendlich viele Primzahlen.

(e) Seien $a, n \in \mathbb{Z}$, $(a,n)=1$ und $d \in \mathbb{N}$. Zeigen Sie:

$$d = \mathrm{ord}_n(a) \Leftrightarrow a^d \equiv 1 \pmod{n} \text{ und } a^{d/q} \not\equiv 1 \pmod{n}$$

für jede Primzahl $q \mid d$

(f) ~~Zeto~~ Sei $a \in \mathbb{Z}$, p prim, $p \nmid a$. Zeigen Sie:

a ist eine Primitivwurzel modulo p

$$\Leftrightarrow a^{(p-1)/q} \not\equiv 1 \pmod{p} \quad \forall q \text{ prim}, q \mid (p-1)$$