**Freie Universität Berlin** SoSe24
**Institut für Mathematik** A. Constantinescu
Stand: 18. April 2024

---

# Zahlentheorie II – Homework 1

Submission: individually or in pairs,
on Whiteboard as `Names_ZT2_H1.pdf` **by 12:00 on Thursday**, the 25th. April 2024.

**Full written proofs are required in support of your answers.**

---

**Problem 1.** **2 points**

Let $(a_n)$ be the recursively defined sequence of integers:

$$a_1 = 2, \qquad a_{n+1} = a_n^2 - a_n + 3$$

Show that none of the $a_n$ is divisible by 19.

**Problem 2.** **2 points**

Let $p$ be a prime. We say that two polynomials $f, g \in \mathbb{Z}[x]$ are congruent modulo $p$ if the coefficients of $f - g$ are divisible by $p$. Find a polynomial $f \in \mathbb{Z}[x]$ such that $f \not\equiv 0 \bmod p$, but $f(a) \equiv 0 \bmod p$ for all $a \in \mathbb{Z}$.

**Problem 3.** **2 points**

Prove that $\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$, where $\phi(n)$ is the Euler totient function and $\mu$ is the Möbius function.

**Problem 4.** **2 points**

Let $\Phi_n$ be the $n$-th cyclotomic polynomial and $\mu$ be the Möbius function. Show that

$$\Phi_n = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}.$$

**Total: 8 points**

**Extra Problem 5.**

Show that the cyclotomic polynomial $\Phi_{12}$ is reducible modulo $p$ for every prime $p$.