Homework 7

due Tuesday, October 22, 11:00

Problem 1. Let $m, n \in \mathbb{N}$ be not coprime. Show that the map

$$\begin{aligned} \mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ a \bmod mn &\mapsto (a \bmod m, a \bmod n) \end{aligned}$$

is not bijective.

Problem 2. Find all solutions to the following equations:

a) $x^2 + x + 34 = \overline{0}$ in $\mathbb{Z}_{81}$

b) $x^2 + x + 47 = \overline{0}$ in $\mathbb{Z}_{2401}$

c) $x^6 - 2x^5 - 35 = \overline{0}$ in $\mathbb{Z}_{6125}$

Problem 3.

a) Use induction to prove the binomial theorem

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

for all $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$.

b) Show that for every polynomial f of degree n with real coefficients

$$f(a+b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!} b^k.$$

If f has integer coefficients and $a \in \mathbb{Z}$, show that the numbers $f^{(k)}(a)/k!$ are integers.

Problem 4. Let $a, b \in \mathbb{Z}$ be coprime. Show that there exists $n \in \mathbb{Z}$ such that

$$(an + b, c) = 1.$$

Hint: use the Chinese Remainder Theorem to find n such that $(an+b) \bmod p = 1 \bmod p$ for every prime factor p of c that does not divide a.