Fall 2019 – Math 328K (52890)

Midterm exam 2

Thursday, October 31, 11:00

- Write your name clearly readable on the top of **every page** you write!
- Prove every statement you write.
- You can use all theorems from the lectures, homeworks and past tests without proof.
- Do not use a red pen.
- No phones, calculators, books, notes, etc. are permitted, except one hand–written sheet of paper.
- Good luck!

Problem 1. Define Euler's totient function ϕ.

Solution 1. For a $n \in \mathbb{N}$, $\phi(n)$ is the number of integers k such that $1 \leq k \leq n$ and $(k, n) = 1$.

Problem 2. Let $m_1, \ldots, m_n \in \mathbb{N}$ be pairwise coprime and $a_1, \ldots, a_n \in \mathbb{Z}$. We write $M = m_1 m_2 \cdots m_n$ and define $x \in \mathbb{Z}_M$ by the following expression:

$$x = a_1 \left(\frac{M}{m_1}\right)^{\phi(m_1)} + a_2 \left(\frac{M}{m_2}\right)^{\phi(m_2)} + \ \ldots \ + a_n \left(\frac{M}{m_n}\right)^{\phi(m_n)} \bmod M.$$

a) Show that x satisfies the following congruences:

$$\begin{aligned} x \bmod m_1 &= a_1 \bmod m_1 \\ x \bmod m_2 &= a_2 \bmod m_2 \\ &\vdots \\ x \bmod m_n &= a_n \bmod m_n \end{aligned}$$

b) Is it the only element of $\mathbb{Z}_M$ with this property? Why / why not?

Solution 2. We compute

$$x \bmod m_1 = a_1 \left(\frac{M}{m_1}\right)^{\phi(m_1)} \bmod m_1 + \sum_{i=2}^{n} a_i \left(\frac{M}{m_i}\right)^{\phi(m_i)} \bmod m_1.$$

Since $m_1, \ldots, m_n$ are pairwise coprime, $M/m_1 = m_2 \cdots m_n$ is coprime to m_1 (see exam 1 question 5). So $(M/m_1)^{\phi(m_1)} \bmod m_1 = 1 \bmod m_1$ by Euler's theorem. On the other hand $m_1 | (M/m_i)$ for every $i = 2, \ldots, n$, so the second summand is $0 \bmod m_1$. Together, we get that $x \bmod m_1 = a_1 \bmod m_1$. We get the other congruences by the same argument.

By the Chinese Remainder Theorem, there is a unique element of $\mathbb{Z}_M$ which is congruent modulo m_i to a_i for every i. By part a), this element must by x.

Problem 3. Find all solutions $x \in \mathbb{Z}_{16}$ for the following equation:

$$x^3 - 4x + 3 = \overline{0}$$

Solution 3. Let $f(x) = x^3 - 4x + 3$, so $f'(x) = 3x^2 - 4$. It is easy to check that $x = \overline{1}$ is the only solution of $f(x) = \overline{0}$ in $\mathbb{Z}_2$. Since $f'(1) \bmod 2 = \overline{1}$, by Hensel's Lemma a unique lift of the solution is a solution in $\mathbb{Z}_4$, a unique lift of that is a solution in $\mathbb{Z}_8$, and a unique lift of that is a solution in $\mathbb{Z}_{16}$. So there is a unique solution in $\mathbb{Z}_{16}$, and we can directly check that it is $\overline{1}$.

Problem 4. Let p be a prime number.

a) Let $a, b \in \mathbb{Z}$ such that $a \mid b$ and $p \nmid a$. Show that

$$\frac{b}{a} \bmod p = (a \bmod p)^{-1} (b \bmod p),$$

where $(a \bmod p)^{-1}$ is the inverse as an element of $\mathbb{Z}_p$.

b) Show that

$$\binom{2p}{p} \bmod p = 2 \bmod p.$$

Problem 5.

a) Note that the expression is well–defined since $a \mid b$ ensures that b/a is an integer and $p \nmid a$ ensures that $a \bmod p$ is invertible. Now $(a \bmod p)(\frac{b}{a} \bmod p) = \frac{ab}{a} \bmod p = b \bmod p$. If we multiply this with $(a \bmod p)^{-1}$, we get the desired result.

b) We would like to apply part a), but first have to make sure the denominator is not divisible by p. So we compute

$$\binom{2p}{p} \bmod p = \frac{(2p)!}{p!p!} \bmod p = (2 \bmod p) \cdot \frac{(p+1)(p+2)\cdots(2p-1)}{1 \cdot 2 \cdots (p-1)} \bmod p.$$

The numerator and denominator are congruent modulo p, so (applying part a) the second factor is $1 \bmod p$, and therefore the whole expression equals $2 \bmod p$.