Fall 2019 – Math 328K (52890)

# Midterm exam 3

*Tuesday, December 3, 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.** For a positive integer $m$, define the notion *primitive root in* $\mathbb{Z}_m$. For which $m$ do they exist?

**Solution 1.** A primitive root is an invertible element $x \in \mathbb{Z}_m^\times$ with $\operatorname{ord}(x) = \phi(m)$, where $\operatorname{ord}(x)$ is the smallest $k \in \mathbb{N}$ such that $x^k = \overline{1}$. A primitive root exists in $\mathbb{Z}_m$ if and only if $m$ is either 2 or 4 or $p^t$ or $2p^t$ for $t \in \mathbb{N}$ and an odd prime $p$.

**Problem 2.** Let $m \in \mathbb{N}$ such that $\mathbb{Z}_m$ has a primitive root and let $d \in \mathbb{N}$ be a divisor of $\phi(m)$. Show that $\mathbb{Z}_m^\times$ contains an element of order $d$.

**Solution 2.** Let $r \in \mathbb{Z}_m^\times$ be a primitive root. We can write every element of $\mathbb{Z}_m^\times$ uniquely as $r^k$ with $0 \leq k < \phi(m)$. By Homework 11 Problem 1

$$\operatorname{ord}(r^k) = \frac{\operatorname{ord}(r)}{(\operatorname{ord}(r), k)} = \frac{\phi(m)}{(\phi(m), k)}$$

for every $k \in \mathbb{Z}$, so $\operatorname{ord}(r^k) = d$ if and only if $(\phi(m), k) = \phi(m)/d$. This is true if and only if $k = \ell \cdot \phi(m)/d$ for an integer $\ell$ and $(d, \ell) = 1$.

There are exactly $\phi(d)$ integers $\ell$ like this in the range $0 \leq \ell < d$, corresponding to $\phi(d)$ integers $k = \ell \cdot \phi(m)/d$ with $(\phi(m), k) = \phi(m)/d$ in the range $0 \leq k < \phi(m)$ and $\phi(d)$ elements $r^{\ell \cdot \phi(m)/d} \in \mathbb{Z}_m^\times$ of order $d$.

**Problem 3.**

a) Find a primitive root in $\mathbb{Z}_{25}$.

b) Find the *number of solutions* $x \in \mathbb{Z}_{25}$ to the equation

$$x^{12} = \overline{16}.$$

**Solution 3.**

a) Since $\operatorname{ord}(x) \mid \phi(m)$ for all $x \in \mathbb{Z}_m^\times$, $\operatorname{ord}(x)$ must be in the set $\{1, 2, 4, 5, 10, 20\}$. Since

$$\overline{2}^1 = \overline{2}, \quad \overline{2}^2 = \overline{4}, \quad \overline{2}^4 = \overline{16}, \quad \overline{2}^5 = \overline{7}, \quad \overline{2}^{10} = \overline{24}$$

and none of these is equal to $\overline{1}$, the order of $\overline{2}$ must be 20, i.e. 2 is a primitive root.

b) Suppose that $x \in \mathbb{Z}_{25}$ is a solution of $x^{12} = \overline{16}$. If $x \notin \mathbb{Z}_{25}^\times$, then $x \bmod 5 = 0 \bmod 5$, hence $0 \bmod 5 = x^{12} \bmod 5 = \overline{16} \bmod 5 = 1 \bmod 5$, a contradiction. So $x \in \mathbb{Z}_{25}^\times$. This means we can take discrete logarithms to get

$$12 \log_2(x) = \log_2(\overline{16}) = \overline{4}$$

as an equation in $\mathbb{Z}_{20}$. Since $(12, 20) = 4$ and this divides 4, there are 4 solutions to this equation (they are $2, 7, 12, 17$), corresponding to 4 solutions of the original equation, namely

$$\overline{2}^2 = \overline{4}, \quad \overline{2}^7 = \overline{3}, \quad \overline{2}^{12} = \overline{21}, \quad \overline{2}^{17} = \overline{22}.$$

**Problem 4.** A natural number $n \in \mathbb{N}$ is called *perfect* if it is equal to the sum of its positive divisors except itself, or equivalently if $\sigma(n) = 2n$.

Show for $k \in \mathbb{N}$ that the number

$$n = 2^{k-1}(2^k - 1)$$

is perfect if and only if $2^k - 1$ is prime.

**Solution 4.** Since $2^{k-1}$ is a power of 2 and $2^k - 1$ is odd, they are coprime. So

$$\sigma(n) = \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)\sigma(2^k - 1).$$

and $2n = 2^k(2^k - 1)$. So $n$ is perfect if and only if $\sigma(2^k - 1) = 2^k$. This is true if and only if $2^k - 1$ is prime, since 1 and $2^k - 1$ are divisors of $2^k - 1$, so the sum of divisors can only by $2^k$ if there are no other divisors.