Math 261 — Exercise sheet 4

http://staff.aub.edu.lb/~nm116/teaching/2017/math261/index.html

Version: October 11, 2017

Answers are due for Monday 16 October, 11AM.

The use of calculators is allowed.

Exercise 4.1: Primitive roots (24pts)

1. (8pts) Find a primitive root for $\mathbb{Z}/7\mathbb{Z}$. Justify your answer in detail.
2. (8pts) Same question for $\mathbb{Z}/11\mathbb{Z}$.
3. (8pts) Same question for $\mathbb{Z}/23\mathbb{Z}$.

Exercise 4.2: More primitive roots (32 pts)

Let $p \in \mathbb{N}$ be prime, and let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a primitive root.

1. (8 pts) Let $a \in \mathbb{Z}$. Give a necessary and sufficient condition on a for g^a to be a primitive root in $\mathbb{Z}/p\mathbb{Z}$.
2. (8 pts) Prove that if a is prime, then g^a is a primitive root in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \not\equiv 1 \pmod{a}$.
3. (8 pts) Show that the previous assertion is no longer valid when a is not assumed to be prime, by finding a counterexample.
4. (8 pts) Is every primitive root of $\mathbb{Z}/p\mathbb{Z}$ of the form g^a for some $a \in \mathbb{Z}$? Justify your answer.

Exercise 4.3: (24 pts)

Prove that $2^{3n+5} + 3^{n+1}$ is divisible by 5 for all $n \in \mathbb{N}$.

Exercise 4.4: A really big number (20 pts)

Compute the remainder of $16^{2^{1000}}$ when divided by 7.

Hint: This number is so large that most calculators and computers won't be able to help you, but congruences and multiplicative orders will...

The exercises below are not mandatory. They are not worth any points, and are given here for you to practise. The solutions will be made available with the solutions to the other exercises.

Exercise 4.5: Largest possible orders

1. Prove that for every $n \in \mathbb{N}$, and for every $x \in \mathbb{Z}/n\mathbb{Z}$, the additive order of x is at most n.

2. Prove that for every $n \in \mathbb{N}$, there exists an $x \in \mathbb{Z}/n\mathbb{Z}$ whose additive order is exactly n.

3. Prove that for every $n \in \mathbb{N}$, and for every $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative order of x is at most $\phi(n)$.

4. Find an $n \in \mathbb{N}$ such that every $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ has multiplicative order $< \phi(n)$.

Exercise 4.6: Possible orders

1. Let $n \in \mathbb{N}$. Explain why the additive order of any $x \in \mathbb{Z}/n\mathbb{Z}$ is a divisor of n, and prove that for any $d \mid n$, there exists an $x \in \mathbb{Z}/n\mathbb{Z}$ of order d.

2. Let $p \in \mathbb{N}$ be a prime. Explain why the multiplicative order of any $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a divisor of $p-1$, and prove that for any $d \mid (p-1)$, there exists an $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ of multiplicative order d.

3. Let $n \in \mathbb{N}$. Is it true that for any $d \mid \phi(n)$, there exists an $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ of multiplicative order d?

4. Suppose that $n \in \mathbb{N}$, and that there exists an $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ of multiplicative order $n-1$. Prove that n must be prime.