Math 261 — Exercise sheet 6

http://staff.aub.edu.lb/~nm116/teaching/2018/math261/index.html

Version: October 23, 2018

Answers are due for Wednesday 31 October, 11AM.

The use of calculators is allowed.

Exercise 6.1: A huge number! (25 pts)

For this exercise, remember that every integer is congruent mod 9 *to the sum of its digits.*

Let $A = 4444^{4444}$, let B be the sum of the digits of A, let C be the sum of the digits of B, and finally let D be the sum of the digits of C.

1. (15 pts) Compute D mod 9.
2. (7 pts) Prove that $D \leqslant 14$.

   Hint: Start with the upper bound $A < 10000^{5000} = 10^{20000}$.
3. (3 pts) What is the exact value of D (as opposed to just mod 9)?

Exercise 6.2: Primitive roots mod 43 (35 pts)

1. (5 pts) Suppose you choose an element of $(\mathbb{Z}/43\mathbb{Z})^\times$ at random. What is the probability that this element is a primitive root? In other words, what is the proportion of elements of $(\mathbb{Z}/43\mathbb{Z})^\times$ that are primitive roots?
2. (15 pts) Find a primitive root $g \in (\mathbb{Z}/43\mathbb{Z})^\times$.
3. (10 pts) What is the multiplicative order of g^{261}, where g is the primitive root found in the previous question?

Exercise 6.3: A multiplicative sequence (40 pts)

The goal of this exercise is to understand the behavior of the sequence $x_n = 2^n$ in $\mathbb{Z}/40\mathbb{Z}$.

1. (3 pts) Why cannot we say that x_n is periodic mod 40 "as usual"?
2. (12 pts) Find a formula for the values of x_n mod 5 in terms of n. You answer should have the form "if n is like this, then $x_n =$ this; if n is like that, then $x_n =$ that; if …".
3. (10 pts) Find a formula for the values of x_n mod 8 in terms of n.

   Hint: Compute x_n *for* $n \leqslant 4$ *"by hand".*
4. (15 pts) Deduce a formula for x_n mod 40. What is the period? What is the length of the "tail"?

   Hint: 中国剩余定理.

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

Exercise 6.4: More primitive roots

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

Exercise 6.5: Even more primitive roots

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

1. 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. 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. Show that the previous assertion is no longer valid when a is not assumed to be prime, by finding a counterexample.
4. 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 6.6

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

Exercise 6.7: Another really big number

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

Exercise 6.8: 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.