Introduction to number theory
Exercise sheet 2

https://www.maths.tcd.ie/~mascotn/teaching/2021/MAU22301/index.html

Version: October 11, 2021

Email your answers to makindeo@tcd.ie by Friday October 22nd, 2PM.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *No primitive roots (100 pts)*

In this exercise, whenever $x \in \mathbb{Z}$ and $n \in \mathbb{N}$, we write $x \bmod n$ for x seen as an element of $\mathbb{Z}/n\mathbb{Z}$. If furthermore x and n are coprime, so that $x \bmod n$ actually lies in $(\mathbb{Z}/n\mathbb{Z})^\times$, we denote by $\mathrm{MO}(x \bmod n)$ the multiplicative order of $x \bmod n$.

We fix two distinct odd primes $p \neq q \in \mathbb{N}$, and we set $n = pq$.

1. (30 pts) Let $x \in \mathbb{N}$ be coprime to n. Prove that

$$\mathrm{MO}(x \bmod n) = \mathrm{lcm}\big(\mathrm{MO}(x \bmod p), \mathrm{MO}(x \bmod q)\big).$$

   Hint: 中國餘數定理.

   Suppose from now on that $g \in \mathbb{Z}$ is a primitive root mod n (in particular, g is coprime to n).

2. (20 pts) Express $\mathrm{MO}(g \bmod n)$ in terms of p and q.

3. (20 pts) Prove that g is a primitive root both mod p and mod q.

   Hint: 相同的提示.

4. (20 pts) Prove that $\mathrm{MO}(g \bmod p)$ and $\mathrm{MO}(g \bmod q)$ are both even.

5. (10 pts) Deduce that such a primitive root $g \bmod n$ cannot exist.

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 2 *An inverse*

1. Use Euclid's algorithm to determine whether 47 is invertible mod 111, and to find its inverse if it is.

2. Solve the equation $47x \equiv 5 \bmod 111$ in $\mathbb{Z}/111\mathbb{Z}$.

Exercise 3 *More inverses*

1. Fix $n \in \mathbb{N}$, let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ be invertible, and let $y \in \mathbb{Z}/n\mathbb{Z}$ be the inverse of x. Prove that x^2, $-x$, and y are also invertible, and find their inverses.

2. Find all the elements of $(\mathbb{Z}/15\mathbb{Z})^\times$, and give the inverse of each of them. What is $\phi(15)$?

   Hint: Use the previous question to save your effort!

Exercise 4 *A system of congruences*

Find an integer $x \in \mathbb{Z}$ such that $x \equiv 12 \bmod 7$ and $x \equiv 7 \bmod 12$.

Exercise 5 *Primes mod 6*

1. Let p be a prime number which is neither 2 nor 3. Prove that either $p \equiv 1 \bmod 6$ or $p \equiv -1 \bmod 6$.

2. Prove that there are infinitely many primes p such that $p \equiv -1 \bmod 6$.

   Hint: Suppose on the contrary that there are finitely many, say $p_1, \cdots, p_k$. Let $N = 6p_1 \cdots p_k - 1$, and consider a prime divisor of N.

3. Why does the same proof fail to show that there are infinitely may primes p such that $p \equiv 1 \bmod 6$?

4. *Dirichlet's theorem on primes in arithmetic progressions*, which is way beyond the scope of this course, states that for all coprime positive integers a and b, there are infinitely many primes p such that $p \equiv a \bmod b$; in particular, there are in fact infinitely many primes p such that $p \equiv 1 \bmod 6$. Why, in the statement of this theorem, is it necessary to assume that a and b are coprime?

Exercise 6 *Euler*

Compute $\phi(2020)$ and $\phi(2021)$.
Hint: $45^2 = 2025$.

Exercise 7 *Factoring with Euler*

Let $n = 93011$. Given than $n = pq$ is a product of two distinct primes, and that $\phi(n) = 92400$, find p and q.

Hint: Consider the polynomial $(x - p)(x - q)$.

Exercise 8 *A really large number*

What is the remainder of $22^{7^{2020}}$ when divided by 17?
Just to be clear: a^{b^c} *means* $a^{(b^c)}$*, as opposed to* $(a^b)^c = a^{bc}$.

Exercise 9 *Inverse Euler*

The goal of this exercise is to find all integers $n \in \mathbb{N}$ such that $\phi(n) = 4$.

1. Prove that if $p \in \mathbb{N}$ is a prime and $v \in \mathbb{N}$ is such that $p^v \mid n$, then $(p-1)p^{v-1} \mid \phi(n)$.

   Hint: When p *is prime, what is* $\phi(p^v)$*?*

2. Using the previous question, prove that if $\phi(n) = 4$, then n cannot be divisible by a prime $p \geq 7$. Also prove that $3^2,\ 5^2 \nmid n$.

3. Find all n such that $\phi(n) = 4$.

   Hint: Think in terms of the factorisation of n*. You should find that there are four such* n *— but you are required to prove this as part of this question!*

Exercise 10 *More inverse Eulers*

This exercise is a bit more difficult, but still doable. The questions are independent from each other.

1. Using the fact that $2018 = 2 \times 1009$ and that 1009 is prime, prove that there is no $n \in \mathbb{N}$ such that $\phi(n) = 2018$.

   Hint: Suppose 1009 *is a factor of* $\phi(n)$*. Where can this factor come from?*

2. Prove that for all $m \in \mathbb{N}$, there are at most finitely many[1] $n \in \mathbb{N}$ such that $\phi(n) = m$.

   Hint: Try to bound the prime factors of n *in terms of* m*.*

3. Prove that $\phi(n)$ is even for all $n \geq 3$.

   Hint: Start with the case when n *is a prime power.*

[1] This means either finitely many or none.

Exercise 11 *Divisibility criteria*

Let $n \in \mathbb{N}$.

1. Prove that n is congruent mod 9 to the sum of its digits. In other words, if $n_0, n_1, n_2, \cdots$ are the digits of n from right to left, so that

$$n = n_0 + 10n_1 + 100n_2 + \cdots = \sum_i n_i 10^i,$$

   then $n \equiv n_0 + n_1 + n_2 + \cdots \bmod 9$.

2. Prove that $9 \mid n$ iff. 9 divides the sum of digits of n.

3. Find a similar criterion to test whether $11 \mid n$.

Exercise 12 *A huge number!*

In this exercise, you may use the first question of the previous exercise: 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. Compute D mod 9.

2. Prove that $D \leq 14$.

   Hint: Start with the upper bound $A < 10000^{5000} = 10^{20000}$.

3. What is the exact value of D (as opposed to just mod 9)?

Exercise 13 *Primitive roots mod 43*

1. 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. Find a primitive root $g \in (\mathbb{Z}/43\mathbb{Z})^\times$.

3. What is the multiplicative order of g^{2020}, where g is the primitive root found in the previous question?

4. Same question for $g^4 3$.

5. Prove that every primitive root in $(\mathbb{Z}/43\mathbb{Z})^\times$ is a power of g.

6. For which $m \in \mathbb{Z}$ is g^m a primitive root?

Exercise 14 *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 15 *A multiplicative sequence*

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

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

   Hint: Compute t_n for $n \leq 4$ "by hand".
4. Deduce a formula for t_n mod 40. What is the period? What is the length of the "tail"?

   Hint: Chinese.

Exercise 16 *A divisibility relation*

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

Exercise 17 *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 $n \geqslant 2$, and that there exists an $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ of multiplicative order $n-1$. Prove that n must be prime.