

Ve203 Discrete Mathematics (Fall 2020)

Assignment 4: Congruencies, Prime Factorization

Date Due: 2:00 PM, Friday, the 9th of October 2020



This assignment has a total of **(33 Marks)**.

Exercise 4.1

In this question we will determine the remainder r of the division of 10^{100} by 247, without using any calculator. Please detail your calculations.

- i) Write 247 as a product of two primes $p_1 < p_2$. Express their gcd as a linear combination, i.e. find x and $y \in \mathbb{Z}$ such that $1 = p_1 \cdot x + p_2 \cdot y$.

(1 Mark)

- ii) Prove that $10^{100} \equiv 3 \pmod{p_1}$ and $10^{100} \equiv 9 \pmod{p_2}$.

(2 Marks)

- iii) Using the Chinese Remainder Theorem, prove that $r = 237$.

(1 Mark)

Exercise 4.2

Find a number $n \in \mathbb{N}$ satisfying both $4^n \equiv 7 \pmod{9}$ and $2^n \equiv 3 \pmod{11}$.

(2 Marks)

Exercise 4.3

Use Fermat's factorization method to find factors of the number 2027651281. Detail all the steps in your calculation.

(2 Marks)

Exercise 4.4

Use Fermat's Little Theorem to compute $5^{2003} \pmod{7}$, $5^{2003} \pmod{11}$ and $5^{2003} \pmod{13}$. Then use the Chinese Remainder Theorem to compute $5^{2003} \pmod{1001}$ (note that $1001 = 7 \cdot 11 \cdot 13$).

(4 Marks)

Exercise 4.5

In the lectures we proved that if p is prime then $(p-1)! \equiv -1 \pmod{p}$.

- i) Prove that the converse is also true, i.e., if $(p-1)! \equiv -1 \pmod{p}$, then p is prime.

(2 Marks)

- ii) Prove that for any odd integer m , $(m-1)! \equiv (-1)^z (z!)^2 \pmod{m}$, where $z = \frac{m-1}{2}$.

(2 Marks)

- iii) Discuss a strategy to assess the primality of an odd integer.

(2 Marks)

Exercise 4.6

If m is a positive integer, the integer a is a quadratic residue of m if $\gcd(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ has a solution. In other words, a quadratic residue of m is an integer relatively prime to m that is a perfect square modulo m . For example, 2 is a quadratic residue of 7 because $\gcd(2, 7) = 1$ and $3^2 \equiv 2 \pmod{7}$ and 3 is a quadratic nonresidue of 7 because $\gcd(3, 7) = 1$ and $x^2 \equiv 3 \pmod{7}$ has no solution.

- i) Which integers are quadratic residues of 11 ?

(2 Marks)

- ii) Show that if p is an odd prime and a is an integer not divisible by p , then the congruence $x^2 \equiv a \pmod{p}$ has either no solutions or exactly two incongruent solutions modulo p .

(2 Marks)

- iii) Show that if p is an odd prime, then there are exactly $(p-1)/2$ quadratic residues of p among the integers $1, 2, \dots, p-1$.

(2 Marks)

If p is an odd prime and a is an integer not divisible by p , the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue of p and -1 otherwise.

- iv) Show that if p is an odd prime and a and b are integers with $a \equiv b \pmod{p}$, then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

(1 Mark)

- v) Prove that if p is an odd prime and a is a positive integer not divisible by p , then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

(2 Marks)

- vi) Show that if p is an odd prime and a and b are integers not divisible by p , then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

(2 Marks)

- vii) Show that if p is an odd prime, then -1 is a quadratic residue of p if $p \equiv 1 \pmod{4}$, and -1 is not a quadratic residue of p if $p \equiv 3 \pmod{4}$.

(2 Marks)

- viii) Find all solutions of the congruence $x^2 = 29 \pmod{35}$.

Hint: Find the solutions of this congruence modulo 5 and modulo 7, and then use the Chinese Remainder Theorem.

(2 Marks)