UNIVERSITY OF LIVERPOOL

MATH 342

EXAMINER: Dr. V. Guletskiĭ, EXTENSION 44042.

TIME ALLOWED: Two and a half hours

Candidates may attempt all questions. Best FIVE answers will be taken into account. Each question carries the same weight.

1.

(i) Prove Euclid's theorem saying that there are infinitely many primes among all positive integers.

5 marks

(ii) State the theorem on division with a remainder. Give the detailed proof of that theorem.

5 marks

(iii) Describe the Euclid's algorithm and explain why the last non-trivial remainder of Euclid's algorithm for two integers a and b is the greatest common divisor of a and b.

5 marks

(iv) Show that 105875 and 109512 are coprime.

5 marks

[20 marks]

2.

(i) Compute the orders of the number 37632 at the primes 2, 3, 5 and 7.

5 marks

(ii) Let p be a prime. Prove that $\operatorname{ord}_p(ab) = \operatorname{ord}_p(a) + \operatorname{ord}_p(b)$ for any two positive integers a and b.

5 marks

(iii) Prove that any positive integer can be factorized in to primes. Then use (ii) to prove the uniqueness of the prime-power factorization.

5 marks

(iv) Show that the product of two positive integers is equal to the product of their greatest common divisor and their least common multiple.

5 marks

[20 marks]

3.

(i) Let a and b be two coprime integers. Show that there exist two integers s and t, such that $sa + tb = 1$.

5 marks

(ii) Let a, b and m be three integers, $a \neq 0$ and $m > 0$. Explain when a congruence $ax \equiv b(\operatorname{mod} m)$ is solvable in x, and describe the procedure of solving this congruence provided it is solvable.

5 marks

(iii) Find all integers x satisfying the following equations: $36x \equiv 38(\operatorname{mod} 22)$ and $143x = 187(\operatorname{mod} 35)$.

5 marks

(v) Find all integers satisfying the system of three equations

$$\begin{cases} 3x \equiv 4(\operatorname{mod} 11) \\ 6x \equiv 3(\operatorname{mod} 13) \\ 9x \equiv 2(\operatorname{mod} 17) \end{cases}$$

5 marks

[20 marks]

4.

(i) Compute the values of Euler's function $\phi(875)$, $\phi(1331)$ and $\phi(109512)$.

5 marks

(ii) Let m be a positive integer, and let a be an integer coprime to m. Prove Euler's theorem which says that $a^{\phi(m)} \equiv 1(\operatorname{mod} m)$.

5 marks

(iii) Prove that the number $4 + 4^6 + 4^{42} + 4^{294}$ is divisible by 7.

5 marks

(iv) Let m be a positive integer. Prove that m is a sum of the values $\phi(d)$, where d runs over all the divisors d of the number m.

5 marks

[20 marks]

5.

(i) Prove that the order of a modulo p divides the value of Euler's function $\phi(m)$.

5 marks

(ii) Let m be a positive integer. Prove the first part of the main theorem about primitive roots saying that if g is a primitive root mod m then $g^t \equiv g^s$ modulo m if and only if $t \equiv s$ modulo $\phi(m)$.

5 marks

(iii) Then prove the second part of the above theorem saying that all the numbers $1, g, g^2, \ldots, g^{\phi(m)-1}$ are pairwise distinct modulo m.

5 marks

(iv) Find a primitive root modulo 11 and then use the above theorem in order to find all the solutions of the equation $8x^3 \equiv 7 (\mathrm{mod}\, 11)$.

5 marks

[20 marks]

6.

(i) Let $m = rs$, where r and s are two integers both strictly bigger than 2 and coprime to each other. Show that if a is an integer coprime to $m = rs$ then $a^{\frac{1}{2}\phi(m)} \equiv 1 (\mathrm{mod}\, m)$.

5 marks

(ii) Show that if $m > 2$ and if there exists at least one primitive root modulo m then the equation $x^2 \equiv 1 (\mathrm{mod}\, m)$ has exactly two solutions modulo m.

5 marks

(iii) Let p be a prime, $p \neq 3$, and let s be a positive integer. Are there primitive roots modulo $m = 3 \cdot p^s$? Explain your answer.

5 marks

(iv) Find all the solutions of the equation $5^x \equiv 11 (\mathrm{mod}\, 17)$.

5 marks

[20 marks]

7.

(i) Let n be an integer, and let p be a prime. What is the quadratic residue of n modulo p? Define the Legendre symbol $\left(\frac{n}{p}\right)$ provided $(n, p) = 1$.

5 marks

(ii) State Euler's Criterion for quadratic residues and give the formulas for $\left(\frac{-1}{p}\right)$ and for $\left(\frac{2}{p}\right)$.

5 marks

(iii) Let p be a prime, and let m and n be two integers both coprime to p. Show that

$$\left(\frac{n}{p}\right)\left(\frac{m}{p}\right) = \left(\frac{nm}{p}\right) .$$

Show also that

$$\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$$

provided $m \equiv n (\operatorname{mod} p)$.

5 marks

(v) State Gauss' Quadratic Reciprocity Law and use it in order to compute the following quadratic residues:

$$\left(\frac{77}{67}\right) , \quad \left(\frac{124}{103}\right) \quad \text{and} \quad \left(\frac{176}{211}\right) .$$

5 marks

[20 marks]