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) State and prove the theorem on division with a remainder (Euclid's property)

(ii) Show that for any two integers a and b their greatest common divisor is the same as the greatest common divisor for a and $b + at$ for any integer t.

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

(iv) Show that 45675 and 6854 are coprime.

(v) Show that 39 and 119 are coprime and find two integers s and t such that $39s + 119t = 1$.

[20 marks]

2.

(i) Compute the orders $\operatorname{ord}_5(15123)$, $\operatorname{ord}_{71}(15123)$, $\operatorname{ord}_{17}(30246)$, $\operatorname{ord}_2(151230)$ and $\operatorname{ord}_{101}(61206)$

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

(iii) State and prove the Fundamental Theorem of Arithmetic.

(iv) Let a and b be two integers, let (a, b) be their greatest common divisor and $[a, b]$ be their least common multiple. Show that $ab = (a, b)[a, b]$.

(v) Compute the number of zeros at the end of the decimal expression of 1000!

[20 marks]

3.

(i) Let a and b be two coprime integers. Prove that there exist two integers s and t such that $as + bt = 1$.

(ii) Let a and b be two integers. Give the necessary and sufficient condition when a congruence of type $ax \equiv b(\operatorname{mod} m)$ is solvable in x. Describe the procedure of solving this congruence provided it is solvable?

(iii) Solve the following equations: $469x \equiv 143(\operatorname{mod} 29)$ and $707x \equiv 118(\operatorname{mod} 1313)$.

(iv) State and prove the Chinese Remainder Theorem.

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

$$\begin{cases} 3x \equiv 3(\operatorname{mod} 9) \\ 7x \equiv 4(\operatorname{mod} 5) \\ 5x \equiv 3(\operatorname{mod} 14) \end{cases}$$

[20 marks]

4.

(i) Define Euler's function ϕ and express $\phi(n)$ in terms of the prime-power decomposition of n for a general n.

(ii) Prove the formula

$$n = \sum_{d|n} \phi(d) \ ,$$

where d runs all the divisors of n.

(iii) Prove Euler's theorem which says that $a^{\phi(m)} \equiv 1(\operatorname{mod} m)$ for any integer a coprime with m.

(iv) Show that 7^{864} is congruent to 1 modulo 864, and that 7^{100} is congruent to 2401 modulo 360.

(v) Show that $5^{162} + 5^{18} + 5^2$ is divisible by 3.

[20 marks]

5.

(i) Let m be a positive integer. Define the order of an integer a modulo m (do not mix up with the notion of the order of an integer at a prime). Prove that the order of a always divides $\phi(m)$.

(ii) Let m be a positive integer. Give the definition of a primitive root mod m. Show 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 $\phi(m)$.

(iii) Let m be a positive integer and let g be a primitive root mod m. Show that all the numbers $1, g, g^2, \ldots, g^{\phi(m)-1}$ are pairwise distinct modulo m.

(iv) Find all primitive roots modulo 7.

(v) Find all the solutions of the equation $5x^3 \equiv 5(\operatorname{mod} 7)$.

[20 marks]

6.

(i) Let m be a positive integer, $m > 2$. Show that $\phi(m)$ is even.

(ii) Prove that the equation $x^2 \equiv 1 (\bmod m)$ has only two solutions modulo m. Find them.

(iii) Prove that primitive roots mod m exist only if m is a power of a prime, i.e. $m = p^s$, or doubled power of a prime, i.e. $m = 2 \cdot p^s$.

(iv) Solve the equation $2x^4 \equiv 22 (\bmod 20)$.

(v) Solve the equation $3x^5 \equiv 101 (\bmod 7)$.

[20 marks]

7.

(i) Define the quadratic residue of n modulo p and the Legendre symbol $\left(\frac{n}{p}\right)$ provided $(n, p) = 1$.

(ii) State Euler's Criterion for quadratic residues and use it to compute $\left(\frac{-1}{p}\right)$ for any prime p.

(iii) State the necessary and sufficient conditions for $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = -1$.

(iv) Let p be a prime. Prove that $\left(\frac{n}{p}\right)\left(\frac{m}{p}\right) = \left(\frac{nm}{p}\right)$ and $\left(\frac{n+sp}{p}\right) = \left(\frac{n}{p}\right)$ for any integers m, n and s, where m and n are not divisible by p.

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

$$\left(\frac{78}{89}\right), \quad \left(\frac{385}{389}\right) \quad \text{and} \quad \left(\frac{66}{139}\right).$$

[20 marks]