PAPER CODE NO.
MATH 342

EXAMINER: **Prof. S.M. Rees**, TEL.NO. 44063
DEPARTMENT: Mathematical Sciences

UNIVERSITY OF LIVERPOOL

MAY2012 EXAMINATIONS

Number Theory

TIME ALLOWED: Two and a half hours.

INSTRUCTIONS TO CANDIDATES: Full marks may be obtained for complete answers to five questions. The best five questions will be taken into account.

1. For x and $y \in \mathbb{Z}$, and $n \in \mathbb{Z}_+$ define

$$x \equiv y \text{ mod } n$$

in terms of division by n. Prove from this definition that

$$(x_1 \equiv y_1 \text{ mod } n \quad \wedge \quad x_2 \equiv y_2 \text{ mod } n) \quad \Rightarrow \quad (x_1 x_2 \equiv y_1 y_2 \text{ mod } n).$$

Find all solutions of the following. In some cases there may be no solutions.

a) $x^2 \equiv 1 \mod 5$.

b) $x^3 \equiv 2 \mod 5$.

c) $2x \equiv 3 \mod 4$.

d) $6x \equiv 8 \mod 14$.

e) Solve the simultaneous equations $\begin{pmatrix} 2x \equiv 3 \mod 5 \\ 5x \equiv 4 \mod 9 \\ 3x \equiv 1 \mod 4 \end{pmatrix}$.

[20 marks]

2. State the Fundamental Theorem of Arithmetic. Let p_n be an enumeration of all the positive primes, with $p_1 = 2$ and $p_n < p_{n+1}$ for all n. Show that p_n exists for all $n \in \mathbb{Z}_+$ and that

$$p_{n+1} \leq \prod_{i=1}^{n} p_i + 1.$$

Define the prime number counting function $\pi(x)$, and write down, with any necessary explanations, the values

$$\pi(23), \quad \pi(28), \quad \pi(p_n), \quad \pi(p_n + 1).$$

Now let $p_n^{(3,4)}$ be an enumeration of all the positive primes which are 3 mod 4 with $p_n^{(3,4)} < p_{n+1}^{(3,4)}$. Write down $p_n^{(3,4)}$ for $n \leq 5$. Show that at least one of the primes dividing

$$4 \prod_{i=2}^{n} p_i^{(3,4)} + 3,$$

must be equal to 3 mod 4. Deduce that $p_{n+1}^{(3,4)}$ exists for all $n \in \mathbb{Z}_+$, that is, that there are infinitely many primes which are 3 mod 4.

[20 marks]

3. State Fermat's Little Theorem.

(i) Use it to prove that $2^{62} + 3^{153}$ is divisible by 31.

(ii) Find all the possible orders of elements of the group of units G_{31}. Give an example of an element of each possible order.

Find all values of $m \in \mathbb{Z}_+$ and $n \in \mathbb{Z}_+$ with $n \geq 2$ such that 7 divides

$$\frac{n^m - 1}{n - 1}.$$

Hint Consider separately the cases $n \not\equiv 1 \mod 7$ and $n \equiv 1 \mod 7$. Think about the possible orders of integers mod 7.

[20 marks]

4. Define Euler's ϕ function. Prove that if p is a positive prime and $a \in \mathbb{Z}_+$ then

$$\phi(p^a) = p^{a-1}(p-1).$$

Also compute the sum $\int p^a$ (using Euler's notation) of the divisors of p^a. Now write down the formulas for $\phi(n)$ and $\int n$, for any $n \in \mathbb{Z}_+$, with $n \geq 2$, in terms of the prime decomposition of n, where

$$n = \prod_{i=1}^{m} p_i^{k_i}$$

for distinct primes p_i and integers $k_i \geq 1$.

Compute $\phi(9!)$ and $\phi\left(\binom{9}{3}\right)$, where $\binom{9}{3} = \dfrac{9!}{3!6!}$.

For p_i and k_i as above, let

$$K = \sum_{i=1}^{m} k_i$$

and

$$P = \mathrm{Max}\{p_i : 1 \leq i \leq m\}.$$

Show that

$$\mathrm{Max}(2^{K-1}, P-1) \leq \phi(n) \leq n \leq P^K.$$

Deduce that

$$\lim_{n \to \infty} \phi(n) = +\infty.$$

[20 marks]

5. Let $n_1 \geq 2$ and $n_2 \geq 2$ be coprime integers. Show that the function

$$F : \mathbb{Z}_{n_1 n_2} \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2};\ F(x \bmod n_1 n_2) = (x \bmod n_1,\ x \bmod n_2)$$

is injective. Use this to show that F is a bijection.
Prove that F maps the group G_n of units mod n to the product $G_{n_1} \times G_{n_2}$ of the groups of units mod n_1 and mod n_2.
Construct F when $n_1 = 3$ and $n_2 = 7$.

Recall that $n \in \mathbb{Z}_+$ is a *pseudoprime to base* a if $a^{n-1} \equiv 1 \mod n$, and n is a *Carmichael number* if n is composite and is a pseudoprime to base a for all $a \in G_n$.
Give Korselt's equivalent definition of a Carmichael number. Use it to verify that 1729 is a Carmichael number.

Now let n be any integer ≥ 2. Show that

$$\{a : a^{n-1} \equiv 1 \mod n\}$$

is a subgroup of G_n.
Now let $n = 21$. Identify all $a \bmod 21$ such that 21 is a pseudoprime to base a.

[20 marks]

6. In this question let $\mathbb{Z}[i]$ be the ring of Gaussian integers, that is

$$\mathbb{Z}[i] = \{s + it : s, t \in \mathbb{Z}\}$$

a) Show that for any integer n, if $n = s^2 + t^2$ for s, $t \in \mathbb{Z}$ then $n \not\equiv 3 \mod 4$.

b) Show that if n, s, $t \in \mathbb{Z}$ and $s + it$ divides n, then $s - it$ divides n and $s^2 + t^2$ divides n^2 in $\mathbb{Z}$. Show also, using the fact that complex conjugation is multiplicative or otherwise, that if $n_1 \in \mathbb{Z}_+$ and $n_2 \in \mathbb{Z}_+$ are both the sums of the squares of two integers, then the same is true for $n_1 n_2$.

c) Using the fact that $\mathbb{Z}[i]$ is a unique factorisation domain, show that if s and t are both non-zero integers and $s + it$ is prime in $\mathbb{Z}[i]$, then $s^2 + t^2$ is prime in $\mathbb{Z}$. Deduce that if $s + it$ divides n in $\mathbb{Z}[i]$ then $s^2 + t^2$ divides n in $\mathbb{Z}$.

d) Let $p \in \mathbb{Z}_+$ be prime in $\mathbb{Z}$ and let $p \equiv 1 \mod 4$. Using the fact that -1 is a quadratic residue mod p, show that ap is a sum of two integer squares for some $a \in \mathbb{Z}_+$. Use unique factorisation of $\mathbb{Z}[i]$ and $\mathbb{Z}$ to show that p is also the sum of two integer squares. Give an example to show that if $n \equiv 1 \mod 4$, then it need not be a sum of two square integers if one of the primes dividing n is equal to $3 \mod 4$.

[20 marks]

7. Define the Legendre symbol

$$\left(\frac{q}{p}\right)$$

for any positive prime p and any integer q coprime to p. Show that if p is any odd prime then

$$\left(\frac{q}{p}\right) \equiv q^{(p-1)/2} \bmod p,$$

stating any theory that you use. Remember that, since p is prime, G_p contains a primitive element. Deduce that

$$F : q \bmod p \mapsto \left(\frac{q}{p}\right) : G_p \to \{\pm 1\}$$

is a group homomorphism. State Gauss' Law of quadratic reciprocity for $\left(\frac{q}{p}\right)$ for any distinct positive primes q and p, including the case $q = 2$. Compute

$$\left(\frac{6}{17}\right) \quad \text{and} \quad \left(\frac{23}{73}\right).$$

Show that if p is any odd prime,

$$\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1 \mod 3.$$

Deduce that there are infinitely many primes that are 1 mod 3.
Hint. Suppose that there are finitely many such primes q_i, with $1 \leq i \leq n$ and let p be any prime dividing $N^2 + 3$, where

$$N = \prod_{i=1}^{n} q_i.$$

[20 marks]