MATH342 Practice Exam

This exam is intended to be in a similar *style* to the examination in May/June 2012. It is not implied that all questions on the real examination will follow the content of the practice questions very closely. You should expect the unexpected, especially at the ends of exam questions, and think things out as best you can.

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

$$x \equiv y \bmod n$$

in terms of division by n. Prove that if $gcd(n, m) = 1$ then

$$mx \equiv my \bmod n \Leftrightarrow x \equiv y \bmod n.$$

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

a) $3x \equiv 6 \bmod 9$.

b) $3x \equiv 5 \bmod 6$.

c) $x^2 + x + 1 \equiv 0 \bmod 5$.

d) $x^2 \equiv 1 \bmod 7$.

e) Solve the simultaneous equations $\begin{pmatrix} 3x \equiv 1 \bmod 7 \\ x \equiv 5 \bmod 6 \\ 3x \equiv 2 \bmod 5 \end{pmatrix}$.

[20 marks]

2. If p and q are positive primes with $p < q$ and n is composite (that is, not prime) for all integers n with $p < n < q$, then the set

$$G(p, q) = \{n \in \mathbb{Z}_+ : p < n < q\}$$

is called a *prime gap* and its *length* is $q - p$.

a) By considering the integers $n! + k$ for $2 \leq k \leq n$ show that there is a prime gap of length $\geq n$ for each $n \in \mathbb{Z}_+$. Find the least possible prime p such that $G(p, q)$ is a prime gap of length 4.

b) State the Fundamental Theorem of Arithmetic. Use it to show that, if n is composite, then n is divisible by a prime p with $p \leq \sqrt{n}$. Use this to show that 89 and 97 are prime.

c) Define the prime number counting function $\pi(x)$. State the Prime Number Theorem.

d) Let p_k $(k \geq 1)$ be an enumeration of all the positive primes with $p_1 = 2$ and $p_k < p_{k+1}$ for all $k \geq 1$ Prove that if n is sufficiently large, then there is a prime gap $G(p_k, p_{k+1})$ with $p_k \leq n$ and $p_{k+1} - p_k > \frac{1}{2} \ln n$.

   Hint: Let m be the largest integer with $p_m \leq n$. Consider $\sum_{k=1}^{m}(p_{k+1} - p_k)$ and apply the Prime Number Theorem to $\pi(n)$.

3. State Fermat's Little Theorem.

(i) Use it to prove that $2^{99} + 3^{98}$ is divisible by 17.

(ii) Find all the possible orders of elements of the group of units G_{17}. Find all primitive elements. Give an example of an element of each possible order.

(iii) Let m and $n \in \mathbb{Z}_+$ with $n \geq 2$, and let $\dfrac{n^m - 1}{n - 1}$ be divisible by 17. Show that either m is even; or $m \equiv 0 \bmod 17$ and $n \equiv 1 \bmod 17$. Find all possible values of n in the cases when m is even but not divisible by 4, or is divisible by 4 but not divisible by 8.

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 $\phi(2016)$ and $\phi(11!)$.
Find all integers n such that $\phi(n) = 10$.

5. Let $n_1 \geq 2$ and $n_2 \geq 2$ be coprime integers. Show that, for integers x and y,

$$x \equiv y \bmod n_1 n_2 \Leftrightarrow (x \equiv y \bmod n_1 \;\wedge\; x \equiv y \bmod n_2).$$

Give an example to show that this is not true in general if n_1 and n_2 are not coprime.

Recall that $n \in \mathbb{Z}_+$ is a *pseudoprime to base* a if $a^{n-1} \equiv 1 \bmod n$, and n is a *Carmichael number* if n is composite and is a pseudoprime to base a for all a in the group G_n of units mod n.

Let $n = 2^{11} - 1 = 2047$. Verify that 2047 is a pseudoprime to base 2. Explain why any prime dividing $2^{11} - 1$ must be 1 mod 11 and find the prime factorisation of 2047.

Give Korselt's equivalent definition of a Carmichael number. Use it to verify that 2821 is a Carmichael number.

Now let n be any integer ≥ 2. Show that

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

is a subgroup of G_n.

Now let $n = 35$. Identify all a mod 35 such that 35 is a pseudoprime to base a.

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 $\mathbb{Z}[i]$ is a Euclidean domain with Euclidean valuation $v(s + it) = s^2 + t^2$.
Hint: Show that if $z \in C$ then there is $q \in \mathbb{Z}[i]$ such that $|z - q|^2 \leq \frac{1}{2}$. If a and $b \in \mathbb{Z}[i]$ with $b \neq 0$, apply this with $z = a/b$.

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) Explain why any integer n which is a sum of two non-zero integer squares is the product of primes with this property and a square of an integer. The square of the integer can be just 1 but there must be at least one prime in the product.

e) Show that there are infinitely many primes which are the sum of two squares.
Hint: Suppose there are just finitely many such primes q_i, $1 \leq i \leq n$. Then let $N_1 = \prod_{i=1}^{n} q_i$ and $N = N_1^2 + 1$. Consider any prime p which divides N.

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. In particular, you may assume the existence of a primitive element in G_p.
Deduce that

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

is a group homomorphism.
State the value of $\left(\frac{-1}{p}\right)$ for any odd prime p.
State Gauss' Law of quadratic reciprocity for $\left(\frac{q}{p}\right)$ for any distinct positive primes q and p, including the case $q = 2$. Deduce from these laws that for any odd prime p

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 \text{ if } p = 1 \text{ or } 3 \bmod 8 \\ -1 \text{ if } p = -1 \text{ or } -3 \bmod 8. \end{cases}$$

Compute

$$\left(\frac{5}{19}\right) \quad \text{and} \quad \left(\frac{46}{89}\right).$$