Queen Mary

UNIVERSITY OF LONDON

B.Sc. EXAMINATION[1]

MAS/202 ALGORITHMIC MATHEMATICS

May 7 2003, 14:30. Duration: 3 hours

Attempt all questions. Marks awarded are shown next to the questions. CALCULATORS ARE NOT PERMITTED.

In essay-type questions, the notation [$\not\in$, n] indicates that the essay should not contain any mathematical symbols whatsoever, apart from numerals. The integer n —when present— prescribes the *approximate* length (in words). In the absence of this notation, mathematical symbols may be used freely.

Quality of presentation is essential for high marks.

---

1. *Basics* [5+5+(3+5)+(3+5)]

(*a*) Prove that, for all $X, Y \in \{\text{TRUE}, \text{FALSE}\}$,

$$X \text{ OR } Y = \text{NOT}((\text{NOT}\,X) \text{ AND } (\text{NOT}\,Y)).$$

(*b*) By tracing the following statement sequence, determine the value of x and y on termination

```
x := 3;
y := −1;
while x ∈ ℤ do
    if x < 0 then
        x := x + 1;
    fi;
    t := x;
    x := −y + 2x/3;
    y := t;
od;
```

(*c*) Consider the recursive algorithm

```
Algorithm A
INPUT: x ∈ ℤ, x > 0
OUTPUT: ??
if x = 1 then
    return 1;
else
    return A(x − 1)/x;
fi;
end;
```

- Compute A(5).
- Explain in one sentence what this algorithm does. [$\not\in$]

(d) Consider the following algorithm

```
Algorithm C
INPUT:  n, S, where n is a positive integer and S = (S_1, ..., S_n)
        is a sequence of n integers.
OUTPUT: ??
Z := 0;
i := 1;
while i ≤ n do
  j := i;
  while j ≤ n do
     Z := Z + S_i;
     j := j + 1;
  od;
  i := i + 1;
od;
return Z;
end;
```

- Write the output specifications.
- Rewrite the algorithm in such a way that it has only one loop.

2. *Arithmetic* [(3+5+5)+(3+6)]

(a) A *Sophie Germain prime* (SG-prime) is a positive odd prime p such that $2p + 1$ is also prime (e.g., $p = 3$).

- Find all SG-primes smaller than 50.
- Using `IsPrime`, write the following algorithm

  `Algorithm SGprime`

  `INPUT`: $x \in \mathbb{N}$.

  `OUTPUT`: TRUE if x is a SG-prime, FALSE otherwise.

  Try to make it efficient (think of the calculations in part (a)).
- Using `SGprime`, write the following algorithm

  `Algorithm NumberSGprimes`

  `INPUT`: $a, b \in \mathbb{N}$, $a < b$.

  `OUTPUT`: n, where n is the number of SG-primes
  in the closed interval $[a, b]$.

(b) Consider the algorithm `Digits`, which computes the sequence of digits of a non-negative integer, to a given base.

- Write it.
- Prove that it is correct.

3. *Modular arithmetic & equivalence* [3+(3+6)+10+6]

(a) Let $a \equiv_m c$ and $b \equiv_m d$. Prove that $ab \equiv_m cd$. All quantitites are integer.

(b) Consider the algorithm `Inverse`, which computes the inverse (if it exists) of an element of $\mathbb{Z}/(m)$.

- Write it.
- Explain how it works, stating the theorem(s) you consider most relevant.

(*c*) Explain the concept of *equivalence relation* and *equivalence class.* [¢, 120]

(*d*) Let E be an equivalence relation on a set X. For all $x \in X$, define $E(x) = \{y \in X \mid xEy\}$. Prove that $\{E(x) \mid x \in X\}$ is a partition of X.

4. *Polynomials* [3+6+6]

(*a*) Define the degree of a polynomial.

(*b*) We represent a polynomial f as a finite sequence $C = (c_1, c_2, \ldots)$ of elements of a commutative ring R, which specifies the coefficients of the polynomial, starting from the constant term: $f = c_1 + c_2x + \cdots$.

Write the following algorithm

`Algorithm Degree`

`INPUT`: C, a finite sequence of elements of R.

`OUTPUT`: d, the degree of the polynomial represented by C.

(*c*) Let $F = \mathbb{Z}/(5)$, and let $c = x^4 + 2x^3 + 3x^2 + 2x + 2$ and $d = 2x^2 + 3$ be polynomials in $F[x]$. Apply the algorithm `ExtendedGCD` to determine $g, s, t \in F[x]$, such that g is a gcd of c and d, and $g = sc + td$. Verify your calculations explicitly.

5. *Vectors* [3+6]

Let $F = \mathbb{Z}/(11)$, and let

$$w_1 = (1,0,7,3) \qquad w_2 = (0,1,3,4) \qquad w_3 = (0,0,0,1) \in F^4.$$

- Is the sequence (w_1, w_2, w_3) in echelon form? Justify your answer.
- Use the algorithm `Sift` to prove that $v = (6,2,4,3) \in \langle w_1, w_2, w_3 \rangle$. Hence write v as a linear combination of w_1, w_2, w_3, verifying your calculations explicitly.

End of examination paper