UNIVERSITY OF EDINBURGH

FACULTY OF SCIENCE AND ENGINEERING

MASTER OF SCIENCE IN COMPUTER SCIENCE

COMPUTER ALGEBRA

Tuesday 25 April 2000

4:00 to 5:30

Examiners:

I. Watson (External)

R.N. Ibbett (Chairman)

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

1. Consider the following procedure written in Maple for computing the greatest common divisor of two univariate polynomials with rational coefficients by means of the Euclidean algorithm.

```
# Input:
#   f,g ..... polynomials in x with rational coefficients.
#   x ....... a name,
# Output:
#   The greatest common divisor of f, g.
euclid_poly:=proc(f,g,x)
  local r0,r1,rt;
  r0:=f; r1:=g;
  if r0=0 and r1=0 then ERROR("both polynomials are zero.")
  elif r0=0 then r1
  elif r1=0 then r0
  else
    while r1<>0 do
      rt:=rem(r0,r1,x);
      r0:=r1; r1:=rt;
    od;
    r0
  fi
end:
```

(a) Would it be sensible to use the parameters `f`, `g` as local variables instead of `r0`, `r1`? Explain your answer briefly. *[3 marks]*

(b) The code is unreliable in one very important respect. Explain the problem and how to fix it (you are not required to supply Maple commands, a description of what to do is sufficient).

Give an example of input that causes the problem. *[4 marks]*

(c) Describe what simple changes you would make to the code so that we could calculate the greatest common divisor of polynomials from $\mathbb{Z}_p[x]$ where p is a prime number.

Would it make sense to do the same when p is not a prime? Explain your answer. *[5 marks]*

(d) Computer algebra systems do not use the Euclidean algorithm for finding the greatest common divisor of univariate polynomials with rational coefficients. Explain why this is the case. *[2 marks]*

QUESTION CONTINUES ON NEXT PAGE

(e) From now on assume that $f, g \in \mathbb{Z}[x]$. Suppose we have an application in which we simply need to know if $\gcd(f, g)$ is a constant but do not need its value otherwise (e.g., we might only need to know if f, g have any common roots in $\mathbb{C}$).

i. Define the resultant of f, g and explain how we can use it to decide if $\gcd(f, g)$ is a constant. [*3 marks*]

ii. In deciding our question we do not need the actual value of the resultant; it suffices to know if it is zero. Calculating determinants over $\mathbb{Z}_p$ where p is a prime is easier than over $\mathbb{Z}$. Describe and justify an algorithm for testing if $\mathrm{Res}(f, g) = 0$ that exploits the fact in the preceding sentence. [**Note:** You may assume that we can compute efficiently a bound on the absolute value of the determinant of any given square matrix.] [*8 marks*]

2. This question is concerned with the real roots of univariate polynomials with rational coefficients. Throughout $p(x)$ (or just p) denotes such a polynomial which is assumed to be non-zero.

   (a) Explain briefly what is meant by the *isolation* of all the real roots of $p(x)$. [*2 marks*]

   (b) Define the *square free part* of $p(x)$ and show how to compute it. Explain its significance for root isolation. [*3 marks*]

   (c) Describe an algorithm for isolating all the real roots of a polynomial (you may assume that we have a method of bounding the roots). In your description you do not need to go into details about optimizations.

   Illustrate the algorithm by using it to isolate the two real roots of $x^2 - 4x + 2$ (you *must* use the algorithm for this rather than any other method). You may assume that the roots are in $(0, 4)$ if this helps your illustration. [*10 marks*]

   (d) This part is concerned with developing an algorithm to find the rational roots of p exactly. From now on we assume that p has integer coefficients and is primitive, i.e., the gcd of the coefficients is 1.

      i. Let $a, b \in \mathbb{Z}$ be such that $b \neq 0$ and $\gcd(a, b) = 1$, so that a/b is in its lowest terms as a fraction. Prove that a/b is a root of p if and only if $bx - a$ divides p in $\mathbb{Z}[x]$.
      [**Notes:** You may assume without proof that $\alpha \in \mathbb{Q}$ is a root of p if and only $x - \alpha$ divides p in $\mathbb{Q}[x]$. You may also use Gauss's Lemma without proof; this states that the content of a product is the product of the contents.] [*4 marks*]

      ii. Let a, b be as in the preceding part and suppose that a/b is a root of p. Let r, s be the coefficients of the highest and lowest degree terms of p respectively. Prove that a divides s and b divides r. [*2 marks*]

      iii. Give a simple algorithm for finding all the rational roots of p (the values being returned as a set of rational numbers). [*4 marks*]

3. This question is concerned with Gröbner bases of ideals of polynomials in one or more indeterminates and with coefficients from a field k.

   (a) Explain what is meant by an *admissible ordering* on power products. [*2 marks*]

   (b) i. Prove that if we have only one indeterminate x then the only admissible ordering is $1 < x < x^2 < x^3 < \cdots$. [*3 marks*]

   ii. Let I be an ideal of $k[x]$ and choose p to be the monic polynomial in I of smallest degree. Show that $\{ p \}$ is the normed reduced Gröbner basis for I. [*6 marks*]

   iii. Suppose that

$$I = (p_1, p_2, \ldots, p_m).$$

   Give a simple method for computing the normed reduced Gröbner basis of I *without* appealing to Buchberger's algorithm. (You are not required to prove the correctness of your method.)
   [**Hint:** Start with the case $m = 2$ bearing the preceding part in mind.] [*5 marks*]

   (c) Let x, y, z be indeterminates over $\mathbb{C}$ and let I be the ideal of $\mathbb{C}[x, y, z]$ generated by

$$\begin{aligned} f &= x^2 - 2xz + z^2, \\ g &= xy - xz - yz + z^2 \\ h &= y^2 - 2yz + z^2. \end{aligned}$$

   In fact $\{ f, g, h \}$ is a Gröbner basis for I w.r.t. the lexicographic ordering where $x >_L y >_L z$.

   i. Explain briefly why we know that f, g, h have infinitely many common zeros just from the format of the given Gröbner basis (i.e., we do not need to carry out any further manipulations).
   Show that, in fact, the set of common zeros of f, g, h is precisely $\{(\alpha, \alpha, \alpha) \mid \alpha \in \mathbb{C}\}$. [*5 marks*]

   ii. It is a simple fact that $I \subseteq \mathbf{I}\,\mathbf{V}(I)$. Prove that this containment is strict, i.e., produce a polynomial p that is in $\mathbf{I}\,\mathbf{V}(I)$ but not in I (you must prove that this is the case).
   Explain briefly why all sufficiently high powers of p are guaranteed to reduce to 0 w.r.t. the given Gröbner basis. [*4 marks*]