Notes for MA591U, Spring 2001
(Symbolic Computation)

Topics in this course

(1) What does this mean:

$$\int e^{x^2} dx \text{ is not expressible in finite terms.}$$

(2) How to integrate rational functions: if $p, q \in \mathbb{Q}[x]$

$$\int \frac{p(x)}{q(x)} dx = R(x) + \sum c_i \log u_i + \sum d_i \arctan v_i$$

where $R(x) \in \mathbb{C}(x)$.

(3) What does this mean:

$$y'' + xy = 0 \text{ is not solvable in finite terms.}$$

(4) Differential Galois Theory with application from latest ISSAC: an efficient test to decide if $P(x, y) \in \mathbb{Q}[x, y]$ is irreducible over $\mathbb{C}[x, y]$.

(5) Nonlinear differential equations $f(y', y) = 0$ where f is a polynomial: what is a singular solution?

Polynomials over k-fields

Let $k[x]$ denote the ring of polynomials in one variable.

DEFINITION: The polynomial p is **irreducible** if $p = p_1 p_2$ implies that $p_1 \in k$ or $p_2 \in k$.

DEFINITION: The **greatest common divisor** of $f, g \in k[x]$ is the monic polynomial d such that $d|a$, $d|b$, and for any $c \in k[x]$,

$$[(c|a) \vee (c|b)] \Rightarrow c|d.$$

FACTS:

(1) We can write every polynomial $f \in k[x]$ as

$$f = \prod_{i=1}^{r} p_i$$

where each p_i is irreducible. Furthermore, if

$$f = \prod_{i=1}^{s} q_i$$

with each q_i irreducible, then $r = s$ and, after reindexing, $p_i = \alpha_i q_i$ for some $\alpha_i \in k$.

(2) Every two polynomials a, b have a unique greatest common divisor.

(3) Every ideal $I \lhd k[x]$ is principal; that is, $\exists d \in k[x]$ so that $I = \langle d \rangle$.

(4) $\langle a, b \rangle = \langle \gcd(a, b) \rangle$.

QUESTION 1: Given $a, b \in k[x]$, find $\gcd(a, b)$, and find u, v so that $ua + vb = \gcd(a, b)$.

SOLUTION, PART A: The Euclidean Algorithm.

Set $r_0 = a$, $r_1 = b$, and divide $r_{i-1} = q_i r_i + r_{i+1}$. Continue dividing until we reach step m where $r_{m+1} = 0$. Then $\gcd(a, b) = r_m$.

SKETCH OF PROOF:

Since $r_{m-1} = q_m r_m + 0$, it is clear that $r_m | r_{m-1}$. The previous step in the algorithm had

$$r_{m-2} = q_{m-1} r_{m-1} + r_m.$$

We can rewrite this as

$$r_{m-2} = (q_{m-1} q_m + 1) r_m$$

so $r_m | r_{m-2}$. Proceeding inductively, we see that $r_m | a$ and $r_m | b$.

Suppose there is another $c \in k[x]$ so that $c|a$ and $c|b$. Let u and v be such that $ua + vb = r_m$. (That such exist, see the Extended Euclidean Algorithm below.) Let s and t be such that $sc = a$ and $tc = b$. Then

$$r_m = u(sc) + v(tc) = (us + vt)c$$

whence $c | r_m$.

EXAMPLE: Let $r_0 = a = x^3 - 1$ and $r_1 = b = x^2 - 1$. Then

$$x^3 - 1 = x(x^2 - 1) + (x - 1)$$

so $q_1 = x$ and $r_2 = x - 1$. Continuing the process,

$$x^2 - 1 = (x + 1)(x - 1) + 0$$

so $q_2 = x + 1$ and $r_3 = 0$. Hence $\gcd(x^3 - 1, x^2 - 1) = r_2 = x - 1$.

SOLUTION, PART B: Extended Euclidean Algorithm.

Define triples $W_i = (t_i, u_i, v_i)$ with $W_0 = (a, 1, 0)$, $W_1 = (b, 0, 1)$, and

$$W_{i+1} = W_{i-1} - q_i W_i.$$

Observe that $t_{i-1} = q_i t_i + r_i$. Eventually we find that $t_j = 0$ and $t_{j-1} = \gcd(a, b)$. We claim that

$$\gcd(a, b) = u_{j-1}a + v_{j-1}b.$$

SKETCH OF PROOF:

Induction: show that at each stage

$$t_i = u_i a + v_i b.$$

EXAMPLE. Continuing the example above,

$$\begin{aligned}
W_0 &= (x^3 - 1, 1, 0) \\
W_1 &= (x^2 - 1, 0, 1) \\
W_2 &= (x^3 - 1, 1, 0) - x(x^2 - 1, 0, 1) = (x - 1, 1, -x) \\
W_3 &= (x^2 - 1, 0, 1) - (x + 1)(x - 1, 1, -x) = (0, -x - 1, x^2 + x + 1).
\end{aligned}$$

So $0 = -(x + 1)(x^3 - 1) + (x^2 + x + 1)(x^2 - 1)$.

FACTORING: We can in general factor any polynomial $p \in \mathbb{Q}[x]$; there is the polynomial-time algorithm of Lenstra, Lenstra, and Levasz for this. This takes too long, though; we would like to try something else. See next set of notes.