GROUP TEST
S.-T YAU COLLEGE MATH CONTESTS 2012

Applied Math. and Computational Math.

Please solve 4 out of the following 5 problems.

1. If the function $u(x)$ is in C^{k+1} (has continuous $(k+1)$-th derivative) on the interval $[0, 2]$, and a sequence of polynomials $p_n(x)$ ($n = 1, 2, 3, ...$) of degree at most k satisfies

$$(1) \qquad |u(x) - p_n(x)| \le \frac{C}{n^{k+1}} \qquad \forall\ 0 \le x \le \frac{1}{n},$$

where the constant C is independent of n, prove

$$|u(x) - p_n(x)| \le \frac{\tilde{C}}{n^{k+1}} \qquad \forall\ \frac{1}{n} \le x \le \frac{2}{n},$$

with another constant $\tilde{C}$ which is also independent of n.

2. Consider the one-dimensional elliptic equation

$$-\frac{d^2}{dx^2}u(x) = f(x), \quad 0 < x < 1,$$

with homogeneous boundary condition, $u(0) = 0$ and $u(1) = 0$, $f \in L^2(0, 1)$.

(i) Describe the standard piecewise linear finite element method for this boundary value problem.

(ii) Is this method stable and convergent? If so, what is the order of convergence?

(iii). In this case, the linear finite element method has a super convergence property at the nodal point x_j ($j = 1, 2, ..., N$), i.e. $u_h(x_j) = u(x_j)$, here u_h is the finite element solution and u is the exact solution. Could you explain why?

3. Let $A = (a_{ij}) \in M_{N\times N}(\mathbb{C})$ be strictly diagonally dominant, that is,

$$|a_{ii}| > \sum_{j=1, j\neq i}^{N} |a_{ij}| \text{ for all } 1 \le i \le N,$$

Assume that $A = I + L + U$ where I is the identity matrix, L and U are the lower and upper triangular matrices with zero diagonal entries.

Now, we consider solving the linear system $Ax = b$ by the following iterative scheme:

$$(*) \quad x^{k+1} = (I+\alpha\Omega L)^{-1}[(I-\Omega)-(1-\alpha)\Omega L-\Omega U]x^k+(I+\alpha\Omega L)^{-1}b$$

where $\Omega := \mathbf{diag}(\omega_1, ...\omega_N)$ and $0 \le \alpha \le 1$. (When $\alpha = 1$, it gives the SOR method.)

(1) Prove that the linear system $Ax = b$ has a unique solution.
(2) Prove that the necessary condition for the convergence of (*) is

$$\prod_{i=1}^{N} |1-\omega_i| < 1$$

(3) Let $M = (I+\alpha\Omega L)^{-1}[(I-\Omega)-(1-\alpha)\Omega L-\Omega U)]$. Prove that the spectral radius $\rho(M)$ of M is bounded by:

$$\rho(M) \le \max_i \frac{|1-\omega_i| + |\omega_i|((|1-\alpha|l_i + u_i)}{1-|\omega_i\alpha|l_i}$$

whenever $|\omega_i\alpha|l_i < 1$ for all $1 \le i \le N$ where $l_i = \sum_{j<i} |a_{ij}|$ and $u_i = \sum_{j>i} |a_{ij}|$.
(4) Using (c), prove that the sufficient condition for the convergence of (*) is

$$0 < \omega_i < \frac{2}{1+l_i+u_i} \quad \text{for all } 1 \le i \le N$$

4. The famous *RSA cryptosystem* is based on the assumed difficulty of factoring integers $N = pq$ (called RSA integers) which are products of two large primes p and q which should be kept secret. Currently p and q are chosen to be about 500 bits long, that is,

$$p, q \approx 2^{500}.$$

Assume someone uses the following algorithm to find secret n-bit primes p and q to form an RSA integer $N = pq$:

- Choose a random odd 500-bit integer s.
- Test the odd numbers s, $s+2$, $s+4$, etc. for primality until the first prime p is found (note the primality testing is very easy nowdays).
- Continue testing $p+2$, $p+4$, $p+6$, etc. for primality until the second prime q is found.
- Compute and publish $N = pq$, but keep p and q secret.

How secure is this procedure? Can you suggest an algorithm to factor an RSA integer $N = pq$ generated this way?

Note that there are about $x/\log x$ primes up to x, where $\log x$ is the natural logarithm. This means that the expected gap between two consecutive n-bit primes is

$$\log 2^n = n \log 2 \approx 0.69 \cdot n.$$

5. The solution $h(r,t)$ of the following Boussinesq equation describes the hight of a circular drop of fluid spreading on a dry surface $h=0$:

$$\frac{\partial h}{\partial t} = \Delta_r(h^2) = \frac{1}{r}\frac{\partial}{\partial r}\left(r\frac{\partial(h^2)}{\partial r}\right), \quad r>0, \quad t>1$$

with

$$\left.\frac{\partial h}{\partial r}\right|_{r=0} = 0, \qquad \int_0^\infty h(r,t) r dr \equiv \frac{1}{64}$$

The solution is positive on a finite range $0 \le r \le r_*(t)$ with $h(r_*(t),t) = 0$ defining a moving "edge" position with no fluid outside of the droplet. For $r > r_*(t)$ truncate the solution beyond the edge to be zero ($h \equiv 0$ for $r > r_*(t)$).

- **(a):** Show that this problem is scale invariant by finding relations $h(r,t) = H(T)\tilde{h}(\tilde{r},\tilde{t})$, $r = R(T)\tilde{r}$, $t = T\tilde{t}$ so that the problem for $\tilde{h}(\tilde{r},\tilde{t})$ is identical to the original problem.
- **(b):** Determine the ODE for the similarity function $\Phi(\eta)$ with $h(r,t) = t^\alpha \Phi(\eta)$, $r = \eta t^\beta$.
- **(c):** Determine the explicit solution for $\Phi(\eta)$ and then use $h(r,t) = t^\alpha \Phi(\eta)$ to find $r_*(t)$ for $t \ge 1$.
  Hint $\int_0^\infty hrdr = \int_0^{r_*} hrdr$.