GROUP TEST
S.-T YAU COLLEGE MATH CONTESTS 2012

Analysis and Differential Equations

Please solve 5 out of the following 6 problems.

1. Let $A = [a_{ij}]$ be a real symmetric $n \times n$ matrix. Define $f : \mathbb{R}^n \to \mathbb{R}$ by $f(x_1, \cdots, x_n) = \exp(-\frac{1}{2}\sum_{i,j=1}^n a_{ij}x_ix_j)$. Prove that f is in $L^1(\mathbb{R}^n)$ if and only if the matrix A is positive definite.

Compute $\int_{\mathbb{R}^n} \exp(-\frac{1}{2}\sum_{i,j=1}^n a_{ij}x_ix_j + \Sigma_{i=1}^n b_ix_i)dx$ when A is positive definite.

2. Let V be a simply connected region in the complex plane and $V \neq \mathbb{C}$. Let a, b be two distinct points in V. Let ϕ_1, ϕ_2 be two one-to-one holomorphic maps of V onto itself. If $\phi_1(a) = \phi_2(a)$ and $\phi_1(b) = \phi_2(b)$, show that $\phi_1(z) = \phi_2(z)$ for all $z \in V$.

3. In the unit interval [0, 1] consider a subset
$E = \{x|$ in the decimal expansion of x there is no $4\}$,
show that E is measurable and calculate its measure.

4. Let $1 < p < \infty, L^p([0,1], dm)$ be the completion of $C[0,1]$ with the norm: $||f||p = (\int_0^1 |f(x)|^p dm)^{\frac{1}{p}}$, where dm is the Lebesgue measure. Show that $\lim_{\lambda\to\infty} \lambda^p m(x||f(x)| > \lambda) = 0$.

5. Let $\mathfrak{F} = \{e_\nu\}, \nu = 1, 2, ..., n$ or $\nu = 1, 2, ...$ is an orthonormal basis in an inner product space H. Let E be the closed linear subspace spanned by $\mathfrak{F}$. For any $x \in H$ show that the following are equivalent: 1) $x \in E$; 2) $||x||^2 = \Sigma_\nu |(x, e_\nu)|^2$; 3) $x = \Sigma_\nu (x, e_\nu)e_\nu$.

Let $H = L^2[0, 2\pi]$ with the inner product $< f, g >= \frac{1}{\pi}\int_0^{2\pi} f(x)g(x)dx$,
$\mathfrak{F} = \{\frac{1}{2}, \cos x, \sin x, ..., \cos nx, \sin nx, ...\}$
be an orthonormal basis. Show that the closed linear sub-space E spanned by $\mathfrak{F}$ is H.

6. Let $\mathcal{H} = L^2[0, 1]$ relative to the Lebesgue measure and define $(Kf)(s) = \int_0^s f(t)dt$ for each f in $\mathcal{H}$. Show that K is a compact operator without eigenvalues.

GROUP TEST
S.-T YAU COLLEGE MATH CONTESTS 2012

Geometry and Topology

Please solve 5 out of the following 6 problems.

1. Prove that the real projective space $\mathbb{RP}^n$ is a differentiable manifold of dimension n.

2. Let M, N be n-dimensional smooth, compact, connected manifolds, and $f : M \to N$ a smooth map with rank equals to n everywhere. Show that f is a covering map.

3. Given any Riemannian manifold (M^n, g), show that there exists a unique Riemannian connection on M^n.

4. Let S^n be the unit sphere in $\mathbb{R}^{n+1}$ and $f : S^n \to S^n$ a continuous map. Assume that the degree of f is an odd integer. Show that there exists $x_0 \in S^n$ such that $f(-x_0) = -f(x_0)$.

5. State and prove the Stokes theorem for oriented compact manifolds.

6. Let M be a surface in $\mathbb{R}^3$. Let D be a simply-connected domain in M such that the boundary ∂D is compact and consists of a finite number of smooth curves. Prove the Gauss-Bonnet Formula:

$$\int_{\partial D} k_g \, ds \; + \sum_j (\pi - \alpha_j) + \iint_D K \, dA \; = \; 2\pi,$$

where k_g is the geodesic curvature of the boundary curve. Each α_j is the interior angle at a vertex of the boundary, K is the Gaussian curvature of M, and the 2-form dA is the area element of M.

GROUP TEST

S.-T YAU COLLEGE MATH CONTESTS 2012

Algebra and Number Theory

Please solve 5 out of the following 6 problems.

1. Let $a_1, \cdots, a_n$ and $b_1, \cdots, b_n$ be complex numbers such that $a_i + b_j \neq 0$ for all $i, j = 1, \cdots, n$. Define $c_{ij} := \dfrac{1}{a_i + b_j}$ for all $i, j = 1, \cdots, n$, and let C be the $n \times n$ determinant with entries c_{ij}. Prove that

$$det(C) = \frac{\prod_{1 \le i < j \le n}(a_i - a_j)(b_i - b_j)}{\prod_{1 \le i, j \le n}(a_i + b_j)}.$$

2. Recall that $\mathbb{F}_7$ is the finite field with 7 elements, and $GL_3(\mathbb{F}_7)$ is the group of all invertible 3×3 matrices with entries in $\mathbb{F}_7$.

(1) Find a 7-Sylow subgroup P_7 of $GL_3(\mathbb{F}_7)$.

(2) Determine the normalizer subgroup N of the 7-Sylow subgroup you found in (a).

(3) Find a 2-Sylow subgroup of $GL_3(\mathbb{F}_7)$.

3. Let V be a finite dimensional vector space with a positive definite quadratic form $(-,-)$. Let $O(V)$ denote the orthogonal group:

$$O(V) = \{g \in GL(V) : \quad (gx, gy) = (x, y), \quad \forall x, y \in V\}.$$

For any non-zero $v \in V$, let s_v denote the reflection on V:

$$s_v(w) = w - 2\frac{(v, w)}{(v, v)}v.$$

(1) Show that $s_v \in O(V)$;

(2) Show that if v and w are vectors in V with $\|v\| = \|w\|$,then there is either a reflection or product of two reflections that takes v into w;

(3) Deduce that every element of the orthogonal group of V can be written as the product of at most $2 \dim V$ reflections.

4. Consider the real Lie group $SL_2(\mathbb{R})$ of 2 by 2 matrices of determinant one. Compute the fundamental group of $SL_2(\mathbb{R})$ and describe the Lie group structure on the universal covering

$$\widetilde{SL}_2(\mathbb{R}) \to SL_2(\mathbb{R}).$$

5. Let $f \in \mathbb{C}[x, y, z]$ be an irreducible homogenous polynomial of degree $d > 0$. For each integer $n \ge d$, define

$$P(n) = \dim_{\mathbb{C}} \mathbb{C}[x, y, z]_n / f \cdot \mathbb{C}[x, y, z]_{n-d}$$

where $\mathbb{C}[x, y, z]_d$ is the subspace of homogenous polynomials of degree n. Show there are constants c such that for n sufficiently large,

$$P(n) = dn + c.$$

6. Let p be an odd prime and $\mathbb{Z}_p$ the p-adic integer which can be defined as the projective limit of $\mathbb{Z}/p^n\mathbb{Z}$ and let $\mathbb{Q}_p$ be its fractional field. Let $\mathbb{Z}_p^\times$ denote the group of invertible elements in $\mathbb{Z}_p$ which is also the projective limit of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

(1) For any integer a is not divisible by p, show that the sequence $(a^{p^n})_n$ convergent to an element $\omega(a) \in \mathbb{Z}_p$ satisfying

$$\omega(a)^{p-1} = 1, \qquad \omega(a) \equiv a \pmod{p}.$$

Moreover, $\omega(a)$ depends only on $a \mod p$.

(2) Define a logarithmic function log on $1 + p\mathbb{Z}_p$ by usual formula:

$$\log(1 + px) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{p^n}{n} x^n.$$

Show that the logarithmic function is convergent and define an isomorphism

$$1 + p\mathbb{Z}_p \to p\mathbb{Z}_p.$$

Moreover, on the dense subgroup $\log(1 + p)\mathbb{Z}$, the inverse is given by

$$\log(1 + p) \cdot x \mapsto (1 + p)^x, \qquad \forall x \in \mathbb{Z}.$$

(3) Deduce from above that $\mathbb{Z}_p^\times \simeq \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$.

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

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

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,

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

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 $|\omega_i\alpha|l_i$ 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

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

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 $\int_0^\infty hrdr = \int_0^{r_*} hrdr$.

GROUP TEST
S.-T YAU COLLEGE MATH CONTESTS 2012

Probability and Statistics

Please solve 5 out of the following 6 problems.

1. Let (X_n) be a sequence of i.i.d. random variables.

1) Assume that each X_n satisfies the exponential distribution with parameter 1 (i.e. $P(X_n \geq x) = e^{-x}, x \geq 0$). Prove that

(a) $P(X > \alpha \log n, i.o.) = 0$, if $\alpha > 1$; $P(X > \alpha \log n, i.o.) = 1$, if $\alpha \leq 1$.

Here "i.o" stands for "infinitely often", and $A_n, i.o.$ stands $\limsup_{n\to\infty} A_n$.

(b) Let $L = \limsup_{n\to\infty}(X_n/\log n)$, then $P(L = 1) = 1$.

2) Assume that each X_n satisfies the Poisson distribution with parameter λ (i.e. $P(X_n = k) = \frac{\lambda^k}{k!}e^{-\lambda}, k = 0, 1, 2, \cdots.$) Put

$$L = \limsup_{n\to\infty}(X_n \log\log n/\log n).$$

Prove that $P(L = 1) = 1$.

2. Let X_i be i.i.d exponential r.v with rate one, $i \geq 1$. Let N be a geometric random variable with success probability p, $0 < p < 1$, i.e. $P(N = k) = (1-p)^{k-1}p, k = 1, 2, \cdots$, and independent of all X_i, $i \geq 1$. Find the distribution of $\sum_{i=1}^N X_i$.

3. Let X and Y be i.i.d real valued r.v's. Prove that $P(|X+Y| < 1) \leq 3P(|X - Y| < 1)$.

4. Suppose $S = X_1 + X_2 + \cdots + X_n$, a sum of independent random variables with X_i distributed Binomial(1, p_i). Show that $\mathbb{P}(S\ even) = 1/2$ if and only if at least one p_i equals 1/2.

5. Let B_θ denote the closed unit ball in $\mathbb{R}^2$ with center θ. Suppose $X_1, X_2, \cdots, X_n$ are independently distributed on B_θ, for an unknown θ in $\mathbb{R}^2$. Denote that maximum likelihood estimator by $\hat{\theta}$. Show that $|\hat{\theta} - \theta| = O_p(1/n)$.

6. Suppose that $X_1, \cdots, X_n$ are a random sample from the Bernoulli distribution with probability of success p_1 and $Y_1, \cdots, Y_n$ be an independent random sample from the Bernoulli distribution with probability of success p_2.

(a) Derive the maximum likelihood ratio test statistic for

$$H_0 : p_1 = p_2 \longleftrightarrow H_1 : p_1 \neq p_2.$$

(Note: No simplification of the resulting test statistic is required. However, you need to give the asymptotic null.)

(b) Compute the asymptotic power of the test with critical region

$$|\sqrt{n}(\hat{p}_1 - \hat{p}_2)/\sqrt{2\hat{p}\hat{q}}| \geqslant z_{1-\alpha}$$

when $p_1 = p$ and $p_2 = p + n^{-1/2}\Delta$, where $\hat{p} = 0.5.\hat{p}_1 + 0.5\hat{p}_2$.