IMC 2012 Team Selection Exam

Duration: 4 hours

June 6, 2012

Question 1 (10 points)

Prove that the matrix $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 \\ 1 & 2 & 3 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ is positive definite.

Solution:

We substract the first row from the others, and do the same with the first column. This gives:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 \\ 1 & 2 & 3 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 3 \end{pmatrix}.$$

Repeating the process for the smaller matrix, we are done.

Question 2 (10 points)

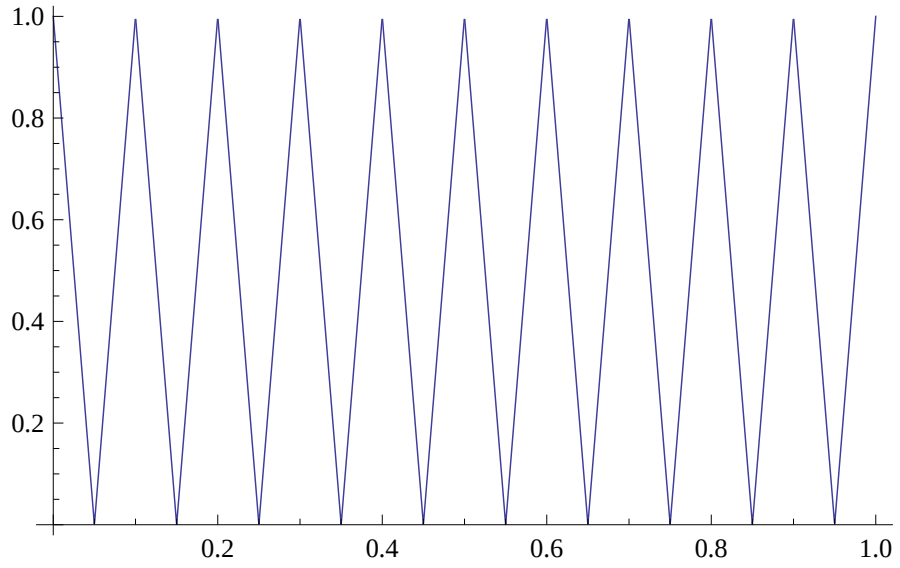
A graph of a continuous function $f : [0, 1] \to [0, 1]$ is a broken line consisting of 10 intervals. The graph of the function $f(f(x))$ is a broken line consisting of n intervals.

1. What is the maximal possible value of n?
2. What is the minimal possible value of n?

Solution:

1. The maximal value of n is 100. This can be easily seen by constructing a zigzag line that goes up and down many times, each time covering the entire domain:

$$f(x) = 2\left|(10x - \lfloor 10x \rfloor) - \frac{1}{2}\right|.$$



In this case, $f(x)$ covers its entire domain 10 times, and for each such time there are 10 intervals. Therefore, $f(f(x))$ is composed of a total of 100 intervals.

2. The minimal value of n is 1. Indeed, it is possible to construct such a function f which is its own inverse, meaning that $f(f(x)) = x$ has one interval. How do we construct such a function? Being its own inverse is equivalent to being symmetric around the line $y = x$. So take any 11 points symmetric with respect to that line, for example $\vec{x}_n = (\cos\frac{90°n}{10}, \sin\frac{90°n}{10})$, $0 \le n \le 10$, and the line f composed of the intervals between two such subsequent points is a funtion, inverse to itself.

Question 3 (10 points)

Let $p(x)$ be a non-constant polynomial with integer coefficients. Prove that there exists a natural number n, such that $p(n)$ has at least 5772 distinct prime divisors.

Solution:

Suppose that there was such a polynomial P. We call a prime q *good* if $P(x) \equiv 0 \pmod q$ has a solution modulo q. Now, suppose that there were 5772 good primes. By the Chinese Remainder theorem, there is a single value of x such that $P(x) = 0 \pmod q$ for each one of the 5772 good primes. In particular, $P(x)$ is divisible by at least 5772 distinct prime numbers, so we are done. As a result, there are no more than 5771 good primes.

However, note that by the definition of good primes, $P(x)$ is never divisible by a bad prime. Thus, we see that $P(x) \in \{q_1^{n_1} \cdots q_{5771}^{n_{5771}}\}$, where $q_1, \ldots, q_{5771}$ are the good primes. We will show that the set $A = \{q_1^{n_1} \cdots q_{5771}^{n_{5771}}\}$ is spread way too thinly for this to be possible.

Indeed, the number of elements in A smaller than N is significantly less than:

$$\log_{q_1} N \cdots \log_{q_{5771}} N = O(\log(N)^{5771}).$$

But, this means that the average distance between such consecutive elements is at least:

$$O\left(\frac{N}{\log(N)^{5771}}\right).$$

However, for values $x < M$, we have that $P(x) = O(M^d)$, where d is the degree of P, and the distance between consecutive values of P is $P(x+1) - P(x) < O(M^{d-1})$. But eventually, $O(M^{d-1}) < O\left(\frac{M^d}{\log(M^d)^{5771}}\right)$, so the distances grow too large for P to skip in one go, a contradiction - as we wanted to show.

Question 4 (10 points)

Let $K \subseteq \mathbb{R}^2$ be a convex shape, symmetric with respect to the origin. Suppose that $\iint_K \operatorname{dist}(\vec{x}, \partial K)\, \mathrm{d}^2\vec{x} > 2$, where $\operatorname{dist}(\vec{x}, \partial K)$ is the distance from $\vec{x}$ to the boundary of K. Prove that K contains at least 3 integer points.

Solution:

Suppose that $\iint_K \operatorname{dist}(\vec{x}, \partial K)\, \mathrm{d}^2\vec{x} > 2$. Now, if $\operatorname{dist}(\vec{0}, \partial K) > 1$, then K would contain a circle of radius more than one around the origin, and such a circle has at least 5 integer points in it, so we win. So, suppose that $\operatorname{dist}(\vec{0}, \partial K) \leq 1$.

We note two more facts: first of all, because K is symmetric, the function $f(\vec{x}) = \operatorname{dist}(\vec{x}, \partial K)$ is also symmetric: $f(-\vec{x}) = f(\vec{x})$. In addition, f is a convex function in K because K is convex (this can be very easily seen). In particular, the maximum of f in K is obtained at 0.

Now, consider the level curves of f, that is: $L_z = \{\vec{x} \in K | f(\vec{x}) = z\}$. Then $L_0 = \partial K$, and the curves are convex shapes contained in one another. In particular, if we denote by $\ell(L_z)$ the length of the curve L_z, then $\ell(L_z)$ is a monotonically decreasing function of z.

The last thing we note is that:

$$\iint_K 1 \cdot \mathrm{d}^2\vec{x} = \int_0^1 \ell(L_z)\, \mathrm{d}z,$$
$$\iint_K \operatorname{dist}(\vec{x}, \partial K)\, \mathrm{d}^2\vec{x} = \int_0^1 z\ell(L_z)\, \mathrm{d}z.$$

So, we see that:

$$\frac{\iint_K \operatorname{dist}(\vec{x}, \partial K)\, \mathrm{d}^2\vec{x}}{\iint_K 1 \cdot \mathrm{d}^2\vec{x}} = \frac{\int_0^1 z\ell(L_z)\, \mathrm{d}z}{\int_0^1 \ell(L_z)\, \mathrm{d}z}.$$

Hence, the right hand side is a weighted average of a quantity ranging from 0 to 1, with a weight which is monotonically decreasing. Thus, it is no more than $\frac{1}{2}$. As a result, we have:

$$\frac{\iint_K \operatorname{dist}(\vec{x}, \partial K)\, \mathrm{d}^2\vec{x}}{\iint_K 1 \cdot \mathrm{d}^2\vec{x}} \leq \frac{1}{2},$$

meaning that:

$$S = \iint_K 1 \cdot \mathrm{d}^2\vec{x} \geq 2 \iint_K \operatorname{dist}(\vec{x}, \partial K)\, \mathrm{d}^2\vec{x} > 4.$$

Therefore, by Minkowski's theorem, we are done.

Question 5 (10 points)

Consider words consisting of zeroes and ones. Several words of length 30 are considered

obscene. Can it happen that there exists an infinite periodic word, which contains no obscene subwords, and that all such infinite words are periodic, and their period is greater than 10^9?

Solution:

It is impossible.

Consider the following directed graph D: its vertices are all words of length 30, and two words u, v have a directed edge $u \to v$ iff there is some word w of length 29 and two letters a, b such that $u = aw$, $v = wb$. Thus, D is a directed graph such that each vertex has two ingoing and two outgoing edges. With this terminology, an infinite word is just an infinite path in this graph, and a word has an obscene subword iff it goes through a vertex corresponding to an obscene word.

We call a vertex *essentially obscene* iff all paths starting there must pass through an obscene word. The information given in the question means that this graph, with all essentially obscene words removed, is a single directed cycle of length at least 10^9. But the size of D is just 2^{30}, which is barely bigger than 10^9. So somehow, we removed almost no vertices from a graph with quite a lot of edges, and we are left with a cycle. There are many easy ways to show that this is impossible.

For example, for each essentially obscene vertex we remove, the number of edges decreases by no more than 4. Initially, there were 2^{31} edges. At the end, the graph is a cycle, so it has no more than 2^{30} edges. So at least 2^{28} vertices were removed. So there are no more than $2^{30} - 2^{28} = \frac{3}{4} \cdot 2^{30}$ vertices left. But there are at least 10^9 vertices left. Therefore, $\frac{3}{4} \cdot 2^{30} \geq 10^9$, which is plainly false.

Question 6 (10 points)

Let A, B be matrices with integer entries, such that $\det A = 1$.

1. Can we claim that $B^{-1}AB$ has integer entries?
2. Can we claim that there is a number n, such that $(B^{-1}AB)^n$ has integer entries?

Solution:

1. The answer is no. For example, if we let:

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$
$$B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix},$$

   then we have:

$$B^{-1}AB = \begin{pmatrix} 0 & -1/2 \\ 2 & 0 \end{pmatrix}.$$

2. The answer is yes. Let us prove this. We will use the following two lemmas to reduce the question to one simple case, which we then easily solve.

Lemma 1. *If the theorem is true for all values of A and some specific value $B = B_1$, and also true for all values of A and some specific value $B = B_2$, then it is also true for all values of A and $B = B_1 B_2$.*

Proof. By our assumption, there is some n_1 such that $(B_1^{-1} A B_1)^{n_1}$ has integer entries. But $(B_1^{-1} A B_1)^{n_1}$ has determinant 1 as well, so there is some n_2 such that $(B_2^{-1}(B_1^{-1} A B_1)^{n_1} B_2)^{n_2} = (B_2^{-1} B_1^{-1} A B_1 B_2)^{n_1 n_2}$ has integer entries. □

Lemma 2. *If $\det B = \pm 1$, then the theorem holds.*

Proof. In fact, $B^{-1} = \frac{1}{\det B} \operatorname{Adj} B$, where $\operatorname{Adj} B$ is the adjoint matrix to B which has integer entries, so B^{-1} has integer entries, meaning that the same applies to $B^{-1} A B$. □

Our proof will be by induction on $\det B$. If $\det B = \pm 1$, we have proven this above. Otherwise, there is some p such that $p | \det B$. Note that since we have seen that the statement is multiplicative on B, we can perform row operations with determinant ± 1 freely.

So, since $p | \det B$, let B_p be the reduction of B modulo p (so it is a matrix over the field $\mathbb{Z}_p$). Then, $\det B_p = 0$. Hence, there is some linear combination of the rows of B_p such that at least one of the rows (say, the first row) has coefficient 1, and the sum is equal to zero.

Going back to the original matrix B, this means that there is some linear combination of the rows of B such that at least one of the rows (say, the first row) has coefficient 1, and the sum is a vector whose entries are divisible by p. So, using row operations with determinant ± 1 (we add all other rows with the above coefficients to the first row), we bring B to a from where its first row is divisible by p. In that form,

$$B = \begin{pmatrix} p & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} B',$$

where B' has integer entries, and a smaller determinant. So by the induction hypothesis, it is sufficient to consider the case where

$$B = \begin{pmatrix} p & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Let us prove this case. We will show that there is some n such that all off-diagonal entries of A^n are divisible by p, which easily implies that

$$(B^{-1} A B)^n = B^{-1} A^n B = \begin{pmatrix} A_{11}^n & \frac{1}{p} A_{12}^n & \frac{1}{p} A_{13}^n & \dots \\ p A_{21}^n & A_{22}^n & A_{23}^n & \dots \\ p A_{31}^n & A_{32}^n & A_{33}^n & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

has integer entries.

In fact, we will show that when A is reduced modulo p to A_p, then there is some n such that $A_p^n = 1$. However, that is actually trivial - since $\det A = 1$ (this is the only place where we actually use this), then A_p is invertible modulo p. But the group $\mathrm{GL}(m, \mathbb{Z}_p)$ of $m \times m$ invertible matrices over $\mathbb{Z}_p$ has a finite order, so taking $n = \#\,\mathrm{GL}(m, \mathbb{Z}_p)$ is good enough. Note that this actually shows that it is sufficient to assume that $\det A$ and $\det B$ are coprime.

Good Luck!