REU APPRENTICE CLASS #1

INSTRUCTOR: LÁSZLÓ BABAI
SCRIBE: ASILATA BAPAT

Monday, June 27, 2011

1. Puzzle Problems

Problem 1. Give a simple condition for when a prime number p can be expressed as the sum of two squares. That is, when do there exist integers a, b such that $p = a^2 + b^2$? Experiment, discover simple pattern, formulate conjecture. Your conjecture will be an "if and only if" statement. One direction will be much easier to prove than the other.

Problem 2. Consider an 8×8 chessboard, with two opposite corners removed. Is it possible to tile this with non-overlapping dominoes?

Problem 3. Suppose you are given thirteen weights, each weight being a real number, with the following property: if any one weight is removed, the remaining twelve can be split into two groups of six weights each, of equal total weight. Prove that all thirteen weights must be equal.

2. Divisibility

Let us recall some basic concepts in divisibility.

Definition 2.1. Let a, b be integers. Then a is said to *divide* b (written $a|b$) if there exists some integer n such that $a \cdot n = b$.

Definition 2.2. Two integers a and b are said to be *relatively prime* if their greatest common divisor is equal to 1.

Problem 4. What is the probability that two positive integers are relatively prime?

The first problem here is to make sense out of the question; there is no natural notion of a "random integer." Instead, we consider two uniformly chosen integers from the set $\{1, \ldots, n\}$; let p_n denote the probability that they are relatively prime. Find the limit $\lim_{n\to\infty} p_n$ (prove that it exists). (Hint: The limit does exist, and is equal to $6/\pi^2$. The fun part is this: assume the limit exists; then prove in a couple of lines that it can only be $6/\pi^2$. Use the fact (Euler) that $\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$.)

Problem 5. What is the title of the novel that describes a quest to find the "ultimate answer" (which turns out to be 42), and then the "ultimate question"?

Problem 6. Let $\pi(n)$ be the number of primes in $\{1, \ldots, n\}$. Prove that:

$$\lim_{n\to\infty} \frac{\pi(n)}{n} = 0.$$

If (a_n) and (b_n) are two sequences of real numbers, we say that $a_n \sim b_n$ if $\lim_{n\to\infty}(a_n/b_n) = 1$. The following theorem is a major result about the asymptotic behaviour of the quantity $\pi(n)$.

Theorem 2.3 (Prime number theorem)**.** *Let* $\ln(n)$ *denote the natural logarithm of* n*. Then,*

$$\pi(n) \sim \frac{n}{\ln(n)}.$$

If $(a_n), (b_n)$ are two sequences of real numbers, then we say that $a_n = \Theta(b_n)$ if there exist positive constants c_1, c_2 such that for all sufficiently large n, we have $c_1|a_n| \le |b_n| \le c_2|a_n|$.

Before the prime number theorem was proved, Chebyshev proved the following weaker but still remarkable result:

$$\pi(n) = \Theta\left(\frac{n}{\ln(n)}\right).$$

3. Zero and the empty set

We know that $0! = 1$ and that $0/0$ is undefined. What is 0^0? The following facts are left as exercises:

$$\lim_{n\to\infty}(1/n)^{1/n} = 1, \quad \lim_{n\to\infty}(1/2^n)^{1/n} = 1/2, \quad \lim_{n\to\infty}(1/n^n)^{1/n} = 0.$$

Convince yourself that $\sum_{i\in\emptyset} a_i = 0$, and $\prod_{i\in\emptyset} a_i = 1$. (So in particular, $0^0 = 1$.)

Problem 7. Show that "almost always," we have:

$$\lim_{\substack{x\to 0+\\ y\to 0+}} x^y = 1.$$

First determine what "almost always" should mean.

4. Vectors and fields

A *vector space* is a set consisting (for the moment) of n-tuples of real numbers, called *vectors*. The following operations are permitted: adding two vectors componentwise, and multiplying each element of the tuple by a fixed scalar (real number).

If $\alpha_1, \dots, \alpha_n$ are real numbers and $v_1, \dots, v_n$ are vectors, then a sum of the form $\alpha_1 v_1 + \cdots + \alpha_n v_n$ is called a *linear combination*. If $\alpha_i = 0$ for every i, then it is called a trivial linear combination.

Definition 4.1. Let $v_1, \dots, v_k$ be vectors. They are said to be *linearly independent* if there is no nontrivial linear combination that equals zero. That is, if $\alpha_1, \dots, \alpha_k$ are real numbers such that $\alpha_1 v_1 + \alpha_k v_k = 0$, then $\alpha_i = 0$ for every i.

If $v_1, \dots, v_k$ is an arbitrary list of vectors, then the maximum number of linearly independent vectors among the v_i is called the *rank* of this list of vectors.

The following theorem will be proved later in the course.

Theorem 4.2 (First Miracle of Linear Algebra). *If $v_1, \dots, v_k$ are linearly independent vectors in $\mathbb{R}^n$ then $k \le n$.*

More generally, any set which permits linear combinations (under natural axioms) will be called a vector space.

The following are examples of vector spaces: $\mathbb{R}^n$, $\mathbb{R}^{k\times n}$ (the space of $k \times n$ matrices, $\mathbb{R}[x]$ (the space of polynomials with real coefficients in one variable x), and the space $C(I)$ of of continuous functions on some interval I.

Problem 8. Let $g(x) = (x - \alpha_1)\cdots(x - \alpha_n)$, where the numbers α_i are distinct real number. Let $f_i(x) = g(x)/(x - \alpha_i)$. Show that the polynomials $f_1, \dots, f_n$ are linearly independent.

Problem 9. Show that the functions $1, \cos x, \sin x, \cos 2x, \sin 2x, \dots$ are all linearly independent. (That is, show that every finite subset is linearly independent.)

Definition 4.3. A *number field* F is a subset of $\mathbb{C}$ that contains 1 and that is closed under the operations of $+, -, \cdot, /$ (except for division by 0).

For example, $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ and the algebraic numbers are all number fields.

Problem 10. Prove that:

1. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a number field.
2. $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt{2} + c\sqrt{4} \mid a, b, c \in \mathbb{Q}\}$ is a number field.

Problem 11. Show that if F is a number field, then $F \supset \mathbb{Q}$.

Now we can consider vector spaces over arbitrary number fields. This means that we fix a field F, the elements of which will be called “scalars,” and perform linear combinations with members of F as the coefficients. As an example, $\mathbb{R}$ is a vector space over $\mathbb{Q}$.

Problem 12. Prove that $1, \sqrt{2}, \sqrt{3}$ are all linearly independent over $\mathbb{Q}$.

5. Some miscellaneous problems

Recall the first rule of Clubtown: no two clubs can have the same set of members. If there are n residents, then there can be at most 2^n clubs.

Problem 13. Suppose that now every club must have an even number of members. What is the maximum number of clubs possible? Prove by a simple bijection that the number of even subsets is equal to the number of odd subsets.

Problem 14. Now consider Eventown, where every club must have an even number of members, and moreover the intersection of any two clubs must have an even number of members. What is the maximum possible number of clubs in Eventown? (Hint: The answer is $2^{\lfloor n/2 \rfloor}$.)

Observe that one way to produce $2^{\lfloor n/2 \rfloor}$ clubs is to pair up people into couples, and treat each couple as one unit. If one member of a unit joins a club, the other also automatically joins. Let us call this the “couples solution.”

Problem 15. Show that there exists a non-couples solution that exhibits the maximum number of clubs.

First construct some system (not necessarily a maximum one) that does not come from any set of couples.

Problem 16. Show that every *maximal* system of clubs in Eventown is a *maximum* system.

Problem 17. Now consider Oddtown: every club must have an odd number of members, and every pairwise intersection must have an even number of members. What is the maximum number of clubs possible? (Hint: The answer is equal to n.)

Observe that the system $\{\{1\}, \ldots, \{n\}\}$ is a permissible system with n clubs.

For any given system, we can construct *membership vectors*. Label the residents of the town by the numbers from 1 to n. For every club C, form a vector where the ith element is 1 if $i \in C$, and 0 otherwise.

Problem 18. Show that the membership vectors of an Oddtown club system are linearly independent. (Hint: First prove this over $\mathbb{Q}$.)

Problem 19. If $v_1, \ldots, v_k$ are vectors in $\mathbb{Z}^n$ that are linearly independent over $\mathbb{Q}$, then show that they are also linearly independent over $\mathbb{R}$.

Let $f(x) = \sum_{i=1}^{n} a_i x^i$. Call f a *prime-exponent polynomial* if $a_i = 0$ for all i that are not prime.

Problem 20. Prove that every non-zero polynomial has a non-zero multiple that is a prime-exponent polynomial.

Consider a regular n-gon inscribed in a circle of radius 1, with consecutive vertices $P_0, P_1, \ldots, P_{n-1}$.

Problem 21. Show that the product of all the lengths $\overline{P_0 P_i}$ is equal to n.

(Hint: polynomials, complex numbers.)