REU APPRENTICE CLASS #3

INSTRUCTOR: LÁSZLÓ BABAI
SCRIBE: MATTHEW WRIGHT

Wednesday, June 29, 2011 – solving problems

1. Problem 2

Idea: Color the cells white and green in a checkerboard pattern. Each tile (domino) covers one white and one green cell, so any number of tiles will always cover the same number of white cells as green cells.

Note that this also shows that if we remove *any* two cells of the same color, we still can't tile the board.

Question: what if we remove two tiles of different colors? Can we always tile in that case?

1.1. How could we have solved this?

One approach: try removing one corner and a different piece, and think about what positions you can remove to get a board you actually can cover. By experimenting a bit, you'll see the checkerboard pattern.

Problem 26. What if we use triominoes (three in a row), and we have an $n \times n$ square with one square removed? If n is divisible by 3 we clearly can't do this, but for all other n the numbers at least work out. In particular, why can't we tile when $n = 101$?

2. Problem 1

Conjecture: $p = a^2 + b^2 \iff p \equiv 1 \pmod 4$. (Recall that $a \equiv v \pmod m$ if and only if $m | a - b$.)

Observation: every odd prime number is congruent to 1 or -1 modulo 4.

We'll prove that if $p = a^2 + b^2$, then $p \equiv 1 \pmod 4$.

If $x = 2m$, then

$$x^2 = 4m^2 \equiv 0 \pmod 4.$$

If $x = 2m + 1$, then

$$x^2 = 4(m^2 - m + 1) \equiv 1 \pmod 4.$$

So $a^2 + b^2$ is $0, 1$, or 2 modulo 4; for odd primes, then, it must be 1.

Note: the other direction is *significantly* harder!

3. Problem 5

Hint: Don't panic!

4. Problem 12

We want to prove that $1, \sqrt{2}, \sqrt{3}$ are linearly independent over $\mathbb{Q}$. Take a linear combination

$$0 = p \cdot 1 + q\sqrt{2} + r\sqrt{3}$$

with $p, q, r \in \mathbb{Q}$. We want to show that this implies $p = q = r = 0$.

We need to somehow take advantage of the square roots. Rearrange the equation to get

$$p + r\sqrt{3} = -q\sqrt{2}.$$

Let's try squaring both sides to get

$$\begin{aligned} \left(p + r\sqrt{3}\right) &= \left(-q\sqrt{2}\right) \\ p^2 + 2pr\sqrt{3} + 3r^2 &= 2q^2 \\ 2pr\sqrt{3} &= 2q^2 - p^2 - 3r^2. \end{aligned}$$

We can conclude that $2pr = 0$ because otherwise $\sqrt{3}$ would have to be rational! We now have two cases: either $p = 0$ or $q = 0$.

Let's start with the case when $p = 0$. The original equation then becomes

$$\begin{aligned} r\sqrt{3} &= -q\sqrt{2} \\ 3r^2 &= 2q^2 \\ \frac{3}{2} &= \left(\frac{q}{r}\right)^2. \end{aligned}$$

Why can $3/2$ not be written in this way? Assume for contradiction that it can. Then for relatively prime integers A, B, we have

$$\begin{aligned} \frac{3}{2} &= (A/B)^2 \\ 2A^2 &= 3B^2. \end{aligned}$$

But B must be even, which means B is divisible by 4. But then A has to be divisible by 2, contradicting the assumption that A and B are relatively prime.

The $q = 0$ case can be handled in the same way.

Question: This shows us that a certain set of three numbers is linearly independent over $\mathbb{Q}$. Can we generalize this? For which sets of square roots does this work?

Clearly if we have 1 and if any other is a square, they're not. But even the set

$$\{1, \sqrt{2}, \sqrt{8}\}$$

isn't, because $\sqrt{8} = 2\sqrt{2}$. What if we only look at squarefree numbers (which are not divisible by the square of any prime)?

It turns out that the set

$$\{\sqrt{n} : n \text{ is squarefree}\}$$

is linearly independent over $\mathbb{Q}$. This is a more difficult problem; as a start, show that

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}$$

is linearly independent.

5. Problem 10

For part (1), we need to show that if $a, b \in \mathbb{Q}$, not both zero, then

$$\frac{1}{a + b\sqrt{2}}$$

is of the form

$$r + s\sqrt{2}$$

for some $r, s \in \mathbb{Q}$.

Multiply by the conjugate:

$$\begin{aligned} \frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \end{aligned}$$

and so we can take $r = \frac{a}{a^2 - 2b^2}$, and $s = \frac{-b}{a^2 - 2b^2}$. The only thing left to show is that $a^2 - 2b^2 \neq 0$. But if it is zero, then

$$a = 2b^2$$

which would imply that $\sqrt{2}$ is rational if a and b are not both zero.

For part (2), we need to show that

$$\frac{1}{a + b^3\sqrt{2} + c^3\sqrt{4}}$$

is in $\mathbb{Q}[\sqrt[3]{2}]$. We use the fact that there is $z \in \mathbb{C}$ such that $z \neq 1$ but $z^3 = 1$. The three solutions to $z^3 = 1$ lie on the unit circle on the complex plane, evenly spaced, and are

$$\begin{aligned} z_0 &= 1 \\ z_1 &= -\frac{1}{2} + i\frac{\sqrt{2}}{2} \\ z_2 &= -\frac{1}{2} - i\frac{\sqrt{2}}{2} \end{aligned}$$

Using the fact that $z_1^2 = z_2$, and $z_2^2 = z_1^4 = z_1 \cdot z_1^3 = z_1$, show that

$$\left(a + b\sqrt[3]{2} + c\sqrt[2]{3}^2\right)\left(a + bz_1\sqrt[3]{2} + cz_1^2\sqrt[2]{3}^2\right)\left(a + bz_2\sqrt[3]{2} + cz_1^2\sqrt[2]{3}^2\right)$$

is rational (ideally without brute force multiplication!). This is analogous to multiplying $(a + b\sqrt{2})$ by $(a - b\sqrt{2})$ to rationalize it.

Remark 1. Every complex number $z = a + bi$ has a *polar form* $z = re^{i\theta}$, since $e^{i\theta} = \cos\theta + i\sin\theta$. Multiplication of complex numbers $z_1 = r_1e^{i\theta_1}$ and $z_2 = r_2e^{i\theta_2}$ in polar form is particularly nice:

$$z_1z_2 = r_1r_2e^{i(\theta_1+\theta_2)}.$$

The conjugate of $z = re^{i\theta}$ is

$$\overline{z} = re^{i(-\theta)}.$$

Note that adding or subtracting 2π to θ gives us the same complex number, so

$$re^{i\theta} = re^{i\psi} \iff \theta - \psi = 2\pi k$$

for some $k \in \mathbb{Z}$, assuming that $r \neq 0$.

If $z = a + bi$, then

$$z + \overline{z} = 2a$$

and

$$z - \overline{z} = 2bi.$$

We write

$$a = Re(z)$$

and

$$b = Im(z).$$

We can write inverses as

$$\frac{1}{a+bi} = \frac{a-bi}{a-bi}\frac{1}{a+bi} = \frac{a-bi}{r^2}.$$

As far as roots of unity go: we're looking for solutions to $z^n = 1$. If

$$z = re^{i\theta},$$

then

$$z^n = r^n e^{in\theta} = 1 = 1 \cdot e^0.$$

Therefore $e^{in\theta} = e^0$ and so $\theta = 2k\pi/n$ for appropriate k, and $r = 1$. Therefore

$$\begin{aligned} \theta_0 &= 0 \\ \theta_1 &= 2\pi/n \\ \theta_2 &= 2 \cdot 2\pi/n \\ &\vdots \\ \theta_{n-1} &= (n-1)2\pi/n. \end{aligned}$$

These form n evenly spaced points on the unit circle on the complex plane.

Problem 27. The sum $z_0 + z_1 + \cdots + z_{n-1}$ of all the nth roots of unity is 0 if $n \geq 2$, and 1 if $n = 1$. Prove this!

Problem 28. For what k is the sum

$$\sum_{i=0}^{n-1} z_i^k = 0?$$

Definition 1. z is a *primitive nth root of unity* if

$$z^n = 1$$

and when $1 \leq j \leq n-1$, then

$$z^j \neq 1.$$

For example, the fourth roots of unity are $1, i, -1, -i$, but only i and $-i$ are primitive fourth roots of unity (we have to raise both of them to the fourth power to get 1).

The sixth roots of unity are positioned along a regular hexagon. Going around the circle, the smallest exponents we need to raise each one to get 1 are $1, 6, 3, 2, 3, 6$. Only the ones that must be raised to the sixth power are primitive roots

Problem 29. If z is a primitive nth root of unity, then for what values of k is z^k a primitive nth root of unity? How many powers of z will be primitive nth roots of unity?

Problem 30. Study

$$S_n = \sum \text{primitive } n\text{th roots of unity.}$$

What can you say or conjecture about S_n? We can see that $S_3 = -1$, $S_4 = 0$, and $S_5 = 1$; what are the rest?

6. More complex numbers

Definition 2. Let $z \in \mathbb{C}$, $|z| = 1$. The *order* of z is the smallest positive n such that $z^n = 1$. If no such n exists, then the order of z is ∞. We write the order of z as $\text{ord}(z)$.

The complex numbers on the unit circle which have finite order are those of the form

$$z = e^{i\theta}$$

with θ a rational multiple of π.

Exercise: prove that $e^{i\theta}$ has finite order if and only if $\theta/\pi \in \mathbb{Q}$.

If $\text{ord}(z_1) = 8$ and $\text{ord}(z_2) = 9$, we know that $\text{ord}(z_1 z_2)$ is at most 72.

Exercise: if $\text{ord}(z) = t$ then $z^n = 1 \iff t|n$.

Note that $\text{ord}(z) = n$ is equivalent to saying that z is a primitive nth root of unity.

So, going back to the question about the order of the product of two complex numbers: suppose $\text{ord}(z_1) = t_1$ and $\text{ord}(z_2) = t_2$. Is it the case that

$$\text{ord}(z_1 z_2) = \text{lcm}(t_1, t_2)?$$

Let $t = \text{lcm}(t_1, t_2)$. There are two things we need to prove. First, that $(z_1 z_2)^t = 1$, but $(z_1 z_2)^n \neq 0$ for any $n < t$. The first of these is clear, which also tells us that $\text{ord}(z_1 z_2)|t$. But are they equal?

Problem 31.

(1) Show that $\text{ord}(z_1 z_2)$ is not necessarily equal to $\text{lcm}(t_1, t_2)$.
(2) Show that if t_1 and t_2 are relatively prime, then $\text{ord}(z_1 z_2) = t_1 t_2$.

7. Problem 8

We want to show that the polynomials $f_1, \dots, f_n$ are linearly independent.

Note that the set of polynomials of degree k is not a subspace of the vector space of all polynomials: the zero polynomial isn't included, and it's not closed under addition. But if we take the set of polynomials of degree *at most* k the we do get a subspace.

Definition 3. Let $\mathbb{R}^{\leq k}[x]$ be the vector space of polynomials of degree $\leq k$.

We can see that $\dim \mathbb{R}^{\leq k}[x] = k + 1$, because the set $\{1, x, \dots, x^k\}$ forms a basis. This means that if we can prove that $f_1, \dots, f_n$ are linearly independent, then we'll in fact have shown that they form a basis for $\mathbb{R}^{\leq k}[x]$! This fact is important to Lagrange interpolation.

Back to the original problem. We want to show that if

$$\sum a_i f_i = 0$$

then $a_i = 0$ for all i. Substitute $x = \alpha_j$. Then

$$f_i(\alpha_j) = \begin{cases} \neq 0 & i = j \\ 0 & i \neq j \end{cases},$$

so

$$0 = \sum a_i f_i(\alpha_j) = a_j f_j(\alpha_j)$$

and so $a_j = 0$.

A polynomial is a formal expression, which we can think of as a sequence of numbers with

$$(a_0, a_1, \ldots)$$

corresponding to

$$\sum_{i=0}^{\infty} a_i x^i.$$

It is a polynomial if all but finitely many of the a_i are zero; we can define addition and multiplication in the usual way. We can also define divisibility:

$$f | g \iff \exists h \in \mathbb{R}[x] \text{ such that } g = f \cdot h.$$

In this way, we can define quotients of polynomials, in the case when the denominator is a factor of the numerator, without actually doing a division; this is how we can think of the polynomials $f_i(x)$ in problem 8.

It's clearly true that if two polynomials are formally equal (have the same coefficients), then they are equal as functions. Is the converse true? That is, if two polynomials have the same value everywhere, is it necessarily the case that they have the same coefficients? We can even simplify the question a bit: if f and g are two polynomials that agree on all values of x, and we let $h(x) = f(x) - g(x)$, must it be the case that $h(x)$ is the zero polynomial?

Problem 32. If $h(x) = 0$ for all values of x, is h the zero polynomial?

8. Problem 3

Hint: Try it for integers first.

9. Problem 16

Call the clubs $C_1, \ldots, C_k$.

Lemma 1. *We can represent a club by its membership vector, which was defined as*

$$v_i = \begin{pmatrix} \alpha_{1i} \\ \alpha_{2i} \\ \vdots \\ \alpha_{ki} \end{pmatrix}$$

where $\alpha_{ji} = 1$ if $j \in C_i$ and $\alpha_{ji} = 0$ if $j \notin C_i$. Under the rules of Oddtown, $v_1, v_2, \ldots, v_k$ are linearly independent over $\mathbb{Q}$, so there can be no more than n of them.

Observe that $|C_i \cap C_j| = v_i \cdot v_j$ (where $\cdot$ here is the dot product of vectors). So we can rewrite the two conditions as

$$v_i \cdot v_j = \begin{cases} \text{even} & i \neq j \\ \text{odd} & i = j \end{cases} .$$

Use this to prove the lemma.

10. Matrices

Problem 33. Show that

$$\operatorname{rank}(A+B) \leq \operatorname{rank}(A) + \operatorname{rank}(B).$$

Definition 4. Let

$$A = (\alpha_{ij}),$$

be $k \times l$,

$$B = (\beta_{jk}),$$

be $l \times m$, and

$$C = (\gamma_{rt})$$

be $k \times m$. Then $C = A \cdot B$ means that

$$\gamma_{rt} = \sum_{s=1}^{l} \alpha_{rs}\beta_{st}.$$

Note that we can multiply two matrices A, B in either direction as long as one is $k \times l$ and the other $l \times k$.

Problem 34. Find two 2×2 matrices A, B such that $A \cdot B \neq B \times A$.

Definition 5. The *trace* of a matrix $A = (\alpha_{ij})$ is

$$\operatorname{tr}(A) = \sum \alpha_{ii}.$$

Problem 35. Show that

$$\operatorname{tr}(AB) = \operatorname{tr}(BA),$$

even if A and B aren't necessarily square.