ADDITIVE COMBINATORICS: LECTURE 1

LEO GOLDMAKHER

We started by discussing administrative matters. The most salient ones:

(1) Please address me by name, preferably 'Leo'.
(2) My email is `lgoldmak@math.toronto.edu`
(3) The course webpage is `www.math.toronto.edu/lgoldmak/APM461/`
(4) I will assume that you have had exposure to elementary analysis ($\epsilon - \delta$ proofs), elementary number theory (modular arithmetic), and elementary algebra (basics of groups, rings, and fields). If you're not sure whether or not you have adequate preparation, email me and we can discuss whether the course is appropriate for you.
(5) There will be no exam in this course; your mark will depend exclusively on homework and a final project (the precise nature of which will be determined later).

Before explaining what additive combinatorics is, we warmed up with some puzzles about sets of numbers. More precisely, given $A, B \subseteq \mathbb{Z}$, set

$$A + B := \{a + b : a \in A, b \in B\} \qquad A - B := \{a - b : a \in A, b \in B\}$$
$$A \cdot B := \{a \cdot b : a \in A, b \in B\} \qquad A \div B := \{a \div b : a \in A, b \in B\}.$$

(In the last operation, we assume that $0 \notin B$.) A simple example: if $A = \{2, 5, 12\}$ and $B = \{0, 3\}$, then

$$A + B = \{2, 5, 12, 5, 8, 15\}.$$

Of course, it's silly to write 5 twice, so really we have

$$A + B = \{2, 5, 8, 12, 15\}.$$

Thus $A + B$ is not as big as it potentially could be, because there are redundancies. (Observe that if there were no coincidences, then $A + B$ would have $|A| \cdot |B|$ distinct elements.)

Occasionally, the number of redudancies can be extreme. For example, let $A = \{1, 2, 3, \dots, n\}$. Then

$$A + A = \{2, 3, \dots, 2n\}.$$

So rather than the posible $\approx \frac{1}{2}n^2$ distinct elements[1], $A + A$ only has $2n - 1$ distinct elements. In other words, there are an extreme number of coincidences in $A + A$ for the above choice of A.

We next observed that for the above choice of A, the set $A - A$ is also unusually small:

$$A - A = \{0, \pm 1, \pm 2, \dots, \pm(n - 1)\}$$

has $2n - 1$ distinct elements, the exact same number as in $A + A$. Is this a coincidence?

Before continuing to explore this set, we make a convenient notation for it:

$$[n] := \{1, 2, \dots, n\}.$$

Date: January 10, 2014.

[1]Addition is commutative, so $A + A$ can't have more than $n(n + 1)/2 \sim \frac{1}{2}n^2$ distinct elements.

We saw above that both $[n] + [n]$ and $[n] - [n]$ are small sets. What about $[n] \cdot [n]$? This proved to be a more difficult problem. By definition,

$$[n] \cdot [n] = \{ab : 1 \leq a, b \leq n\},$$

but saying anything more explicit about it seems difficult. By considering the $n \times n$ multiplication table (alternatively, the 'Gal matrix'), we see that $|[n] \cdot [n]| \leq n^2$. More precisely, by symmetry of the table (i.e. commutativity of multiplication), we have

$$\Big|[n] \cdot [n]\Big| \leq \frac{1}{2} n(n-1).$$

Thinking about this problem in terms of multiplication tables is visually appealing. In this language, we are trying to determine how many distinct entries appear in an $n \times n$ multiplication table. This question, called the *multiplication table problem*, was first tackled by the great Hungarian mathematician Erdős, who proved that

$$\Big|[n] \cdot [n]\Big| = o(n^2).$$

(Recall that $f(x) = o\Big(g(x)\Big)$ means that $\frac{f(x)}{g(x)} \to 0$ as $x \to \infty$.) In fact, much more precise results are known. For example, there exists a constant $\delta > 0$ such that

$$\Big|[n] \cdot [n]\Big| \ll \frac{n^2}{(\log n)^\delta} \tag{1}$$

where $f(x) \ll g(x)$ means exactly the same thing as $f(x) = O\Big(g(x)\Big)$, which in term means exactly the same thing as $\frac{f(x)}{g(x)}$ is bounded for all 'reasonable' values of x. (Note that this differs from the typical CS use of big Oh notation, which implicitly assumes that the input is large.) The strongest result we have on this problem, due to Kevin Ford (see his paper in *Annals of Mathematics*, 2008), is the asymptotic

$$\Big|[n] \cdot [n]\Big| \asymp \frac{n^2}{(\log n)^\delta (\log \log n)^{3/2}},$$

where $\delta \approx 0.08$ can be written down exactly. (The notation $f(x) \asymp g(x)$ means $f(x) \ll g(x) \ll f(x)$.)

So much for upper bounds on the size of $[n] \cdot [n]$. What about lower bounds? After some brainstorming, we realized that the multiplication table of primes up to n has all distinct entries, up to symmetry: if we throw away all the entries above the main diagonal, all the remaining entries are distinct. This shows that

$$\begin{aligned}\Big|[n] \cdot [n]\Big| &\geq \frac{1}{2}\pi(n)\Big(\pi(n)+1\Big) \\ &\gg \pi(n)^2,\end{aligned}$$

where $\pi(n)$ denotes the number of primes less than or equal to n. (For example, $\pi(7.3) = 4$.) This is a nice-looking lower bound, but unless we can say something about primes, it's useless. Fortunately, quite a bit is known about the distribution of primes. In particular, one of the great achievements of analytic number theory is the following:

Theorem 1 (Prime Number Theorem)**.** $\pi(x) \sim \frac{x}{\log x}$*, where* $\log$ *denotes the natural logarithm.*

Here the notation $f(x) \sim g(x)$ means $\frac{f(x)}{g(x)} \to 1$ as $x \to \infty$. Thus, the prime number theorem can be equivalently restated in the form

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right),$$

as a main term and an error term which is small relative to the main term. Getting a more precise estimate of this form is a one of the major open problems in analytic number theory today. It turns out that a better approximation (conjectured by Gauss) to $\pi(x)$ is

$$\pi(x) \sim \int_2^x \frac{dt}{\log t};$$

this is a better approximation than $\frac{x}{\log x}$ because it turns out that it gives a smaller error term. How small? This is perhaps the most notorious conjecture in mathematics:

Conjecture 2 (Riemann Hypothesis)**.**

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O(\sqrt{x} \log x). \tag{2}$$

Unfortunately, even the most sophisticated methods available give pathetic approximations to this conjecture. For example, it is an open problem to prove the existence of a $\delta > 0$ such that the error term in (2) is $\ll x^{1-\delta}$.

In any event, we deduce from the prime number theorem and our earlier insight about multiplication tables that

$$\Big|[n] \cdot [n]\Big| \gg \pi(n)^2 \gg \frac{n^2}{(\log n)^2}. \tag{3}$$

Even though no one knows a precise formula for the size of $[n] \cdot [n]$, the upper and lower bounds (1) and (3) give a reasonably accurate idea of how it grows with n, which we can crudely express in the form

$$\Big|[n] \cdot [n]\Big| = n^{2-o(1)},$$

where $o(1) \to 0$ as $n \to \infty$.

EXERCISE 1: What can you say about the set $[n] \div [n]$?

In summary, we've seen that $[n] + [n]$ is tiny – in fact, it is as small as possible – while $[n] \cdot [n]$ is essentially as large as possible. This can be colloquially interpreted as saying that $[n]$ has a lot of structure with respect to addition, and behaves randomly with respect to multiplication. Are there sets which have a lot of structure with respect to multiplication, instead? A bit of thought leads to the following set:

$$2^{[n]} := \{2^0, 2^1, 2^2, \dots, 2^{n-1}\}.$$

EXERCISE 2:

(a) Describe the set $2^{[n]} \cdot 2^{[n]}$, and prove that it has $\ll n$ elements.
(b) Describe the set $2^{[n]} + 2^{[n]}$, and prove that it has $\gg n^2$ elements.
(c) Describe the set $2^{[n]} - 2^{[n]}$, and prove that it has $\gg n^2$ elements.
(d) Describe the set $2^{[n]} \div 2^{[n]}$, and prove that it has $\ll n$ elements.

Thus, $[n]$ is structured with respect to addition and random with respect to multiplication, while $2^{[n]}$ is structured with respect to multiplication and random with respect to addition. Are there sets which are random with respect to both addition and multiplication? Sure – actually, most sets are. A more interesting question is whether there are any sets which are structured with respect to both addition and multiplication. Erdős and Szemerédi conjectured that the answer is no. More precisely:

Conjecture 3 (Erdős-Szemerédi)**.** *Given any $A \subseteq \mathbb{Z}$, we have*

$$\max\{|A+A|, |A \cdot A|\} = |A|^{2-o(1)}.$$

This conjecture is wide open. The strongest result towards it is the following:

Theorem 4 (Solymosi, Adv. in Math, 2009)**.** *Given any $A \subseteq \mathbb{R}$, we have*

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{4/3-o(1)}.$$

This tells us that any finite set of *real* numbers must be somewhat random with respect to multiplication or addition (or both!).[2] Actually, Solymosi proved a much stronger result.

Theorem 5 (Solymosi, Adv. in Math, 2009)**.** *Given any $A, B \subseteq \mathbb{R}$, we have*

$$|AB| \cdot |A+A| \cdot |B+B| \gg \frac{|A|^2|B|^2}{\log\left(|A| \cdot |B|\right)}.$$

Taking $A = B$ in the above theorem yields the lower bound

$$|AA| \cdot |A+A|^2 \gg \frac{|A|^4}{\log |A|}, \tag{4}$$

which immediately implies Theorem 4. But it also implies more.

Corollary 6. *Suppose $A \subseteq \mathbb{R}$ has a lot of multiplicative structure, in the sense that $|AA| \ll |A|$. Then $|A+A| \gg |A|^{3/2-o(1)}$.*

More impressively, we deduce

Corollary 7. *Suppose $A \subseteq \mathbb{R}$ has a lot of additive structure, in the sense that $|A+A| \ll |A|$. Then $|AA| = |A|^{2-o(1)}$.*

This result provides some theoretical evidence for the Erdős-Szemerédi conjecture, although of course it is a rather special case. It also demonstrates that Solymosi's lower bound (4) is essentially optimal.

It is difficult to assess the strength of Corollary 7. Certainly its conclusion is very strong, but how restrictive is the hypothesis? Later this term we will see that it is *very* restrictive: there are few sets which are highly structured with respect to addition. We postpone giving a precise statement, but roughly, we will prove the following.

Theorem 8 (Freiman-Ruzsa)**.** *Suppose $A \subseteq \mathbb{Z}$ is highly structured with respect to addition, in the sense that $|A+A| \ll |A|$. Then A 'looks like' an arithmetic progression.*

[2] Konyagin and Rudnev have recently extended this result to all subsets of $\mathbb{C}$; their paper is available on the arXiv.

This fundamental result was discovered and proved by G. Freiman in the 1960s. However, the theorem was a bit ahead of its time, and Freiman's proof was quite complicated. A few decades later, I. Ruzsa discovered a much easier (and beautiful!) proof of Freiman's result; Ruzsa's proof ignited widespread interest in the subject. A couple of years ago, G. Petridis introduced an innovation which shortened the proof further.

It's worth pointing out that the converse to the Freiman-Ruzsa theorem is also true: if A looks like an arithmetic progression, then $|A+A|$ will be tiny. To get a feel for this, consider $A := \{5n : n \leq N\}$. Then $A = 5[N]$, whence

$$|A + A| = \Big|5([N] + [N])\Big| = \Big|[N] + [N]\Big| = 2N - 1 \ll |A|.$$

Thus, the Freiman-Ruzsa theorem colloquially asserts that the only subsets of $\mathbb{Z}$ which are highly structured with respect to addition are arithmetic progressions.

One might imagine an analogous statement for sets which are highly structured with respect to multiplication: $A \subseteq \mathbb{Z}$ satisfies $|AA| \ll |A|$ iff A looks like a geometric progression. Since no set of integers can simultaneously look like an arithmetic progression and a geometric progression, at least one of $|AA|$ and $|A + A|$ must be decently large. Actually, this is just a restatement of our earlier intuition for the Erdős-Szemerédi conjecture: no set should be highly structured with respect to both addition and multiplication.

Next lecture, we will prove Solymosi's theorem, and indicate a proof of Erdős' multiplication table problem. We will then reconsider the results of this lecture in the context of a general field – a maneuver which will allow us to develop applications to computer science.

WWW.MATH.TORONTO.EDU/LGOLDMAK/APM461/
E-mail address: lgoldmak@math.toronto.edu