REU 2006 · Discrete Math · Lecture 2

Instructor: László Babai
Scribe: Megan Guichard
Editors: Sourav Chakraborty and Duru Turkoglu

June 22, 2006. Last updated June 26, 2006 at 1:50pm.

Handouts:

1. Lecture 1: LB, Chapters 2 and 4
2. Lecture 2: Matoušek-Nešetřil

2.1 Roots of unity

Definition 1. A **complex n^{th} root of unity** is a complex number z such that $z^n = 1$. We can write $z_k = \cos\left(k\frac{2\pi}{n}\right) + i\sin\left(k\frac{2\pi}{n}\right)$. So the n^{th} roots of unity are the vertices of a regular n-gon in the complex plane.

Definition 2. A **primitive** n^{th} root of unity is z such that $z^n = 1$ and $z^\ell \neq 1$ for all $1 \leq \ell \leq (n-1)$. In other words, the multiplicative order of z is n.

Exercise 3. Prove that z_k is a primitive n^{th} root of unity if and only if $\gcd(k, n) = 1$.

Therefore from the above exercise we can conclude that the number of primitive n^{th} roots of unity is $\varphi(n)$.

Exercise 4. Prove that $\sum_{d|n} \varphi(d) = n$.

Theorem 5. For all $n \neq 1$ the sum of all the n^{th} roots of unity is 0, that is, if $n \neq 1$,

$$S_n \stackrel{\text{def}}{=} \sum_{k=0}^{n-1} z_k = 0 \tag{2.1.1}$$

Proof. We will give two different proof of the theorem.
Geometric proof: Consider the n different n^{th} roots of unity. Note that the vectors

corresponding to the roots form a regular n-gon in complex plane. So, their sum S_n has rotational symmetry, that is, if we rotate each vector by $2\pi/n$, then we get the same set of vectors. So S_n is fixed under rotation by $2\pi/n$. Therefore, if $n \neq 1$, then S_n must be 0.
Algebraic Proof: Notice that rotation by $2\pi/n$ is the same as multiplication by z_1. Hence, $z_j = z_1^j$. So,

$$S_n = z_1^0 + z_1^1 + \cdots + z_1^{n-1} \Rightarrow z_1 S = z_1^1 + \cdots + z_1^n \tag{2.1.2}$$

By definition, $z_1^n = 1$ and $z_1 \neq 1$. So $z_1 S = S_n$. Thus $S_n z_1 - S_n = S_n(z_1 - 1) = 0$. □

Corollary 6. $\sum_{k=0}^{n-1} \cos(k2\pi/n) = 0$.

Exercise 7. Find a closed-form expression for $\sum_{k=0}^{n-1} \cos(ak + b)$. [Hint: Look at a geometric property of $\sum \cos(ak + b) + i \sin(ak + b)$.]

Definition 8. Let $R_n = \sum_k' z_k$ be the sum of the primitive n^{th} roots of unity.

Now let us study what is can be the value of R_n.

Note that is n is a prime then $R_n = -1$.

Consider the case when $n = pq$, where p and q are primes. Then

$$S_{pq} = R_{pq} + R_p + R_q + R_1 = R_{pq} + (-1) + (-1) + 1$$

Since $S_n = 0$ so we have $R_{pq} = 1$.

Exercise 9. Prove that $R_n = \mu(n)$, the Möbius function.

2.2 Probability

Refer to Chapter 7 in László Babai's notes for an introduction to finite probability theory

Suppose we pick a random nonnegative integer x uniformly at random, what does this mean? Furthermore how can we define "the probability" that $x \equiv 3 \pmod 4$.

We should define the probability as follows:

$$\Pr(x \equiv 3 \pmod 4) := \lim_{n\to\infty} \Pr(x \equiv 3 \pmod 4) \tag{2.2.1}$$

This probability P_n, depending on n, is

$$P_n = \frac{\lfloor \frac{n+1}{4} \rfloor}{n}$$

that we have $|P_n - \frac{1}{4}| \leq \frac{1}{n}$; therefore $P_n \to \frac{1}{4}$.

Now, what about $\Pr(\gcd(x,y)=1)$, for "random" $x, y \in \mathbb{N}$. It is $\leq 3/4 = (1-\frac{1}{4})$, since we have the probabilities $\Pr(2|x) = \Pr(2|y) = \frac{1}{2}$. Similarly, there is an $8/9$ chance that they are not both multiples of 3.

The important question is: Are these two events independent? If they are independent then we would be able to multiply the probabilities of those for each prime to find the solution to this problem. So when do we say that two events independent?

Definition 10. For two events, the definitions of **positively(negatively) correlated** and **independent** are given in the *Chapter 7 of Babai's Lecture Notes.*

Exercise 11. For x in $\{0, 1, \ldots, n-1\}$, how are the events "$2|x$" and "$3|x$" correlated? In particular, when are they independent? More generally, when are the events "divisible by p" and "divisible by q" independent?
Remark: certainly if $pq|n$, then $p|x$ and $q|x$ are independent, but surprisingly this is not the only case.

It is not true that for all n, divisibility by 2 and 3 are independent. But it turns out, for large n these events are almost independent, more specifically for $x \in \{0, 1, \ldots, n-1\}$,

$$|\Pr(2|x)\Pr(3|x) - \Pr(6|x)| \to 0 \text{ as } n \to \infty$$

So we have,

$$\Pr(\gcd(x,y)=1) \leq (1-\frac{1}{4})(1-\frac{1}{9})$$

Similarly for the first finitely many primes $p_1, p_2, \ldots, p_k$,

$$\Pr(\gcd(x,y)=1) \leq \prod_{p \in \{p_1,\ldots,p_k\}} (1-\frac{1}{p^2})$$

So what happens if we take the infinite product?

Exercise 12. Prove: $\Pr(\gcd(x,y)=1) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.6079....$
Hint: we had an exercise that $\zeta(s) = 1/\prod_p (1-1/p^s)$.
Remark: When an exercise is used multiple times, it is a good indication that you should write it up at some point.

Let $p_n = \Pr_{x,y \in \{0,\ldots,n-1\}}(\gcd(x,y)=1)$; the probability that we are looking for is $\lim_{n\to\infty} p_n$. The proof of the existence of the limit is rather tedious so you may assume that the limit exists. Given that this limit exists, it is a two-line proof that it *must* be $6/\pi^2$.

Exercise 13. Relate the probability $\Pr(\gcd(x,y)=1) = 6/\pi^2$ to the average value of $\varphi(n)$. (Recall that $\frac{1}{n^2}\sum_{k=1}^{n} \varphi(k) \to 3/\pi^2$.)

2.3 Fibonacci numbers

The Fibonacci numbers are defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. So the Fibonacci numbers are 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...

Let's look at the ratios of consecutive Fibonacci numbers.

1/0	1/1	2/1	3/2	5/3	8/5	13/8	21/15 ...
	1	2	1.5	1.333	1.6	1.375	...

Theorem 14. Let $L = \lim_{n\to\infty} \frac{F_{n+1}}{F_n}$. Then the limit L exists and its value is the golden ratio, that is, $L = \frac{1+\sqrt{5}}{2} = \gamma \approx 1.6$.

The proof of this theorem is difficult. But assuming that the limit L exist we will give a simple proof.

Note that the golden-ratio is the solution to the equation $L = 1 + 1/L$.

Proof. We have $F_n = F_{n-1} + F_{n-2}$, so

$$F_n/F_{n-1} = 1 + F_{n-2}/F_{n-1} \tag{2.3.1}$$

so if we take limit on both sides we get $L = 1 + 1/L$, and the result follows. □

Exercise 15. If $d(n)$ is the number of divisors of n prove that $d(n) < 2\sqrt{n}$.

Exercise 16. Prove that for all $\epsilon > 0$ there exists n_0 such that for all $n > n_0$ we have $(d(n) < n^{\epsilon})$.

Exercise 17. Prove that for all $\epsilon > 0$ there exists n_0 such that for all $n > n_0$ we have $(d(n) < n^{\frac{c+\epsilon}{\ln\ln n}})$. Find the best c. [Hint: use the Prime Number Theorem.]

2.4 Least common multiples and order of permutation

Let n be a positive integer. Let $0 < k_1 \leq k_2 \leq \cdots \leq k_r$ be a partition of n, that is, $n = k_1 + \cdots + k_r$. We are interested in studying $lcm[k_1, \ldots, k_r]$.

This is very similar to studying permutations on n elements. Consider a permutation π on n elements. The permutation can we uniquely written as a product of disjoint cycles. Let the cycles of π be of size $k_1, k_2, \ldots, k_r$. Then note that the $lcm[k_1, \ldots, k_r]$ is same as the order of π.

Suppose we have fixed n. What is the maximum order of a permutation on n elements? This is same as writing $n = k_1 + \cdots + k_r$ where $lcm[k_i]$ is as large as possible.

Consider $k_1 = 2$, $k_2 = 3$, $k_3 = 5$, etc. This doesn't give exactly the right answer, but it is close to being right in some sense. Let $M(n)$ be the maximum order of a permutation on

n elements; certainly $M(n) \geq \prod_{p \leq x} p =: M^*(n)$, where x is the largest number such that $\sum_{p \leq x} \leq n$.

Exercise* 18. Prove that $\ln M(n) \sim \ln M^*(n)$.

Exercise 19 (E.Landau 1904). Prove that $\ln M^*(n) \sim \sqrt{n \ln n}$. [Hint: Prime Number Theorem.]

Erdös-Turan-Goncharou showed that the "typical" order of a permutation is around $n^{(1/2)\ln n}$. Precisely, if π is a random permutation of n elements, then with high probability (the probability approaches 1 as n goes to ∞),

$$\ln(\text{order of}\pi) \sim \frac{1}{2}(\ln n)^2 \tag{2.4.1}$$

Take a permutation π uniformly at random. Let ℓ_1 be the length of the cycle containing 1. Since there are n possible places that 1 can go are all equally likely, we get $\Pr(\ell_1 = 1) = \frac{1}{n}$.

Now let us consider the, $\Pr(\ell_1 = n)$. There are $n-1$ choices for $\pi(1)$, because 1 is excluded. Then there are $n-2$ choices for $\pi(\pi(1))$, and so on. So we have $\Pr(\ell_1 = n) = \frac{(n-1)!}{n!} = \frac{1}{n}$.

Exercise 20. Let π be a random permutation on n elements and ℓ_1 be the size of the cycle in π containing 1. Give a beautiful proof that $\Pr(\ell = k) = \frac{1}{n}$. [Hint: give a clear bijection between the set of permutations where 1 is in a cycle of length k with $(n-1)!$.]

Suppose we have a permutation π on n elements. Define $c_k(\pi)$ to be the number of k-cycles in π.

If the permutation π is chosen at random, what is the **expected number** of cycles of length k? Call this expected value c_k.
What is c_n? A permutation can have at most one cycle of size n. And by our earlier argument probability that the permutation is an n cycle is $\frac{1}{n}$. So $c_n = \frac{1}{n}$.
What is c_1? For each number between 1 and n, the probability that that number is in a cycle of length 1 is $1/n$, so the expected value of c_1 is $\frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n} = 1$.

Example 21. In the permutation $(12)(34)(567)$, $c_1(\pi) = 0$, $c_2(\pi) = 2$, $c_3(\pi) = 1$), and $c_k(\pi) = 0$ for $k > 3$.

Exercise 22. Prove that the expected number of cycles in a random permutation is asymptotically equal to $\ln n$.

Pick a permutation π. What is the order of π? If it consists of a single cycle, then it has order n. If it consists of two cycles, the order is $\leq n^2/4 < n^2$. In general, if the number of cycles is $\leq s$, then the order of π is $< n^s$. (Actually, $(n/s)^s$, but asymptotically this doesn't matter.)

2.5 Partitions of n

Given a natural number n, we can look at all of the ways of writing n as a sum of natural numbers. (Natural numbers start at 1.)

Example 23.

$$\begin{aligned} 5 &= 1+1+1+1+1 \\ &= 1+1+1+2 \\ &= 1+1+3 \\ &= 1+2+2 \\ &= 1+4 \\ &= 2+3 \\ &= 5 \end{aligned}$$

These are all possible partitions of 5.

Let $p(n)$ be the number of partitions of n. By the above example we have $p(5) = 7$.

Theorem 24. There exist constants $c_1, c_2 > 1$ such that, for all sufficiently large n,

$$c_1^{\sqrt{n}} < p(n) < c_2^{\sqrt{n}}. \tag{2.5.1}$$

Proof. First, let us observe the lower bound. We need to find c_1 such that $p(n) \geq c_1^{\sqrt{n}}$. So we need to find some way of producing distinct partitions that gives about this many partitions.

Imagine that we have a partition of n into k distinct terms which are greater than 2. So $n = a_1 + \cdots + a_k$. To produce a different partition we can modify each a_i by reducing 0 or 1, and fill the partition with 1's to sum up to the same value. For example, $44 = 3+7+13+21$ might change to $2+6+13+20+1+1+1$.

By this procedure we can create 2^k distinct partitions (2 choice for each term). These partitions will be different, since all of the terms are distinct and greater than 2.

Notice that $3+4+\cdots+(k+2) = \frac{k(k+5)}{2}$. Thus the maximum k to satisfy $\frac{k(k+5)}{2} < n$ will be $\sim \sqrt{2n}$. Therefore we have proved $c_1^{\sqrt{n}} \leq p(n)$ for any $c_1 < 2^{\sqrt{2}}$.

Now, what about the upper bound?

Let $p(n,k)$ be the number of partitions of n into at most k terms. Let $q(n,k)$ be the number of partitions of n into terms, *each of which* is $\leq k$.

Example 25. $p(5,2) = 3$, because we have $5 = 1+4 = 2+3 = 5$.

$q(5,2) = 3$, because $5 = 1+1+1+1+1 = 1+1+1+2 = 1+2+2$.

Lemma 26. $p(n,k) = q(n,k)$.

Proof. pictures with boxes flipped over a 45° line □

Suppose we say that a term $\leq \sqrt{n}$ is "small" and a term $> \sqrt{n}$ is "large." Define

$$\widetilde{p}(n) = \sum_{k \leq n} p(k)$$

Similarly, define $\widetilde{p}(n,k) = \sum_{m \leq n} p(m,k)$ and $\widetilde{q}(n,k)$ likewise. Then

$$\widetilde{p}(n) \leq \widetilde{p}(n, \sqrt{n})\widetilde{q}(n, \sqrt{n})$$

Why? Every partition $n = a_1 + a_2 + \cdots + a_m$ can be split into two parts, one with all small terms and one with large terms. The part with large terms will eventually have less than $\sqrt{n}$ terms, since each of the terms is large. Obviously, each of these parts are represented in $\widetilde{p}(n, \sqrt{n})$ and $\widetilde{q}(n, \sqrt{n})$, and furthermore there is an over count, but that's okay.

Now, $\widetilde{p}(n,k) \leq \binom{n+k}{k}$, by the following argument: Imagine we have n boxes and k dividers. Choose the dividers out of $n+k$ objects and then let $a_1 = \#$ of boxes until first divider, $a_2 = \#$ of boxes between first and second dividers, $\ldots$, $a_k = \#$ of boxes between $(k-1)^{\text{st}}$ and k^{th} dividers, with $\sum a_i \leq n$. This over counts, because some partitions may be counted multiple times.

Still, these analysis give a bound of $\widetilde{p}(n,k) \leq n^k = e^{k \ln n}$. Here k is on the order of $\sqrt{n}$, which is good, but there is an extra factor of $\ln n$, which is less good.

However, we can modify this approach to give the expression we want. □

Exercise 27. Complete the above proof for the upper bound.
Hint: Asymptotic Notation handout. (*Chapter 2*)

2.6 Generating functions

Let $a_0, a_1, a_2, \ldots$ be a sequence of numbers. The associated function

$$f(x) = \sum_{n=0}^{\infty} a_n x^n \tag{2.6.1}$$

is called the **generating function** associated to the sequence.

Example 28.

- $1, 1, 1, \ldots$ gives $f(x) = 1 + x + x^2 + \cdots = \frac{1}{1-x}$.
- $\frac{1}{0!}, \frac{1}{1!}, \frac{1}{2!}, \ldots$ gives $f(x) = \sum \frac{x^n}{n!} = e^x$.

If all $a_i \geq 0$, then $\forall x > 0$, if $f(x)$ is convergent, then

$$a_n \leq \frac{f(x)}{x^n} = \cdots + a_n + \cdots . \tag{2.6.2}$$

Let

$$P(x) = (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^3 + x^6 + \cdots)\cdots = \prod_{k=1}^{\infty}(\sum_{j=0}^{\infty} x^{kj}) \tag{2.6.3}$$

Then, for example, the coefficient of x^5 is $p(5)$, because the number of ways we can get an x^5 from the product. Similarly, the coefficient of x^n is $p(n)$.

Notice that actually

$$P(x) = \prod_{k=1}^{\infty} \frac{1}{1 - x^k} \tag{2.6.4}$$

So

$$\ln P(x) = -\sum_{k=1}^{\infty} \ln (1 - x^k) \tag{2.6.5}$$

For all $0 < x < 1$, $p(n) \leq \frac{P(x)}{x^n}$. Also, $-\ln (1 - y) = y + \frac{y^2}{2} + \frac{y^3}{3} + \cdots$. So

$$\ln p(n) = -n \ln x - \sum_{k=1}^{\infty} \ln (1 - x^k) = -n \ln x + \sum_{k=1}^{\infty}\sum_{j=1}^{\infty} \frac{x^{kj}}{j} = -n \ln x + \sum_{j=1}^{\infty} \frac{1}{j} \sum_{k} x^{kj} \tag{2.6.6}$$

thus

$$\ln p(n) \leq -n \ln x + \sum_{j} \frac{1}{j} \frac{x^j}{1 - x^j} \leq -n \ln x + \sum \frac{1}{j} \frac{x^j}{(1 - x) j x^{j-1}} = -n \ln x + \frac{x}{1 - x} \sum \frac{1}{j^2} \tag{2.6.7}$$

because

$$1 - x^j = (1 - x)(1 + x + \cdots + x^{j-1}) \geq (1 - x) j x^{j-1} \tag{2.6.8}$$

for $0 < x < 1$. Also

$$\ln p(n) \leq -n \ln x + \frac{x}{1 - x} \frac{\pi^2}{6} = -n \ln \frac{y}{1 + y} + y \frac{\pi^2}{6} \tag{2.6.9}$$

where $y = \frac{x}{1-x}$, $x = \frac{y}{1+y}$. Note $0 < x < 1$ if and only if $0 < y < \infty$. So the above turns into

$$n \ln 1 + \frac{1}{y} + y \frac{\pi^2}{6} \leq \frac{n}{y} + y \frac{\pi^2}{6} = 2 \frac{n}{\sqrt{6n}/\pi} = \sqrt{2/3} \pi \sqrt{n} \tag{2.6.10}$$

This uses some facts: $\ln 1 + z \leq z$.

If $y^2 = \frac{6n}{\pi^2}$ then $n/y = y\pi^2/6$.