Analytic and Combinatorial Number Theory, summer term, 2017

Martin Klazar*

May 29, 2017

Contents

Lecture 1, February 28, 2017

This year I plan to cover (at least) two topics: 1. Dirichlet's theorem on primes in arithmetic progression and 2. combinatorial and asymptotic theory of integer partitions. After that we will see.

Dirichlet's theorem (*DT*) says: if $a, m \in \mathbb{N} = \{1, 2, \dots\}$ satisfy that $(a, m) = 1$ (a and m are coprime) then the infinite arithmetic progression

$$a,\ a+m,\ a+2m,\ a+3m,\ a+4m,\ \dots$$

contains infinitely many prime numbers. We reserve letters p and q to denote primes.

DT was proved by P. L. Dirichlet in 1837, indisputedly in the case $m = p$. Before I give an analytic proof of the general case I will tell you an elementary

*klazar@kam.mff.cuni.cz

proof of P. Erdős from 1935 (when Erdős was 22 years old) of a particular case of DT. Erdős's proof (EP) works for moduli m such that

$$\sigma = \sigma(m) := \sum_{p<m,\,(p,m)=1} \frac{1}{p} < 1\,.$$

For example, $m = 5$ has $\sigma = \frac{1}{2} + \frac{1}{3} = \frac{5}{6} < 1$, $m = 6$ has $\sigma = \frac{1}{5} < 1$ and EP works for these two moduli. For $m = 7$ we have $\sigma = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = \frac{31}{30} > 1$ and EP seems not to work for modulus 7. But things get better for $m = 14 = 2 \cdot 7$ as $\sigma = \frac{1}{3} + \frac{1}{5} + \frac{1}{11} + \frac{1}{13} = \frac{1504}{2145} < 1$, EP works for modulus 14 and hence we get an elementary proof of DT for modulus 7 as well.

Which numbers m satisfy $\sigma(m) < 1$? Using asymptotics of $\sum_{p<x} 1/p$ it is easy to show that the set of such m is (unfortunately) finite. In 1993 P. Moree determined all m with $\sigma(m) < 1$: their set M has 55 elements,

$$M = \{1,\, 2,\, 3,\, 4,\, 5,\, 6,\, 8,\, 9,\, 10,\, 12,\, \ldots,\, 390,\, 420,\, 630,\, 840\}$$

(at the end of the lecture I give references listing M in full). If some multiple of m lies in M, we have an elementary proof of DT for modulus m. The smallest $m \in \mathbb{N}$ when this fails and $km \notin M$ for every $k \in \mathbb{N}$ is $m = 29$.

Problem 1. *Is it possible to strengthen the elementary method of Erdős and cover larger set of moduli than M? Can one give an elementary proof of DT for the modulus $m = 29$?*

So I will prove, after Erdős and in an elementary way,

Theorem 2. *If $a, m \in \mathbb{N}$ are coprime and $\sigma(m) = \sum_{p<m,\,(p,m)=1} \frac{1}{p} < 1$ then $a + nm$ is a prime number for infinitely many $n \in \mathbb{N}$.*

For the proof we need some notation. We assume that $1 \le a < m$, $(a, m) = 1$, $p_1, \ldots, p_h$ are the primes smaller than m and not dividing it (so the sum of their reciprocals is $\sigma(m)$), and for $i = 1, 2, \ldots, h$ we define $q_i \in \mathbb{N}$, $1 \le q_i < m$, by

$$p_i q_i \equiv a \pmod{m}\,,$$

so $q_i = a/p_i$ modulo m. Clearly, $(q_i, m) = 1$. For $n \in \mathbb{N}$ we set

$$P_n(a, m) := \frac{(a+m)(a+2m)\ldots(a+nm)}{n!}$$

and if n is divisible by $p_1 p_2 \ldots p_h$ we define

$$Q_n(a, m) := \frac{P_n(a, m)}{P_{n/p_1}(q_1, m) P_{n/p_2}(q_2, m) \ldots P_{n/p_h}(q_h, m)}\,.$$

The heart of EP rests in prime factorizations of the fractions $Q_n(a, m)$. Let us review the order function ord_p. For nonzero $n \in \mathbb{Z}$ ($\mathbb{Z}$ denotes the ring of integers) we set $\mathrm{ord}_p(n) = k \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$ where k is maximum with

$p^k \,|\, n$. We define $\mathrm{ord}_p(0) = +\infty$. For $\alpha = \frac{a}{b} \in \mathbb{Q}$ ($\mathbb{Q}$ denotes the field of fractions) we define

$$\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b) \ .$$

Thus $\mathrm{ord}_p(\alpha) \in \mathbb{Z} \cup \{+\infty\}$ and does not depend on the particular fraction representation of α (since ord_p is additive on $\mathbb{Z}$). It is not hard to prove the following three basic properties of the order function: the first is that for every nonzero $\alpha \in \mathbb{Q}$ we have

$$\alpha = \prod_p p^{\mathrm{ord}_p(\alpha)} \ ,$$

the second is additivity, $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$ for every $\alpha, \beta \in \mathbb{Q}$, and the third says that

$$\mathrm{ord}_p(\alpha + \beta) \geq \min(\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)) \ ,$$

with equality if $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$. For $k \in \mathbb{Z}$ we say that p^k divides $\alpha \in \mathbb{Q}$ if $\mathrm{ord}_p(\alpha) \geq k$.

Proposition 3. *Let $a, m, \sigma = \sigma(m), p_i, q_i, P_n(a,m)$, and $Q_n(a,m)$ be as above.*

1. *For $n \to \infty$ and divisible by $p_1 p_2 \dots p_h$,*

$$Q_n(a,m) = m^{(1-\sigma)n + o(n)} \ .$$

2. *If $(p,m) = 1$ and $k = \mathrm{ord}_p(P_n(a,m))$ then $1 \leq p^k < (n+1)m$.*

3. *If $p \,|\, m$ and $\sigma \leq 1$ then $\mathrm{ord}_p(Q_n(a,m)) \leq 0$.*

4. *If $n \geq m$ and is divisible by $p_1 p_2 \dots p_h$, $p > \sqrt{(n+1)m}$ and is not a modulo m, and $p = p^1$ divides $P_n(a,m)$ then there is an $i \in \{1, 2, \dots, h\}$ such that p divides $P_{n/p_i}(q_i, m)$.*

We prove the proposition later. Now we deduce DT for the arithmetic progression $a + nm$ when $\sigma(m) < 1$. Let $n \in \mathbb{N}$ be at least m and a multiple of $p_1 p_2 \dots p_h$. Then, for any prime p and $k = \mathrm{ord}_p(Q_n(a,m))$,

$$\begin{aligned}
p \geq (n+1)m &\quad\Rightarrow\quad k = 0 \ \text{ (by 2 of Prop. 3)} \\
p > \sqrt{(n+1)m} &\quad\Rightarrow\quad k \leq 1 \ \text{ (dtto)} \\
p > \sqrt{(n+1)m} \ \&\ p \not\equiv a \pmod{m} &\quad\Rightarrow\quad k \leq 0 \ \text{ (by 2 and 4 of Prop. 3)} \\
p \leq \sqrt{(n+1)m} &\quad\Rightarrow\quad p^k < (n+1)m \\
&\qquad\qquad \text{(by 2 and 3 of Prop. 3)} \ .
\end{aligned}$$

So, by 1 of Prop. 3 and these bounds on the exponents in the prime factorization

of $Q_n(a,m)$ we have

$$\begin{aligned} m^{(1-\sigma)n+o(n)} &= Q_n(a,m) = \prod_p p^{\mathrm{ord}_p(Q_n(a,m))} \\ &\le \prod_{p\le\sqrt{(n+1)m}} (n+1)m \prod_{p<(n+1)m,\, p\equiv a \,(\mathrm{mod}\, m)} p \\ &\le ((n+1)m)^{\sqrt{(n+1)m}} \prod_{p<(n+1)m,\, p\equiv a \,(\mathrm{mod}\, m)} p\,. \end{aligned}$$

The last power is $m^{o(n)}$ and so

$$\prod_{p<(n+1)m,\, p\equiv a \,(\mathrm{mod}\, m)} p > m^{(1-\sigma)n+o(n)}$$

as $n\to\infty$ through the multiples of $p_1p_2\dots p_h$. As $1-\sigma>0$, the lower bound goes to $+\infty$ and therefore the set of p with $p\equiv a\,(\mathrm{mod}\, m)$ must be infinite.

It remains to prove Proposition 3. We utilize the next lemma.

Lemma 4. *Let $a\in\mathbb{Z}$, $d,m,n\in\mathbb{N}$, $(d,m)=1$,*

$$A=\{a+m,\, a+2m,\, \dots,\, a+nm\}$$

and $A(d) := \#k\in A$ such that $d\,|\,k$.

1. *$A(d)=\lfloor n/d\rfloor$ or $\lfloor n/d\rfloor+1$.*
2. *$A(d)=\lfloor n/d\rfloor+1$ iff d divides $a+jm$ for some $j\in\mathbb{N}$ with $j\le n-d\lfloor n/d\rfloor$ (= the residue of n after division by d).*
3. *If $A=\{1,2,\dots,n\}$ ($a=0,m=1$) then always $A(d)=\lfloor n/d\rfloor$.*
4. *$\mathrm{ord}_p(\prod_{k\in A}k)=\sum_{i\ge1}A(p^i)$. This in fact holds for any finite set $A\subset\mathbb{Z}$.*

Proof. 1 and 2. If $j,k\in\mathbb{Z}$ are non-congruent modulo d then so are $a+jm, a+km$ (since d and m are coprime). Hence every interval $I\subset\mathbb{Z}$ of length d contains exactly one $j\in I$ such that $a+jm$ is a multiple of d, and shorter intervals contain at most one such j. We partition $\{1,2,\dots,n\}$ into the short interval $R=\{1,2,\dots,n-d\lfloor n/d\rfloor\}$ and $\lfloor n/d\rfloor$ intervals with length d each. The result on general intervals I implies that $A(d)=\lfloor n/d\rfloor+\delta$ where $\delta\in\{0,1\}$ and is 1 iff there is a $j\in R$ with $d\,|\,a+jm$.

3. This follows from 1 and 2 but also is clear by itself.
4. Immediate from

$$\textstyle\sum_{i\ge1}A(p^i)=\#\{(i,k)\in\mathbb{N}\times A\mid p^i\,|\,k\}=\sum_{k=1}^m\mathrm{ord}_p(k)=\mathrm{ord}_p(\prod_{k\in A}k)\,.$$

□

Parts 3 and 4 give the well-known formula

$$\mathrm{ord}_p(n!) = \sum_{i\geq 1} \lfloor n/p^i \rfloor$$

of A.-M. Legendre. Parts 1+2 and 4 extend it to general n-term arithmetic progression A. I leave for you to prove the following as an exercise.

Corollary 5. *Let $k \in \mathbb{N}_0$ and $a, n \in \mathbb{N}$ with $a \geq n$. Then*

$$p^k \mid \binom{a}{n} \Rightarrow p^k \leq a \quad \textit{and even} \quad p^k \mid n\binom{a}{n} \Rightarrow p^k \leq a\ .$$

In the next lecture we prove by means of the lemma Proposition 3 and finish thereby EP of the particular case of DT. References:

- G. Lejeune Dirichlet, Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, *Abh. der Königlich Preuss. Akad. der Wiss.* (1837), 45–81.
- P. Erdős, Über die Primzahlen gewisser arithmetischer Reihen, *Math. Z.* **39** (1935), 473–491.
- M. Klazar, Analytic and Combinatorial Number Theory II, *KAM-DIMATIA-Series* 2010-969, iv+46 pp.
- P. Moree, Bertrand's postulate for primes in arithmetical progressions, *Computers Math. Applic.* **26** (1993), 35–43.

As I mentioned, Dirichlet's argument proving DT is complete only for prime modulus m and he extended it to general modulus later. I adapted EP from the article of P. Erdős in the above preprint of mine which contains the complete list of 55 $m \in \mathbb{N}$ with $\sigma(m) < 1$, taken from the article of P. Moree.

Lecture 2, March 7, 2017

The last corollary implies a lower bound on the *prime counting function* $\pi(x) := \#p \leq x$: since $p^k \mid \binom{2n}{n} \Rightarrow p^k \leq 2n$ and (by induction) $\binom{2n}{n} \geq 2^n$, we have

$$2^n \leq \binom{2n}{n} \leq (2n)^{\pi(2n)} \quad \text{and} \quad \frac{(2^{-1}\log 2)(2n)}{\log(2n)} \leq \pi(2n)\ ,$$

hence $\pi(x) \gg x/\log x$ for every real $x > 2$.

Let us prove Proposition 3. 1. Multiplying over $j = 1, 2, \ldots, n$ the inequalities $jm < a + jm < (j+1)m$ and dividing the result by $n!$ we get

$$m^n = \frac{n!m^n}{n!} < P_n(a,m) < \frac{(n+1)!m^n}{n!} = (n+1)m^n \quad \text{and} \quad P_n(a,m) = m^{n+o(n)}\ .$$

Substituting this asymptotics for $P_n(a,m)$ and $P_{n/p_i}(q_i,m)$ in $Q_n(a,m)$ we get

$$Q_n(a,m) = \frac{m^{n+o(n)}}{m^{n/p_1+o(n)}m^{n/p_2+o(n)}\dots m^{n/p_h+o(n)}} = m^{n(1-\sigma)+o(n)} .$$

2. If p is coprime to m, $A = \{a+m, a+2m, \dots, a+nm\}$ and $B = \{1, 2, \dots, n\}$ then Lemma 4 gives that

$$k = \mathrm{ord}_p(P_n(a,m)) = \sum_{i\geq 1}(A(p^i) - B(p^i)) = \sum_{i\geq 1}(\lfloor n/p^i \rfloor + \delta_i - \lfloor n/p^i \rfloor)$$

where $\delta_i \in \{0,1\}$ and $\delta_i = 0$ if $p^i > a + nm$. Thus we have a finite sum of 0s and 1s with the number of summands equal to the maximum i satisfying $p^i \leq a + nm$. Thus $k \geq 0$ and $p^k \leq a + nm < (1+n)m$.

3. Now p divides m and $\sigma \leq 1$. Since $(a,m) = (q_i,m) = 1$, the prime p divides none of the numbers $a + jm$ and $q_i + jm$ for $j \in \mathbb{Z}$ and therefore

$$\mathrm{ord}_p(Q_n(a,m)) = -\mathrm{ord}_p(n!/((n/p_1)!(n/p_2)!\dots(n/p_h)!)) \leq 0$$

because

$$\frac{n!}{(n/p_1)!(n/p_2)!\dots(n/p_h)!} \in \mathbb{N} .$$

This follows from $\frac{n}{p_1} + \frac{n}{p_2} + \dots + \frac{n}{p_h} = \sigma n \leq n$ (every multinomial coefficient $\frac{n!}{m_1!m_2!\dots m_k!}$, with $n, m_i \in \mathbb{N}_0$ and $m_1 + m_2 + \dots + m_k = n$, is a natural number).

4. The assumptions imply that $(p,m) = 1$ as $p > m$ and that $p^2 > (n+1)m > a + nm$. Since $\mathrm{ord}_p(P_n(a,m)) \geq 1$ (in fact $= 1$), Lemma 4 gives that for some $j \in \mathbb{N}$,

$$a + jm = pb,\ b \in \mathbb{N} \ \text{ and } \ 1 \leq j \leq l := n - p\lfloor n/p \rfloor .$$

We assume that j is minimum with this property. Since the congruence $a \equiv px$ modulo m has a solution $x \in \{1, 2, \dots, m-1\}$ (as $(p,m) = 1$) we see that $1 \leq b < m$. But $b = 1$ is not possible as p is not a modulo m. So $1 < b < m$ and since $(b,m) = 1$ (as $(a,m) = 1$), there is an $i \in \{1, 2, \dots, h\}$ such that p_i divides b and $b = p_i c$ with $c \in \mathbb{N}$. Substituting this for b and for a the expression $a = p_i q_i + tm$, $t \in \mathbb{Z}$, from the definition of q_i we get

$$p_i q_i + (t+j)m = pp_i c \ \text{ and } \ q_i + j'm = pc$$

where $j' = (t+j)/p_i \in \mathbb{Z}$ (since $(p_i, m) = 1$, p_i divides $t + j$). Since $q_i < m$ and $p > m$, $j' \geq 1$. If we show that

$$j' \leq l' := n/p_i - p\left\lfloor \frac{n/p_i}{p} \right\rfloor$$

we will be done because then $\mathrm{ord}_p(P_{n/p_i}(q_i,m)) = 1$ by Lemma 4. Suppose for the contrary that $0 \leq l' < j'$. Then, since $t \leq 0$ ($a < m$ and $p_i q_i > 0$),

$$l' < j' = \frac{t+j}{p_i} \leq \frac{j}{p_i} \ \text{ and } \ 0 \leq p_i l' < j \leq l < p .$$

But the equality defining l' shows that $p_i l'$ is also n minus an integral multiple of p and hence $p_i l'$ is the unique remainder of n after division by p and $p_i l' = l$. But this contradicts the above bound $p_i l' < l$. Thus $j' \leq l'$ and we are done. □

As an algebraic intermezzo before the analytic proof of full DT we prove its another particular case, this time for infinitely many cases.

Proposition 6. *For every $m \in \mathbb{N}$ there exist infinitely many $n \in \mathbb{N}$ such that $1 + nm$ is a prime number.*

Proof. We assume, as we may, that $m \geq 3$ and use the factorization

$$x^m - 1 = f(x)g(x), \ \ f, g \in \mathbb{Z}[x] \ ,$$

where

$$f(x) = \prod_{j=1,\,(j,m)=1}^{m} \left(x - e^{2\pi i j/m}\right) \ \text{ and } \ g(x) = \prod_{j=1,\,(j,m)>1}^{m} \left(x - e^{2\pi i j/m}\right) \ .$$

Thus we just split the linear factors in $x^m - 1 = \prod_{j=1}^{m}(x - e^{2\pi i j/m})$ into two groups, depending on whether $(j, m) = 1$ or not. It is not immediately clear from the definition that $f, g \in \mathbb{Z}[x]$ and we will prove it in a lemma later.

In fact,

$$f(x) = \Phi_m(x) \ \text{ and } \ g(x) = \prod_{d \,|\, m,\, d<m} \Phi_d(x)$$

where for $n \in \mathbb{N}$,

$$\Phi_n(x) := \prod_{j=1,\,(j,n)=1}^{n} \left(x - e^{2\pi i j/n}\right)$$

is the *n-th cyclotomic polynomial*. In Lemma 7 below (in the next lecture) we show that every $\Phi_n \in \mathbb{Z}[x]$ and hence $f, g \in \mathbb{Z}[x]$. The factorization

$$x^n - 1 = \prod_{d \,|\, n} \Phi_d(x)$$

is clear (we split $j \in \{1, 2, \ldots, n\}$ into groups according to (j, n)) and since $\deg \Phi_n = \varphi(n)$ $(= |\{j \in \mathbb{N} \mid 1 \leq j \leq n, (j, n) = 1\}|)$, comparison of degrees yields the identity

$$n = \sum_{d \,|\, n} \varphi(d)$$

which is also immediate without use of cyclotomic polynomials.

Now f and g have no common root and are coprime elements of $\mathbb{Q}[x]$. Bachet's identity gives

$$\alpha(x)f(x) + \beta(x)g(x) = 1$$

for some $\alpha, \beta \in \mathbb{Q}[x]$ (the ring $\mathbb{Q}[x]$ is Euclidean and hence every ideal in it is principal). Clearing denominators in the coefficients in $\alpha(x)$ and $\beta(x)$, for appropriate $c \in \mathbb{N}$ with $a = c\alpha$ and $b = c\beta$ we have

$$a(x)f(x) + b(x)g(x) = c,\ a, b \in \mathbb{Z}[x]\ .$$

Clearly, we may assume that $c \geq 2$.

We shall finish the proof in the next lecture.

Lecture 3, March 14, 2017

Since $m \geq 3$, $\varphi(m) = \deg f(x) \geq 2$ and $|f(x)| > 1$ whenever $|x| \geq 2$. Thus there exists a prime p dividing the integer $f(c)$. We show that $p \equiv 1 \pmod{m}$ (and then we show how to produce infinitely many such p). Since $f(c)$ divides $c^m - 1$, so does p. We show that m is minimum with $c^m \equiv 1 \pmod{p}$ and so c has order m modulo p. If not there would be a divisor d of m, $d < m$, such that $c^d \equiv 1 \pmod{p}$. Since $c^d - 1 = \prod_{e \,|\, d} \Phi_e(c)$, the definition of $g(x)$ implies that $c^d - 1$ divides $g(c)$ and so does p. But then the last displayed equation gives that p divides c and so p divides 1, a contradiction. Hence m is the order of c modulo p. The little theorem of Fermat says that $c^{p-1} \equiv 1 \pmod{p}$ and thus m divides $p - 1$ and $p \equiv 1 \pmod{m}$.

For every $k \in \mathbb{N}$ we take a prime $p(km)$ that is 1 modulo km. Then, as $p(km) > km$, the sequence $(p(m), (p(2m), (p(3m), \dots)$ goes to $+\infty$ and contains infinitely many distinct primes, all congruent to 1 modulo m. □

But it still remains to prove integrality of cyclotomic polynomials, which I forgot to do in the lecture. Let us do it in the write-up.

Lemma 7. *For every $n \in \mathbb{N}$, $\Phi_n(x) \in \mathbb{Z}[x]$.*

Proof. We prove by induction on n the stronger result that $\Phi_n(x) \in \mathbb{Z}[x]$ and $\Phi_n(0) = \pm 1$. For $n = 1$ it holds as $\Phi_1(x) = x - 1$. For $n > 1$ we denote the coefficient of x^k in $\Phi_n(x)$ as a_k, in $\prod_{d \,|\, n,\, d<n} \Phi_d(x)$ as b_k, and in $x^n - 1$ as c_k. We have $c_k \in \mathbb{Z}$ and $c_0 = -1$ and, by induction, $b_k \in \mathbb{Z}$ and $b_0 = \pm 1$. Then

$$c_0 + c_1 x + \cdots = x^n - 1 = \prod_{d \,|\, n} \Phi_d(x) = (a_0 + a_1 x + \dots)(b_0 + b_1 x + \dots)$$

and comparison of coefficients gives the system of equations $c_0 = a_0 b_0$, $c_1 = a_1 b_0 + a_0 b_1$, … with the unknowns a_k. It solves uniquely for $a_0, a_1, \dots$ and due to $b_0 = \pm 1$ and $c_0 = -1$ we see that each $a_k \in \mathbb{Z}$ and $a_0 = \pm 1$. □

Proof of general Dirichlet's theorem

We prove Dirichlet's theorem in the following stronger form.

Theorem 8 (Dirichlet, 1837). *If $a, m \in \mathbb{N}$ with $(a, m) = 1$ then*

$$\sum_{p=a+mn\le x} \frac{\log p}{p} = \frac{\log x}{\varphi(m)} + O(1) \text{ for } x > 1 \,.$$

We obtain the proof by a series of propositions.

The *von Mangoldt function* $\Lambda : \mathbb{N} \to [0, +\infty)$ has values $\Lambda(n) = \log p$ if $n = p^k$ for $k \in \mathbb{N}$, and $\Lambda(n) = 0$ else.

Proposition 9. *For every $n \in \mathbb{N}$,*

$$\sum_{d \mid n} \Lambda(d) = \log n \,.$$

Proof. Let $n = p_1^{a_1} \dots p_k^{a_k}$ be the prime decomposition of n. By the definition of Λ and the properties of logarithm the sum indeed equals

$$\sum_{i=1}^{k} \sum_{j=1}^{a_i} \log p_i = \sum_{i=1}^{k} \log(p_i^{a_i}) = \log(p_1^{a_1} \dots p_k^{a_k}) \,.$$

□

Proposition 10.

$$\sum_{p\le x} \log p < (2 \log 2)x \quad \text{for } x > 1 \,.$$

Proof. For every $n \in \mathbb{N}$,

$$\prod_{n+1<p\le 2n+1} p \le \binom{2n+1}{n} < 4^n, \quad \text{hence} \quad \sum_{n+1<p\le 2n+1} \log p < (2 \log 2)n$$

— every prime in the range divides $\binom{2n+1}{n} = \frac{(2n+1)2n\dots(n+1)}{n!}$, and $\binom{2n+1}{n} = \binom{2n+1}{n+1}$ are two binomial coefficients in the expansion of $2 \cdot 4^n = (1+1)^{2n+1}$. We use the last displayed inequality to prove by induction on $m = \lfloor x \rfloor \in \mathbb{N}$ the bound

$$\sum_{p\le m} \log p < (2 \log 2)m \,,$$

from which the stated bound follows. For $m = 1, 2$ it holds, and it holds by induction for even $m > 2$ because then the sum is the same as for $m-1$. Suppose that $m = 2n + 1 > 1$ is odd. By induction and the inequality,

$$\begin{aligned} \sum_{p\le m} \log p &= \sum_{p\le n+1} \log p + \sum_{n+1<p\le 2n+1} \log p \\ &< (2 \log 2)(n+1) + (2 \log 2)n = (2 \log 2)m \,. \end{aligned}$$

□

Proposition 11

$$\sum_{n\le x}\Lambda(n) < 3x \quad \textit{for } x>1\ .$$

Proof. Using the bound in Proposition 10 and the fact that the maximum of $(\log x)/\sqrt{x}$ for $x>1$ equals $2/e$, we have

$$\begin{aligned}\sum_{n\le x}\Lambda(n) &= \sum_{p\le x}\log p + \sum_{p^k\le x,\ k\ge 2}\log p\\ &< (2\log 2)x + (2\log 2)\sum_{k=2}^{\lfloor \log x/\log 2\rfloor} x^{1/k}\\ &< (2\log 2)x + 2x^{1/2}\log x < (2\log 2 + 4/e)x < 3x\ .\end{aligned}$$

□

Proposition 12.

$$\sum_{n\le x}\log n = x\log x + O(x) \quad \textit{for } x>1\ .$$

Proof. This follows from the inequalities

$$\int_1^{\lfloor x\rfloor}\log t\ dt \le \sum_{n\le x}\log n \le \int_2^{\lfloor x\rfloor+1}\log t\ dt$$

and from $\int \log t = t\log t - t$. □

In the next proposition we prove Theorem 8 for $m=1,2$.

Proposition 13.

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1) \quad \textit{for } x>1\ .$$

Proof. We have

$$\begin{aligned}x\log x + O(x) &= \sum_{n\le x}\log n = \sum_{n\le x}\sum_{d\,|\,n}\Lambda(d) \text{ (Propositions 12 and 9)}\\ &= \sum_{d\le x}\Lambda(d)\sum_{n\le x,\ d\,|\,n} 1 = \sum_{d\le x}\Lambda(d)\lfloor x/d\rfloor \text{ (swapping sums)}\\ &= x\sum_{d\le x}\frac{\Lambda(d)}{d} + \delta\sum_{d\le x}\Lambda(d),\ -1\le\delta\le 0\ (\lfloor\alpha\rfloor = \alpha - \{\alpha\})\\ &= x\Big(\sum_{p\le x}\frac{\log p}{p} + \sum_{p^k\le x,\ k\ge 2}\frac{\log p}{p^k}\Big) + O(x)\ (\Lambda,\text{ Prop. 11})\\ &= x\sum_{p\le x}\frac{\log p}{p} + O(x)\ (\textstyle\sum_{n,k\ge 2}(\log n)/n^k \text{ converges})\end{aligned}$$

and dividing by x gives the result. □

For $a, m \in \mathbb{N}$ we define the indicator functions

$$\chi_0,\ \mathbb{I}_{a,m} :\ \mathbb{N} \to \{0,1\}$$

by $\chi_0(n) = 1 \iff (n,m) = 1$ and $\mathbb{I}_{a,m}(n) = 1 \iff n \equiv a \pmod m$. A function $\chi :\ \mathbb{N} \to \mathbb{C}$ is *completely multiplicative* if $\chi(1) = 1$ and $\chi(ab) = \chi(a)\chi(b)$ for every $a, b \in \mathbb{N}$. It is *strongly bounded* if $\sum_{n \le x} \chi(n) = O(1)$ for $x > 1$, that is, there is a constant $c > 0$ such that $|\sum_{i=1}^{n} \chi(i)| < c$ for every $n \in \mathbb{N}$. By $\overline{\chi}$ we denote the conjugate function

$$\overline{\chi}(n) := \overline{\chi(n)}\ .$$

Note that strong boundedness implies boundedness, and that if χ is completely multiplicative and (strongly) bounded then $|\chi(n)| \le 1$ for every $n \in \mathbb{N}$. The heart of the proof of Dirichlet's theorem is the following expression of $\mathbb{I}_{a,m}$ as a linear combination of completely multiplicative and, with one exception, strongly bounded functions. Interestingly, even though $\mathbb{I}_{a,m}$ has values just 0 and 1, the functions in the combination are complex-valued.

Proposition 14. *For every $m \in \mathbb{N}$ there is a finite set $D = D_m$ of functions $\chi :\ \mathbb{N} \to \mathbb{C}$ with the following properties.*

1. *$\chi_0 \in D$, $\chi \in D \Rightarrow \overline{\chi} \in D$, every $\chi \in D$ is completely multiplicative and, except χ_0, strongly bounded.*

2. *For every $a \in \mathbb{N}$, $(a,m) = 1$, there exist coefficients $c_\chi = c_{a,\chi} \in \mathbb{C}$, $\chi \in D$, such that $c_{\chi_0} = 1/\varphi(m)$ and*

$$\mathbb{I}_{a,m} = \sum_{\chi \in D} c_\chi \chi = \frac{\chi_0}{\varphi(m)} + \sum_{\chi \in D \setminus \{\chi_0\}} c_\chi \chi\ .$$

If $a \equiv 1$ modulo m then $c_\chi = 1/\varphi(m)$ for every $\chi \in D$.

We postpone the proof for a while.

Lecture 4, March 21, 2017

Proposition 15. *For every $m \in \mathbb{N}$ and $\chi \in D_m \setminus \{\chi_0\}$,*

$$L(1,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n} \neq 0\ .$$

We postpone the proof for a while and proceed to the proof of Dirichlet's theorem. The next inequality is a key tool for bounding sums in that proof. It is in fact needed to prove that the previous infinite series $L(1,\chi)$, $\chi \neq \chi_0$, converges.

Proposition 16 (Abel's inequality). *Let $a_i \in \mathbb{C}, b_i \in \mathbb{R}$, $i = 1, 2, \ldots, n$, with $b_1 \geq b_2 \geq \cdots \geq b_n \geq 0$. Let $A_i = a_1 + a_2 + \cdots + a_i$. Then*

$$|a_1 b_1 + a_2 b_2 + \cdots + a_n b_n| \leq \max_{1 \leq i \leq n} |A_i| \cdot b_1 \ .$$

Proof. We set $A_0 = b_0 = b_{n+1} = 0$. Then

$$\begin{aligned} \left| \sum_{i=1}^{n} a_i b_i \right| &= \left| \sum_{i=1}^{n} (A_i - A_{i-1}) b_i \right| = \left| \sum_{i=0}^{n} A_i b_i - \sum_{i=0}^{n} A_i b_{i+1} \right| \\ &= \left| \sum_{i=1}^{n} A_i (b_i - b_{i+1}) \right| \leq \sum_{i=1}^{n} |A_i| (b_i - b_{i+1}) \\ &\leq \max_{1 \leq i \leq n} |A_i| \sum_{i=1}^{n} (b_i - b_{i+1}) = \max_{1 \leq i \leq n} |A_i| \cdot b_1 \ . \end{aligned}$$

□

Proposition 17. *For every $m \in \mathbb{N}$ and $\chi \in D_m \backslash \{\chi_0\}$,*

$$L(1, \chi) \neq 0 \Rightarrow \sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} = O(1), \ x > 1 \ .$$

Proof. Let m and χ be as stated, $x > 1$ and $L(1, \chi) \neq 0$. Then

$$\begin{aligned} O(1) &= \sum_{n \leq x} \frac{\chi(n) \log n}{n} \text{ (Abel's inequality, } \chi \text{ is strongly bounded)} \\ &= \sum_{n \leq x} \frac{\chi(n)}{n} \sum_{d \,|\, n} \Lambda(d) \text{ (Proposition 9)} \\ &= \sum_{d \leq x} \frac{\chi(d) \Lambda(d)}{d} \sum_{e \leq x/d} \frac{\chi(e)}{e} \text{ } (\chi \text{ is c. multiplicative, swapping sums)} \\ &= \sum_{d \leq x} \frac{\chi(d) \Lambda(d)}{d} (L(1, \chi) - O(d/x)) \text{ (Abel's inequality, } \chi \text{ s. bounded)} \\ &= L(1, \chi) \sum_{d \leq x} \frac{\chi(d) \Lambda(d)}{d} - O(1/x) \sum_{d \leq x} \Lambda(d) \text{ } (\chi \text{ is bounded)} \\ &= L(1, \chi) \sum_{d \leq x} \frac{\chi(d) \Lambda(d)}{d} + O(1) \text{ (Proposition 11)} \end{aligned}$$

and dividing by $L(1, \chi)$ we get the result. □

(This proposition was inserted and the proof of the next one was modified after the course was finished to make logical dependence between propositions clear.)

Proposition 18. *For every $m \in \mathbb{N}$ and $\chi \in D_m \backslash \{\chi_0\}$,*

$$L(1,\chi) \neq 0 \Rightarrow \sum_{p \leq x} \frac{\chi(p)\log p}{p} = O(1),\ x > 1\ .$$

Proof. Let m and χ be as stated, $x > 1$ and $L(1,\chi) \neq 0$. Then

$$\begin{aligned} O(1) &= \sum_{d \leq x} \frac{\chi(d)\Lambda(d)}{d} \text{ (Proposition 17)} \\ &= \sum_{p \leq x} \frac{\chi(p)\log p}{p} + \sum_{p^k \leq x,\, k \geq 2} \frac{\chi(p^k)\log p}{p^k} \text{ (definition of } \Lambda) \\ &= \sum_{p \leq x} \frac{\chi(p)\log p}{p} + O(1) \text{ } (\chi(n) = O(1),\ \textstyle\sum_{n,k\geq 2}(\log n)/n^k \text{ converges})\ . \end{aligned}$$

□

Proposition 19. *If $\chi_0 \in D_m$ then*

$$\sum_{p \leq x} \frac{\chi_0(p)\log p}{p} = \log x + O(1),\ x > 1\ .$$

Proof. For $x > 1$ the sum equals

$$\sum_{p \leq x} \frac{\log p}{p} - \sum_{p \leq x,\, p \mid m} \frac{\log p}{p} = \log x + O(1) \text{ (Proposition 13)}\ .$$

□

Proof of Theorem 8 and hence of Dirichlet's theorem. Let $a, m \in \mathbb{N}$ be coprime numbers and $x > 1$. Then

$$\begin{aligned} \sum_{p = a+mn \leq x} \frac{\log p}{p} &= \sum_{p \leq x} \frac{\mathbb{I}_{a,m}(p)\log p}{p} \\ &= \sum_{p \leq x} \sum_{\chi \in D} c_\chi \chi(p) \frac{\log p}{p} \text{ (Proposition 14)} \\ &= \sum_{\chi \in D} c_\chi \sum_{p \leq x} \frac{\chi(p)\log p}{p} \text{ (swapping sums)} \\ &= \frac{1}{\varphi(m)} \sum_{p \leq x} \frac{\chi_0(p)\log p}{p} + \sum_{\chi \in D\backslash\{\chi_0\}} c_\chi \sum_{p \leq x} \frac{\chi(p)\log p}{p} \\ &\quad \text{(Proposition 14)} \\ &= \frac{\log x}{\varphi(m)} + O(1) \text{ (Propositions 19 and 18)}\ . \end{aligned}$$

□

We prove Proposition 15, assuming Proposition 14. We first treat the case when χ is a real function. Then Proposition 14 is not needed.

Proposition 20 (Proposition 15 for real χ). *If $\chi : \mathbb{N} \to \mathbb{R}$ is completely multiplicative and strongly bounded then*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n} \neq 0 \, .$$

For the proof we need two lemmas.

Lemma 21 (the AGM inequality). *If $a_1, a_2, \ldots, a_n$ are nonnegative real numbers then $(a_1 + a_2 + \cdots + a_n)/n \geq (a_1 a_2 \ldots a_n)^{1/n}$.*

Proof. Derivatives show that $e^{x-1} \geq x$ for every $x \geq 0$. Let $a = (a_1 + a_2 + \cdots + a_n)/n > 0$. For $i = 1, 2, \ldots, n$ we set $x_i = a_i/a$ and multiply the n inequalities $e^{x_i - 1} \geq x_i$:

$$1 = \exp((a_1 + a_2 + \cdots + a_n)/a - n) \geq a_1 a_2 \ldots a_n / a^n \, .$$

This is, after rearrangement, the AGM inequality. □

Lemma 22. *If $t \in [0, 1)$ and $b_n = (n(1-t))^{-1} - t^n/(1-t^n)$, $n \in \mathbb{N}$, then $1 = b_1 \geq b_2 \geq \cdots \geq 0$.*

Proof. Since $b_n \to 0$, it suffices to prove that $b_n - b_{n+1} \geq 0$ for every n. Now $(1-t)(b_n - b_{n+1})$ equals

$$\frac{1}{n(n+1)} - \frac{t^n = t^{(n-1)/2} \cdot t^{n/2} \cdot t^{1/2}}{(1 + t + t^2 + \cdots + t^{n-1})(1 + t + t^2 + \cdots + t^n)} \, .$$

The AGM inequality gives $(1 + t + t^2 + \cdots + t^{n-1})/n \geq (t^{0+1+2+\cdots+n-1})^{1/n} = t^{(n-1)/2}$ and $(1 + t + t^2 + \cdots + t^n)/(n+1) \geq t^{n/2}$. It follows that the displayed difference is indeed nonnegative. □

Proof of Proposition 20. Assume for contradiction that $\sum \chi(n)/n = 0$ and

take for $t \in [0,1)$ the b_n from the previous lemma. Then for $t \in [0,1)$,

$$\begin{aligned} O(1) &= -\sum_{n=1}^{\infty} \chi(n) b_n \text{ (Abel's ineq., } \chi \text{ strongly bounded, Lemma 22)} \\ &= \sum_{n=1}^{\infty} \frac{\chi(n) t^n}{1-t^n} - \frac{1}{1-t} \sum_{n=1}^{\infty} \frac{\chi(n)}{n} \text{ (the definition of } b_n) \\ &= \sum_{n=1}^{\infty} \chi(n) \sum_{k=1}^{\infty} t^{kn} \text{ } (L(1,\chi) = 0, \text{ geometric series}) \\ &= \sum_{m=1}^{\infty} t^m \sum_{n \mid m} \chi(n) \text{ (swapping sums by absolute convergence)} \\ &= \sum_{m=1}^{\infty} t^m \prod_{i=1}^{r} \sum_{j=0}^{a_i} \chi(p_i)^j \text{ } (\chi \text{ is c. multiplicative, } m = p_1^{a_1} \dots p_r^{a_r}) \, . \end{aligned}$$

For $\chi(p_i) \neq 1$ the last sum equals $(1-\chi(p_i)^{a_i+1})/(1-\chi(p_i))$, and for $\chi(p_i) = 1$ it is $a_i + 1$. But $|\chi(p_i)| \leq 1$ and thus each of the last sums is nonnegative and so is the last product. For $m = p^2$ the last product is even $1 + \chi(p) + \chi(p)^2 = (1/2 + \chi(p))^2 + 3/4 \geq 3/4$. Thus we have a power series $\sum_{m \geq 1} c_m t^m$ that is on the one hand bounded for $t \in [0,1)$ but on the other hand its coefficients $c_m \geq 0$ for every $m \in \mathbb{N}$ and $c_m \geq 3/4$ for infinitely many m, hence for $t \to 1^-$ its sum goes to $+\infty$. This is a contradiction. □

It remains to prove Proposition 15 for nonreal $\chi \in D_m$. We will treat all $\chi \in D_m$ together, using part 2 of Proposition 14. We use properties of the *Möbius function* $\mu : \mathbb{N} \to \{-1, 0, 1\}$ that has values $\mu(1) = 1$, $\mu(p_1 p_2 \dots p_k) = (-1)^k$ (the p_i are distinct), and $\mu(n) = 0$ if n is not a product of distinct primes.

Proposition 23. *The Möbius function has the following properties.*

1. *For $n \in \mathbb{N}$, $\sum_{d \mid n} \mu(d)$ is 1 for $n = 1$ and 0 else.*
2. *If $f, g : \mathbb{N} \to \mathbb{C}$ are related by $f(n) = \sum_{d \mid n} g(d)$, then this relation is inverted by $g(n) = \sum_{d \mid n} \mu(n/d) f(d)$.*
3. *For $n \in \mathbb{N}$ and $x > 0$, $\sum_{d \mid n} \mu(d) \log(x/d)$ is $\log x$ for $n = 1$ and $\Lambda(n)$ else.*

Lecture 5, March 28, 2017

Proof. 1. The case $n = 1$ is trivial, let $n \geq 2$ and $n = p_1^{a_1} \dots p_k^{a_k}$ be its prime factorization with $k \geq 1$. The stated sum then, by the definition of μ, equals

$$\sum_{X \subset [k]} (-1)^{|X|} = \sum_{i=0}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0 \, .$$

2. Let f and g be as given and $n \in \mathbb{N}$. Then

$$\sum_{d\,|\,n} \mu(n/d) f(d) = \sum_{ab=n} \mu(a) f(b) = \sum_{acd=n} \mu(a) g(c) = \sum_{c\,|\,n} g(c) \sum_{a\,|\,n/c} \mu(a) = g(n)\ ,$$

expressing f in terms of g and using part 1.

3. For $n = 1$ this is true, let $n \geq 2$. We invert by part 2 the identity in Proposition 9 and use also part 1:

$$\Lambda(n) = \sum_{d\,|\,n} \mu(d) \log(n/d) = (\log n) \sum_{d\,|\,n} \mu(d) - \sum_{d\,|\,n} \mu(d) \log d = -\sum_{d\,|\,n} \mu(d) \log d\ .$$

This equals to the stated sum; expand it by $\log(x/d) = \log x - \log d$ and use again part 1. □

Proposition 24. *Let $m \in \mathbb{N}$. For $\chi \in D$, where D is given in Proposition 14, and $x > 1$ we define $S(\chi, x) := \sum_{n \leq x} \chi(n)\Lambda(n)/n$. Then*

1. *$S(\chi_0, x) = \log x + O(1)$,*
2. *if $\chi \neq \chi_0$ and $L(1, \chi) \neq 0$ then $S(\chi, x) = O(1)$, and*
3. *if $\chi \neq \chi_0$ and $L(1, \chi) = 0$ then $S(\chi, x) = -\log x + O(1)$.*

Proof. 1. This follows from Proposition 19. Its sum differs from the present one at most by the sum of the convergent series $\sum_{n,k \geq 2} \chi_0(n^k)(\log n)/n^k$.

2. This was proved by Proposition 17.

3. Let $\chi \neq \chi_0$, $L(1, \chi) = 0$ and $x > 1$, then

$$\begin{aligned}
S(\chi, x) &= -\log x + \sum_{n \leq x} \frac{\chi(n)}{n} \sum_{d\,|\,n} \mu(d) \log(x/d) \ \text{(3 of Prop. 23)} \\
&= -\log x + \sum_{d \leq x} \frac{\chi(d)\mu(d) \log(x/d)}{d} \sum_{e \leq x/d} \frac{\chi(e)}{e} \\
&\quad \text{(c. multiplicativity of } \chi\text{, swapping sums)} \\
&= -\log x + \sum_{d \leq x} \frac{\chi(d)\mu(d) \log(x/d)}{d} (L(1, \chi) - O(d/x)) \\
&\quad \text{(Abel's inequality, } \chi \text{ strongly bounded)} \\
&= -\log x + \frac{1}{x} O\Big(\sum_{d \leq x} \log(x/d) \Big) \ (|\chi(d)\mu(d)| \leq 1,\ L(1, \chi) = 0) \\
&= -\log x + O(1)\ .
\end{aligned}$$

The last bound follows from Proposition 12: $\sum_{d \leq x} \log(x/d) = \lfloor x \rfloor \log x - \sum_{d \leq x} \log d = x \log x + O(\log x) - (x \log x + O(x)) = O(x)$. □

Proof of Proposition 15 for nonreal χ. We assume for contradiction that $\chi \in D\backslash\{\chi_0\}$ is such that $\chi \neq \overline{\chi}$ and $L(1,\chi) = 0$. By the definition of $L(1,\chi)$, also $L(1,\overline{\chi}) = 0$. Thus $N := |\{\chi \in D\backslash\{\chi_0\} \mid L(1,\chi) = 0\}| \geq 2$. But, for $x > 1$,

$$\begin{aligned} 0 &\leq \sum_{n=1+mk\leq x} \frac{\Lambda(n)}{n} = \sum_{n\leq x} \frac{\mathbb{I}_{1,m}(n)\Lambda(n)}{n} \text{ (Λ is nonnegative)} \\ &= \sum_{n\leq x} \frac{1}{\varphi(m)} \sum_{\chi\in D} \frac{\chi(n)\Lambda(n)}{n} \text{ (2 of Proposition 14)} \\ &= \sum_{\chi\in D} \frac{S(\chi,x)}{\varphi(m)} = \frac{(1-N)\log x}{\varphi(m)} + O(1) < \frac{-\log x}{\varphi(m)} + O(1) \\ &\quad \text{(swapping sums, Proposition 24, } N \geq 2) \text{ .} \end{aligned}$$

For large x we get a contradiction. □

Now it only remains to prove Proposition 14. We show that the existence of the functions D_m is due to a general algebraic construction of group characters. Here a group $G = (G,\cdot)$ means a finite Abelian group. If G is such a group, its *character* is a homomorphism $\chi : G \to \mathbb{C}^\times$ to the multiplicative group of nonzero complex numbers. We denote the set of characters of G by G^*. It is easy to see that for every $\chi \in G^*$, $\chi(1_G) = 1$ and every value $\chi(g)$ is an $|G|$-th root of 1. In particular, always $|\chi(g)| = 1$ and thus $1/\chi = \overline{\chi}$. Every G possesses the character $\chi_0 \in G^*$ that is constantly 1 and is called *principal character*. The set G^* is a group too, with the operation $(\chi\psi)(g) := \chi(g)\psi(g)$. The inverse is $\chi^{-1} = 1/\chi$ and χ_0 is the neutral element. The next proposition implies that group characters other than χ_0 exist.

Proposition 25. *If $G \subset H$ is an extension of groups such that H/G is a cyclic group (i.e., is generated by a single element), then every $\chi \in G^*$ has exactly $|H/G|$ extensions to a $\psi \in H^*$ and $|H^*|/|G^*| = |H/G|$.*

Proof. Let $n = |H/G|$ and jG, $j \in H\backslash G$, be a generator of H/G. Every $h \in H$ has then a unique expression $h = j^r g$ with $0 \leq r < n$ and $g \in G$. If $\psi \in H^*$ extends $\chi \in G^*$ then $\psi(h) = \psi(j)^r\chi(g)$; also $\psi(j)^n = \chi(j^n)$ since $j^n \in G$. So for a fixed $\chi \in G^*$ each $\psi \in H^*$ extending it is given by the formula

$$\psi(h) = \psi_\alpha(h) = \alpha^r\chi(g)$$

where $h = j^r g$ is the unique expression for h and $\alpha \in \mathbb{C}$ is an n-th root of the number $\chi(j^n) \in \mathbb{C}$. There are exactly n numbers α and $\alpha \neq \beta$ implies $\psi_\alpha \neq \psi_\beta$ (take $h = j$). However, we have to show that each mapping ψ_α is a character of H. Let $h_1 = j^{r_1}g_1$ and $h_2 = j^{r_2}g_2$ be two elements of H with $0 \leq r_1, r_2 < n$ and $g_1, g_2 \in G$, and let $\alpha \in \mathbb{C}$ satisfy $\alpha^n = \chi(j^n)$. So $\psi_\alpha(h_1)\psi_\alpha(h_2) = \alpha^{r_1}\chi(g_1)\alpha^{r_2}\chi(g_2) = \alpha^{r_1+r_2}\chi(g_1g_2)$. If $r_1 + r_2 < n$ then

$$\psi_\alpha(h_1h_2) = \psi_\alpha(j^{r_1+r_2}g_1g_2) = \alpha^{r_1+r_2}\chi(g_1g_2) = \psi_\alpha(h_1)\psi_\alpha(h_2) \text{ .}$$

Else $r_1 + r_2 = n + s$ with $0 \leq s < n$, but then again

$$\psi_\alpha(h_1h_2) = \psi_\alpha(j^s j^n g_1 g_2) = \alpha^s \chi(j^n)\chi(g_1g_2) = \alpha^s\alpha^n\chi(g_1g_2) = \psi_\alpha(h_1)\psi_\alpha(h_2)\ .$$

Thus $\psi_\alpha \in H^*$.

The equality $|H^*|/|G^*| = |H/G|$ follows from the fact that the mapping $H^* \ni \psi \mapsto \psi \,|\, G$ is a mapping from H^* to G^* that is, as we have just proved, $|H/G|$ to 1. □

Proposition 26. *Let G be a group. Then $|G^*| = |G|$ and for every $g \in G$ different from 1_G there is a $\xi \in G^*$ with $\xi(g) \neq 1$.*

Proof. We set $G_0 = \{1_G\}$. If $G = G_0$, we finish. Else we take a $g \in G\backslash G_0$ and set $G_1 = \langle G_0 \cup \{g\}\rangle$. If $G = G_1$, we finish. Else we take a $g \in G\backslash G_1$, set $G_2 = \langle G_1 \cup \{g\}\rangle$, and continue in the suggested way. After finitely many steps we finish because $|G_0| < |G_1| < \cdots \leq |G|$. In this way we get a chain of group extensions $\{1_G\} = G_0 \subset G_1 \subset \ldots \subset G_k = G$ such that each factor G_{i+1}/G_i is cyclic. Hence

$$\begin{aligned} |G| &= \prod_{i=0}^{k-1} |G_{i+1}|/|G_i| \text{ (telescoping product)} \\ &= \prod_{i=0}^{k-1} |G_{i+1}/G_i| \text{ (cardinality of factorgroups)} \\ &= \prod_{i=0}^{k-1} |G^*_{i+1}|/|G^*_i| \text{ (Proposition 25)} \\ &= |G^*| \text{ (telescoping product)}\ . \end{aligned}$$

If $g \in G$ is not 1_G, then there is a $\chi \in \langle g\rangle^*$ with $\chi(g) \neq 1$ because $|\langle g\rangle^*| = |\langle g\rangle| \geq 2$. We use $\langle g\rangle = G_1$ in the above chain of extensions and extend by it, using Proposition 25, $\chi \in G_1^*$ to a $\xi \in G^*$. This ξ is as required. □

Lecture 6, April 4, 2017

Proposition 27 (orthogonal relations). *Let G be a group, $g \in G$, and $\chi \in G^*$. Then $\sum_{h\in G} \chi(h)$ is $|G|$ if χ is principal and 0 else, and $\sum_{\psi\in G^*} \psi(g)$ is $|G|$ if $g = 1_G$ and 0 else.*

Proof. The first halves of the two claims are trivial since each summand equals 1 (and $|G^*| = |G|$ by Proposition 26). Let $\chi \neq \chi_0$. Thus $\chi(j) \neq 1$ for some $j \in G$. The mapping $h \mapsto jh$ permutes G. Thus

$$\sum_{h\in G} \chi(h) = \sum_{h\in G} \chi(jh) = \chi(j) \sum_{h\in G} \chi(h)\ ,$$

which implies that the considered sum is 0. For the second claim we assume that $g \neq 1_G$ and argue in the same way in the group G^*. We need a $\xi \in G^*$ with $\xi(g) \neq 1$, which exists by Proposition 26. $\square$

Proof of Proposition 14. For a given $m \in \mathbb{N}$ we take the multiplicative group G_m of residues modulo m coprime to m; $|G_m| = \varphi(m)$. We extend each $\chi \in G_m^*$ to residues r mod m not coprime to m by $\chi(r) = 0$. For $\chi \in G_m^*$ we define $\chi' : \mathbb{N} \to \mathbb{C}$ by $\chi'(n) = \chi(n \bmod m)$. We set

$$D_m = \{\chi' \mid \chi \in G_m^*\} .$$

These mappings are called *Dirichlet characters modulo* m. Clearly, $\chi'_0 \in D_m$ and D_m is closed to complex conjugation because G_m^* is. In the same way every $\chi' \in D_m$ inherits complete multiplicativity from χ. The numbers coprime to m in any interval $I \subset \mathbb{N}$, $|I| = m$, are exactly the $\varphi(m)$ representatives of G_m. By Proposition 27, for any $\chi' \in D_m$, $\chi' \neq \chi'_0$, one has $\sum_{n\in I} \chi'(n) = \sum_{g\in G_m} \chi(g) = 0$. Thus for every $n \in \mathbb{N}$ and such χ' one has

$$\left|\sum_{i=1}^{n} \chi'(i)\right| = \left|\sum_{i=r}^{n} \chi'(i)\right| \leq \sum_{i=r}^{n} |\chi'(i)| \leq m - 1$$

by splitting $1, 2, \ldots, n$ into $\lfloor n/m \rfloor$ intervals of length m and the residual interval $r, r+1, \ldots, n$ of length at most $m-1$. Thus every $\chi' \in D_m \backslash \{\chi'_0\}$ is strongly bounded. Let $a \in \mathbb{N}$ be coprime to m; we take a $b \in \mathbb{N}$ such that $ab \equiv 1$ modulo m. Then, by Proposition 27, for every $n \in \mathbb{N}$ we have

$$\begin{aligned}\sum_{\chi'\in D_m} (\chi'(b)/\varphi(m))\chi'(n) &= \frac{1}{\varphi(m)} \sum_{\chi'\in D_m} \chi'(bn) \\ &= \frac{1}{|G_m|} \sum_{\chi\in G_m^*} \chi(bn \bmod m) = \mathbb{I}_{a,m}(n) ,\end{aligned}$$

which gives the required coefficients $c_{\chi'} = \chi'(b)/\varphi(m)$. Clearly,

$$c_{\chi'_0} = \chi'_0(b)/\varphi(m) = 1/\varphi(m) .$$

Finally, if $a \equiv 1$ modulo m then $b \equiv 1$ as well and each coefficient is $\chi'(b)/\varphi(m) = 1/\varphi(m)$. $\square$

This completes the proof of Theorem 8. The general Dirichlet's theorem is proven. $\square$

We mention reference for the proof that is due to H. N. Shapiro (1922–2013) and its characteristic feature is Proposition 24 —

- H. N. Shapiro, On primes in arithmetic progression. II, *Ann. of Math. (2)* **52** (1950), 231–243

— and conclude the part of the course on DT by three lose problems.

The first problem asks if one can prove Dirichlet's theorem by a purely algebraic argument based on formal Dirichlet series. One easily proves in this way that the set of prime numbers is infinite. By part 1 of Proposition 23 we have the formal identity

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1 \ .$$

If there are finitely many primes then the second series is finite because $\mu(u) \neq 0$ only for those finitely many n that are products of distinct primes. But formal equalities of the type

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \cdot \sum_{n=1}^{k} \frac{a_n}{n^s} = \sum_{n=1}^{l} \frac{b_n}{n^s} \ ,$$

with $a_n, b_n \in \mathbb{C}$ and $a_1 = \cdots = a_{i-1} = 0 \neq a_i$, are impossible: on the left side after multiplying the two series, infinitely many coefficients of $1/n^s$ are nonzero (for example if $n = k! + i$, $2 \cdot k! + i$, $3 \cdot k! + i$, ... when the coefficient equals a_i) but the right side has only finitely many nonzero coefficients. Could not we prove in a similar fashion the whole Dirichlet's theorem?

The second lose problem asks about the role of complex numbers $\mathbb{C}$ in proofs of DT. Their main role is not in using complex analysis in some proofs of DT when L-functions $L(s, \chi) = \sum \chi(n)/n^s$, $s \in \mathbb{C}$ are treated analytically, but in the remarkable identity ($a, m, n \in \mathbb{N}$ and $(a, m) = 1$)

$$\mathbb{I}_{a,m}(n) = \sum_{\chi \in D_m} c_\chi \cdot \chi(n)$$

that has a real, in fact 0-1 function on the left side but complex coefficients c_χ and complex-valued functions χ on the right side; every χ is completely multiplicative and, except χ_0, strongly bounded (Proposition 14). Could one in some precise sense prove that complex linear combinations like this cannot be avoided and replaced with real ones? What if D_m may be infinite?

The third problem is not lose but quite concrete. Is it true that if $\chi : \mathbb{N} \to \mathbb{C}$ is completely multiplicative, not identically zero (hence $\chi(1) = 1$) and strongly bounded then

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} \neq 0 \ ?$$

I stress that χ here are more general than Dirichlet characters, for example we may set $\chi(2) = 1$ and $\chi(p) = (-1)^{(p-1)/2}/(p-1)$ for $p > 2$ (and extend multiplicatively to $\chi(n)$). Proposition 20 proves it for real χ.

Asymptotic and combinatorial theory of (integer) partitions

A *partition of* $n \in \mathbb{N}$ is any ordered tuple $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k)$ of natural numbers such that $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n$. Let $p(n)$, $n \in \mathbb{N}$, be the

partition function, the number of such partitions of n. We define $p(0) = 1$. For example, $p(6) = 11$ as the partitions of 6 are

$$6,\ 51,\ 42,\ 411,\ 33,\ 321,\ 3111,\ 222,\ 2211,\ 2111,\ \text{ and }\ 111111\ .$$

We will prove

Theorem 28 (Hardy–Ramanujan, 1918; Uspensky, 1920). *For $n \to \infty$,*

$$p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi(2/3)^{1/2} n^{1/2}} \ .$$

But we start with something easier. The number of compositions of $n \in \mathbb{N}$ with $k \in \mathbb{N}$ parts, $c(n,k)$, is the number of the above tuples without order, and $c(n)$ is the total number compositions of n, with any number of parts. Then, as is well known,

$$c(n,k) = \binom{n-1}{k-1} \ \text{ and } \ c(n) = 2^{n-1} \ .$$

One easily proves it by bijecting compositions of n with the placements of separators in $n-1$ gaps in a row of n dots. The order of λ_i makes counting partitions much more difficult. For a set $A \subset \mathbb{N}$ we denote by $p_A(n)$ the number of partitions of n with all parts $\lambda_i \in A$. For finite A it is not hard to derive asymptotics of such restricted partition function.

Theorem 29 (Schur, 1926). *Suppose $A = \{a_1, a_2, \ldots, a_k\} \subset \mathbb{N}$ and $\gcd(A) = 1$. Then for $n \in \mathbb{N}$,*

$$p_A(n) = \frac{n^{k-1}}{a_1 a_2 \ldots a_k \cdot (k-1)!} + O(n^{k-2}) \ .$$

The case $\gcd(A) = d > 1$ easily reduces to $d = 1$ by cancelling the common factor d.

We base the proof on the following two auxiliary results.

Proposition 30 (generalized geometric series). *If $m \in \mathbb{N}$ and $\alpha \in \mathbb{C}$ then, formally,*

$$\frac{1}{(1-\alpha x)^m} = \sum_{n=0}^{\infty} \binom{n+m-1}{m-1} (\alpha x)^n = \sum_{n=0}^{\infty} \left(\frac{n^{m-1}}{(m-1)!} + O(n^{m-2}) \right) (\alpha x)^n$$

(for $n = 0$ the expression in big brackets is 1).

Proof. Differentiate formally

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots$$

$m-1$ times, divide the result by $(m-1)!$, and substitute αx for x. □

Proposition 31 (partial fractions). *Let $p_1, \dots, p_k \in \mathbb{C}[x]$ be pairwise coprime nonzero polynomials.*

1. *For some $q_1, \dots, q_k \in \mathbb{C}[x]$,*

$$\frac{1}{p_1 p_2 \dots p_k} = \frac{q_1}{p_1} + \frac{q_2}{p_2} + \dots + \frac{q_k}{p_k} \, .$$

2. *If in addition each $p_i = r_i^{m_i}$ where each $r_i \in \mathbb{C}[x]$ has degree 1 and $m_i \in \mathbb{N}$ then for some $\beta_{i,j} \in \mathbb{C}$,*

$$\frac{1}{p_1 p_2 \dots p_k} = \sum_{i=1}^{k} \sum_{j=1}^{m_i} \frac{\beta_{i,j}}{r_i^j} \, .$$

Proof. 1. Since $\mathbb{C}[x]$ is an Euclidean ring, it is PID and Bachet's identity holds in it: if $p_1, p_2 \in \mathbb{C}[x]$ are coprime then for some $q_1, q_2 \in \mathbb{C}[x]$,

$$1 = q_2 p_1 + q_1 p_2 \quad \text{and so} \quad \frac{1}{p_1 p_2} = \frac{q_1}{p_1} + \frac{q_2}{p_2} \, .$$

Iterating gives the identity for k polynomials instead of two.

2. Express the reciprocal of $p_1 p_2 \dots p_k$ as in part 1, write each q_i as a linear combination with coefficients in $\mathbb{C}$ of the powers $1, r_i, r_i^2, \dots, r_i^l, \dots$ (this is possible since r_i are linear), and cancel the common powers of r_i in the resulting fractions $r_i^l / r_i^{m_i}$. You get the stated identity plus possibly an additional term $q \in \mathbb{C}[x]$ on the right side, coming from the fractions with $l \geq m_i$. But sending x to $+\infty$ shows that q is in fact identically zero and is not present. □

Lecture 7, April 11, 2017

Proof of Theorem 29. For $d, e \in \mathbb{N}$ we denote $\alpha_{d,e} = e^{2\pi i \cdot e/d} \in \mathbb{C}$, the d-th root of 1 lying on $|z| = 1$ at the e-th position, counted modulo d counterclockwise from the point 1. Then, for $a \in \mathbb{N}$,

$$1 - x^a = \prod_{j=0}^{a-1} (1 - \alpha_{a,j} x) \, .$$

For the generating function of the numbers $p_A(n)$, $A = \{a_1, \dots, a_k\} \subset \mathbb{N}$ (k distinct numbers), we have the formula

$$\sum_{n=0}^{\infty} p_A(n) x^n = \frac{1}{(1 - x^{a_1})(1 - x^{a_2}) \dots (1 - x^{a_k})} =: \frac{1}{D_A(x)} \, .$$

This identity follows from the geometric series expansion $(1 - x^a)^{-1} = 1 + x^a + x^{2a} + \dots$ and the definition of $p_A(n)$ and holds formally in the ring $\mathbb{C}[[x]]$ of

formal power series (and the condition $\gcd(A) = 1$ is not needed for it). Using the above factorization of $1 - x^a$, we split the denominator $D_A(x)$ in pairwise coprime powers of linear polynomials:

$$D_A(x) = \prod_{l=1}^{k} \prod_{j=0}^{a_l - 1} (1 - \alpha_{a_l,j} x) = \prod_{(d,\, \exists\, l:\, d \,|\, a_l)} \prod_{(e,\, 0 \le e < d,\, (d,e)=1)} (1 - \alpha_{d,e} x)^{m_d}$$

where $m_d \in \mathbb{N}$ counts the parts a_l divisible by $d \in \mathbb{N}$. This follows by bringing each fraction j/a_l in $\alpha_{a_l,j}$ to the lowest terms and grouping together identical factors. Applying part 2 of Proposition 31 we get the identity

$$\sum_{n=0}^{\infty} p_A(n) x^n = \sum_{d,\, \ldots} \sum_{e,\, \ldots} \sum_{j=1}^{m_d} \frac{\beta_{d,e,j}}{(1 - \alpha_{d,e} x)^j} = \frac{1}{D_A(x)}, \ \beta_{d,e,j} \in \mathbb{C}$$

(we sum over the same sets of d and e as in the products). We expand the fractions in the middle according to Proposition 30 and compare coefficients of x^n with the left side. The asymptotically largest contribution comes from the fractions with maximum j, which under the condition $\gcd(A) = 1$ is attained uniquely: $j = m_1 = k$ but $m_d < k$ for $d > 1$. Thus, as $\alpha_{1,0} = 1$ and $|\alpha_{d,e}| = 1$,

$$p_A(n) = \frac{\beta_{1,0,k} n^{k-1}}{(k-1)!} + O(n^{k-2}) \ .$$

It remains to determine $\beta_{1,0,k}$. Since

$$D_A(x) = (1-x)^k (\textstyle\sum_{i=0}^{a_1 - 1} x^i) \ldots (\sum_{i=0}^{a_k - 1} x^i) \ ,$$

for $x \to 1$ we have

$$\frac{1}{D_A(x)} \sim \frac{1}{(1-x)^k a_1 \ldots a_k} \ .$$

The second equality in the above identity then implies $\beta_{1,0,k} = \frac{1}{a_1 \ldots a_k}$. □

We can get from the partial fractions decomposition of $1/D_A(x)$ much more than just an asymptotics, we get an *effective* formula for $p_A(n)$. We have in mind a quite concrete meaning of "effective": since the number $p_A(n)$ has $\Theta(\log n)$ (binary, decadic) digits, an effective algorithm computing the function $n \mapsto p_A(n)$ is one working in time polynomial in $\log n$. As we show now, such an algorithm is implicit in the partial fractions decomposition of $1/D_A(x) = \sum_{n \ge 0} p_A(n) x^n$. Recall that a *quasipolynomial (with period $m \in \mathbb{N}$)* is a function $f : \mathbb{Z} \to \mathbb{C}$ for which there exist m polynomials $p_0, p_1, \ldots, p_{m-1} \in \mathbb{C}[x]$ such that

$$n \equiv i \pmod m \Rightarrow f(n) = p_i(n) \ .$$

Equivalently,

$$f(n) = a_0(n) + a_1(n) n + \cdots + a_r(n) n^r$$

for some m-periodic functions $a_0, \ldots, a_r : \mathbb{Z} \to \mathbb{C}$. A prototypical example is $(m = 2)$

$$p_{\{1,2\}}(n) = \lfloor n/2 \rfloor + 1 = a_0(n) + (1/2) n$$

where $a_0(n) = 1$ for even n and $a_0(n) = 1/2$ for odd n.

Theorem 32 (Bell, 1943). *For every finite set $A = \{a_1, a_2, \ldots, a_k\} \subset \mathbb{N}$ the function*

$$\mathbb{N} \to \mathbb{N}_0,\ n \mapsto p_A(n)\ ,$$

is a quasipolynomial with period $m = \operatorname{lcm}(A)$ and rational coefficients. Hence $n \mapsto p_A(n)$ can be computed in $O(\log^2 n)$ steps.

Proof. The above identity and Proposition 30 give the formula

$$p_A(n) = \sum_{d,\ldots} \sum_{e,\ldots} \sum_{j=1}^{m_d} \beta_{d,e,j} \binom{n+j-1}{j-1} \alpha_{d,e}^n\ .$$

Since the binomial coefficients are polynomials in n (with degree $j-1$) and $n \mapsto \alpha_{d,e}^n$ are $m = \operatorname{lcm}(A)$-periodic functions, we see that $p_A(n)$ is a quasipolynomial with period m. It has coefficients in $\mathbb{Q}$ (we know that they lie in $\mathbb{C}$) because one can express coefficients of a polynomial from its values by Lagrange interpolation and two polynomials with sufficiently many equal values coincide.

For a rational polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_r x^r = (\ldots((a_r x + a_{r-1})x + a_{r-2})x + \ldots)x + a_0$$

and $n \in \mathbb{N}$ we compute the value $f(n)$ by $2r$ multiplications and additions of two fractions whose numerators and denominators have size $O(f(n)) = O(n^r)$. This takes time $O(\log^2 n)$ (we multiply and add two integers as in elementary school). □

I give credit to E. T. Bell (1883–1960)

- E. T. Bell, Interpolated denumerants and Lambert series, *Amer. J. Math.* **65** (1943), 382–386

only for the first half of the theorem (and even this had been known before, to J. Sylvester in the 19th century), polynomial time algorithms were of course unheard of in Bell's time.

We return to the unrestricted partition function $p(n)$ counting all partitions of n.

Proposition 33. *For every $n > 1$,*

$$\log p(n) = \Theta(n^{1/2})\ .$$

We defer the proof for a while and look at the question of computing $p(n)$. An effective computation in this case is one taking time polynomial in n because $p(n)$ has roughly $n^{1/2}$ digits.

Proposition 34. *The partition function*

$$\mathbb{N} \to \mathbb{N},\ n \mapsto p(n)\ ,$$

can be computed in time $O(n^{5/2})$.

Proof. For $k, n \in \mathbb{N}$ let $p_k(n)$ be the number of partitions λ of n with k parts. Then $p_k(n) \in \mathbb{N}_0$, $p_k(n) = 0$ if $k > n$, $p_1(n) = p_n(n) = 1$ for every $n \in \mathbb{N}$, $p(n) = p_1(n) + p_2(n) + \cdots + p_n(n)$ and, crucially, for $1 < k < n$ we have the recurrence

$$p_k(n) = p_k(n-k) + p_{k-1}(n-1) \; .$$

Indeed, the first summand counts the λ with smallest part ≥ 2 (decrease each part by 1), and the second the λ with the smallest part 1 (delete it). Thus for the input $n \in \mathbb{N}$ we can generate the array

$$(p_k(m) \mid 1 \leq k \leq m \leq n)$$

with $n(n+1)/2$ terms by $(n-2)(n-1)/2$ additions of numbers with size $\leq p(n)$. Further $n-1$ additions of such numbers produce $p(n)$. This takes time $O(n^2 \cdot n^{1/2}) = O(n^{5/2})$. □

Other recurrences for $p(n)$ (e.g. the pentagonal recurrence) are more elegant and efficient but also take more effort to derive. In fact, F. Johansson in

- F. Johansson, Efficient implementation of the Hardy–Ramanujan–Rademacher formula, *LMS J. Comput. Math.* **15** (2012), 341–359

gave an algorithm computing $p(n)$ in time $n^{1/2+o(1)}$. It is an almost optimum algorithm as it takes $\gg n^{1/2}$ steps just to write $p(n)$ down.

Proof of Proposition 33. We first lowerbound $p(n)$, which is easy. For $n \geq 4$ we take the maximum $m \in \mathbb{N}$ such that $1+2+\cdots+m = m(m+1)/2 < n/2$, thus $m = \Theta(n^{1/2})$. Then $p(n) \geq 2^m$, which gives the lower bound, because for every subset $X \subset [m] = \{1, 2, \ldots, m\}$ there is a partition λ_X of n, and $\lambda_X \neq \lambda_Y$ if $X \neq Y$, namely the partition $\sum_{i \in X} i + (n - \sum_{i \in X} i) = n$.

I started proving the upper bound on $\log p(n)$ but will repeat it in the next lecture.

Lecture 8, April 18, 2017

We prove the upper bound in two ways and in fact we prove two slightly different bounds.

The first proof. We prove by the generating function

$$\sum_{n=0}^{\infty} p(n) t^n = F(t) := \prod_{k=1}^{\infty} \frac{1}{1-t^k}, \; t \in (0,1) \; ,$$

the upper bound

$$p(n) < \frac{\pi}{\sqrt{6(n-1)}} e^{c\sqrt{n}}, \; n \geq 2 \; ,$$

where $c = 2\sqrt{\zeta(2)} = \pi\sqrt{2/3}$ (since $\zeta(2) = \pi^2/6$).

Since $F(t) > p(n)t^n + p(n+1)t^{n+1} + \cdots > p(n)(t^n + t^{n+1} + \dots) = p(n)\frac{t^n}{1-t}$ ($p(n)$ increases), we have

$$\begin{aligned}
\log p(n) &< \log F(t) - n\log t + \log(1-t) \\
&= \sum_{k=1}^{\infty} \log\frac{1}{1-t^k} - n\log t + \log(1-t) \\
&= \sum_{k=1}^{\infty}\sum_{j=1}^{\infty} \frac{t^{jk}}{j} - n\log t + \log(1-t) \\
&= \sum_{j=1}^{\infty} \frac{t^j}{j(1-t^j)} - n\log t + \log(1-t) \\
&< \frac{t}{1-t}\sum_{j=1}^{\infty}\frac{1}{j^2} - n\log t + \log(1-t) = \frac{t\zeta(2)}{1-t} - n\log t + \log(1-t) \\
&= \frac{\zeta(2)}{u} + n\log(1+u) + \log\frac{u}{1+u} \quad (t = 1/(1+u),\ u > 0) \\
&< \frac{\zeta(2)}{u} + (n-1)u + \log u
\end{aligned}$$

where on the third line we used the Taylor expansion of logarithm, on the fourth we exchanged summation by absolute convergence and summed the inner geometric series, on the fifth we used the bound $\frac{1-t^j}{1-t} = 1 + t + t^2 + \cdots + t^{j-1} > jt^{j-1}$ for $j \in \mathbb{N}$, and on the last we applied the bound $\log(1+u) < u$ for $u > 0$. Setting $u = \sqrt{\zeta(2)/(n-1)}$ and applying $\exp(\cdot)$ we get the stated bound.

The second proof. We prove by a recurrence the upper bound,

$$p(n) \le e^{c\sqrt{n}},\ n \in \mathbb{N}_0\ ,$$

where again $c = 2\sqrt{\zeta(2)} = \pi\sqrt{2/3}$. The recurrence we use is

$$p(n) = \frac{1}{n}\sum_{i,j\ge 1} ip(n-ij) = \frac{1}{n}\sum_{l\ge 1}\sigma(l)p(n-l)$$

where $\sigma(l) = \sum_{d\,|\,l} d$ is the sum of divisors function, $p(0) = 1$ and $p(m) = 0$ if $m < 0$. For example,

$$\begin{aligned}
p(6) &= \frac{\sigma(1)p(5) + \sigma(2)p(4) + \sigma(3)p(3) + \sigma(4)p(2) + \sigma(5)p(1) + \sigma(6)p(0)}{6} \\
&= \frac{1\cdot 7 + 3\cdot 5 + 4\cdot 3 + 7\cdot 2 + 6\cdot 1 + 12\cdot 1}{6} = \frac{34+32}{6} = 11\ .
\end{aligned}$$

To prove the recurrence, for given $n, j \in \mathbb{N}$ with $j \le n$ and $\lambda \in P(n)$ (where $P(n)$ is the set of all partitions of n) we denote by $f_\lambda(j)$ the number of parts j in λ and by $f(j) = \sum_{\lambda\in P(n)} f_\lambda(j)$ the number of parts j in all partitions of n. We claim that

$$f(j) = \sum_{i\ge 1} p(n-ij)\ .$$

This follows by counting in two ways the pairs

$$A = \{(\lambda, i) \mid \lambda \in P(n),\, 1 \le i \le f_\lambda(j)\}$$

— $f(j) = \sum_{\lambda \in P(n)} f_\lambda(j) = |A| = \sum_{i \ge 1} \#\{\lambda \in P(n) \mid f_\lambda(j) \ge i\} = \sum_{i \ge 1} p(n - ij)$ because the partitions of n containing at least i parts j are in bijection, by deleting i parts j, with $P(n - ij)$. Thus, summing all $p(n)$ partitions $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_k = n$, we get

$$np(n) = \sum_{\lambda \in P(n)} \lambda = \sum_{j \ge 1} j \cdot f(j) = \sum_{j \ge 1} j \sum_{i \ge 1} p(n - ij)\ ,$$

our recurrence.

We apply this recurrence by means of the bounds ($l, n \in \mathbb{N}$ and $l \le n$)

$$\sqrt{n - l} \le \sqrt{n} - \frac{l}{2\sqrt{n}}$$

— $\frac{\sqrt{n} - \sqrt{n-l}}{1} = \frac{l}{\sqrt{n} + \sqrt{n-l}}$ — and ($x > 0$)

$$\frac{e^{-x}}{(1 - e^{-x})^2} = \frac{1}{(e^{x/2} - e^{-x/2})^2} < \frac{1}{x^2}$$

— $e^{x/2} - e^{-x/2} = x + \sum_{k \ge 1} c_k x^{2k+1}$ with all $c_k > 0$. We also use the expansion $\sum_{k \ge 1} k x^k = \frac{x}{(1-x)^2}$ (see Proposition 30).

Now $p(n) \le e^{c\sqrt{n}}$ obviously holds for $n = 0, 1$, and we may assume that $n \ge 2$. Then

$$\begin{aligned}
p(n) &= \frac{1}{n} \sum_{i,j \ge 1} i p(n - ij) \le \frac{1}{n} \sum_{ij \le n} i e^{c\sqrt{n - ij}} \\
&\le \frac{e^{c\sqrt{n}}}{n} \sum_{i,j \ge 1} i e^{-cij/2\sqrt{n}} = \frac{e^{c\sqrt{n}}}{n} \sum_{j \ge 1} \frac{e^{-cj/2\sqrt{n}}}{\left(1 - e^{-cj/2\sqrt{n}}\right)^2} \\
&< \frac{e^{c\sqrt{n}}}{n} \sum_{j \ge 1} \frac{1}{(cj/2\sqrt{n})^2} = \frac{e^{c\sqrt{n}}}{n} \cdot \frac{4n}{c^2} \sum_{j \ge 1} \frac{1}{j^2} \\
&= e^{c\sqrt{n}}\ .
\end{aligned}$$

The first $=$ is from the recurrence, the second $\le$ is by induction, the third $\le$ is by the above bound on the root, the fourth $=$ is by summing the generalized geometric series, the fifth $<$ is by the above bound on the exponential, and the last $=$ follows from $\sum_{j \ge 1} 1/j^2 = \zeta(2)$ and $c^2 = 4\zeta(2)$. □

The first proof is taken from

- J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, UK, 1992, p. 140

and the second from

- M. B. Nathanson, *Elementary Methods in Number Theory*, Springer, New York, 2000, pp. 457 and 465–469.

Proof of the asymptotics $p(n) \sim \frac{1}{4\sqrt{3}n} e^{c\sqrt{n}}$

with $c = 2\sqrt{\zeta(2)} = \pi\sqrt{2/3} = 2.56509\ldots$. Now we will prove Theorem 28.

Proposition 35. *Let* $z \in (-1, 1)$,

$$\Phi(z) = \sqrt{(1-z)/2\pi} \cdot e^{\pi^2(1+z)/12(1-z)} ,$$

and $q_n \in \mathbb{R}$ *be the Taylor coefficients of this function,* $\Phi(z) = \sum_{n\geq 0} q_n z^n$. *Then, for* $n \to \infty$,

$$q_n \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{2n/3}}$$

(the same asymptotics as for $p(n)$*).*

Proof. We begin with the Laplace integral

$$\int_{-\infty}^{+\infty} e^{-t^2}\, dt = \sqrt{\pi} .$$

Linear substitution $t := at - b$, $a, b \in \mathbb{R}$ and $a > 0$, in it gives the formula

$$\int_{-\infty}^{+\infty} e^{-a^2t^2} e^{2abt}\, dt = \frac{e^{b^2}\sqrt{\pi}}{a} .$$

Setting $a^2 = 1 - z$ and $b^2 = \pi^2/6(1-z)$ we get

$$\int_{-\infty}^{+\infty} e^{zt^2} e^{\pi t\sqrt{2/3} - t^2}\, dt = \sqrt{\pi/(1-z)} \cdot e^{\pi^2/6(1-z)}$$

and represent $\Phi(z)$ by an integral:

$$\Phi(z) = \frac{e^{-\pi^2/12}(1-z)}{\pi\sqrt{2}} \int_{-\infty}^{+\infty} e^{zt^2} e^{\pi t\sqrt{2/3} - t^2}\, dt .$$

Expanding $\Phi(z)$ and e^{zt^2} and comparing coefficients of z^n we get an integral formula for q_n. From it we will extract, by exchanging $n \to \infty$ and $\int$, the stated asymptotic relation for q_n.

Lecture 9, April 25, 2017

So, as $e^{zt^2} = \sum_{n\geq 0} z^n t^{2n}/n!$, comparison of coefficients gives

$$q_n = \frac{e^{-\pi^2/12}}{\pi\sqrt{2}} \int_{-\infty}^{+\infty} \left(\frac{t^{2n}}{n!} - \frac{t^{2n-2}}{(n-1)!} \right) e^{\pi t\sqrt{2/3} - t^2}\, dt \; .$$

Let $t = s + \sqrt{n}$. The exponent in the integrand then is

$$\pi t\sqrt{2/3} - t^2 = \pi^2/12 + \pi\sqrt{2n/3} - n - 2s\sqrt{n} + s^2 - 2(s - \pi/2\sqrt{6})^2$$

and the difference in the brackets becomes

$$\begin{aligned} \frac{t^{2n}}{n!}\left(1 - \frac{n}{t^2}\right) &= \frac{n^n(1+s/\sqrt{n})^{2n}}{n!} \cdot \frac{s^2 + 2s\sqrt{n}}{(s+\sqrt{n})^2} \\ &= \frac{n^{n+1/2}}{n \cdot n!}(1+s/\sqrt{n})^{2n} \cdot 2s \cdot \frac{1 + s/2\sqrt{n}}{(1+s/\sqrt{n})^2} \; . \end{aligned}$$

Thus with

$$C_n = \frac{e^{\pi\sqrt{2n/3}}}{\pi n\sqrt{2}} \cdot \frac{n^{n+1/2}}{e^n n!}$$

and

$$K_n(s) = \frac{1 + s/2\sqrt{n}}{(1+s/\sqrt{n})^2} \left((1+s/\sqrt{n}) e^{-s/\sqrt{n} + s^2/2n} \right)^{2n}$$

we get

$$q_n = C_n \int_{-\infty}^{+\infty} K_n(s) \cdot 2s \cdot e^{-2(s-\pi/2\sqrt{6})^2}\, ds \; .$$

The point of this transformation is that $\lim_{n\to\infty} K_n(s) = 1$ for any fixed s because

$$(1+s/\sqrt{n}) e^{-s/\sqrt{n} + s^2/2n} = e^{\log(1+s/\sqrt{n}) - s/\sqrt{n} + s^2/2n} = e^{O_s(n^{-3/2})} \; .$$

If we can exchange $n \to \infty$ and $\int$, the claimed asymptotics for q_n follows:

$$C_n \sim \frac{e^{\pi\sqrt{2n/3}}}{2\pi^{3/2} n}$$

by the Stirling asymptotics $n! \sim \sqrt{2\pi n}(n/e)^n$,

$$\begin{aligned} \int_{-\infty}^{+\infty} 2s \cdot e^{-2(s-\pi/2\sqrt{6})^2}\, ds &= \int_{-\infty}^{+\infty} (u + \pi/2\sqrt{3}) \cdot e^{-u^2}\, du \\ &= \frac{\pi}{2\sqrt{3}} \int_{-\infty}^{+\infty} e^{-u^2}\, du = \frac{\pi^{3/2}}{2\sqrt{3}} \end{aligned}$$

by the Laplace integral again ($\int_{-\infty}^{+\infty} u e^{-u^2}\, du = 0$ since the integrand is an odd function), and so

$$\begin{aligned} q_n &= C_n \int_{-\infty}^{+\infty} K_n(s) \cdot 2s \cdot e^{-2(s-\pi/2\sqrt{6})^2}\, ds \\ &\sim \frac{e^{\pi\sqrt{2n/3}}}{2\pi^{3/2} n} \cdot \frac{\pi^{3/2}}{2\sqrt{3}} = \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}} \; . \end{aligned}$$

The exchange of the limit and integral is justified by the dominated convergence theorem. We find a nonnegative real function $f(s)$ such that $\int_{-\infty}^{+\infty} f < \infty$ and $|I_n(s)| \le f(s)$ for every $s \in \mathbb{R}$ and $n \in \mathbb{N}$, where $I_n(s) = K_n(s) \cdot 2s \cdot e^{-2(s-\pi/2\sqrt{6})^2}$ is the integrand. For $x \ge 0$ the function xe^{1-x} attains maximum 1 at $x = 1$. If $s \ge 0$ we set $x = 1 + s/\sqrt{n}$ and see that $|K_n(s)| \le |\frac{\cdots}{\cdots}| \cdot |(\cdots)^{2n}| < 1 \cdot (e^{s^2/2n})^{2n} = e^{s^2}$. Hence for $s \ge 0$ we have the bound

$$|I_n(s)| \le 2s|K_n(s)|e^{-2(s-\pi/2\sqrt{6})^2} \le 2s \cdot e^{-s^2+O(s)} =: f(s) \; .$$

For $s \le 0$ we set $x = (1 + s/\sqrt{n})^2$ and get $(1 + s/\sqrt{n})^2 e^{-2s/\sqrt{n}} \le e^{s^2/n}$, hence $|1 + s/\sqrt{n}|e^{-s/\sqrt{n}} \le e^{s^2/2n}$ and

$$\begin{aligned} |K_n(s)| &\le \frac{|\cdots|}{|\cdots|}\big(|1 + s/\sqrt{n}| \cdot e^{-s/\sqrt{n}+s^2/2n}\big)^{2n} \\ &\le \frac{|s|}{|\cdots|}|1 + s/\sqrt{n}|^2 e^{s^2-2s/\sqrt{n}}\big(|1 + s/\sqrt{n}| \cdot e^{-s/\sqrt{n}}\big)^{2n-2} \\ &\le |s|e^{s^2-2s/\sqrt{n}} e^{(n-1)s^2/n} = |s|e^{2s^2+1-(1+s/\sqrt{n})^2} \le |s|e^{2s^2+1} \; . \end{aligned}$$

So, for $s \le 0$,

$$|I_n(s)| \le 2|s| \cdot |K_n(s)|e^{-2(s-\pi/2\sqrt{6})^2} \le 2s^2 e^{2\pi s/\sqrt{6}+O(1)} =: f(s) \; .$$

Clearly, this $f(s)$ has a finite integral over $\mathbb{R}$ and the dominated convergence theorem applies. □

But what has $\Phi(z)$ to do with the numbers $p(n)$? It approximates their generating function

$$F(z) := \sum_{n\ge 0} p(n)z^n = \prod_{n\ge 1} \frac{1}{1-z^n}, \; z \in \mathbb{C} \text{ with } |z| < 1$$

(this basic Euler's identity, which we used already for $z \in (0, 1)$, should have been proven but we skip the proof now). The functions $\Phi(z)$ and $F(z)$ are close when $z \in \mathbb{C}$ with $|z| < 1$ is near to 1.

Proposition 36. *If $z \in \mathbb{C}$ with $|z| < 1$ and $|1 - z| \le 2(1 - |z|)$ then, as $z \to 1$,*

$$F(z) = (1 + O(1 - z))\Phi(z) \; .$$

We defer the proof of this key result for some time and proceed to show how it implies that $p(n) \sim q_n$. We need an easy lemma.

Lemma 37. *If $z \in \mathbb{C}$ with $|z| < 1$ then*

$$|F(z)| < e^{(1-|z|)^{-1}+|1-z|^{-1}} \; .$$

Proof. In fact, this lemma turns out not so easy, but let us first 'prove' it and then discuss where is the problem. Taking logarithm of Euler's identity yields

$$\log F(z) = \sum_{n,m\geq 1} \frac{z^{nm}}{m} = \sum_{m\geq 1} \frac{z^m}{m(1-z^m)}$$

(by the Taylor expansion of the logarithm, exchange of summation by absolute convergence, and summation of the geometric series). So for $z \in \mathbb{C}$ with $|z| < 1$ we get, by the triangle inequality and since $|1 - z^m| \geq 1 - |z|^m$,

$$\begin{aligned} |\log F(z)| &\leq \frac{|z|}{|1-z|} + \sum_{m\geq 2} \frac{|z|^m}{m(1-|z|^m)} \\ &< \frac{1}{|1-z|} + \frac{1}{1-|z|} \sum_{m\geq 2} \frac{1}{m^2} \cdot \frac{m}{|z|^{-1} + |z|^{-2} + \cdots + |z|^{-m}} \\ &< \frac{1}{|1-z|} + \frac{1}{1-|z|} \sum_{m\geq 2} \frac{1}{m^2} < \frac{1}{|1-z|} + \frac{1}{1-|z|} \, . \end{aligned}$$

As $|\log F(z)| = |\log|F(z)| + i \arg(F(z))| \geq \log|F(z)|$, by applying $\exp(\cdot)$ we get the stated bound.

The problem is of course in the application of complex logarithm, in $\log F(z)$. We did not introduce this function and it is tricky to justify its required properties. The way around it is to show instead that

$$F(z) = \exp\big(\textstyle\sum_{m\geq 1} z^m/m(1-z^m)\big)$$

— the function $\exp(z) = \sum_{m\geq 0} z^m/m!$ is unproblematic. I return to it later. □

Recall that $\Phi(z) = \sum_{n\geq 0} q_n z^n$ where $\Phi(z)$ is defined in Proposition 35. The next result and Proposition 35 clearly prove the Hardy–Ramanujan–Uspensky asymptotics for $p(n)$ in Theorem 28.

Proposition 38. *For $n \to \infty$,*

$$p(n) = q_n + O\big(n^{-5/4} e^{\pi\sqrt{2n/3}}\big) \, .$$

Proof. Let $C = C_n$ be the circle $|z| = 1 - \pi/\sqrt{6n}$. By the Cauchy formula (from complex analysis),

$$p(n) - q_n = \frac{1}{2\pi i} \int_C \frac{F(z) - \Phi(z)}{z^{n+1}} \, dz \, .$$

We split C in the two arcs

$$A = \{z \in C \mid |1-z| < \pi\sqrt{2/3n}\} \quad \text{and} \quad B = C \backslash A \, .$$

For $z \in C$, $|z|^{-n} = e^{-n\log(1-(1-|z|))} = e^{\pi(n/6)^{1/2} + O(1)}$ and $|z|^{-1} \ll 1$. Thus by the definition of $\Phi(z)$, the previous lemma and triangle inequality we have

$$\begin{aligned}
\int_B \frac{F(z)-\Phi(z)}{z^{n+1}}\,dz &\ll \int_B |z|^{-n}\left(e^{|1-z|^{-1}+(1-|z|)^{-1}}+e^{\pi^2/6|1-z|}\right)\,|dz| \\
(z\in B \text{ and } z\in C) &\ll e^{\pi\sqrt{n/6}}\left(e^{(\sqrt{3n/2}+\sqrt{6n})/\pi}+e^{(\pi/6)\sqrt{3n/2}}\right) \\
&= e^{\sqrt{n}(\pi/\sqrt{6}+(1/\pi)(\sqrt{3/2}+\sqrt{6}))}+e^{\pi\sqrt{n}\sqrt{3/8}} \\
&\ll e^{\sqrt{n}\pi a}\,,
\end{aligned}$$

where $0<a<\sqrt{2/3}$ because $3/8<2/3$ and, since $1/\pi<\pi/9$, $\pi/\sqrt{6}+(1/\pi)(\sqrt{3/2}+\sqrt{6})<\pi(1/\sqrt{6}+(1/9)(\sqrt{3/2}+\sqrt{6}))=\cdots=\pi\sqrt{2/3}$.

The main contribution to the integral comes from the arc A and we bound it by means of the definition of $\Phi(z)$, Proposition 36 (note that the arc A satisfies its assumption) and the bound $|A|\ll n^{-1/2}$ on the length of A (in the previous bound we used the trivial $|B|\ll 1$):

$$\begin{aligned}
\int_A \frac{F(z)-\Phi(z)}{z^{n+1}}\,dz &\ll \int_A |z|^{-n}\cdot|1-z|^{3/2}\cdot e^{\pi^2/6|1-z|}\,|dz| \\
&\ll e^{\pi\sqrt{n/6}}\cdot n^{-3/4}\cdot e^{\pi\sqrt{n/6}}\cdot n^{-1/2} \\
&= n^{-5/4}e^{\pi\sqrt{2n/3}}
\end{aligned}$$

($|1-z|\ll n^{-1/2}$ by $z\in A$ and $|1-z|\ge 1-|z|=\pi/\sqrt{6n}$ by $z\in C$). Hence

$$\begin{aligned}
p(n)-q_n &= \frac{1}{2\pi i}\int_C \frac{F(z)-\Phi(z)}{z^{n+1}}\,dz=\frac{1}{2\pi i}\int_A\ldots+\frac{1}{2\pi i}\int_B\ldots \\
&= O\left(n^{-5/4}e^{\pi\sqrt{2n/3}}\right)\,.
\end{aligned}$$

□

We return to the proof of Lemma 37 and show how to circumvent complex logarithm. It suffices to show that for every $z\in\mathbb{C}$ with $|z|<1$ we have

$$\frac{1}{1-z}=\exp\left(\sum_{m\ge 1}\frac{z^m}{m}\right)$$

where, of course, $\exp(z)=e^z=\sum_{n\ge 0}\frac{z^n}{n!}$ (for every $z\in\mathbb{C}$). Then, using the basic identity $\exp(y)\exp(z)=\exp(y+z)$, we get (more precisely, we use limit form of the identity in the infinite product)

$$\begin{aligned}
F(z)=\prod_{n\ge 1}\frac{1}{1-z^n} &= \exp\left(\sum_{n\ge 1}\sum_{m\ge 1}\frac{z^{nm}}{m}\right)=\exp\left(\sum_{m\ge 1}\sum_{n\ge 1}\frac{z^{nm}}{m}\right) \\
&= \exp\left(\sum_{m\ge 1}\frac{z^m}{m(1-z^m)}\right)
\end{aligned}$$

and, since for every $z \in \mathbb{C}$ one has $|e^z| = e^{\mathrm{re}(z)} \le e^{|z|}$,

$$|F(z)| \le \exp(|\cdots|) < \cdots < \exp\left(|1-z|^{-1} + (1-|z|)^{-1}\right) ,$$

as in the previous proof of Lemma 37.

Let $f(z) = \frac{1}{1-z}$ $(z \in \mathbb{C}\backslash\{1\})$ and $g(z) = \exp\left(\sum_{m\ge1} \frac{z^m}{m}\right)$ $(|z| < 1)$. Clearly,

$$\frac{f'}{f} = \frac{(1-z)^{-2}}{(1-z)^{-1}} = \frac{1}{1-z} \quad \text{and} \quad \frac{g'}{g} = \frac{\exp(\cdots)\sum_{m\ge1} z^{m-1}}{\exp(\cdots)} = \frac{1}{1-z} .$$

So $\frac{f'}{f} = \frac{g'}{g}$ which implies that $(f/g)' = 0$ and $f(z) = cg(z)$ for some constant $c \in \mathbb{C}$. Since $f(0) = g(0) = 1$, $c = 1$ and $f(z) = g(z)$ and we complete the alternative proof of Lemma 37.

But it still remains to prove Proposition 36. For the proof we need three lemmas. First we recall the notion of total variation of a function. If $L \subset \mathbb{C}$ is a halfline (or a straight segment or a line) and $f : L \to \mathbb{C}$ is a function, we define the *total variation* $V_L(f) \in [0, +\infty]$ *of* f *over* L as

$$V_L(f) = \sup\left(|f(a_2) - f(a_1)| + |f(a_3) - f(a_2)| + \cdots + |f(a_n) - f(a_{n-1})|\right)$$

where $(a_1 < a_2 < \cdots < a_n) \subset L$ runs through all finite tuples of points on L, ordered according to the direction of L.

Lemma 39. *Suppose $g : L \to \mathbb{C}$ is an integrable function defined on a halfline $L \subset \mathbb{C}$ going from the origin and $0 \ne w \in L$. Then*

$$\left| w\sum_{n=1}^{\infty} g(nw) - \int_L g(u)\, du \right| \le |w| V_L(g) .$$

Lemma 40. *Let*

$$g(x) = \frac{1}{x(e^x-1)} - \frac{1}{x^2} + \frac{e^{-x}}{2x}$$

and $L \subset \mathbb{C}$ be a halfline going from the origin and lying in the halfplane $\mathrm{re}(z) > 0$. Then

$$\int_L g = \int_0^{+\infty} g(x)\, dx = -\frac{\log(2\pi)}{2} .$$

Lemma 41. *Suppose that L and g are as in the previous lemma, and in addition L lies in the sector $|\arg(z)| < K < \pi/2$. Then*

$$V_L(g) \ll_K 1 .$$

Proof. It follows that

$$V_L(g) = \int_L |g'(z)| \cdot |dz| .$$

(We justify this formula for total variation later.)

Since

$$g'(z) = -\frac{1}{z^2(e^z-1)} - \frac{e^z}{z(e^z-1)^2} + \frac{2}{z^3} - \frac{e^{-z}}{2z} - \frac{e^{-z}}{2z^2}$$

and $|e^z| = e^{\mathrm{re}(z)}$, for $z \in L$ and $z \to \infty$ the middle term $|\cdots| \ll |z|^{-3}$ dominates because each of the other four terms goes to 0 exponentially fast, as $\ll e^{-c|z|}$ for a constant $c = c(K) > 0$. Thus the portion of the integral for $z \in L$ with $|z| \geq 1$, say, converges (as $\int_1^{+\infty} x^{-3}\,dx < \infty$).

The function $g(z)$ is holomorphic for $|z| < 2\pi$, hence $|g'(z)|$ is bounded for $|z| < 1$, because the poles at $z = 0$ of the three summands cancel out and singularities closest to the origin are $z = \pm 2\pi i$. Indeed,

$$\frac{1}{x(e^x-1)} = \frac{1}{x^2 + x^3/2 + \ldots} = x^{-2} - \frac{x^{-1}}{2} + \ldots \quad \text{and} \quad \frac{e^{-x}}{2x} = \frac{x^{-1}}{2} - \ldots\,.$$

Thus also the portion of the integral for $z \in L$ with $|z| < 1$ converges. □

Proof. (Proof of Lemma 39.) Without loss of generality $L = [0, +\infty)$. Let $w > 0$ and $N \in \mathbb{N}$. Then

$$\begin{aligned}
&\left| w \sum_{n=1}^{N} g(nw) - \int_0^{Nw} g(u)\,du \right| \\
&= w \left| \int_0^1 \left(\sum_{n=0}^{N-1} (g(nw+w) - g(nw+uw)) \right) du \right| \\
&\leq w \int_0^1 \left(\sum_{n=0}^{N-1} |g(nw+w) - g(nw+uw)| \right) du \leq w \int_0^1 V_L(g)\,du \\
&= w V_L(g)\,.
\end{aligned}$$

Sending $N \to \infty$ we get the stated bound. □

Proof. (Proof of Lemma 40.) The first equality follows as usual from Cauchy's theorem. In more details, for $R > 0$ we denote by L_R the initial segment of L of length R (going from 0 to $z \in L$ with $|z| = R$), by K_R the arc of the circle $|z| = R$ going from the end of L_R to the point R on the real axis, and by C_R the closed curve formed by L_R, K_R, and the interval $[R, 0]$ ($[0, R]$ traversed backwards). Then

$$\int_{L_R} g = \int_0^R g(x)\,dx + \int_{C_R} g - \int_{K_R} g = \int_0^R g(x)\,dx + O(1/R)$$

because $\int_{C_R} g = 0$ by Cauchy's theorem (g is holomorphic on C_R and its interior) and $|\int_{K_R} g| \leq \max_{K_r} |g| \cdot |K_R| \ll R^{-2}R = 1/R$. For $R \to +\infty$ we get equality of both integrals.

By the dominated convergence theorem we have

$$\int_0^{+\infty} g(x)\,dx = \lim_{N\to\infty} \int_0^{+\infty} (1-e^{-Nx})g(x)\,dx\,.$$

We evaluate the last integral:

$$\begin{aligned}
&\int_0^{+\infty} (1-e^{-Nx})g(x)\,dx \\
&= \int_0^{+\infty} \frac{1-e^{-Nx}}{e^x-1}\cdot\frac{1+x-e^x}{x^2}\,dx + \int_0^{+\infty}(1-e^{-Nx})\frac{e^{-x}}{2x}\,dx \\
&= \sum_{k=1}^{N}\int_0^{+\infty} e^{-kx}\frac{1+x-e^x}{x^2}\,dx + \frac{1}{2}\int_0^{+\infty}\frac{e^{-x}-e^{-(N+1)x}}{x}\,dx \\
&= -\sum_{k=1}^{N}\int_0^{+\infty} e^{-kx}\left(\int_0^1 te^{(1-t)x}\,dt\right)dx + \frac{1}{2}\int_0^{+\infty}\left(\int_1^{N+1} e^{-tx}\,dt\right)dx \\
&= -\sum_{k=1}^{N}\int_0^1\left(\int_0^{+\infty} te^{(1-t-k)x}\,dx\right)dt + \frac{1}{2}\int_1^{N+1}\left(\int_0^{+\infty} e^{-tx}\,dx\right)dt \\
&= -\sum_{k=1}^{N}\int_0^1 \frac{t\,dt}{k+t-1} + \frac{1}{2}\int_1^{N+1}\frac{dt}{t} \\
&= \sum_{k=1}^{N}((k-1)\log(k/(k-1))-1) + \frac{\log(N+1)}{2} \\
&= N\log N - \sum_{k=1}^{N}\log k - N + \frac{\log(N+1)}{2} = -\log(\sqrt{2\pi}) + o(1)
\end{aligned}$$

because of the Stirling asymptotics $\sum_{k=1}^{N}\log k = \log(N!) = N\log N - N + \frac{1}{2}\log N + \log(\sqrt{2\pi}) + o(1)$ and because $\log(N+1) = \log N + \log(1+1/N) = \log N + O(1/N)$. We note that in the fourth equality we used Fubini's theorem to exchange order of integration but we will not prove it here. However, later we will prove the Stirling asymptotics for factorial. □

We come to the last proof that completes derivation of the partition function asymptotics.

Proof. (Proof of Proposition 36.) We want to show that

$$\frac{F(z)}{\Phi(z)} = 1 + O(1-z) \text{ for } z\to 1 \text{ via } |z|<1 \text{ with } |1-z|\le 2(1-|z|)$$

where $F(z) = \prod_{n=1}^{\infty} 1/(1-z^n)$ and $\Phi(z) = (\frac{1-z}{2\pi})^{1/2}\exp(\frac{\pi^2(1+z)}{12(1-z)})$. We change the variable to w by $z = e^{-w}$, $w = a+bi \in \mathbb{C}$. This is always possible if $z \neq 0$. By $2\pi i$-periodicity of the exponential function and since $|z|<1$, we can

take w with $|b| \le \pi$ and $a > 0$. The conditions that $|z| < 1$, z is near 1, and $|1-z| \le 2(1-|z|)$ imply that $|\arg(w)| = |\arctan(b/a)| < K < \pi/2$ for some constant K. Indeed, then both a and b are close to 0 and we have

$$|z| = e^{-a} = 1 - a + O(a^2) \;\text{ and }\; |1-z| \ge |\mathrm{im}(z)| = e^{-a}|\sin b| = |b| + O(b^2)\ ,$$

thus $2 \ge \frac{|1-z|}{1-|z|} \ge (1+o(1))|b/a|$ and for z as stated and sufficiently near to 1 the point $w = a + bi$ lies in the angular sector with $K = \arctan 3$, say. Further, for $z \to 1$ with $|z| < 1$ we have relations

$$w = O(1-z) \;\text{ and }\; \frac{1}{w} = \frac{1}{1-z} - \frac{1}{2} + O(1-z)\ .$$

Indeed, $z = e^{-w} = 1 - w + O(w^2) = 1 - w(1+o(1))$ yields

$$w = \frac{1-z}{1+o(1)} = (1-z)(1+o(1)) = O(1-z)\ ,$$

and $z = e^{-w} = 1 - w + \frac{w^2}{2} + O(w^3)$ gives

$$\frac{1}{1-z} = \frac{1}{w(1 - w/2 + O(w^2))} = \frac{1 + w/2 + O(w^2)}{w} = \frac{1}{w} + \frac{1}{2} + O(w)\ .$$

We finish the proof with the help of the familiar expression

$$F(z) = \exp\left(\sum_{m\ge1} \frac{z^m}{m(1-z^m)}\right) = \exp\left(\sum_{m\ge1} \frac{1}{m(e^{mw}-1)}\right),\ |z| < 1\ .$$

Using the function $g(x)$ of Lemma 40 and expansions $\frac{\pi^2}{6} = \sum_{n\ge1} \frac{1}{n^2}$ and $1 - z = \exp(-\sum_{n\ge1} z^n/n)$, $|z| < 1$, we have

$$\begin{aligned} F(z) &= e^{\frac{\pi^2}{6w}} \cdot (1-e^{-w})^{\frac12} \cdot \exp\left(w \sum_{m\ge1}\left(\frac{1}{mw(e^{mw}-1)} - \frac{1}{m^2w^2} + \frac{e^{-mw}}{2mw}\right)\right) \\ &= e^{\pi^2/6w} \cdot (1-z)^{1/2} \cdot \exp\left(w \sum_{m\ge1} g(mw)\right) \\ &= e^{\pi^2/6w} \cdot (1-z)^{1/2} \cdot e^{-\log(2\pi)/2 + O(w)} \end{aligned}$$

— the last line by Lemmas 39–41 applied to the halfline $L \subset \mathbb{C}$ starting at the origin and going through w. Finally, by the above relations between w and z,

$$\begin{aligned} \frac{F(z)}{\Phi(z)} &= \frac{e^{\pi^2/6w} \cdot (1-z)^{1/2} \cdot e^{-\log(2\pi)/2 + O(w)}}{((1-z)/2\pi)^{1/2} \cdot e^{\pi^2(1+z)/12(1-z)}} \\ &= \exp\left(\frac{\pi^2}{6}\left(\frac{1}{1-z} - \frac12 + O(1-z)\right) - \frac{\pi^2(1+z)}{12(1-z)} + O(1-z)\right) \\ &= e^{O(1-z)} = 1 + O(1-z),\ z \to 1 \text{ with } |z| < 1\ . \end{aligned}$$

□

The proof of Theorem 28 on asymptotics of $p(n)$ from lecture 6 is finished.

Lecture 12, May 16, 2017

Well, not completely. We used quite a few tools and results from analysis and now we at least recapitulate them, if we do not prove them (we will deduce Stirling's formula, though).

1. The Laplace or Gauss integral $\int_{-\infty}^{+\infty} e^{-t^2}\,dt = \sqrt{\pi}$ (Wikipedia says that it is the Gaussian or Euler–Poisson integral).

2. Exchange of $\int$ and $\sum$ (in deducing the asymptotics of q_n), justified by uniform convergence.

3. *Stirling's formula* $n! \sim \sqrt{2\pi n}(n/e)^n$. Later we give three proofs for it.

4. *Dominated convergence theorem* — if (f_n), $f_n : X \to \mathbb{R}$, is a sequence of measurable functions defined on a measure space (X, Σ, μ) such that $f_n \to f$ (pointwise convergence) and there is an integrable function $g : X \to \mathbb{R}$ such that for every $n \in \mathbb{N}$ and $x \in X$ one has $|f_n(x)| \le g(x)$, then $\int_X |f - f_n| \to 0$.

5. $\sum_{n\ge 0} p(n) z^n = \prod_{n\ge 1} 1/(1 - z^n)$, for every $z \in \mathbb{C}$ with $|z| < 1$.

6. *Cauchy's formula* — if $f : D \to \mathbb{C}$ is holomorphic on a domain $D \subset \mathbb{C}$ containing 0 and $C \subset D$ is a closed curve that winds once in the positive sense around 0 and the interior of C is contained in D, then the coefficients a_n in $f(z) = \sum_{n\ge 0} a_n z^n$ are given by

$$a_n = \frac{1}{2\pi i} \int_C \frac{f(z)\,dz}{z^{n+1}}\,.$$

   This is a theory in itself that includes other results, for example *Cauchy's theorem* $\int_C f = 0$.

7. The formula for total variation of a nice function f on a halfline $L \subset \mathbb{C}$: $V_L(f) = \int_L |f'(z)| \cdot |dz|$.

8. Fubini's theorem:

$$\int\int = \int\int\,.$$

9. Euler's formula $\zeta(2) = \sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$.

We could include here the *Laplace method* for deriving asymptotics for integrals of the type $\int f(n, x)\,dx$, $n \to \infty$. This is explained in the Wikipedia article or in an appendix of the (online available) book

- P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, Cambridge, 2009.

The asymptotics $p(n) \sim e^{\pi\sqrt{2n/3}}/4n\sqrt{3}$ was proven first by G. Hardy (1877–1947) and S. Ramanujan (1887–1920) in

- Asymptotic formulæ in combinatory analysis, *Proc. London Math. Soc*, **17** (1918), 75–115

and, independently, by Ja. V. Uspenskij (1883–1947) in

- Asimptotičeskije vyraženija čislovych funkcij, vstrečajuščichsja v zadačach o razbienii čisel na slagaemye, *Izvestija Rossijskoj Akademii Nauk*, **14** (1920), 199–218.

In the article of Hardy and Ramanujan the *circle method* was born. Uspenskij was born in the town Urga in outer Mongolia and died in San Francisco. For that matter, Hardy was born in Cranleigh, England and died in Cambridge, and Ramanujan was born in Erode, India and died in Kumbakonam, India. It is worth to look in the two articles, both are available on-line. Hardy and Ramanujan aim not only on asymptotics but for an explicit formula for $p(n)$ in terms of an infinite series (more precisely, asymptotic series). Uspenskij's goal is the asymptotics but he also derives it for other two partition functions, for the number of partitions in distinct parts, and in distinct odd parts.

The proof we presented in the previous lectures belongs to D. J. Newman (1930–2007):

- A simplified proof of the partition formula, *Michigan Math. J.*, **9** (1962), 283–287

and Chapter II in

- *Analytic Number Theory*, Springer, Berlin, 1998.

Newman is best known for his simplification of the proof of Prime Number Theorem (see his book).

P. Erdős (1913–1996) gave an elementary proof, based on a recurrence, of the incomplete asymptotics $p(n) \sim ce^{\pi\sqrt{2n/3}}/\sqrt{n}$ and Newman completed it by calculating that $c = 1/4\sqrt{3}$.

Three proofs of Stirling's asymptotics $n! \sim \sqrt{2\pi n}(n/e)^n$

The 1st proof, by sum of logarithms. We use the expression

$$\log(n!) = \int_{1/2}^{n+1/2} \log x \, dx + c_1 + O(1/n), \ n \in \mathbb{N} \, ,$$

where c_1 is a real constant. To prove it, note that for $m \in \mathbb{N}$ we have the formula

$$\int_{m-1/2}^{m+1/2} \log x \, dx = \log m + O(m^{-2}) \, .$$

Indeed,

$$\begin{aligned}
\int_{\dots}^{\dots} \dots &= [x\log x - x]_{m-1/2}^{m+1/2} \\
&= m\log\left(\frac{m+\frac{1}{2}}{m-\frac{1}{2}}\right) + \frac{\log(m^2-\frac{1}{4})}{2} - 1 \\
&= m\log\left(1+\frac{1}{m-\frac{1}{2}}\right) + \frac{1}{2}\log\left(1-\frac{1}{4m^2}\right) + \log m - 1 \\
&= \frac{m}{(m-1/2)} - \frac{m}{2(m-1/2)^2} - 1 + O(m^{-2}) + \log m \\
&= \frac{-1/2}{2(m-1/2)^2} + O(m^{-2}) + \log m = \log m + O(m^{-2}) \ ,
\end{aligned}$$

by the Taylor expansion $\log(1+x) = \sum_{n\geq 1}(-1)^{n+1}x^n/n$, $|x| < 1$. Since $\sum_{m=1}^{n} O(m^{-2}) = \sum_{m=1}^{\infty} O(m^{-2}) - \sum_{m>n}^{n} O(m^{-2}) = -c_1 + O(1/n)$,

$$\sum_{m=1}^{n} \log m = \log(n!) \ ,$$

and integral is additive in integration intervals, summation of the formula for $m = 1, 2, \dots, n$ gives the expression for $\log(n!)$.

Thus

$$\begin{aligned}
\log(n!) &= \int_{1/2}^{n+1/2} \log x \ dx + c_1 + O(1/n) \\
&= [x\log x - x]_{1/2}^{n+1/2} + c_1 + O(1/n) \\
&= (n+1/2)\log(n+1/2) - (n+1/2) + c_2 + O(1/n) \\
&= n\log n - n + (\log n)/2 + c_3 + O(1/n)
\end{aligned}$$

as $\log(n+1/2) = \log n + 1/2n + O(1/n^2)$ and

$$n! = e^{\log(n!)} = c(1+O(1/n))\sqrt{n}\left(\frac{n}{e}\right)^n$$

where $c = e^{c_3} > 0$.

It remains to show that $c = \sqrt{2\pi}$. Newman remarks at the end of Chapter II in his book that in the derivation of $p(n) \sim e^{\pi\sqrt{2n/3}}/4n\sqrt{3}$ Stirling's asymptotics is used twice so that the constant c cancels out, and hence the weaker form with undetermined c suffices. But we determine c, by means of the integral

$$I_n = \int_0^{\pi/2} (\cos x)^n \ dx, \ n \in \mathbb{N}_0 \ .$$

Clearly, $I_0 = \pi/2$ and $I_1 = 1$. Integration by parts shows that, for $n \geq 2$,

$$\begin{aligned} I_n &= \int_0^{\pi/2} (\sin x)'(\cos x)^{n-1}\, dx \\ &= [\dots]_0^{\pi/2} + (n-1)\int_0^{\pi/2} (\sin x)^2(\cos x)^{n-2}\, dx \\ &= 0 - 0 + (n-1)(I_{n-2} - I_n) \quad (\sin^2 x = 1 - \cos^2 x) \end{aligned}$$

and so, for $n \geq 2$,

$$I_n = \frac{n-1}{n} I_{n-2}\ .$$

Since $(\cos x)^n$ is positive and decreases with n on $(0, \pi/2)$, we also have

$$I_n < I_{n-1} < I_{n-2} \quad \text{and} \quad 1 < \frac{I_{n-1}}{I_n} < \frac{I_{n-2}}{I_n} = 1 + \frac{1}{n-1}\ .$$

Hence

$$\lim_{n\to\infty} \frac{I_{n-1}}{I_n} = 1\ .$$

On the other hand, solving the recurrence for I_n we get

$$I_{2n} = \frac{(2n-1)!!}{(2n)!!} \cdot \frac{\pi}{2} \quad \text{and} \quad I_{2n+1} = \frac{(2n)!!}{(2n+1)!!}$$

(the double factorial is defined as the product $x!! = x(x-2)(x-4)\dots$, truncated at the last positive term), and thus (using that $(2n)!! = 2^n n!$ and substituting the incomplete Stirling's formula)

$$\begin{aligned} \frac{I_{2n}}{I_{2n+1}} &= \frac{(2n)!^2(2n+1)}{(2^n n!)^4} \cdot \frac{\pi}{2} \\ &\sim \frac{\left(c\sqrt{2n}(2n/e)^{2n}\right)^2 2n}{\left(2^n c\sqrt{n}(n/e)^n\right)^4} \cdot \frac{\pi}{2} \\ &= \frac{2\pi}{c^2}\ . \end{aligned}$$

Hence $1 = 2\pi/c^2$ and $c = \sqrt{2\pi}$. □

The 2nd proof, by Laplace's method. Now we use the famous expression

$$n! = \int_0^{+\infty} e^{-x} x^n\, dx,\ n \in \mathbb{N}_0\ .$$

Denoting the integral by I_n we have $I_0 = 0 - (-1) = 1$ and for $n \geq 1$ by integration by parts,

$$\begin{aligned} I_n &= \int_0^{+\infty} \left(-e^{-x}\right)' x^n\, dx = [\dots]_0^{+\infty} + n\int_0^{+\infty} e^{-x} x^{n-1}\, dx \\ &= 0 - 0 + nI_{n-1}\ . \end{aligned}$$

Thus $I_n = nI_{n-1}$ and indeed $I_n = n!$. Substitution $x = n(1+y)$ gives

$$n! = I_n = e^{-n} n^{n+1} \int_{-1}^{+\infty} \left(e^{-y}(1+y)\right)^n \, dy$$

— this transformation moves the peak of the integrand to zero ($e^{-y}(1+y)$ is on $[-1,+\infty)$ nonnegative, on $[-1,0]$ increases from 0 to 1, and on $[0,+\infty)$ decreases exponentially fast from 1 to 0^+). Near zero we moreover have

$$\begin{aligned} e^{-y}(1+y) &= e^{\log(1+y)-y} = e^{-y^2/2+y^3/3-y^4/4+\dots} = e^{-y^2/2} e^{y^3/3-y^4/4+\dots} \\ &= e^{-y^2/2}(1+O(y^3)),\ |y| < 1/2 \end{aligned}$$

— the point is that the linear part in the exponent cancelled out.

We take a $\delta = \delta(n) > 0$ that goes sufficiently fast to 0 as $n \to \infty$, namely such that $n\delta(n)^3 \to 0$ (later we will need to restrict $\delta(n)$ further so that it does not go to 0 too fast). Then

$$\int_{-1}^{+\infty} \left(e^{-y}(1+y)\right)^n \, dy = \int_{-1}^{-\delta} \cdots + \int_{-\delta}^{\delta} \cdots + \int_{\delta}^{+\infty} \cdots =: J_1 + J + J_2 \, .$$

We evaluate or estimate these integrals. Since, for $|y| \le \delta$,

$$\cdots = \left(e^{-y}(1+y)\right)^n = e^{-ny^2/2}(1+O(y^3))^n = e^{-ny^2/2}(1+O(ny^3))$$

— the last transformation is justified by $n\delta^3 \to 0$ (we use that $(1+\Delta)^n = e^{n\log(1+\Delta)} = e^{n(\Delta-\Delta^2/2+\dots)} = e^{O(n\Delta)} = 1+O(n\Delta)$ if $|n\Delta| < c < 1$) — we may write

$$\begin{aligned} J &= \int_{-\delta}^{\delta} \cdots = (1+O(n\delta^3)) \int_{-\delta}^{\delta} e^{-ny^2/2} \, dy \\ &= (1+O(n\delta^3)) \left(\int_{-\infty}^{+\infty} e^{-ny^2/2} \, dy - 2\int_{\delta}^{+\infty} e^{-ny^2/2} \, dy \right) \\ &=: (1+O(n\delta^3))\,(J_3 - 2J_4) \end{aligned}$$

(the integrand is an even function).

Lecture 13, May 23, 2017

J_3 is up to a simple substitution the Gaussian integral, evaluated in Lemma 42 below:

$$J_3 = \sqrt{\frac{2}{n}} \int_{-\infty}^{+\infty} e^{-t^2} \, dt = \sqrt{\frac{2\pi}{n}} \, .$$

Note that $J_1, J_2, J_4 \ge 0$. Since $\left(e^{-y}(1+y)\right)^n$ has for $y \in [-1,-\delta]$ maximum at $y = -\delta$,

$$J_1 \le |(1+O(n\delta^3))| \cdot (1-\delta) \cdot e^{-n\delta^2/2} \ll e^{-n\delta^2/2} \, .$$

Similarly, $(e^{-y}(1+y))^n$ has for $y \in [\delta, +\infty)$ maximum at $y = \delta$. For $y \to +\infty$ this function goes exponentially fast to 0 and therefore we again have

$$J_2 \ll \int_\delta^1 \left(e^{-y}(1+y)\right)^n \le |(1+O(n\delta^3))| \cdot (1-\delta) \cdot e^{-n\delta^2/2} \ll e^{-n\delta^2/2}$$

(as $\int_\delta^{+\infty} \cdots = \int_\delta^1 \cdots + \int_1^2 \cdots + \int_2^3 \cdots + \cdots \ll \int_\delta^1 \dots$). This applies to J_4 too and

$$J_4 \ll e^{-n\delta^2/2} .$$

For these bounds to go to 0 with $n \to \infty$, we need $n\delta(n)^2 \to +\infty$. We set $\delta = \delta(n) = n^{\varepsilon/3-1/2}$, for small $\varepsilon \in (0, 1/2)$. Then both requirements on δ are met and

$$\begin{aligned} \int_{-1}^{+\infty} \left(e^{-y}(1+y)\right)^n \, dy &= (1+O(n\delta^3))\left(\sqrt{\frac{2\pi}{n}} + O(e^{-n\delta^2/2})\right) + O(e^{-n\delta^2/2}) \\ &= \sqrt{\frac{2\pi}{n}} + O(n^{-1+\varepsilon}) \end{aligned}$$

because $O(n\delta^3)\sqrt{2\pi/n} = O(n^{-1+\varepsilon})$ and other error terms have much smaller order $O(e^{-n^{2\varepsilon/3}})$. Thus, finally,

$$n! = \frac{n^{n+1}}{e^n}(\sqrt{2\pi/n} + O(n^{-1+\varepsilon})) = \sqrt{2\pi n}(n/e)^n(1 + O(n^{\varepsilon-1/2})) .$$

This error term is worse than the $O(n^{-1})$ term in the first proof □

We evaluate the Gaussian integral, which was used several times.

Lemma 42 (Gaussian integral).

$$\int_{-\infty}^{+\infty} e^{-t^2} \, dt = \sqrt{\pi} .$$

Proof. It suffices to show that $(\int_0^{+\infty} e^{-t^2} \, dt)^2 = \pi/4$ because the integrand is

an even function. Indeed,

$$\begin{aligned}
\left(\int_0^{+\infty} e^{-t^2}\,dt\right)^2 &= \int_0^{+\infty} e^{-t^2}\,dt \int_0^{+\infty} e^{-u^2}\,du \\
&= \int_0^{+\infty}\left(\int_0^{+\infty} e^{-t^2-u^2}\,du\right)dt \\
&= \int_0^{+\infty}\left(\int_0^{+\infty} te^{-t^2(1+v^2)}\,dv\right)dt \\
&= \int_0^{+\infty}\left(\int_0^{+\infty} te^{-t^2(1+v^2)}\,dt\right)dv \\
&= \int_0^{+\infty}\left[\frac{-e^{-t^2(1+v^2)}}{2(1+v^2)}\right]_{t=0}^{+\infty} dv \\
&= \int_0^{+\infty}\frac{dv}{2(1+v^2)} = \frac{[\arctan v]_0^{+\infty}}{2} \\
&= \frac{\pi/2-0}{2} = \frac{\pi}{4}\,.
\end{aligned}$$

On the third line we used the substitution $u = tv$, and on the fourth line Fubini's theorem. □

The 3rd proof, by circle method. Another integral representation for factorial is

$$\frac{1}{n!} = \frac{1}{2\pi i}\int_C \frac{e^z\,dz}{z^{n+1}},\ n \in \mathbb{N}_0\,,$$

for any counter-clockwise oriented circle $C \subset \mathbb{C}$, centered at the origin. This follows from the expansion $e^z = \sum_{n\geq 0} z^n/n!$ and Cauchy's formula (which is an application of the residue theorem). If C has radius $r > 0$ then for $z \in C$ we have

$$z = re^{i\theta},\ \theta \in [-\pi, \pi)\,.$$

So

$$\frac{1}{n!} = \frac{1}{2\pi i}\int_{-\pi}^{\pi} \frac{e^{re^{i\theta}}}{(re^{i\theta})^{n+1}}\cdot\frac{d}{d\theta}re^{i\theta} = \frac{1}{2\pi}\frac{e^r}{r^n}\int_{-\pi}^{\pi} e^{r(e^{i\theta}-1)-ni\theta}\,d\theta\,.$$

Denoting the exponent $f(r,\theta)$, for θ near 0 we have $f(r,\theta) = r(i\theta - \theta^2/2 + O(\theta^3)) - ni\theta$ and see that the linear part in θ vanishes if $r = n$. Thus we set the radius of C to be n and get $f(n,\theta) = -n\theta^2/2 + O(n\theta^3)$.

To obtain asymptotics for the integral, we proceed as in the second proof and split the integral in two at some $\varphi = \varphi(n) \in (0,\pi)$,

$$\int_{-\pi}^{\pi} e^{f(n,\theta)}\,d\theta = \int_{-\varphi}^{\varphi} e^{f(n,\theta)}\,d\theta + \int_{\varphi}^{\pi}\left(e^{f(n,\theta)} + e^{f(n,-\theta)}\right)\,d\theta\,.$$

If $n\varphi(n)^3 \to 0$, the same computation as in the 2nd proof gives

$$\int_{-\varphi}^{\varphi} e^{f(n,\theta)}\,d\theta = (1+O(n\varphi^3))\left(\sqrt{2\pi/n} + O(e^{-n\varphi^2/2})\right)\,.$$

Since for $\theta \in [\varphi, \pi]$,

$$\left|e^{f(n,\theta)}\right| = \left|e^{f(n,-\theta)}\right| = e^{n(\cos\theta - 1)} \le e^{n(\cos\varphi - 1)} \ll e^{-n\varphi^2/2}$$

(as $\cos\varphi = 1 - \varphi^2/2 + O(\varphi^3)$ for $|\varphi| < 1/2$), the second integral is $O(e^{-n\varphi^2/2})$. We set again $\varphi = n^{-1/2+\varepsilon/3}$, $\varepsilon \in (0, 1/2)$, and have like before

$$\frac{1}{n!} = \frac{1}{2\pi}\frac{e^n}{n^n}\left(\sqrt{\frac{2\pi}{n}} + O(n^{-1+\varepsilon})\right) = \left(1 + O(n^{-1/2+\varepsilon})\right)\frac{1}{\sqrt{2\pi n}}\left(\frac{e}{n}\right)^n .$$

Taking the reciprocal value, we have Stirling's formula for $n!$. □

The three proofs of $n! \sim \sqrt{2\pi n}(n/e)^n$ are taken from the book of Flajolet and Sedgewick, mentioned in the previous lecture.

The 4th proof, by multidimensional circle method? This is just an idea, but I have not seen it anywhere in the literature. Yet another integral representation of factorial expresses it as

$$n! = \frac{1}{(2\pi i)^n}\int_{C_1}\dots\int_{C_n}\frac{(x_1 + x_2 + \dots + x_n)^n}{(x_1 x_2 \dots x_n)^2}\, dx_1\, dx_2 \dots dx_n,\ n \in \mathbb{N}\,,$$

for some n counter-clockwise oriented circles $C_j \subset \mathbb{C}$, given by $|x_j| = r_j > 0$. The equality follows by expanding the power in the numerator and noting that for $j_1, \dots, j_n \in \mathbb{Z}$,

$$\begin{aligned}&\int_{C_1}\dots\int_{C_n} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}\, dx_1\, dx_2 \dots dx_n \\ &= \begin{cases} (2\pi i)^n & \dots \quad j_1 = j_2 = \dots = j_n = -1 \\ 0 & \dots \quad \text{else}\,. \end{cases}\end{aligned}$$

This representation differs from the three previous ones, in three respects. The integrand is not a transcendental function (log or exp) but is rational. The equality follows not from the arithmetic definition of factorial ($n! = n \cdot (n-1)!$) but from the combinatorial one ($n!$ is the number of permutations of an n-element set). Finally, n variables are involved and not just one.

Multidimensional circle method is used with success in enumerative combinatorics. For example, the number $\mathrm{RT}(n)$ of *(labelled) regular tournaments* with n vertices, which is the number of those orientations of the $\binom{n}{2}$ edges of the complete graph K_n (out of all $2^{n(n-1)/2}$ orientations) for which exactly $\frac{n-1}{2}$ edges enter every vertex (and hence also exactly $\frac{n-1}{2}$ edges leave it), is expressed by the multidimensional Cauchy integral ($n \in \mathbb{N}$)

$$\mathrm{RT}(n) = \frac{1}{(2\pi i)^n}\int_{C_1}\dots\int_{C_n}\frac{\prod_{1\le j<k\le n}(x_j^{-1}x_k + x_j x_k^{-1})}{x_1 x_2 \dots x_n}\, dx_1\, dx_2 \dots dx_n\,.$$

After the above discussion for $n!$, this equality should be clear. B. D. McKay could prove in

- The asymptotic numbers of regular tournaments, Eulerian digraphs and Eulerian oriented graphs, *Combinatorica*, **10** (1990), 367–377

by means of this integral formula that for any $\varepsilon > 0$, as $n \to \infty$ through odd values,

$$\mathrm{RT}(n) = (1 + O(n^{-1/2+\varepsilon}))\left(\frac{2^{n+1}}{\pi n}\right)^{(n-1)/2} (n/e)^{1/2} .$$

Of course, $\mathrm{RT}(n) = 0$ for even n. For example, $\mathrm{RT}(3) = 2$. The other two asymptotics proven in this article concern numbers of Eulerian digraphs with n vertices:

$$\begin{aligned} \mathrm{ED}(n) &= (1 + O(n^{-1/2+\varepsilon}))\left(\frac{4^n}{\pi n}\right)^{(n-1)/2} n^{1/2} e^{-1/4} \\ \mathrm{EOG}(n) &= (1 + O(n^{-1/2+\varepsilon}))\left(\frac{3^{n+1}}{4\pi n}\right)^{(n-1)/2} n^{1/2} e^{-3/8} . \end{aligned}$$

Precise definitions of graphs counted follow from integral formulas, in which the above $x_j^{-1}x_k + x_j x_k^{-1}$ is replaced with, respectively, $(1+x_j^{-1}x_k)(1+x_j x_k^{-1})$ and $1 + x_j^{-1}x_k + x_j x_k^{-1}$.

And that's all, thank you for your attention.

Acknowledgment. I want to thank Kr. Zemková for pointing out to me confusing references between Propositions in the proof of Dirichlet's theorem. In the present version this problem is fixed by insertion of Proposition 17.