PMATH 740 Lecture 1: May 2, 2012

Analytic Number Theory
home page at `www.math.uwaterloo.ca/~snew`
outline, assignments, solutions

(Introduction to)
Analytic Number Theory by Apostol
Chapter 1, Chapter 5.

Chapter 1: Fundamental Theorem of Arithmetic
Theorem: (Division Algorithm)
Given a, $b \in \mathbb{Z}$ with $a \neq 0$ there exist unique q, $r \in \mathbb{Z}$ with $b = qa + r$, $0 \leq r < |a|$.

Definition: For a, $b \in \mathbb{Z}$ we say a *divides* b (or a is a *factor of* b or b is a multiple of a) when $b = qa$ for some $q \in \mathbb{Z}$.

basic facts

$0 \mid a \iff a = 0$ $\qquad$ $a \mid 0$ for all $a \in \mathbb{Z}$

$1 \mid a$ for all $a \in \mathbb{Z}$ $\qquad$ $a \mid 1$ for $a = \pm 1$

Definition: For a, $b \in \mathbb{Z}$ we say that d is the *greatest common divisor* of a and b when

$d \geq 0$

$d \mid a$ and $a \mid b$, and

if $c \mid a$ and $c \mid b$ then $c \mid d$

basic facts

$\gcd(0, 0) = 0$

$\gcd(0, a) = |a|$

if $a \mid b$ then $\gcd(a, b) = |a|$

$\gcd(a, b) = \gcd(b, a)$

$\gcd(a, b) = \gcd(|a|, |b|)$

$\gcd(ac, bc) = |c| \gcd(a, b)$

If $b = qa + r$ then $\gcd(a, b) = \gcd(b, r)$

Theorem: (Euclidean Algorithm with Back-Substitution)
Given a, $b \in \mathbb{Z}$

$$d = \gcd(a, b) \text{ exists}$$

and there exist x, $y \in \mathbb{Z}$ such that $ax + by = d$
Proof: If $b \mid a$ then

$$d = \gcd(a, b) = |b|$$

and we can easily find x, y.
Suppose $0 < b < a$ and $b \nmid a$.

We apply the division algorithm repeatedly to get

$$\begin{aligned} a &= bq_1 + r_1 && 0 < r_1 < b \\ b &= r_1q_2 + r_2 && 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3 && 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} + r_{n+1} && r_{n+1} = 0 \end{aligned}$$

Then $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n$

This method of finding $\gcd(a,b)$ is called the Euclidean Algorithm

$$\begin{aligned} \text{We have } \gcd(a,b) &= r_n = r_{n-2} - r_{n-1}q_n \\ &= r_{n-2}u_1 + r_{n-1}u_2 \qquad \text{where } u_1 = 1,\ u_2 = -q_n \\ &= r_{n-2}u_1 + (r_{n-3} - r_{n-2}q_{n-1})u_2 \\ &= r_{n-3}u_2 + r_{n-2}u_3, \qquad u_3 = u_1 - q_{n-1}u_2 \\ &= r_1u_{n-2} + r_2u_{n-1} \\ &= r_1u_{n-2} + (b - r_1q_2)u_{n-1} \\ &= bu_{n-1} + r_1u_n, \qquad u_n = u_{n-2} - q_2u_{n-1} \\ &= bu_{n-1} + (a - bq_1)u_n \\ &= au_n + bu_{n+1}, \qquad u_{n+1} = u_{n-1} - q_1u_n \end{aligned}$$

Thus we can define $u_1 = 1$, $u_2 = -q_n$, $u_n = u_{k-2} - q_{n-k+2}u_{k-1}$ and then we can take $x = u_n$, $y = u_{n+1}$ to get $ax + by = d$.

$$\begin{array}{rrrrrr} 2 & 1 & 3 & 1 & 2 & 2 \\ 429\overline{)1196} & 338\overline{)429} & 91\overline{)338} & 65\overline{)91} & 26\overline{)65} & 13\overline{)26} \\ \underline{858} & \underline{338} & \underline{273} & \underline{65} & \underline{52} & \underline{26} \\ 338 & 91 & 65 & 26 & 13 & 0 \end{array}$$

$\therefore d = \gcd(a,b) = 13$
We have

k	1	2	3	4	5	6
u_k	1	-2	3	-11	14	-39

$\therefore (1196)(14) + (429)(-39) = 13$

Definition: For $a,\ b \in \mathbb{Z}$ we say that a and b are *coprime* when $\gcd(a,b) = 1$.

basic facts

$\gcd(a,b) = 1 \iff \exists x, y \in \mathbb{Z} \quad ax + by = 1$

If $d = \gcd(a,b)$ then $\gcd(a/d, b/d) = 1$.

If $a \mid c$ and $b \mid c$ and $\gcd(a,b) = 1$ then $ab \mid c$.

If $a \mid bc$ and $\gcd(a,b) = 1$ then $a \mid c$.

Theorem: (The linear diophantine equation theorem)
Let $a,\ b,\ c \in \mathbb{Z}$ with $a,\ b$ not both zero. Consider the equation $ax + by = c$. This equation has an integer solution $(x,y) \iff \gcd(a,b) \mid c$ and in this case if (x_0,y_0) is one solution then the general solution is $(x,y) = (x_0,y_0) + t(-b/d, a/d)$ for $t \in \mathbb{Z}$ where $d = \gcd(a,b)$.

Definition: Let $n \in \mathbb{Z}$. n is called *prime* when $n > 1$ and n has exactly 2 positive divisors, namely 1 and n. n is called *composite* when $n > 1$ and $\exists k, l$ with $1 < k, l < n$, $n = kl$.

basic facts

for $a \in \mathbb{Z}$ either $p \mid a$ or $\gcd(p, a) = 1$

for a, $b \in \mathbb{Z}$ if $p \mid ab$ then either $p \mid a$ or $p \mid b$

for $a_i \in \mathbb{Z}$ if $p \mid a_1 a_2 \cdots a_l$ then $p \mid a_i$ for some i

for $a \in \mathbb{Z}$ if $p \mid a^n$ then $p \mid a$ where $n \in \mathbb{Z}^+$

If n is composite then n has a prime factor p with $p \leq \sqrt{n}$.

PMATH 740 Lecture 2: May 4, 2012

Ch. 1 F.T.A.
basic facts

for p prime, $a \in \mathbb{Z}$, $\gcd(p, a) = \begin{cases} p & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \end{cases}$

for $1 < n \in \mathbb{Z}$, if n is composite then n has a prime factor p with $p \leq \sqrt{n}$
for p prime, $ab \in \mathbb{Z}$ if $p \mid ab$ then $p \mid a$ or $p \mid b$

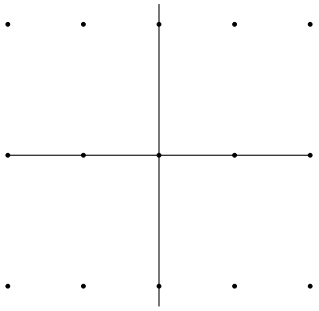
Theorem: (Euclid's)
There are infinitely many primes
Proof: Suppose that p_1, p_2, ..., p_l are *all* the primes. Let $n = p_1 p_2 \cdots p_l + 1$. Then n has a prime factor p. But $p \neq p_i$ for any i since $p_i \nmid n$ (since n is divided by p_i is 1)

Theorem: (The Sieve of Eratosthenes)
We can list all primes $p \leq n$ for a given integer n as follows:
list all integers from 1 to n
cross off 1 since it is not prime
circle the smallest remaining number, namely 2; it is prime
cross off all other multiples of 2 since they are composite
circle the smallest remaining number, namely 3; it is prime
continue until we circle a prime $p \geq \sqrt{n}$ and then all remaining numbers are prime

Theorem: (The Fundamental Theorem of Arithmetic)
Every integer $n > 1$ can be written uniquely as

$$n = p_1^{e_1} \cdots p_m^{k_m}$$

with m, p_i, $k_i \in \mathbb{Z}$
$m \geq 1$, each p_i is prime, $p_1 < p_2 < \cdots < p_m$, each $k_i \geq 1$.
In $\mathbb{Z}_{12}$, $3 = 3 \cdot 3 \cdot 3 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = \cdots$
In $\mathbb{Z}[\sqrt{3}i] = \{ a + b\sqrt{3}i : a, b \in \mathbb{Z} \}$



$(1+\sqrt{3}i)(1-\sqrt{3}i) = 4 = 2 \cdot 2$

basic facts
for $n = p_1^{k_1} \cdots p_m^{k_m}$ where the p_i are distinct primes and $k_i \geq 0$
then the positive divisors d of n are the numbers of the form $d = p_1^{j_1} \cdots p_m^{j_m}$ with $0 \leq j_i \leq k_i$ for all i

for $a = p_1^{k_1} \cdots p_m^{k_m}$, $b = p_1^{l_1} \cdots p_m^{l_m}$ we have

$$\begin{aligned} \gcd(a,b) &= p_1^{\min(k_1,l_1)} p_2^{\min(k_2,l_2)} \cdots \\ \operatorname{lcm}(a,b) &= p_1^{\max(k_1,l_1)} \cdots \\ \gcd(a,b)\operatorname{lcm}(a,b) &= ab \end{aligned}$$

(where $\operatorname{lcm}(a,b)$ needs to be defined)

we can also define $\gcd(a_1, \ldots, a_l)$ and $\operatorname{lcm}(a_1, \ldots, a_l)$ for $a_1, \ldots, a_l \in \mathbb{Z}$
Similar formulas hold for their prime factorizations.

Unsolved Problems
Goldbach's Conjecture: every even $n > 4$ is a sum of 2 primes
$n^2 + 1$ Conjecture: $\exists \infty$ many primes of the form $n^2 + 1$
Do there exist infinitely many primes of any of the forms

$$2^n \pm 1,\ n^n \pm 1,\ n! \pm 1$$

Twin Primes Conjecture: there exist infinitely many pairs of primes p, q with $|p - q| = 2$.
$\forall n \in \mathbb{Z}^+ \ \exists$ prime p with $n^2 < p < (n+1)^2$

Definition: For a prime p and $n \in \mathbb{Z}^+$ the *exponent of* p in n, written $e_p(n)$, is the largest $k \geq 0$ such that $p^k \mid n$
Example: Find a formula for $e_p(n!)$
Solution: In the list 1, 2, ..., n the multiples of p are

$$p, 2p, \ldots$$

and the number of these is

$$\left\lfloor \frac{n}{p} \right\rfloor$$

the # of multiples of p^2 is

$$\left\lfloor \frac{n}{p^2} \right\rfloor$$

and so on:

$$\therefore e_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Example: The # of zeros at the end of 100! is

$$e_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor + \left\lfloor \frac{100}{125} \right\rfloor = 20 + 4 = 24$$

Definition: For $n \in \mathbb{Z}^+$

$$\begin{aligned} d(n) = \tau(n) &= \text{the \# of positive divisors of } n, \\ &= \sum_{d \mid n} 1 \\ \sigma(n) &= \text{the sum of the positive divisors of } n \\ &= \sum_{d \mid n} d \end{aligned}$$

Example: Find a formula for $\tau(n)$ and $\sigma(n)$ when $n = p_1^{k_1} \cdots p_m^{k_m}$.
Solution: $d \mid n \iff d = p_1^{j_1} \cdots p_m^{j_m}$ for some $0 \le j \le k_i$
There are $k_i + 1$ choices for j_i
$\therefore \tau(n) = \prod_{i=1}^{m}(k_i + 1)$

$$\begin{aligned}
\text{Also } \sigma(n) &= \sum_{d|n} d \\
&= \sum_{0\le j_1\le k_1} \sum_{0\le j_2\le k_2} \cdots \sum_{0\le j_m\le k_m} p_1^{j_1} p_2^{j_2} \cdots p_m^{j_m} \\
&= \prod_i \Big(\sum_{0\le j_i\le k_i} p_i^{d_i} \Big) \\
&= \prod_{i=1}^{m} (1 + p_i + p_i^2 + \cdots + p_i^{k_i}) \\
&= \prod_{i=1}^{m} \frac{p_i^{k_i+1} - 1}{p_i - 1}
\end{aligned}$$

Example: For which $n \in \mathbb{Z}^+$ is $\tau(n)$ odd?
Answer: n is a square
Example: Show that $\sum_{p \text{ primes}} \frac{1}{p} = \infty$.

PMATH 740 Lecture 3: May 7, 2012

$$\begin{aligned}
\tau(n) &= \#\text{ of divisors of } n = \prod p_i^{k_i} \\
&= \prod_i (k_i + 1) \\
\sigma(n) &= \sum_{d|n} d
\end{aligned}$$

Example: Show

$$\sum_{p \text{ prime}} \frac{1}{p} = \sum_{i=1}^{\infty} \frac{1}{p_i} = \infty$$

where p_i is the ith prime.
Solution: Suppose, for a contradiction that $\sum_{i=1}^{\infty} \frac{1}{p_i}$ converges.
Choose $n \in \mathbb{Z}^+$ so that

$$\sum_{i>n} \frac{1}{p_i} < \frac{1}{2}$$

Let $a = p_1 p_2 \cdots p_n$.
Consider the arithmetic progression

$$1 + a, 1 + 2a, 1 + 3a, \ldots .$$

Note that none of the primes p_1, p_2, …, p_n are factors of any of these numbers $1 + ka$, $k \in \mathbb{Z}^+$.
Notice that the sum

$$\Big(\sum_{i>n} \frac{1}{p_i} \Big)^m$$

is a sum of terms of the form

$$\frac{1}{p_{i_1} p_{i_2} \cdots p_{i_m}} \text{ with each } i_j > n.$$

Each of the numbers $1 + ka$, $k \in \mathbb{Z}^+$ is one of the terms in $(\sum_{i>n} \frac{1}{p_i})^m$ for some m.

$$\therefore \sum_{i=1}^{\infty} \frac{1}{1+ka} \leq \sum_{m=1}^{\infty} \Big(\sum_{i>n} \frac{1}{p_i} \Big)^m$$
$$\leq \sum_{m=1}^{\infty} \Big(\frac{1}{2} \Big)^m = 1$$

But this is not possible since $\sum_{k=1}^{\infty} \frac{1}{1+ka}$ diverges by the integral test since

$$\int_2^{\infty} \frac{1}{1+xa} \, \mathrm{d}x = \frac{1}{a} \ln(1+xa) \Big|_2^{\infty} = \infty.$$

Ch. 5 Congruences
Definition: $a = b \bmod n$ when $a = b + kn$ for some $k \in \mathbb{Z}$

basic facts:

$$a = b \bmod n$$
$$\iff a - b = 0 \bmod n$$
$$\iff n \mid (a - b)$$

equivalence mod n is an equivalence relation $a = a \bmod n$
$a = b \bmod n \implies b = a \bmod n$
$(a = b \bmod n$ and $b = c \bmod n \implies a = c \bmod n)$
addition and multiplication mod n are well-defined.
If $a_1 = a_2 \bmod n$ and $b_1 = b_2 \bmod n$ then $a_1 + b_1 = a_2 + b_2 \bmod n$ and $a_1 b_1 = a_2 b_2 \bmod n$.

Care is needed for division

$$ab = ac \bmod n \implies b = c \bmod n$$
$$ab = ac \bmod an \iff b = c \bmod n$$

Definition: $\mathbb{Z}_n$ is the ring of integers modulo n:
for $a \in \mathbb{Z}$ write $[a] = \{ x \in \mathbb{Z} : x = a \bmod n \}$
Then $\mathbb{Z}_n = \{ [a] : a \in \mathbb{Z} \} = \{[0], [1], \ldots, [n-1]\}$
We shall write $[a]$ as a.

Theorem: (Linear Congruence Theorem)
For $n \in \mathbb{Z}^+$, a, $b \in \mathbb{Z}$ consider the congruence

$$ax = b \bmod n.$$

It has a solution $x \iff d \mid b$ where $d = \gcd(a, n)$ and if $x = x_0$ is one solution the general solution is

$$x = x_0 \bmod \frac{n}{d}.$$

Equivalently, $ax = b$ has a solution $x \in \mathbb{Z}_n \iff d \mid b$ and if $x = x_0$ is one solution in $\mathbb{Z}_n$ then there are exactly d solutions

$$x = x_0 + t\frac{n}{d} \text{ with } t = 0, 1, \ldots, d-1.$$

Proof: This is a rewording of the Linear Diophantine Equation Theorem.

Corollary: For $a \in \mathbb{Z}_n$, a has a multiplicative inverse a^{-1}
$\iff$ we can solve $ax = 1 \bmod n$

$\iff \gcd(a, n) = 1$
When $\gcd(a, n) = 1$ we have $ab = ac \bmod n$
$\iff b = c \bmod n$

Definition: U_n is the *group* of units modulo n

$$U_n = \{\, a \in \mathbb{Z}_n : \gcd(a, n) = 1 \,\}.$$

note that for a, $b \in \mathbb{Z}$ (or a, $b \in \mathbb{Z}_n$) if a, $b \in U_n$ then $ab \in U_n$

Theorem: (The Chinese Remainder Theorem)
Let $n_1, \ldots, n_m \in \mathbb{Z}^+$, $a_1, \ldots, a_m \in \mathbb{Z}$.
Consider $x = a_i \bmod n_i$ for $1 \le i \le m$.
This system of congruences has a solution $\iff$ $\gcd(n_i, n_j) \mid (a_i - a_j)$ for all $i \neq j$ and if $x = x_0$ is one solution then the general solution is

$$x = x_0 \bmod \operatorname{lcm}(n_1, \ldots, n_m)$$

Proof: Consider the case $n = 2$

$$\begin{aligned} x &= a_1 \bmod n_1 \\ x &= a_2 \bmod n_2 \end{aligned} \tag{1}$$

We have a solution when

$$x = a_1 + kn_1 = a_2 + ln_2 \tag{2}$$

has a solution (k, l)
equivalently, when

$$\gcd(n_1, n_2) \mid (a_1 - a_2)$$

(from the LDET). In this case, if (k_0, l_0) is a solution to (2)

$$(\text{so } x_0 = a_1 + k_0 n_1 = a_2 + l_0 n_2 \text{ is a solution to (1)})$$

then the general solution to (2) is

$$(k, l) = (k_0, l_0) + t\Big(\frac{n_2}{d}, \frac{n_1}{d}\Big)$$

and then

$$\begin{aligned} x = a_1 + kn_1 &= a_1 + \Big(k_0 + \frac{tn_2}{d}\Big)n_1 \\ &= (a_1 + k_0 n_1) + \frac{tn_1 n_2}{d} \\ &= x_0 \bmod \operatorname{lcm}(n_1, n_2) \end{aligned}$$

Suppose, inductively, that our theorem holds for any system of $m - 1$ congruences.

Consider m congruences

$$x = a_i \bmod n_i \qquad 1 \le i \le m$$

If $x = x_0$ is a solution to all m congruences, then it is also a solution to each pair

$$\begin{aligned} x &= a_i \bmod n_i \\ x &= a_j \bmod n_j \end{aligned}$$

So (as above) $\gcd(n_i, n_j) \mid (a_i - a_j)$ for all $i \neq j$.
Also, x_0 is a solution to the first $m - 1$ congruences so by the Inductive Hypothesis the general solution to the first $n - 1$ congruences is

$$x = x_0 \bmod \operatorname{lcm}(n_1, \ldots, n_{l-1}).$$

So the system of m congruences is equivalent to the pair

$$x = x_0 \bmod \operatorname{lcm}(n_1, \ldots, n_{m-1})$$
$$x = a_m \bmod n_m$$

The general solution is

$$x = x_0 \bmod \operatorname{lcm}(\operatorname{lcm}(n_1, \ldots, n_{m-1}), n_m)$$

Exercise: show that

$$\operatorname{lcm}(\operatorname{lcm}(n_1, \ldots, n_{m-1}), n_m) = \operatorname{lcm}(n_1, \ldots, n_m).$$

It remains to show that if $\gcd(n_i, n_j) \mid (a_i - a_j)$ for all $i \neq j$ then a solution $x = x_0$ exists.

Suppose $\gcd(n_i, n_j) \mid (a_i - a_j)$ for all $i \neq j$.
By the induction hypothesis there is a solution $x = a$ to the first $m - 1$ congruences and the system of all m congruences is equivalent to

$$x = a \operatorname{lcm}(n_1, \ldots, n_{m-1})$$
$$x = a_m \bmod n_m$$

We need to show that a solution to this pair of congruences exists, that is we must show

$$\gcd(\operatorname{lcm}(n_1, \ldots, n_{m-1}), n_m) \mid (a - a_m)$$

PMATH 740 Lecture 4: May 9, 2012

CRT $\exists$ solution to

$$x = a_i \bmod n_i \qquad 1 \leq i \leq m$$
$$\iff \gcd(n_i, n_j) \mid (a_i - a_j) \text{ for all } i \neq j$$

and then if $x = x_0$ is one solution, the general solution is

$$x = x_0 \bmod \operatorname{lcm}(n_1, \ldots, n_m).$$

We need to show that if the condition is satisfied then a solution exists.
We suppose

$$\gcd(n_i, n_j) \mid a_i - a_j \text{ for all } i \neq j.$$

By the Inductive Hypothesis we can find a solution $x = a$ to the first $m - 1$ congruences and then the full system is equivalent

$$x = a \bmod \operatorname{lcm}(n_1, \ldots, n_{m-1})$$
$$x = a_m \bmod n_m$$

We need to show that

$$\gcd(\operatorname{lcm}(n_1, \ldots, n_{m-1}), n_m) \mid (a - a_m).$$

exercise: show that

$$\gcd(\operatorname{lcm}(n_1, \ldots, n_{m-1}), n_m) = \operatorname{lcm}(\gcd(n_1, n_m), \ldots, \gcd(n_{m-1}, n_m))$$

For $1 \leq i \leq m - 1$ we have

$$a = a_i \bmod n_i$$
$$a - a_m = a_i - a_m \bmod n_i$$
$$a - a_m = a_i - a_m \bmod d \text{ for any divisor } d \mid n_i$$
$$a - a_m = a_i - a_m \bmod \gcd(n_i, n_m)$$
$$a - a_m = 0 \bmod \gcd(n_i, n_m)$$

$\therefore$ $x = a - a_m$ is a solution to the system $x = 0 \bmod \gcd(n_i, n_m)$ for $1 \leq i \leq m-1$. By the Induction Hypothesis

$$a - a_m = 0 \bmod \operatorname{lcm}(\gcd(n_1, n_m), \ldots, \gcd(n_{m-1}, n_m)).$$

Example: Solve

$$\begin{aligned} x &= 5 \bmod 12 \\ x &= 8 \bmod 9 \\ x &= 11 \bmod 30 \end{aligned}$$

Solution: First we solve the first 2 congruences.

$$\begin{aligned} x = 5 \bmod 12 &\iff x = \ldots, -7, 5, 17, 29, \ldots \\ x = 8 \bmod 9 &\iff x = \ldots, -1, 8, 17, \ldots \end{aligned}$$

$\therefore$ $x = 17$ is one solution
$\therefore$ the general solution (to the first 2) is

$$\begin{aligned} x &= 17 \bmod \operatorname{lcm}(12, 9) \\ &= 17 \bmod 36 \end{aligned}$$

The system of 3 congruences is equivalent to

$$\begin{aligned} x &= 17 \bmod 36 \\ x &= 11 \bmod 30 \end{aligned}$$

x is a solution when

$$x = 17 + 36k = 11 + 30l \text{ for some } k,\ l \in \mathbb{Z}$$

$$\begin{aligned} 36k - 30l &= -6 \\ 6k - 5l &= -1 \end{aligned}$$

A solution is given by

$$\begin{aligned} (k_0, l_0) &= (-1, -1) \\ x_0 &= 17 + 36k_0 \quad (= 11 + 30l_0) \\ &= 17 - 36 \\ &= -19 \end{aligned}$$

By the CRT, the general solution is

$$\begin{aligned} x &= -19 \bmod \operatorname{lcm}(36, 30) \\ &= -19 \bmod \frac{36 \cdot 30}{6} \\ &= -19 \bmod 180 \\ &= 161 \bmod 180 \end{aligned}$$

Euler ϕ Function (or Euler's totient function)
For $n \in \mathbb{Z}^+$ we define

$$\phi(n) = |U_n| = |\{\, a \in \mathbb{Z}_n : \gcd(a, n) = 1 \,\}|$$

Example: Find a formula for $\phi(n)$ where $n = p_1^{k_1} \cdots p_l^{k_l}$ where the p_i are distinct primes and each $k_i \geq 1$.
Solution: Note that for a, $b \in \mathbb{Z}^+$ with $\gcd(a,b) = 1$ then the maps

$$f\colon \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b \text{ and}$$
$$g\colon \mathbb{Z}_a \times \mathbb{Z}_b \to \mathbb{Z}_{ab}$$

given by $f(x) = (x, x)$
$g(k,l) =$ the unique solution x modulo ab to

$$x = k \bmod a$$
$$x = l \bmod b$$

are inverses of each other and $f\colon U_{ab} \to U_a \times U_b$ (since if $\gcd(x, ab) = 1$ then $\gcd(x,a) = 1 = \gcd(x,b)$) and $g\colon U_a \times U_b \to U_{ab}$ (exercise).
Thus

$$|U_{ab}| = |U_a \times U_b| = |U_a||U_b|$$
$$\phi(ab) = \phi(a)\phi(b)$$
$$\therefore \phi(p_1^{k_1} \cdots p_l^{k_l}) = \phi(p_1^{k_1}) \cdots \phi(p_l^{k_l})$$

Also for p prime we have

$$\phi(p) = |U_p| = \{1, 2, \ldots, p-1\} = p - 1$$

and more generally for $k \geq 1$

$$\begin{aligned}
\phi(p^k) &= |U_{p^k}| \\
&= |\{1, 2, 3, \ldots, p^k\} \setminus \{1 \cdot p, 2p, \ldots, p^{k-1} \cdot p\}| \\
&= p^k - p^{k-1} = p^{k-1}(p-1) \\
\therefore \phi\Big(\prod p_i^{k_i}\Big) &= \prod \phi(p_i^{k_i}) \\
&= \prod (p_i^{k_i} - p_i^{k_i - 1}) = \prod p_i^{k_i - 1}(p_i - 1) \\
&= \prod p_i^{k_i}\Big(1 - \frac{1}{p_i}\Big) = n \prod \Big(1 - \frac{1}{p_i}\Big)
\end{aligned}$$

Theorem: (Euler Fermat Theorem)
For $a \in U_n$, $a^{\phi(n)} = 1 \in U_n$
Proof: Let $a \in U_n$
Say $U_n = \{a_1, a_2, \ldots, a_{\phi(n)}\}$ (where the a_i are distinct).
Note that $aa_i = aa_j$
$\iff a_i = a_j$
$\iff i = j$
So the elements aa_i are also distinct.

$$\therefore \{aa_1, aa_2, \ldots, aa_{\phi(n)}\} = U_n = \{a_1, a_2, \ldots, a_{\phi(n)}\}$$

Multiply the elements together to get

$$\prod (aa_i) = \prod a_i.$$

Divide by $\prod a_i \in U_n$ to get $\prod_{i=1}^{\phi(n)} a = 1$

$$a^{\phi(n)} = 1.$$

Corollary: (Fermat's Little Theorem)
If $a \in U_p$ where p is prime then $a^{p-1} = 1 \in U_p$
Proof: $\phi(p) = p - 1$.

Fermat Primes
Definition: A *Fermat prime* is a prime of the form $2^k + 1$ for some $k \in \mathbb{Z}^+$.

k	1	2	3	4	5	6	7	8	9	10
2^k+1	$\boxed{3}$	$\boxed{5}$	9	$\boxed{17}$	33	65	129	$\boxed{257}$	513	1025

It appears that $2^k + 1$ is prime $\iff$ k is a power of 2.
Example: Show that if $2^k + 1$ is prime then k is a power of 2.
Solution: Suppose that k is *not* a power of 2, say $2^l \cdot q$ where q is odd.

$$\text{Then } 2^k + 1 = 2^{2^l q} + 1 = (2^l)^q + 1 = \big(2^{2^l} + 1\big)\big((2^{2^l})^{q-1} - (2^{2^l})^{q-2} + \cdots + 1\big)$$

and $1 < 2^{2^l} - 1 < 2^k + 1$.
So $2^k + 1$ is not prime.

Definition: For $n \in \mathbb{Z}_+$, $2^{2^n} + 1$ is called the nth Fermat number
Example: Show that F_5 is not prime.
Solution: We guess that 641 is a factor.
Note that $641 = 625 + 16 = 5^4 + 2^4$ and $641 = 640 + 1 = 5 \cdot 2^7 + 1$ so we have

$$\begin{aligned} F_5 &= 2^{2^5} + 1 \\ &= 2^{32} + 1 \\ &= (2^4 2^{28} + 1) \\ &= (641 - 5^4) \cdot 2^{28} + 1 \\ &= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 \\ &= 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641 \cdot 2^{28} - 641^4 + 4 \cdot 641^3 - 6 \cdot 641^2 + 4 \cdot 641 \end{aligned}$$

PMATH 740 Lecture 5: May 11, 2012

Fermat Primes $F_n = 2^{2^n} + 1$
Example: Show that $F_n = F_0 F_1 F_2 \cdots F_{n-1} + 2$, for $n \geq 1$.
Solution: $F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$
$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5 = F_0 + 2$
Fix $n \geq 1$ and suppose that $F_n = F_0 F_1 F_2 \cdots F_{n-1} + 2$.

$$\begin{aligned} F_{n+1} - 2 &= 2^{2^{n+1}} - 1 \\ &= (2^{2^n})^2 - 1 \\ &= (2^{2^n} + 1)(2^2 - 1) \\ &= F_n(F_n - 2) \\ &= F_n(F_0 F_1 \cdots F_{n-1}) \\ &= F_0 F_1 \cdots F_n, \text{ so} \\ F_{n+1} &= F_0 F_1 \cdots F_n + 2. \end{aligned}$$

Example: Show that for $k \neq l$, we have $\gcd(F_k, F_l) = 1$.
Proof: Say $0 \leq k < l$.
Then $F_l = F_0 F_1 \cdots F_k \cdots F_{l-1} + 2$

Recall that if $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

$$\begin{aligned}\therefore \gcd(F_l, F_k) &= \gcd(F_k q + 2, F_k), \text{ with } q = \frac{F_0 F_1 \cdots F_{l-1}}{F_k} \\ &= \gcd(F_k, 2) \\ &= 1 \text{ or } 2\end{aligned}$$

and $\gcd(F_k, F_l) \neq 2$, since F_k and F_l are odd.

Mersenne Primes
Definition: A *Mersenne prime* is a prime of the form $2^k - 1$ with $k \in \mathbb{Z}^+$. We have:

k	1	2	3	4	5	6	7	8	9	10
$2^k - 1$	1	$\boxed{3}$	$\boxed{7}$	15	$\boxed{31}$	63	$\boxed{127}$	255	511	1023

It appears that $2^k - 1$ is prime $\iff$ k is prime.
Example: Show that if $2^k - 1$ is prime, then k is prime.
Indeed, show that if $a^k - 1$ is prime with $a \geq 2$ and $k \geq 1$, then $a = 2$ and k is prime.
Solution: If $a \geq 3$ then

$$(a^k - 1) = (a - 1)(a^{k-1} + a^{k-2} + \cdots + 1)$$

and $1 < a - 1 < a^k - 1$, so $a^k - 1$ is not prime.
$\therefore$ we need $a = 2$.
If k is not prime, say $k = rs$ with $1 < r$, s, then:

$$(2^k - 1) = (2^{rs} - 1) = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 1)$$

and $1 < 2^r - 1 < 2^{rs} - 1$.

Definition: The nth Mersenne number is $M_n = 2^n - 1$.
Example: Show that M_{11} is composite.
Solution: $M_{11} = 2^{11} - 1 = 2047$
$\lfloor \sqrt{2047} \rfloor = 45$, so we test every $p \leq 45$ to see if it is a factor.
We try 2, 3, 5, 7, 11, 13, 17, 19. They are not factors.
But (23 works): $\therefore 2047 = 23 \cdot 89$.

Example: Show that for k, $l \in \mathbb{Z}^+$, if $\gcd(k, l) = 1$, then $\gcd(M_k, M_l) = 1$.
Solution: Suppose $\gcd(M_k, M_l) \neq 1$, say $\gcd(M_k, M_l) = d > 1$
Then $d \mid M_k$, $d \mid 2^k - 1$, $2^k - 1 = 0 \bmod d$, $2^k = 1 \bmod d$
Let m be the smallest positive integer such that $2^m = 1 \bmod d$.
Note that $m > 1$, since $2^1 = 2 \neq 1 \bmod d$, since $d > 1$.

Note that $m \mid k$, since if we write $k = mq + r$ with $0 \leq r < m$ then

$$1 = 2^k = 2^{mq+r} = (2^m)^q \cdot 2^r = 1^q \cdot 2^r = 2^r$$

so $r = 0$ by the choice of m.

Similarly, $m \mid l$.
So, $m \mid \gcd(k, l)$, $\therefore \gcd(k, l) \neq 1$. □

Perfect Numbers
Definition: A *perfect number* is a positive integer $n \in \mathbb{Z}^+$ which is the sum of its proper divisors.

$$n = \sum_{d|n, d \neq n} d = \sigma(n) - n$$

That is, $\sigma(n) = 2n$.
The first few Mersenne primes are

k	2	3	5	7
$M_k = 2^k - 1$	3	7	31	127

The first few perfect numbers are

$$\begin{aligned} 6 &= 2 \cdot 3 = 1 + 2 + 3 \\ 28 &= 4 \cdot 7 = 1 + 2 + 4 + 7 + 14 \\ 496 &= 16 \cdot 31 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 \end{aligned}$$

It appears that the perfect numbers are the number of the form $2^{p-1}M_p$, where M_p is a Mersenne prime.
Remark: It is not known whether there exist any odd perfect numbers.
Theorem: Every even perfect number is of the form $n = 2^{p-1}M_p$, for some Mersenne prime p.
Proof: Suppose $n = 2^{p-1}M_p$, where M_p is a Mersenne prime.
(Recall: $\sigma(\prod p_i^{k_i}) = \prod \sigma(p_i^{k_i})$, $\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1}-1}{p-1}$)

$$\begin{aligned} \text{Then } \sigma(n) &= \sigma(2^{p-1}M_p) \\ &= \sigma(2^{p-1})\sigma(M_p), \text{ since } M_p \text{ is an odd prime} \\ &= (1 + 2 + 2^2 + \cdots + 2^{p-1})(1 + M_p), \text{ since } M_p \text{ is prime} \\ &= (2^p - 1)(1 + M_p) \\ &= 2^p + 2^p M_p - 1 - M_p = 2^p M_p = 2(2^{p-1}M_p) = 2n. \end{aligned}$$

Conversely, suppose n is an even perfect number, say $n = 2^{p-1}q$, where $p \geq 2$, and q is odd.

$$\begin{aligned} \text{Then } \sigma(n) = 2n &\implies \sigma(2^{p-1})\sigma(q) = 2^p q \\ &\implies (2^p - 1)\sigma(q) = 2^p q \end{aligned}$$

$\therefore 2^p - 1 \mid q$, say $q = (2^p - 1)k$,

$$\begin{aligned} \text{so } (2^p - 1)\sigma(q) &= 2^p(2^p - 1)k \\ \sigma(q) &= 2^p k \end{aligned}$$

Note that $k \mid q$ and $q \mid q$ and $k + q = k + (2^p - 1)k = 2^p k = \sigma(q)$
$\therefore k$ and q are *all* of the divisors of q
$\therefore k = 1$ and q is prime, and we have

$$q = (2^p - 1)k = 2^p - 1 = M_p.$$

PMATH 740 Lecture 6: May 14, 2012

Typos on A1
2(b) $a^{l(n)+m(n)} = a \bmod n$ should be $a^{l+m} = a^m \bmod n$
4(b) Let p be a prime should be
let $p \neq 2$ be a prime.

Example: Show that U_{50} is cyclic and find every generator in every subgroup of U_{50}.
Solution: $\phi(50) = \phi(2 \cdot 25) = \phi(2)\phi(25) = 1 \cdot 20 = 20$.
$U_{50} = \{1, 3, 7, 9, 11, 13, 17, 19, \ldots, 49\}$

k	0	1	2	3	4	5	6	7	8	9	10	11
3^k	1	3	9	27	31	43	29	37	11	33	49	-3

$\therefore \operatorname{ord}_{50}(3) = 20 = |U_{50}|$, $U_{50} = \langle 3 \rangle$
The divisors of 20 are 1, 2, 4, 5, 10, 20.
The subgroups of U_{50} are

$$\begin{aligned}
\langle 3^1 \rangle &= U_{50} \\
\langle 3^2 \rangle &= \{3^0, 3^2, 3^4, 3^6, 3^8, 3^{10}, 3^{12}, 3^{14}, 3^{18}\} \\
\langle 3^4 \rangle &= \{3^0, 3^4, 3^8, 3^{12}, 3^{16}\} \\
\langle 3^5 \rangle &= \{3^0, 3^5, 3^{10}, 3^{15}\} \\
\langle 3^{10} \rangle &= \{3^0, 3^{10}\} \\
\langle 3^{20} \rangle &= \{3^0\}
\end{aligned}$$

Example: Show that for $n \in \mathbb{Z}^+$

$$\sum_{d|n} \phi(n) = n.$$

Solution: For all $n \in \mathbb{Z}_n$ the order of a is a divisor $d \mid n$.
For each $d \mid p$, let

$$A_d = \{\, a \in \mathbb{Z}_n : \operatorname{ord}_n(a) = d \,\}.$$

Then $\mathbb{Z}_n$ is the disjoint union

$$\mathbb{Z}_n = \bigcup_{d|n} A_d$$

$$n = |\mathbb{Z}_n| = \sum_{d|n} |A_d|$$

But the elements in A_d are the generators of the cyclic subgroup of Z_n of order d.
The # of generators of this cyclic group is $\phi(d)$
$\therefore A_d = \phi(d)$.

$H \subset G$, $a \in G$
cosets

$$aH = \{\, ax : x \in H \,\}$$

For a, $b \in G$ either $aH = bH$ or $aH \cap bH \neq \emptyset$ and $|aH| = |H|$.
$|G| = \underbrace{|G/H|}_{\#\text{ of cosets}} |H|$
$\therefore |H| \mid |G|$
For $a \in G$, $\operatorname{ord}(a) = |\langle a \rangle|$, $\operatorname{ord}(a) \mid |G|$
$a^{|G|} = 1$
EFT and FℓT are special cases.

$\mathbb{Z}_n$, U_n, $C_n = \{n\text{th roots of } 1\} \subset \mathbb{S}^1 = \{\, z \in \mathbb{C}^* : |z| = 1 \,\} \subset \mathbb{C}^*$

$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_l}$
$n_1 \mid n_2$, $n_2 \mid n_3$, $\ldots$, $n_{l-1} \mid n_l$
$G \cong \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{k_m}}$
$p_1 \leq p_2 \leq \cdots \leq p_m$
if $p_i = p_{i+1}$ then $k_i \leq k_{i+1}$
If $\gcd(a, b) = 1$ then $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$

$$\phi(ab) = \phi(a)\phi(b)$$

$\mathbb{Z}_{20} = \mathbb{Z}_{4 \cdot 5} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_5$

Ch. 10 Primitive Roots
The Group of Units
Problem: determine the structure (up to isomorphism) of U_n
Example: $U_{50} \cong \mathbb{Z}_{20}$

Definition: If U_n is cyclic then a generator of U_n is called a *primitive root* mod n.
Theorem: For $a,\ b \in \mathbb{Z}^+$ if $\gcd(a,b) = 1$ then $U_{ab} \cong U_a \oplus U_b$.
Proof: We saw that the map $f : U_{ab} \to U_a \times U_b$ given by $f(x) = (x, x)$ is bijective. Also, f is a homomorphism.
Corollary: When $n = \prod_{i=1}^{l} p_i^{k_i}$ where the p_i are distinct primes and each $k_i \geq 1$,

$$U_n = \bigoplus_{i=1}^{l} U_{p_i^{k_i}}$$

Theorem: $U_2 = \{1\}$, $U_4 = \{1, 3\} = \langle 3 \rangle \cong \mathbb{Z}_2$.
For $n \geq 3$, $U_{2^n} = \{\, \pm 5^k : 0 \leq k < 2^{n-2} \,\} \cong \langle -1 \rangle \oplus \langle 5 \rangle$ with $\langle -1 \rangle = \{1, -1\} \cong \mathbb{Z}_2$ and $\langle 5 \rangle \cong \mathbb{Z}_{2^{n-2}}$.
Proof: For $n \geq 3$, U_{2^n} is *not* cyclic because the elements -1, $2^{n-1} \pm 1$ have order 2, but a cyclic group can only have $\phi(2) = 1$ element of order 2.

$$U_8 = \{1, 3, 5, 7\}$$
$$U_{16} = \{1, 3, 5, 7, 11, 13, 17, 19\}$$

We wish to show that

$$\operatorname{ord}_{2^n}(5) = 2^{n-2}.$$

We know $\operatorname{ord}(5) \mid |U_{2^n}| = \phi(2^n) = 2^{n-1}$
$\therefore \operatorname{ord}(5) = 2^k$ for some $k \leq n-1$.
We cannot have $\operatorname{ord}(5) = 2^{n-1}$ since U_{2^n} is not cyclic, so $\operatorname{ord}(5) = 2^k$ for some $k \leq n-2$ (so $5^{2^{n-3}} \neq 1$, $5^{2^{n-2}} = 1 \bmod 2^n$)
We find $e_2(5^{2^k} - 1)$ for all k.

We have

$$5^{2^0} - 1 = 5^1 - 1 = 4 \qquad e_2(4) = 2$$
$$5^{2^1} - 1 = 5^2 - 1 = 24 \qquad e_2(24) = 3$$
$$5^{2^2} - 1 = 5^4 - 1 = 624 \qquad e_2(624) = 4$$

Suppose $e_2(5^{2^k} - 1) = k + 2$ where $k \geq 1$
say $5^{2^k} - 1 = 2^{k+2} q$ with q odd

$$\begin{aligned} \text{Then } 5^{2^{k+1}} - 1 &= (5^{2^k})^2 - 1 = (2^{k+2}q + 1)^2 - 1 \\ &= 2^{2k+4} q^2 + 2^{k+3} q \\ &= 2^{k+3} (\underbrace{q + 2^{k+1} q^2}_{\text{odd}}) \end{aligned}$$

By induction $e_2(5^{2^k} - 1) = k + 2$ for all $k \geq 0$.
$\therefore \operatorname{ord}_{2^n} 5 = 2^{n-2}$

$$\begin{aligned} \therefore \langle 5 \rangle &= \{\, 5^k : 0 \leq k < 2^{n-2} \,\} \\ &\cong \mathbb{Z}_{2^{n-2}} \end{aligned}$$

and we have

$$U_{2^n} = \{\, \pm 5^n : 0 \leq k < 2^{n-2} \,\}$$

since the elements 5^k, $0 \le k < 2^{n-2}$ are distinct, and the elements -5^k for $0 \le k < 2^{n-2}$ are distinct *and*

$$5^k \neq -5^l \text{ for } 0 \le k, l < 2^{n-2}$$

since $5^k = 1 \bmod 4$, $-5^l = -1 \bmod 4$

The map $f\colon \langle -1\rangle \oplus \langle 5\rangle \to U_{2^n}$ given by $f(e, 5^k) = e5^k$ is an isomorphism.

PMATH 740 Lecture 7: May 16, 2012

Theorem: For an odd prime p and for $k \in \mathbb{Z}^+$, U_{p^k} is cyclic.

(1) U_p is cyclic

(2) If $U_p = \langle a\rangle$ then either $U_{p^2} = \langle a\rangle$ or $U_{p^2} = \langle a + p\rangle$

(3) If $U_{p^2} = \langle b\rangle$ then $U_{p^k} = \langle b\rangle$ for all $k \ge 2$

Proof:

(1) We have

$$\phi(p) = |U_p| = p - 1$$

We need to show that there is an element $a \in U_p$ with $\mathrm{ord}_p(a) = p-1$. We show that for every $d \mid (p-1)$ there exist $\phi(d)$ elements of order d in U_p.

For a divisor $d \mid (p-1)$ let

$$A_d = \{\, a \in U_p : \mathrm{ord}_p(a) = d \,\}$$

Note that U_p is the disjoint union

$$U_p = \bigcup_{d|(p-1)} A_d$$

so

$$p - 1 = |U_p| = \sum_{d|(p-1)} |A_d|$$

But recall that

$$p - 1 = |U_p| = \sum_{d|(p-1)\phi(d)}$$

so it suffices to show that

$$|A_d| \le \phi(d) \text{ for all } d \mid (p-1)$$

We shall show that if $|A_d| \neq 0$ then $|A_d| = \phi(d)$. Suppose $|A_d| \neq 0$ (so $A_d \neq \emptyset$). Choose $a \in U_p$ with $\mathrm{ord}_p(a) = d$. Then

$$\langle a\rangle = \{1, a, a^2, \ldots, a^{d-1}\}$$

with the a^i distinct for $0 \le i < d$. For each i, the element $x = a^i$ satisfies $x^d = a^{id} = (a^d)^i = 1$. So the elements

$$1,\ a,\ a^2,\ \ldots,\ a^{d-1}$$

are the roots of the polynomial $f(x) = x^d - 1$ over the field $\mathbb{Z}_p$. For every $x \in A_d$ we have $x^d = 1$ so x is a root of $f(x) = x^d - 1$ so $x = a^i$ for some i with $0 \le i < d$. But a^k has order d.

$$\begin{aligned} &\iff a^k \text{ generates } \langle a\rangle \\ &\iff \gcd(k, d) = 1 \\ &\iff k \in U_d \\ \therefore |A_d| &= \#\text{ of } k \in U_d \\ &= \phi(d) \end{aligned}$$

(2) Suppose $U_p = \langle a \rangle$, but $U_{p^2} \neq \langle a \rangle$ (We wish to show that $U_{p^2} = \langle a + p \rangle$. Let $n = \text{ord}_{p^2}(a)$. Since $\text{ord}_{p^2}(a) \mid |U_{p^2}|$ we have $n \mid p(p-1)$.

$$\begin{aligned} \text{Also } a^n &= 1 \bmod p^2 \\ \text{so } a^n &= 1 \bmod p \end{aligned}$$

$\therefore n$ is a multiple of $\text{ord}_p(a)$
$\therefore (p-1) \mid n$ (since $U_p = \langle a \rangle$ so $\text{ord}_p\, a = p-1$)
Since $(p-1) \mid n$ and $n \mid p(p-1)$ we have $n = p-1$ or $n = p(p-1)$.

$$\begin{aligned} \text{Since } U_{p^2} &\neq \langle a \rangle \\ n &= p-1 \end{aligned}$$

Now let $m = \text{ord}_{p^2}(a+p)$. Note that $a = a + p \bmod p$ so $U_p = \langle a \rangle = \langle a + p \rangle$. As above,

$$m = p-1 \text{ or } m = p(p-1)$$

We need to show that $m \neq p-1$. We shall show that $(a+p)^{p-1} \neq 1 \bmod p^2$. We have

$$\begin{aligned} (a+p)^{p-1} &= a^{p-1} + (p-1)a^{p-2} \cdot p + \text{terms involving } p^2 \\ (a+p)^{p-1} &= a^{p-1} - a^{p-2}p \bmod p^2 \\ &= 1 - a^{p-2}p \bmod p^2 \\ &\neq 1 \bmod p^2 \end{aligned}$$

since $a \in U_p$ so $a^{p-2} \in U_p$ so $p \nmid a^{p-2}$

(3) Suppose $U_{p^2} = \langle b \rangle$.[1)]
Suppose, inductively, that $U_{p^k} = \langle b \rangle$. Let $n = \text{ord}_{p^{k+1}}\, b$. Then $n \mid |U_{p^{k+1}}|$ so $n \mid p^k(p-1)$.
Also $b^n = 1 \bmod p^{k+1}$ so $b^n = 1 \bmod p^k$.
$\therefore n$ is a multiple of $\text{ord}_{p^k}(b)$ that is $p^{k-1}(p-1) \mid n$.
Since $p^{k-1}(p-1) \mid n$ and $n \mid p^k(p-1)$ we have $n = p^{k-1}(p-1)$ or $n = p^k(p-1)$.
We need to show that $n \neq p^{k-1}(p-1)$.
We shall show that

$$b^{p^{k-1}(p-1)} \neq 1 \bmod p^{k+1}.$$

Consider $b^{p^{k-2}(p-1)}$.
Since $U_{p^k} = \langle b \rangle$ we also have $U_{p^{k-1}} = \langle b \rangle$
$\therefore b^{|U_{p^{k-1}}|} = 1 \bmod p^{k-1}$ that is $b^{p^{k-2}(p-1)} = 1 \bmod p^{k-1}$ (1).
Also, since $\text{ord}_{p^k}(b) = p^{k-1}(p-1)$
$\therefore b^{p^{k-2}(p-1)} \neq 1 \bmod p^k$ (2)
From (1) and (2)

$$b^{p^{k-2}(p-1)} = 1 + tp^{k-1}$$

for some t with $p \nmid t$.

[1)] Aside:

$$\begin{aligned} \phi(p^k) &= p^{k-1}(p-1) \\ \phi(p^{k+1}) &= p^k(p-1) \end{aligned}$$

So we have

$$\begin{aligned} b^{p^{k-1}(p-1)} &= (1+tp^{k-1})^p \\ &= 1 + tp^k + \binom{p}{2} t^2 p^{2k-2} + \text{higher order terms in } p \\ &= 1 + tp^k \bmod p^{k+1} \\ &\neq 1 \bmod p^{k+1} \end{aligned}$$

Summary: for $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ where the p_i are distinct primes and each $k_i \geq 1$ we have

$$U_n = U_{p_1^{k_1}} \oplus U_{p_2^{k_2}} \oplus \cdots \oplus U_{p_l^{k_l}}$$

and $U_2 = \{1\}$, $U_4 = \{1,3\} = \langle 3 \rangle \cong \mathbb{Z}_2$, $U_{2^k} = \langle -1, 5 \rangle \cong \langle -1 \rangle \oplus \langle 5 \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-2}}$ for $k \geq 3$ and $U_{p^k} = \mathbb{Z}_{p^{k-1}(p-1)}$ for an odd prime p and $k \geq 1$.

Corollary: For $n \in \mathbb{Z}^+$, U_n is cyclic

$$\iff n = 1,\ 2,\ 4,\ p^k,\ 2p^k$$

where p is an odd prime and $k \geq 1$
(since $\phi(n)$ is even when $n \neq 1, 2$)

PMATH 740 Lecture 8: May 18, 2012

No class Monday
(next class Tuesday)

Gauss' Structure Theorem

$$U_{\prod p_i^{k_i}} \cong \prod U_{p_i^{k_i}}$$

$U_2 = \{1\}$, $U_4 = \{1,3\}$, $U_{2^k} = \langle -1, 5 \rangle \cong \langle -1 \rangle$[2] $\oplus$ $\langle 5 \rangle$[3]
$U_{p^k} \cong \mathbb{Z}_{p^{k-1}(p-1)}$
Corollary: U_n is cyclic (equivalently $\exists$ primitive root mod n)
$\iff n = 1, 2, 4, p^k, 2p^k$
Proof: $\phi(p^k)$ is even except when $p = 2$, $k = 1$ and $\mathbb{Z}_a \oplus \mathbb{Z}_b$ is cyclic $\iff \gcd(a,b) = 1$

Definition: For a finite abelian group G, the *universal exponent* of G is

$$\kappa(G) = \max_{a \in G}(\text{ord}(a))$$

For $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_l}$ with $n_1 \mid n_2$, $n_2 \mid n_3$, $\ldots$, $n_{l-1} \mid n_l$ we have

$$\kappa(G) = n_l$$

and for all $a \in G$

$$\text{ord}(a) \mid n_l = \kappa(G).$$

For $G = U_n$ we write

$$\kappa(n) = \kappa(U_n)$$

For $n = \prod_{i=1}^{l} p_i^{k_i}$ where the p_i are distinct primes and each $k_i \geq 1$ we have

$$\kappa(n) = \text{lcm}(\kappa(p_1^{k_1}), \ldots, \kappa(p_l^{k_l}))$$

[2] $\cong \mathbb{Z}_2$
[3] $\cong \mathbb{Z}_{2^{k-2}}$

with $\kappa(2) = 1$, $\kappa(4) = 2$, $\kappa(2^k) = \frac{1}{2}\phi(2^k) = 2^{k-2}$, $\kappa(p^k) = \phi(p^k) = p^{k-1}(p-1)$.

Example: Find the number of $x \in \mathbb{Z}_n$ such that $x^2 = 1$, where $n = \prod_{i=1}^{l} p_i^{k_i}$
Solution: Note that when $x^2 = 1 \bmod n$ we must have $\gcd(x, n) = 1$ so $x \in U_n$.

When p_i is odd $U_{p_i^{k_i}}$ is cyclic and $|U_{p_i^{k_i}}|$ is even so $U_{p_i^{k_i}}$ has one element of order 1 and one of order 2 so there are 2 solutions to $x^2 = 1$ in $U_{p_i^{k_i}}$.
In U_2 there is 1 solution (no elements of order 2).
In U_4 there are 2 solutions.
In U_{2^k} there are 2 solutions. ($U_{2^k} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-2}}$ so there are 2 solutions in each of Z_2, $Z_{2^{k-2}}$)
The number of solutions to $x^2 = 1$ in U_n for $n = \prod p_i^{k_i}$ with $p_1 < p_2 < \cdots < p_l$ is

$$\begin{array}{ll} 2^l & \text{if } p_1 \neq 2 \\ 2^{l-1} & \text{if } p_1 = 2,\ k_1 = 1 \\ 2^l & \text{if } p_1 = 2,\ k_1 = 2 \\ 2^{l+1} & \text{if } p_1 = 2,\ k \geq 3 \end{array}$$

Primality Testing
Theorem: (Wilson's) Let $n \in \mathbb{Z}^+$. Then $2 \leq n \in \mathbb{Z}$ is prime

$$\iff (n-1)! = -1 \bmod n$$

Proof: Suppose $n = p$ is prime.
Then for all $a \in U_p$

$$a^{p-1} = 1 \bmod p$$

so each $a \in U_p$ is a root of $f(x) = x^{p-1} - 1$ over $\mathbb{Z}_p$.
$\therefore$ The roots of $f(x)$ are the elements 1, 2, ..., $p-1 \in U_n$.

$$x^{p-1} - 1 = f(x) = (x-1)(x-2)\cdots(x-(p-1))$$

Put in $x = 0$ to get

$$\begin{aligned} -1 &= (-1)(-2)\cdots(-(p-1)) \\ &= (-1)^{p-1}(p-1)! \\ &= (p-1)! \qquad \text{if } p \text{ is odd so } (-1)^{p-1} = 1 \end{aligned}$$

and when $p = 2$,

$$(p-1)! = 1! = 1 = -1 \bmod 2$$

Conversely, suppose n is composite, say $n = kl$ with $1 < k, l < n$.

$$\begin{aligned} (n-1)! &= 1 \cdot 2 \cdots k \cdots (n-1) \\ &= 0 \bmod k \\ \text{and } 0 &= -1 \bmod k \\ \text{so } (n-1)! &\neq -1 \bmod k \\ \therefore (n-1)! &\neq -1 \bmod n \end{aligned}$$

Definition: If n is prime then

$$b^n = b \bmod n \text{ for all } b \in \mathbb{Z} \text{ (by F}\ell\text{T)}$$

Given $2 \leq n \in \mathbb{Z}$, for $b \in \mathbb{Z}^+$ if $b^n = b \bmod n$ then we say n *passes* the *base* b *test* for primality (in this case, n is probably prime)

if $b^n \neq b \bmod n$ we say n *fails* the base b test (in this case n is composite)
When n passes the base b test but is composite, we call n a *base b pseudo prime*.
A base 2 pseudo prime is just called a *pseudo prime*.
If n is a base b pseudo prime for *every* base b then n is called a *Carmichael* number.
Example: Show that 341 is a pseudo prime (it's the smallest one).
Solution: $n = 341 = 11 \cdot 31$
We need to show that

$$2^n = 2 \bmod n$$
$$2^{341} = 2 \bmod 341$$

mod 11, powers repeat every $\phi(11) = 10$ terms so $2^{341} = 2^1 = 2 \bmod 31$, powers repeat every $\phi(31) = 30$ terms so $2^{341} = 2^{11}$ and we have

k	0	1	2	3	4	5
2^k	1	2	4	8	16	1

so powers of 2 repeat every 5 terms so

$$2^{341} = 2^1 = 2 \bmod 31$$

$\therefore 2^{341} = 2 \bmod 341$ by CRT

Example: Show that if n is a pseudo prime then so is $M_n = 2^n - 1$.
Solution: Suppose n is a pseudo prime.
Since n is composite so M_n is composite.

$$[n = kl \implies M_n = 2^n - 1 = (2^k - 1)((2^k)^{l-1} + \cdots + 1)]$$

and we have $2^n = 2 \bmod n$.
Say $2^n - 2 = nq$ (we need to show that

$$2^{M_n} = 2 \bmod M_n$$
$$2^{2^n-1} = 2 \bmod 2^n - 1)$$

$$\begin{aligned} \text{Then } 2^{2^n-1} - 2 &= 2^{nq+1} - 2 \\ &= 2(2^{nq} - 1) \\ &= 2(2^n - 1)((2^n)^{q-1} + \cdots + 1) \end{aligned}$$

$\therefore (2^n - 1) \mid 2^{2^n-1} - 2$, $2^{2^n-1} = 2 \bmod 2^n - 1$
Corollary: There are infinitely many pseudo primes.

For $2 < n \in \mathbb{Z}$, n is a Carmichael Number

$$\iff n = p_1 p_2 \cdots p_l$$

for some distinct primes p_i with $l \geq 2$ such that

$$(p_i - 1) \mid (n - 1)$$

for all i.

PMATH 740 Lecture 9: May 22, 2012

For $2 \leq n \in \mathbb{Z}$, n is a *Carmichael number* when n is composite and $b^n = b \bmod n$ for all $b \in \mathbb{Z}$.

Example: Show that $2 \leq n \in \mathbb{Z}$ is a Carmichael number if and only if

$$n = \prod_{i=1}^{l} p_i$$

for some distinct primes $p_1, \ldots, p_l$ with $l \geq 2$ such that $(p_i - 1) \mid (n-1)$ for all i.
Solution: Suppose $n = p_1 p_2 \cdots p_l$ where the p_i are distinct primes with $l \geq 2$ and $(p_i - 1) \mid (n-1)$ for all i.
Then n is composite since $l \geq 2$ and for $b \in \mathbb{Z}$,
for each i, if $p_i \mid b$ then $b^n = 0 = b \bmod p_i$
and if $p_i \nmid b$ then $b^{p_i - 1} = 1 \bmod p_i$
so $b^m = 1 \bmod p_i$ for any multiple m of $p_i - 1$
$\therefore b^{n-1} = 1 \bmod p_i$
$\therefore b^n = b \mod p_i$
Since $b^n = b \bmod p_i$ for all i we have $b^n = b \bmod n$ by the CRT.

Conversely, suppose that n is a Carmichael number. Say $n = \prod_{i=1}^{l} p_i^{k_i}$ where $p_1, p_2, \ldots, p_l$ are distinct primes with $l \geq 2$ (since n is composite) and each $k_i \geq 1$.
Since n is a Carmichael number
$b^n = b \bmod n$ for all $b \in \mathbb{Z}$
$\therefore b^n = b$ for all $b \in U_n$
$b^{n-1} = 1 \bmod n$ for all $b \in U_n$
$\therefore n - 1$ is a multiple of $\operatorname{ord}_n(b)$ for all $b \in U_n$ in particular, $n-1$ is a multiple of $\kappa(n) = \operatorname{lcm}(\kappa(p_i^{k_i}))$.
If we had $k_i = 2$ for some i then we would have $p_i \mid \kappa(p_i^{k_i})$

Aside: for p odd

$$\kappa(p^k) = \phi(p^k) = p^{k-1}(p-1)$$

and

$$\kappa(2) = 1,\ \kappa(4) = 2,\ \kappa(2^n) = \tfrac{1}{2}\phi(2^k) = 2^{k-2}$$

but then since $\kappa(p_i^{k_i}) \mid n-1$ we would have $p_i \mid (n-1)$
but $p_i \mid n$ so this is not possible.
So we have $k_i = 1$ for all i, and $n = p_1 p_2 \cdots p_l$ and $(n-1)$ is a multiple of $\kappa(n) = \operatorname{lcm}(\kappa(p_i)) = \operatorname{lcm}(p_i - 1)$
so $(p_i) \mid (n-1)$ for all i

Exercise: If $n = p_1 p_2 \cdots p_l$ is a Carmichael number then no $p_i = 2$ and $l \geq 3$.

Example: Note that $3 \cdot 11 \cdot 17 = 561$ is a Carmichael number since $2 \mid 560$, $10 \mid 560$, $16 \mid 560$

Remark: There are infinitely many Carmichael number.

Miller's Test: Let $n \geq 3$ be odd. Write $n - 1 = 2^k q$ with q odd. If n is prime

$$\begin{aligned} b^{n-1} &= 1 \bmod n \text{ for } 1 \leq b < n \\ b^{q2^k} - 1 &= 0 \bmod n \\ 0 = (b^q)^{2^k} &= ((b^q)^{2^{k-1}})(b^{q2^{k-1}} - 1) \\ &= (b^{q2^{k-1}} + 1)(b^{q2^{k-2}} + 1)(b^{q2^{k-2}} - 1) \\ 0 &= (b^{q2^{k-1}} + 1)(b^{q2^{k-2}} + 1) \cdots (b^{q2} + 1)(b^q + 1)(b^q - 1) \bmod n \end{aligned}$$

(and $\mathbb{Z}_n$ is a field) and so either $b^q = 1 \bmod n$ or $b^{q2^i} = -1$ for some $i = 0, 1, \ldots, k-1$

PRIMES is in P: $(x+b)^n = x^n + b \bmod \mathbb{Z}_n[x]/(x^r - 1)$

Chapter 9 Quadratic Residues
Problem: given $a \in \mathbb{Z}_n$ or U_n determine whether $a = x^2$ for some $x \in U_n$
Definition: $Q_n = \{\, a \in U_n : a = x^2 \text{ for some } x \in U_n \,\}$ is called the group of *quadratic residues* modulo n

Note Q_n is a group (since $1 \in Q_n$, if $a = x^2$ and $b = y^2$ then $ab = (xy)^2$, and if $a = x^2$ then $a^{-1} = (x^{-1})^2$)

Note: The bijection

$$f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \oplus \mathbb{Z}_b$$

given by $f(x) = (x, x)$ in the case that $\gcd(a, b) = 1$ gives an isomorphism

$$f : Q_{ab} \to Q_a \oplus Q_b$$

since if $u = x^2 \in U_{ab}$ then $u = x^2 \in U_a$ and $u = x^2 \in U_b$
and if $u = z^2 \in U_a$ and $v \in y^2 \in U_b$
and if we solve $w = x \bmod a$ and $w = y \bmod b$
then $w^2 \in Q_{ab}$

$$\begin{aligned} \text{with } w^2 = x^2 &= u \in Q_a \\ w^2 = y^2 &= v \in Q_b \end{aligned}$$

Note: $U_2 = \{1\}$, $Q_2 = \{1\}$
$U_4 = \{1, 3\}$, $Q_4 = \{1\}$
$U_{2^k} = \{\pm 5^i\}$, $|U_{2^k}| = 2^{k-1}$
$Q_{2^k} = \{+5^{2i}\}$, $|Q_{2^k}| = 2^{k-3}$

for p an odd prime $U_{p^k} = \langle u \rangle$ for some $u \in U_{p^k}$ and $Q_{p^k} = \langle u^2 \rangle$ and $\phi(p^k) = p^{k-1}(p-1)$ is even so $\langle Q_{p^k} \rangle = \frac{1}{2}\langle U_{p^k} \rangle = \frac{1}{2}p^{k-1}(p-1)$

Given $a \in U_{p^k} = \langle u \rangle$
$a = u^k$ for some k

PMATH 740 Lecture 10: May 23, 2012

Chapter 9 Quadratic Residues

$$Q_n = \{\, x^2 : x \in U_n \,\}$$

Problem: given $a \in U_n$ determine whether $a \in Q_n$

for $\gcd(k, l) = 1$

$$\begin{aligned} U_{kl} &\cong U_k \oplus U_l \\ Q_{kl} &\cong U_k \oplus Q_l \end{aligned}$$

It suffices to consider U_{p^k} for p prime.

$U_2 = \{1\}$, $Q_2 = \{1\}$
$U_4 = \{1, 3\}$, $Q_4 = \{1\}$
$U_{2^k} = \{\pm 5^i\}$, $Q_{2^k} = \{+5^{2i}\}$, $|Q_{2^k}| = \frac{1}{4}|U_{2^k}| = \frac{1}{4}\phi(2^k) = 2^{k-3}$
$U_{p^k} = \langle u \rangle = \{u^i\}$, $Q_{p^k} = \langle u^2 \rangle = \{u^{2i}\}$, $|Q_{p^k}| = \frac{1}{2}|U_{p^k}| = \frac{1}{2}\phi(p^k) = \frac{1}{2}p^{k-1}(p-1)$

Example: For $a \in U_{2^k}$ with $k \geq 3$ we have $a \in Q_{2^k} \iff a = 1 \bmod 8$

$$U_{2^k} = \langle \pm 5^i \rangle = \{5^0, 5^2, 5^4, \ldots\}^{4)} \cup \{5^1, 5^3, 5^5, \ldots\}^{5)} \cup \{-5^0, -5^2, \ldots\}^{6)} \cup \{-5^1, -5^3, \ldots\}^{7)}$$

4) $= Q_{2^k} = \{\, a \in U_{2^k} : a = 1 \bmod 8 \,\}$
5) $5 \bmod 8$
6) $7 \bmod 8$
7) $3 \bmod 8$

Note: For an odd prime p,

$$a \in Q_{p^k} \iff a \in Q_p$$

Proof: Say $U_{p^k} = \langle u \rangle$. Then $U_p = \langle u \rangle$.

$$\begin{aligned} a \in Q_{p^k} &\iff a = u^k \text{ for some even } k \\ &\iff a \in U_p \end{aligned}$$

Our problem is reduced to the following:
given $a \in U_p$ where p is an odd prime, determine whether $a \in Q_p$

Definition: For an odd prime p and for $a \in \mathbb{Z}$, we define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = (a|p) = \begin{cases} 0 & \text{if } a \notin U_p \text{ (i.e., } p \mid a) \\ 1 & \text{if } a \in Q_p \\ -1 & \text{if } a \in U_p \setminus Q_p \end{cases}$$

Note: For $a \in U_p = \langle u \rangle$ with say $a = u^k$, $a \in Q_p \iff k$ is even so

$$\left(\frac{a}{p}\right) = (-1)^k$$

Theorem: Let p be an odd prime and let a, $b \in \mathbb{Z}$. Then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Proof: if $p \mid a$ or $p \mid b$ (so $a \notin U_p$ or $b \notin U_p$) then $p \mid ab$ so

$$\left(\frac{ab}{p}\right) = 0 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

If a, $b \in U_p = \langle u \rangle$ with $a = u^k$, $b = u^l$ then $ab = u^{k+l}$ so

$$\begin{aligned} \left(\frac{ab}{p}\right) &= (-1)^{k+l} = (-1)^k(-1)^l \\ &= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \end{aligned}$$

Theorem: (Euler's criterion)
For an odd prime p and for $a \in \mathbb{Z}$,

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}.$$

Proof: If $p \mid a$ so $a \notin U_p$ then $\left(\frac{a}{p}\right) = a = a^{(p-1)/2} = 0$
Suppose $a \in U_p = \langle u \rangle$, say $a = u^k$.
Note: $u^{(p-1)/2} = -1$ because $u^{(p-1)/2} \neq 1$, $(u^{(p-1)/2})^2 = u^{p-1} = 1$ so $\text{ord}(u^{(p-1)/2}) = 2$ but -1 is the only element in the cyclic group U_p of order 2.

$$\begin{aligned} \therefore \left(\frac{a}{p}\right) &= (-1)^k = (u^{(p-1)/2})^k \\ &= (u^k)^{(p-1)/2} = a^{(p-1)/2}. \end{aligned}$$

Theorem: (Gauss' Lemma)
Let p be an odd prime.

Let $P = \{1, 2, 3, \ldots, \frac{p-1}{2}\}$, $N = \{-1, -2, \ldots, -\frac{p-1}{2}\}$ (so that U_p is the disjoint union $U_p = P \cup N$.)
Then for $a \in U_p$

$$\left(\frac{a}{p}\right) = (-1)^{|aP \cap N|}$$

(where $aP = \{a1, a2, \ldots, a\frac{p-1}{2}\}$)
Proof: Note that for k, $l \in P$

$$\begin{aligned} ak = al &\implies a(k-l) = 0 \implies k = l \in U_p \\ ak = -al &\implies a(k+l) = 0 \implies k = -l \end{aligned}$$

but $k \in P$ and $-l \in N$ so $k \neq -l$.
Thus aP consists of one element from each pair $\{\pm 1\}$, $\{\pm 2\}$, $\ldots$, $\{\pm\}\frac{p-1}{2}$.
For each $k \in P$ choose $e_k \in \{\pm 1\}$ so that $e_k ab \in P$. Thefn

$$\begin{aligned} P &= \{1, 2, \ldots, \frac{p-1}{2}\} \\ &= \{e_1 a1, e_2 a2, \ldots, e_{(p-1)/2} a\frac{p-1}{2}\} \end{aligned}$$

Multiply the elements to get

$$\begin{aligned} \left(\frac{p-1}{2}\right)! &= \prod_{k \in P} e_k \cdot a^{(p-1)/2} \cdot \left(\frac{p-1}{2}\right)! \\ 1 &= \prod_{k \in P} e_k \cdot a^{(p-1)/2} \end{aligned}$$

Note that

$$\begin{aligned} \prod_{k \in P} e_k &= (-1)^{\#\text{ of } k \in P \text{ such that } e_k = -1} \\ &= (-1)^{\#\text{ of } k \in P \text{ such that } ak \in N} \\ &= (-1)^{|aP \cap N|} \end{aligned}$$

$\therefore (-1)^{|aP \cap N|} \cdot a^{(p-1)/2} = 1$
$a^{(p-1)/2} = (-1)^{|aP \cap N|}$

Theorem: (Quadratic Reciprocity)
Let p, q be distinct odd primes. Then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

unless $p \equiv q \equiv 3 \bmod 4$ in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.
Equivalently

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

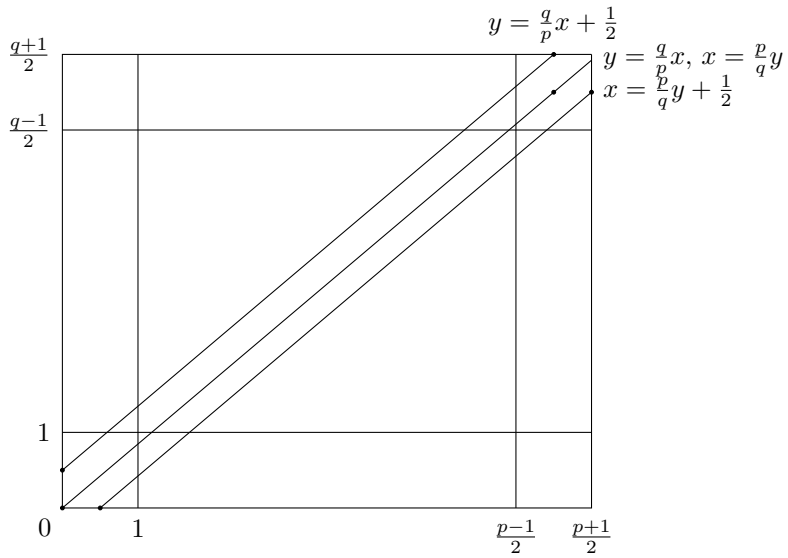
Proof: Let $P = \{1, 2, \ldots, \frac{p-1}{2}\}$
$N = \{-1, -2, \ldots, -\frac{p-1}{2}\}$
$Q = \{1, 2, \ldots, \frac{q-1}{2}\}$
$M = \{-1, -2, \ldots, -\frac{q-1}{2}\}$
so that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{|qP \cap N|}(-1)^{|pQ \cap M|} = (-1)^{|qP \cap N| + |pQ \cap M|}$$

$$\begin{aligned} |qP \cap N| &= \#\text{ of } x \in P \text{ with } qx \in N \bmod p \\ &= \#\text{ of } x \in P \text{ such that } \exists y\ qx - py \in N \end{aligned}$$

and

$$\begin{gathered} qx - py \in N \iff py - qx \in P \\ \iff 1 \le py - qx \le \tfrac{p-1}{2} \\ \iff 0 < py - qx < \tfrac{p}{2} \\ \iff qx < py < qx + \tfrac{p}{2} \\ \iff \tfrac{q}{p}x < y < \tfrac{q}{p}x + \tfrac{1}{2} \\ |qP \cap N| = \#(x,y) \in R = [1, \tfrac{p-1}{2}] \times [1, \tfrac{q-1}{2}] \\ \text{with } \tfrac{q}{p}x < y < \tfrac{q}{p} + \tfrac{1}{2} \end{gathered}$$



PMATH 740 Lecture 11: May 25, 2012

EC $\left(\frac{a}{p}\right) = a^{(p-1)/2}$
GL $\left(\frac{a}{p}\right) = (-1)^{|aP \cap N|}$

Theorem: (Quadratic Reciprocity)
For p, q distinct odd primes

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \text{ unless } p = q = 3 \bmod 4$$

in which case $\left(\frac{q}{p}\right) \neq \left(\frac{p}{q}\right)$.

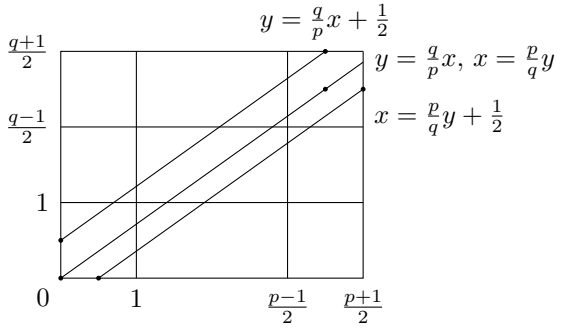
Equivalently,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$$

Proof: P, N $\quad$ Q, M
$\left(\frac{q}{p}\right) = (-1)^{|qP \cap N|}$
$|qP \cap N| = \#$ of x in P such that $qx \in N$ as elements in U_p

$qx - py \in N$ for some $y \in \mathbb{Z}$

$$\begin{aligned} qx - py &\iff py - qx \in P \\ &\iff 1 \le py - qx \le \frac{p-1}{2} \\ &\iff 0 < py - qx < \frac{p}{2} \\ &\iff qx < py < qx + \frac{p}{2} \\ &\iff \frac{q}{p}x < y < \frac{q}{p}x + \frac{1}{2} \end{aligned}$$



$$\therefore |qP \cap N| = \#\text{ of } (x,y) \in R = \left[1, \frac{p-1}{2}\right] \times \left[1, \frac{q-1}{2}\right] \subseteq \mathbb{Z}^2$$

strictly between $y = \frac{q}{p}x$ and $y = \frac{q}{p}x + \frac{1}{2}$.

Similarly $|pQ \cap M| = \#$ of $(x,y) \in R$ strictly between

$$x = \frac{p}{q}y \text{ and } x = \frac{p}{q}y + \frac{1}{2}.$$

Note that since $\gcd(p,q) = 1$, there are no points in R on the line $y = \frac{p}{q}x$.
We have

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{|qP \cap N| + |pQ \cap M|}$$

$|qP \cap N| + |pQ \cap M| = \#$ of $(x,y) \in R$ between $y = \frac{q}{p}x + \frac{1}{2}$, $x = \frac{p}{q}y + \frac{1}{2}$.
These lines are symmetric in R.
$\therefore |qP \cap N| + |pQ \cap M| = \#$ of (x,y) in $R - 2(\#$ of (x,y) in R with $y \ge \frac{q}{p} + \frac{1}{2})$

$$\begin{aligned} \therefore (-1)^{|qP \cap N| + |pQ \cap M|} &= (-1)^{\#\text{ of } (x,y) \text{ in } R} \\ &= (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} \\ &= (-1)^{(p-1)(q-1)/4} \end{aligned}$$

Example: Show that for an odd prime p,

$$\begin{aligned} -1 \in Q_p &\iff p = 1 \bmod 4 \\ 2 \in Q_p &\iff p = \pm 1 \bmod 8 \\ -2 \in Q_p &\iff p = 1, 3 \bmod 8 \\ 3 \in Q_p &\iff p = \pm 1 \bmod 12 \\ &\vdots \end{aligned}$$

Solution: By Euler's criterion,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } \frac{p-1}{2} \text{ is even} \\ -1 & \text{if } \frac{p-1}{2} \text{ is odd} \end{cases} = \begin{cases} 1 & \text{if } p = 1 \bmod 4 \\ -1 & \text{if } p = 3 \bmod 4 \end{cases}$$

By Gauss' Lemma

$$\left(\frac{2}{p}\right) = (-1)^{|2P \cap N|}$$

Case 1: $p = 1 \bmod 4$ (so $\frac{p-1}{2}$ is even),

$$P = \left\{1, 2, \ldots, \frac{p-1}{4}, \frac{p+3}{4}, \ldots, \frac{p-1}{2}\right\}$$
$$2P = \left\{2, 4, \ldots, \underbrace{\frac{p-1}{2}}_{\in P}\right\} \cup \left\{\underbrace{\frac{p+3}{2}}_{\in N}, \ldots, p-1\right\}$$
$$\text{So } |2P \cap P| = \frac{p-1}{4}$$
$$|2P \cap N| = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$$
$$\therefore \left(\frac{2}{p}\right) = (-1)^{(p-1)/4}$$
$$= \begin{cases} 1 & \text{if } \frac{p-1}{2} \text{ is even} \\ -1 & \text{if } \frac{p-1}{4} \text{ is odd} \end{cases}$$
$$= \begin{cases} 1 & \text{if } p = 1 \bmod 8 \\ -1 & \text{if } p = 5 \bmod 8 \end{cases}$$

Case 2: $p = 3 \bmod 4 = 3, 7 \bmod 8$ (so $\frac{p-1}{2}$ is odd)

$$P = \left\{1, 2, \ldots, \frac{p-3}{4}, \frac{p+1}{4}, \ldots, \frac{p-1}{2}\right\}$$
$$2P = \left\{2, 4, \ldots, \underbrace{\frac{p-3}{2}}_{\in P}\right\} \cup \left\{\underbrace{\frac{p+1}{2}}_{\in N}, \ldots, p-1\right\}$$

So $|2P \cap P| = \frac{p-3}{4}$, $\cap 2P \cap N = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$

$$\therefore \left(\frac{2}{p}\right) = (-1)^{|2P \cap N|} = (-1)^{(p+1)/4} = \begin{cases} 1 & \text{if } \frac{p+1}{4} \text{ is even} \\ -1 & \text{if } \frac{p+1}{4} \text{ is odd} \end{cases} = \begin{cases} 1 & \text{if } p = 7 \bmod 8 \\ -1 & \text{if } p = 3 \bmod 8 \end{cases}$$

$$\therefore \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p = 1, 7 \bmod 8 \\ -1 & \text{if } p = 3, 5 \bmod 8 \end{cases}$$

Is $-2 \in Q_p$?

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p = 1 \bmod 4, \text{ i.e., } p = 1, 5 \bmod 8 \\ -1 & p = 3 \bmod 4, \text{ i.e., } p = 3, 7 \bmod 8 \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p = 1, 7 \bmod 8 \\ -1 & p = 3, 5 \bmod 8 \end{cases}$$

$$\therefore \begin{array}{c|cccc} p & 1 & 3 & 5 & 7 \\ \hline \left(\frac{-2}{p}\right) & 1 & 1 & -1 & -1 \end{array}$$

$$\therefore \left(\frac{-2}{p}\right) = \begin{cases} 1 & p = 1, 3 \bmod 8 \\ -1 & p = 5, 7 \bmod 8 \end{cases}$$

Is $3 \in Q_p$? $3 \notin Q_3$, so let $p > 3$.

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & p = 1 \bmod 4 \\ -\left(\frac{p}{3}\right) & p = 3 \bmod 4 \end{cases}$$

$$= \begin{cases} \begin{cases} 1 & p = 1 \bmod 4, p = 1 \bmod 3, \text{ i.e., } p = 1 \bmod 12 \\ -1 & p = 1 \bmod 4, p = 2 \bmod 3, \text{ i.e., } p = 5 \bmod 12 \end{cases} \\ \begin{cases} 1 & p = 3 \bmod 4, p = 2 \bmod 3, \text{ i.e., } p = 11 \bmod 12 \\ -1 & p = 3 \bmod 4, p = 1 \bmod 3, \text{ i.e., } p = 7 \bmod 12 \end{cases} \end{cases}$$

$$\therefore \left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p = 1, 11 \bmod 12 \\ -1 & \text{if } p = 5, 7 \bmod 12 \end{cases}$$

Example:

(1) Is $7 \in Q_{43}$?

(2) Is $136 \in Q_{421}$?

(3) Is $468 \in Q_{697}$?

For (1), we give 4 solutions:
In U_{43},

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
x^2	1	4	9	16	25	36	6	21	38	14	35	15	40	24	10	41	31	23	17	13	11	11
7^x	7	6	−1	−7	−6	−1			−1			1			−1			1			−1	
$7x$	7	14	21	−15	−8	−1	6	13	20	−16	−9	−2	5	12	19	−17	−10	−3	4	11	18	

squares $\implies 7 \notin Q_{43}$
E.C.: $\left(\frac{7}{43}\right) = 7^{21} = -1$
G.L.: $(-1)^{|7P \cap Q|} = (-1)^9 = -1$
Q.R.: $\left(\frac{7}{43}\right) = -\left(\frac{43}{7}\right) = -\left(\frac{1}{7}\right) = -1$

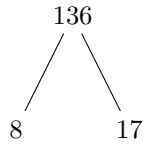
PMATH 740 Lecture 12: May 28, 2012

Is $136 \in Q_{421}$?
Is $468 \in Q_{697}$?

Is $136 \in Q_{421}$?
Solution: $\lfloor\sqrt{421}\rfloor = 20$ try $p = 2, 3, 5, 7, 11, 13, 17, 19$

$$\begin{array}{rrr} & 32 & \\ 13\overline{)421} & & \\ & 39 & \\ & 31 & \\ & 26 & \\ & 5 & \end{array} \qquad \begin{array}{rrr} & 24 & \\ 17\overline{)421} & & \\ & 34 & \\ & 81 & \\ & 68 & \\ & 13 & \end{array} \qquad \begin{array}{rrr} & 22 & \\ 19\overline{)421} & & \\ & 38 & \\ & 41 & \\ & 38 & \\ & 3 & \end{array}$$

$\therefore$ 421 is prime



$2 \in Q_p \iff p = \pm 1 \bmod 8$

$$\begin{aligned} \left(\frac{136}{421}\right) &= \left(\frac{8}{421}\right)\left(\frac{17}{421}\right) \\ &= \left(\frac{2}{421}\right)^3\left(\frac{17}{421}\right) \\ &= \left(\frac{2}{421}\right)\left(\frac{17}{421}\right) \\ &= -\left(\frac{17}{421}\right) \\ &= -\left(\frac{421}{17}\right) = -\left(\frac{13}{17}\right) \\ &= -\left(\frac{17}{13}\right) = -\left(\frac{4}{13}\right) = -\left(\frac{2}{13}\right)^2 = -1 \end{aligned}$$

$\therefore 136 \notin Q_{421}$

Is $468 \in Q_{697}$? **Solution:** $\lfloor\sqrt{697}\rfloor = 26$
we try $p = 2, 3, 5, 7, 11, 13, 17, 19, 23$

$$\begin{array}{rrr} & 41 & \\ 697\overline{)17} & & \end{array}$$

mod 17

$$\left(\frac{468}{17}\right) = \left(\frac{9}{17}\right) = \left(\frac{3}{17}\right)^2 = 1$$

$\therefore 468 \in Q_{17}$
mod 41

$$\begin{aligned} \left(\frac{468}{41}\right) &= \left(\frac{17}{41}\right) = \left(\frac{41}{17}\right) \\ &= \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) \\ &= \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) \\ &= -\left(\frac{1}{3}\right) = -1 \end{aligned}$$

$\therefore 468 \notin Q_{41}$
$\therefore 468 \notin Q_{697}$

Remark: we can extend the Legendre symbol to the Jacobi symbol $\left(\frac{a}{b}\right)$ defined for a, $b \in \mathbb{Z}^+$ with b odd by defining

$$\left(\frac{a}{\prod p_i^{k_i}}\right) = \prod \left(\frac{a}{p_i}\right)^{k_i}$$

Verify that the Jacobi symbol satisfies

$$\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$$
$$\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right)$$
$$\left(\frac{a}{c}\right) = \left(\frac{b}{c}\right) \text{ when } a = b \bmod c$$
$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}$$
$$\left(\frac{-1}{a}\right) = \begin{cases} 1 & a = 1 \bmod 4 \\ -1 & a = 3 \bmod 4 \end{cases}$$
$$\left(\frac{2}{a}\right) = \begin{cases} 1 & a = 1, 7 \bmod 8 \\ -1 & a = 3, 5 \bmod 8 \end{cases}$$

Example: Find $f \in \mathbb{Z}[x]$ which has a root mod n for every $n \in \mathbb{Z}^+$ but no root in $\mathbb{Z}$.
Solution: try $f(x) = (x^2 - p)(x^2 - q)(x^2 - pq)$ with $p \in Q_q$, $q \in Q_p$ and one of p, $q = 1 \bmod 8$
Example: let $f(x) = (x^2 - 13)(x^2 - 17)(x^2 - 221)$
Then f has real roots $\pm\sqrt{13}$, $\pm\sqrt{17}$, $\pm\sqrt{221}$
Let p be prime.
If $p = 2$ we have $17 = 1 \bmod 8$ so $17 \in Q_{2^k}$ for all $k \geq 1$
so we can solve $f(x) = 0 \bmod 2^k$
if $p = 13$ then

$$\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = 1$$

so $17 \in Q_{13}$ so $17 \in Q_{13^k}$ for all $k \in \mathbb{Z}^+$
if $p = 17$ then

$$\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = 1 \text{ so } 13 \in Q_p$$

so $13 \in Q_{p^k}$ for all $k \in \mathbb{Z}^+$
if $p \neq 2, 13, 17$

$$\left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{221}{p}\right)$$

so one of $\left(\frac{13}{p}\right)$, $\left(\frac{17}{p}\right)$, $\left(\frac{221}{p}\right)$ is 1, so either $13 \in Q_p$, $17 \in Q_p$, $221 \in Q_p$ so again we can solve

$$f(x) = 0 \bmod p^k.$$

For $n = \prod p_i^{k_i}$ we can find a_i with $f(a_i) = 0 \bmod p_i^{k_i}$ then solve $x = a_i \bmod p_i^{k_i}$ for all i and then $f(x) = f(a_i) = 0 \bmod p_i^{k_i}$ for all i, so $f(x) = 0 \bmod n$

Example: Let p be an odd prime.
Show that $p = x^2 + y^2$ for some x, $y \in \mathbb{Z} \iff p = 1 \bmod 4$

Solution: Suppose $p = x^2 + y^2$. Note that $p \nmid x$ (since $p \mid x \implies p \mid x^2 \implies p \mid p - x^2 = y \implies p \mid y \implies p^2 \mid x^2 + y^2 = p$ #) and $p \nmid y$ so x, $y \in U_p$.

$$\text{Then } x^2 + y^2 = 0$$
$$x^2 = -y^2$$
$$(xy^{-1})^2 = -1$$
$$\therefore -1 \in Q_p$$
$$\therefore p = 1 \bmod 4$$

Suppose $p = 1 \bmod 4$.
Then $-1 \in Q_p$, say $x^2 = -1 \bmod p$
say $x^2 + 1 = kp$, $k \in \mathbb{Z}$

We work in the ring

$$\mathbb{Z}[i] = \{\, a + ib : a, b \in \mathbb{Z} \,\}$$

where we have $kp = (x + i)(x - i)$.

In $\mathbb{Z}[i]$ we have a division algorithm (given a, $b \in \mathbb{Z}[i]$ with $b \neq 0$, choose $q \in \mathbb{Z}[i]$ nearest to $\frac{a}{b} \in \mathbb{C}$ then let $r = a - qb$ to get $a = qb + r$ with $0 \leq |r| < |b|$) so there is a Euclidean algorithm in $\mathbb{Z}[i]$ and we can use it to prove that in $\mathbb{Z}[i]$

$$p \text{ is irreducible} \iff p \text{ is prime}^{8)}$$

$p \mid ab \implies a$ or b is a unit, i.e., a or $b \in \{\pm 1, \pm i\}$

We have $kp = x^2 + 1 = (x + i)(x - i)$. If p was irreducible (or prime) then $p \mid x + i$ or $p \mid x - i$ (since the multiples of p in $\mathbb{Z}[i]$ are of the form $p(a + ib) = pa + ipb$)
$\therefore p$ is irreducible in $\mathbb{Z}[i]$
say $p = zw$, $|z|, |w| \neq 1$ then $p^2 = |7|^2 |w|^2$
$\therefore |z|^2 = |w|^2 = p$
For $z = a + ib$, $p = |z|^2 = a^2 + b^2$

Dirichlet's Theorem
For any k, $l \in \mathbb{Z}^+$ with $\gcd(k, l) = 1$ there exist infinitely many primes p with $p = k \bmod l$.

PMATH 740 Lecture 13: May 30, 2012

$\exists \infty$ primes $p = k \mod l$ when $\gcd(k, l) = 1$

Example: Show that there exist infinitely many primes of each of the forms

$$p = 1 \bmod 4 \tag{1}$$
$$p = 3 \bmod 4 \tag{2}$$
$$p = 1 \bmod 8 \tag{3}$$
$$p = 3 \bmod 8 \tag{4}$$

(1) $1 \bmod 4$
Suppose there are only finitely many primes p with $p = 1 \bmod 4$, say p_1, p_2, $\ldots$, p_l. Consider $n = (2p_1 p_2 \cdots p_l)^2 + 1$. Let p be a prime factor of n. Note that $p \neq p_i$ for any i since $n = 1 \bmod p_i$ so

[8)] $p \mid ab \implies p \mid a$ or $p \mid b$

$p_i \nmid n$. Since $p \mid n$, $\therefore n = 0 \bmod p$.

$$\begin{aligned} \therefore (2p_1 \cdots p_l)^2 + 1 &= 0 \bmod p \\ -1 &= (2p_1 \cdots p_l)^2 \bmod p \\ \therefore -1 &\in Q_p \\ \therefore p &= 1 \bmod 4 \end{aligned}$$

(2) $p = 3 \bmod 4$
Suppose there are finitely many, say $p_1, \ldots, p_l$. Consider $n = 4p_1p_2 \cdots p_l - 1$ (note that $n = 3 \bmod 4$). The prime factors of n are odd so they are all of the form

$$p = 1, 3 \bmod 4.$$

Not every prime factor of n can be equal to $1 \bmod 4$ (since $n = 3 \bmod 4$). $\therefore n$ has a prime factor $p = 3 \bmod 4$. And $p \neq p_i$ for any i since $p_i \nmid n$.

(3) $p = 1 \bmod 8$
Suppose there are finitely many such primes p. Consider $n = (2p_1 \cdots p_l)^4 + 1$. Let p be a prime factor of n. Then $n = 0 \bmod p$.

$$\begin{aligned} \therefore (2p_1 \cdots p_l)^4 &= -1 \bmod p \\ (2p_1 \cdots p_l)^8 &= 1 \bmod p \\ \therefore \operatorname{ord}_p(2p_1 \cdots p_l) &= 8 \\ \therefore 8 \mid |U_p|,\ 8 &\mid p - 1 \\ \therefore p &= 1 \bmod 8 \end{aligned}$$

Also, $p \neq p_i$ for any i.

(4) $p = 3 \bmod 8$.
Suppose there are only finitely many such primes, say

$$p_1, p_2, \ldots, p_l.$$

Consider $n = (p_1p_2 \cdots p_l)^2 + 2$. Let p be a prime factor of n. Then $n = 0 \bmod p$

$$(p_1p_2 \cdots p_l)^2 = -2 \bmod p$$

Note that n is odd so p is odd

$$\begin{aligned} -2 &\in Q_p \\ \therefore p &= 1, 3 \bmod 8 \end{aligned}$$

Since each $p_i = 3 \bmod 8$, $p_i^2 = 1 \bmod 8$ so $n = 3 \bmod 8$. Not every prime factor can be equal to $1 \bmod 8$. $\therefore n$ has a prime factor $p = 3 \bmod 8$ and $p \neq p_i$ for any i.

Chapter 2 Arithmetical Functions
Definition: An *arithmetic function* is a function $f\colon \mathbb{Z}^+ \to \mathbb{C}$, f is called *multiplicative* when

$$f(kl) = f(k)f(l) \qquad \text{for all } k, l \text{ with } \gcd(k, l) = 1$$

(equivalently when $f(\prod p_i^{k_i}) = \prod f(p_i^{k_i})$ and $f(1) = 1$). f is called *completely multiplicative* when $f(kl) =$

$f(k)f(l)$ for all $k, l \in \mathbb{Z}^+$ (equivalently, when $f(\prod p_i^{k_i}) = \prod f(p_i)^{k_i}$)

Examples:

$$p_n = p(n) = \text{the } n\text{th prime}$$

$$\tau(n) = \#\text{ of distinct divisors of } n = \sum_{d|n} 1$$

$$\sigma(n) = \text{sum of divisors of } n = \sum_{d|n} d$$

$$\sigma_x(n) = \sum_{d|n} d^x \qquad (x \in \mathbb{Z}^+ \text{ or } x \in \mathbb{R} \text{ or } x \in \mathbb{C})$$

Euler: $\phi(n) = |U_n|$

$$u(n) = 1 \text{ for all } n$$

$$I(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{when } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$N(n) = n \text{ for all } n$$

Möbius: $\mu(n) = \begin{cases} (-1)^l & \text{when } n \text{ is a product of } l \text{ distinct primes } l \geq 0 \\ 0 & \text{otherwise (when } n \text{ is not square free)} \end{cases}$

Mangoldt: $\Lambda(n) = \begin{cases} \log p & \text{when } p \text{ is prime and } n = p^k \text{ for some } k \in \mathbb{Z}^+ \\ 0 & \text{otherwise} \end{cases}$

Liouville: $\lambda\left(\prod p_i^{k_i}\right) = (-1)^{\sum k_i}$

Some other functions include

$$\pi(x) = \#\text{ of primes } p \leq x = \sum_{p \leq x} 1$$

Riemann: $\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$ for $1 < x \in \mathbb{R}$

Chebyshev: $\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{l^k \leq x} \log p$

$$\vartheta(x) = \sum_{p \leq x} \log p$$

$$\begin{aligned}
\tau\Big(\prod p_i^{k_i}\Big) &= \prod \tau(p_i^{k_i}) = \prod (k_i+1) \\
\sigma\Big(\prod (p_i^{k_i})\Big) &= \prod \sigma(p_i^{k_i}) = \prod (1+p_i+p_i^2+\cdots p_i^{k_i}) \\
\sigma_k(n) &= \sum_{d|n} d^k \text{ for } n = \prod p_i^{k_i} \\
&= \sum_{\substack{1\le i_1\le k_1 \\ \vdots \\ 1\le i_l\le k_l}} (p_1^{i_1}\cdots p_l^{i_l})^k \\
&= \Big(\sum_{1\le i_1\le k_1} p_1^{ki_1}\Big)\cdots\Big(\sum_{1\le i_l\le k_l} p_l^{ki_l}\Big) \\
&= \prod \sigma_k(p_i^{k_i}) \\
&= \prod (1+p_1^k+p_2^{2k}+\cdots+p_l^{k_l k})
\end{aligned}$$

The Möbius Function

$$\mu(n) = \begin{cases} (-1)^l & \text{when } n \text{ is a product of } l \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

Theorem:

$$\sum_{d|n} \mu(d) = I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$$

Proof: For $n = \prod (p_i^{k_i}) \neq 1$

$$\sum_{d|n} \mu(d) = \sum_{\substack{d \text{ squarefree} \\ d|n}} \mu(l)$$

(the squarefree divisors of n are $p_1^{e_1}p_2^{e_2}\cdots p_l^{e_l}$ with $e_i \in \{0,1\}$)

$$\begin{aligned}
&= \sum_{\substack{e_1\in\{0,1\} \\ \vdots \\ e_l\in\{0,1\}}} \mu(p_1^{e_1}\cdots p_l^{e_l}) \\
&= \sum_{\substack{e_1\in\{0,1\} \\ \vdots \\ e_l\in\{0,1\}}} (-1)^{e_1}(-1)^{e_2}\cdots(-1)^{e_l} \\
&= \Big(\sum_{e_1\in\{0,1\}} (-1)^{e_1}\Big)\Big(\sum_{e_2\in\{0,1\}} (-1)^{e_2}\Big)\cdots\Big(\sum_{e_l\in\{0,1\}} (-1)^{e_l}\Big) \\
&= (1-1)(1-1)\cdots(1-1) \\
&= 0
\end{aligned}$$

when $n = 1$, $\mu(n) = \sum_{d|n} \mu(d) = \mu(1) = 1$

Theorem: (The Möbius Inversion Formula)

(1) For $f\colon \mathbb{Z}^+ \to \mathbb{C}$, if $g(n) = \sum_{d|n} f(d)$, then $f(n) = \sum_{d|n} \mu(d)g(\frac{n}{d}) = \sum_{\substack{k,l \\ kl=n}} \mu(k)g(l)$.

(2) For $f\colon [1,\infty) \to \mathbb{C}$, if $g(x) = \sum_{n\le x} f(\frac{x}{n})$, then $f(x) = \sum_{n\le x} \mu(n) g(\frac{x}{n})$.

PMATH 740 Lecture 14: June 1, 2012

$\mu(n)$, $\Lambda(n)$, $\lambda(n)$
$\pi(x)$, $\psi(x)$, $\Theta(x)$
$\zeta(x)$, $1 < x$

Möbius

$$\mu(n) = \begin{cases} (-1)^l & \text{when } n \text{ is a product of } l \ge 0 \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

Theorem:

$$\sum_{d|n} \mu(d) = I(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Theorem: (Möbius Inversion Formula)
For $f\colon \mathbb{Z}^+ \to \mathbb{C}$, if $g(n) = \sum_{d|n} f(d)$ then

$$\begin{aligned} f(n) &= \sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big) \\ &= \sum_{\substack{k,l \\ kl=n}} \mu(k) g(l) \end{aligned}$$

For $f\colon [1,\infty) \to \mathbb{C}$ if $g(x) = \sum_{n\le x} f(\frac{x}{n})$ then $f(x) = \sum_{n\le x} \mu(n) g(\frac{x}{n})$
Proof: Let $f\colon \mathbb{Z}^+ \to \mathbb{C}$. Define $g\colon \mathbb{Z}^+ \to \mathbb{C}$ by $g(n) = \sum_{d|n} f(d)$. Then[9)]

$$\begin{aligned} \sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big) &= \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} f(e) \\ &= \sum_{\substack{d,e \\ de|n}} \mu(d) f(e) \\ &= \sum_{e|n} \sum_{d|\frac{n}{e}} \mu(d) f(e) \\ &= \sum_{e|n} f(e) \Big(\sum_{d|\frac{n}{e}} \mu(d) \Big) \\ &= \sum_{e|n} f(e) \underbrace{I\Big(\frac{n}{e}\Big)}_{=1 \text{ only when } e=n} \\ &= f(n) \end{aligned}$$

Let $f\colon [1,\infty) \to \mathbb{C}$. Define $g\colon [1,\infty) \to \mathbb{C}$ by

$$g(x) = \sum_{n\le xx} f\Big(\frac{x}{n}\Big).$$

[9)] Aside: $g(m) = \sum_{e|m} f(e)$ for $d, e \in \mathbb{Z}^+$

$$d \mid n,\ e \mid \frac{n}{d} \iff de \mid n$$

Then[10)]

$$\begin{aligned}
\sum_{n\le x}\mu(n)g\Big(\frac{x}{n}\Big) &= \sum_{n\le x}\mu(n)\sum_{m\le\frac{x}{n}} f\Big(\frac{x/n}{m}\Big)\\
&= \sum_{\substack{n,m\\ nm\le x}}\mu(n)f\Big(\frac{x}{nm}\Big)\\
&= \sum_{\substack{k,l\\ kl\le x}}\mu(k)f\Big(\frac{x}{kl}\Big)\\
&= \sum_{n\le x}\sum_{\substack{k,l\\ kl=n}}\mu(k)f\Big(\frac{x}{n}\Big)^{11)}\\
&= \sum_{n\le x}\sum_{d|n}\mu(d)f\Big(\frac{x}{n}\Big)\\
&= \sum_{n\le x} f\Big(\frac{x}{n}\Big)\Big(\sum_{d|n}\mu(d)\Big)\\
&= \sum_{n\le x} f\Big(\frac{x}{n}\Big)\underbrace{I(n)}_{=1 \text{ only when } n=1}\\
&= f\Big(\frac{x}{1}\Big) = f(x).
\end{aligned}$$

Example:

$$\begin{aligned}
\tau(n) &= \sum_{d|n} 1 = \sum_{d|n} u(d)\\
\therefore u(n) &= \sum_{d|n}\mu(d)\tau\Big(\frac{n}{d}\Big)\\
\therefore 1 &= \sum_{\substack{k,l\\ kl=n}}\mu(k)\tau(l)
\end{aligned}$$

Example:

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} N(d)$$

($N(n) = n$ for all n)

$$\begin{aligned}
N(n) &= \sum_{d|n}\mu(d)\sigma\Big(\frac{n}{d}\Big)\\
n &= \sum_{\substack{k,l\\ kl=n}}\mu(k)\sigma(l)
\end{aligned}$$

[10)] Aside: $g(y) = \sum_{m\le y} f(\frac{y}{m})$ for $n,\, m \in \mathbb{Z}^+$

$$n \le x,\, m \le \frac{x}{n} \iff nm \le x$$

[11)] Aside: $n = kl,\, k = d$

Example:

$$\begin{aligned} n &= \sum_{d|n} \phi(d) \\ N(n) &= \sum_{d|n} \phi(d) \\ \phi(n) &= \sum_{d|n} \mu(d) N\Big(\frac{n}{d}\Big) \\ \phi(n) &= \sum_{d|n} \frac{n\mu(d)}{d} \end{aligned}$$

Remark: If $f\colon \mathbb{Z}^+ \to \mathbb{C}$ is multiplicative and $g\colon \mathbb{Z}^+ \to \mathbb{C}$ is defined by

$$g(n) = \sum_{d|n} f(d)$$

then g is multiplicative.
Proof: For $a, b \in \mathbb{Z}^+$ with $\gcd(a,b) = 1$ each divisor $d \mid ab$ can be expressed uniquely as $d = kl$ where $k \mid a$, $l \mid b$.

$$\begin{aligned} g(ab) &= \sum_{d|ab} f(d) \\ &= \sum_{\substack{k,l \\ k|a, l|b}} f(kl) \\ &= \sum_{\substack{k,l \\ k|a, l|b}} f(k)f(l) \\ &= \Big(\sum_{k|a} f(k)\Big)\Big(\sum_{l|b} f(l)\Big) \\ &= g(a)g(b) \end{aligned}$$

Remark: We can define a product, called the *Dirichlet product*, on the set of arithmetic functions by

$$\begin{aligned} (f * g)(n) &= \sum_{d|n} f(a) g\Big(\frac{n}{d}\Big) \\ &= \sum_{\substack{k,l \\ kl=n}} f(k)g(l) \end{aligned}$$

This product is commutative and associative and $I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$ is the identity. If $f(1) \neq 0$ then f has an inverse $g = f^{-1}$ which is given by a recursive formula

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d \neq n}} f\Big(\frac{n}{d}\Big) g(d).$$

The set of arithmetic functions f with $f(1) \neq 0$ is a group under $*$. The set of multiplicative arithmetic functions is a subgroup.

Example: The Mangoldt function

$$\Lambda(n) = \begin{cases} \log p & \text{if } p \text{ is prime} \\ 0 & \text{otherwise} \end{cases}$$

Find $\sum_{d|n} \Lambda(d)$.

Solution: For $n = 1$, $\sum_{d|n} \Lambda(d) = \Lambda(1) = 0$. For $n = \prod_{i=1}^{l} p_i^{k_i}$ where the p_i are distinct primes and each $k_i \geq 1$,

$$\begin{aligned} \sum_{d|n} \Lambda(d) &= \sum_{p^k|n} \Lambda(p^k) \\ &= \sum_{p^k|n} \log p \\ &= \sum_{i=1}^{l} \sum_{1 \leq j_i \leq k_i} \log p_i \\ &= \sum_{i=1}^{l} k_i \log p_i \\ &= \sum_{i=1}^{l} \log p_i^{k_i} \\ &= \log \prod_{i}^{k_i} = \log n \\ \therefore \sum_{d|n} \Lambda(d) &= \log n \end{aligned}$$

Example: By Möbius Inversion

$$\begin{aligned} \Lambda(n) &= \sum_{d|n} \mu(d) \log\Big(\frac{n}{d}\Big) \\ &= \underbrace{\sum_{d|n}}_{=1 \text{ only when } n=1} \mu(d) \log n - \sum_{d|n} \mu(d) \log d \\ &= \log n \Big(\sum_{d|n} \mu(d) \Big) - \sum_{d|n} \mu(d) \log d \\ &= \log n \quad \underbrace{I(n)}_{\begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}} - \sum_{d|n} \mu(d) \log d \\ \Lambda(n) &= -\sum_{d|n} \mu(d) \log d \end{aligned}$$

Example: Liouville's Function

$$\lambda(n) = (-1)^l \text{ when } n \text{ is a product of } l \geq 0 \text{ primes (not necessarily distinct)}$$

Find $\sum_{d|n} \lambda(d)$.

Solution: For $n = 1$

$$\sum_{d|n} \lambda(d) = \lambda(1) = 1$$

For $n = \prod_{i=1}^{l} p_i^{k_i}$ with each $k_i \geq 1$

$$\begin{aligned}\sum_{d|n} \lambda(d) &= \sum_{\substack{0\leq j_1\leq k_1\\ \vdots \\ 0\leq j_l\leq k_l}} \lambda\Big(\prod_{i=1}^{l} p_i^{j_i}\Big) \\ &= \sum_{\substack{0\leq j_1\leq k_1\\ \vdots \\ 0\leq j_l\leq k_l}} (-1)^{j_1}(-1)^{j_2}\cdots(-1)^{j_l} \\ &= \prod_{i=1}^{l}\Big(\underbrace{\sum_{0\leq j_i\leq k_i}(-1)^{j_i}}_{=1-1+1-1+\cdots\pm 1}\Big)\end{aligned}$$

For each i,

$$\begin{aligned}\sum_{0\leq j_i\leq k_i}(-1)^{j_i} &= 1-1+1-1+\cdots+(-1)^{k_i} \\ &= \begin{cases}1 & \text{if } k_i \text{ is even}\\ 0 & \text{if } k_i \text{ is odd}\end{cases}\end{aligned}$$

$$\therefore \sum_{d|n}\lambda(d) = \prod \sum_{0\leq j_i\leq k_i}(-1)^{j_i} = \begin{cases}1 & \text{if every } k_i \text{ is even}\\ 0 & \text{otherwise}\end{cases}$$

For all $n \in \mathbb{Z}^+$, $\sum_{d|n}\lambda(d) = \begin{cases}1 & \text{if } n \text{ is a square}\\ 0 & \text{otherwise}\end{cases}$

$$\zeta(x) = \sum_{n=1}^{\infty}\frac{1}{n^x}$$

Find $\zeta(2k)$ for $k \in \mathbb{Z}^+$.

PMATH 740 Lecture 15: June 4, 2012

Riemann Zeta Function

$$\zeta(z) = \sum_{n=1}^{\infty}\frac{1}{n^z} \qquad \text{for } \Re(z) > 1$$

For $z = x + iy$

$$|n^z| = |e^{z\log n}| = |e^{x\log n + iy\log n}| = e^{x\log n} = n^x = n^{\Re(z)}.$$

$$\begin{aligned}\Big|\sum_{n=1}^{\infty}\frac{1}{n^z}\Big| &\leq \sum_{n=1}^{\infty}\Big|\frac{1}{n^z}\Big| \\ &= \sum_{n=1}^{\infty}\frac{1}{n^{\Re(z)}}\end{aligned}$$

This converges by the Integral Test when $\Re(z) > 1$.

$$\begin{aligned}(\text{Indeed, } \int_1^\infty \frac{1}{t^x}\,\mathrm{d}t &= \Big[\frac{t^{-x+1}}{-x+1}\Big]_1^\infty \\ &= \Big[\frac{-1}{(x-1)t^{x-1}}\Big]_1^\infty \\ &= \frac{1}{x-1} \text{ for } x > 1)\end{aligned}$$

Thus $\sum_{n=1}^\infty \frac{1}{n^z}$ converges absolutely for $\Re(z) > 1$ so $\zeta(x) = \sum_{n=1}^\infty \frac{1}{n^z}$ is well defined for $\Re(z) > 1$

Theorem: (Euler Product Formula)

$$\zeta(z) = \sum_{n=1}^\infty \frac{1}{n^z} = \prod_p \frac{1}{1-\frac{1}{p^z}} = \prod_{i=1}^\infty \frac{1}{1-\frac{1}{p_i^z}} \text{ where } p_i \text{ is the } i\text{th prime}$$

for $\Re(z) > 1$.

Proof: The lth partial product is

$$\begin{aligned}P_l &= \prod_{i=1}^l \frac{1}{1-\frac{1}{p_i^z}} \\ &= \prod_{i=1}^l (1 + \frac{1}{p_i^z} + \frac{1}{p_i^{2z}} + \cdots) \qquad (\text{since } \Big|\frac{1}{p^z}\Big| = \frac{1}{p^{\Re(z)}} \le \frac{1}{2^1} = \frac{1}{2}) \\ &= \prod_{i=1}^l \sum_{k_i=0}^\infty \frac{1}{p_i^{k_i z}} \\ &= \sum_{k_1 \ge 0, \ldots, k_l \ge 0} \frac{1}{p_1^{k_1 z} p_2^{k_2 z} \cdots p_l^{k_l z}} \text{ (since the infinite series converge absolutely)}^{12)} \\ &= \sum_{n \in A_l} \frac{1}{n^z} \text{ where } A_l \text{ is the set of positive integers whose prime factors are in } \{p_1, \ldots, p_l\} \\ |\zeta(z) - P_l(z)| &= \Big|\sum_{n \in \mathbb{Z}^+} \frac{1}{n^z} - \sum_{n \in A_l} \frac{1}{n^z}\Big| \\ &= \Big|\sum_{n \notin A_l} \frac{1}{n^z}\Big| \\ &\le \sum_{n \notin Z_l} \frac{1}{n^x} \text{ where } x = \Re(z) > 1 \\ &\le \sum_{n > p_l} \frac{1}{n^x} \to 0 \text{ as } l \to \infty \text{ since } \sum \frac{1}{n^x} \text{ converges and } p_l \to \infty\end{aligned}$$

Example:

$$\begin{aligned}\zeta(z)\sum_{n=1}^{\infty}\frac{\mu(n)}{n^z} &= \sum_{k=1}^{\infty}\frac{1}{k^z}\sum_{l=1}^{\infty}\frac{\mu(l)}{l^z}\\ &= \sum_{k,l}\frac{\mu(l)}{(kl)^z}\ \text{(by abs convergence)}\\ &= \sum_{n}\sum_{d|n}\frac{\mu(d)}{n^z}\\ &= \sum_{n}\frac{1}{n^z}\sum_{d|n}\mu(d)\\ &= \sum_{n}\frac{1}{n^z}\underbrace{I(n)}_{=1\text{ only when }n=1}\\ &= \frac{1}{1^z} = 1\end{aligned}$$

$\therefore \zeta(z) \neq 0$ for all $\Re(z) > 1$ and $\frac{1}{\zeta(z)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^z}$

Exercise: Let $f\colon \mathbb{Z}^+ \to \mathbb{C}$. Suppose $\sum_{n=1}^{\infty} f(n)$ converges absolutely. Show that if f is multiplicative then

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}(1 + f(p) + f(p^2) + f(p^3) + \cdots)$$

and if f is completely multiplicative then

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}\frac{1}{1 - f(p)}$$

Exercise: Apply this formula to $f(n) = \frac{\mu(n)}{n^z}$.

Calculation of $\zeta(2n)$ for $n \in \mathbb{Z}^+$.

$$\zeta(2n) = \sum_{n=1}^{\infty}\frac{1}{k^{2n}}$$

Euler's Informal Calculation

For a polynomial with n distinct roots α_i

$$f(x) = a_n\prod(x - \alpha_i)$$

If the $\alpha_i \neq 0$

$$f(x) = a_0\prod\Big(1 - \frac{x}{\alpha_i}\Big)$$

$$f(x) = f(0)\prod_{i}\Big(1 - \frac{x}{\alpha_i}\Big)$$

---

12)

$$\Big(\sum_i a_i\Big)\Big(\sum_j b_j\Big) = \sum_{i,j} a_i b_j$$

when we have absolute convergence

By analogy,

$$\begin{aligned}\frac{\sin x}{x} &= 1 \prod_{0\le k\in\mathbb{Z}} \Big(1 - \frac{x}{kx}\Big) \\ &= \prod_{k=1}^{\infty} \Big(1 - \frac{x^2}{(k\pi)^2}\Big)\end{aligned}$$

Example: when $x = \frac{\pi}{2}$,

$$\begin{aligned}\frac{2}{\pi} &= \prod \Big(1 - \frac{\pi^2/4}{(k\pi)^2}\Big) \\ &= \prod \Big(1 - \frac{1}{4k^2}\Big) = \prod \Big(\frac{4k^2-1}{4k^2}\Big) \\ &= \prod \Big(\frac{2k-1}{2k} \cdot \frac{2k+1}{2k}\Big) \\ &= \frac{1}{2}\cdot\frac{3}{2}\cdot\frac{3}{4}\cdot\frac{5}{4}\cdot\frac{5}{6}\cdot\frac{7}{6}\cdots\end{aligned}$$

This is Wallis' Formula.

$$\frac{\sin x}{x} = \prod_{k=1}^{\infty} \Big(1 - \frac{x^2}{(k\pi)^2}\Big)$$

$$1 - \frac{1}{6}x^2 + \frac{1}{24}x^2 - \cdots = 1 - \sum_{k=1}^{\infty} \frac{1}{(k\pi)^2} x^2 + \cdots$$

$$\therefore \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$$

$$\log \frac{\sin x}{x} = \sum_{k=1}^{\infty} \log\Big(1 - \frac{x^2}{(k\pi)^2}\Big)$$

$$\frac{x\cos x - \sin x}{x^2} \cdot \frac{x}{\sin x} = \sum_{k=1}^{\infty} \frac{-\frac{2x}{(k\pi)^2}}{1 - \frac{x^2}{(k\pi)^2}}$$

$$x\cot x - 1 = -2\sum_{k=1}^{\infty} \frac{\frac{x^2}{(k\pi)^2}}{1 - \frac{x^2}{(k\pi)^2}}$$

$$\begin{aligned}x\cot x &= 1 - \sum_{k=1}^{\infty}\sum_{n=1}^{\infty} \Big(\frac{x^2}{(k\pi)^2}\Big)^n \\ &= 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \frac{x^{2n}}{(k\pi)^{2n}} \\ &= 1 - \frac{2}{\pi^{2n}} \sum_{n=1}^{\infty} \underbrace{\Big(\sum_{k=1}^{\infty} \frac{1}{k^{2n}}\Big)}_{\zeta(2n)} x^{2n}\end{aligned}$$

$$\begin{aligned}\therefore \zeta(n) &= \sum_{k=1}^{\infty} \frac{1}{k^{2n}} \\ &= -\frac{\pi^{2n}}{2}(\text{coefficient of } x^{2n} \text{ in } x\cot x)\end{aligned}$$

To find this coefficient write $x\cot x = \sum_{n=0}^{\infty} c_{2n}x^{2n}$

$$x\cot x = \frac{\cos x}{\frac{\sin x}{x}}$$

$$\frac{\sin x}{x}\cdot x\cot x = \cos x$$

$$(1 - \frac{1}{3!}x^2 + \frac{1}{5!}x^4 - \cdots)(c_0 + c_2x^2 + c_4x^4 + \cdots) = 1 - \frac{1}{2!}x^2 + \frac{1}{4!}x^4 - \cdots$$

$$c_0 = 1$$

$$c_2 - \frac{1}{3!}c_0 = -\frac{1}{2!} \qquad c_2 = -\frac{1}{2} + \frac{1}{6} = -\frac{1}{3}$$

$$c_4 - \frac{1}{3!}c_2 + \frac{1}{5!}c_0 = \frac{1}{4!} \qquad c_4 = \frac{1}{24} - \frac{1}{18} - \frac{1}{120} = \frac{15 - 20 - 3}{360} = \frac{-8}{360} = \frac{-1}{45}$$

$$\zeta(2) = -\frac{\pi^2}{2}\Big(-\frac{1}{3}\Big) = \frac{\pi^2}{6}$$

$$\zeta(4) = -\frac{\pi^4}{2}\Big(-\frac{1}{45}\Big) = \frac{\pi^4}{90}$$

PMATH 740 Lecture 16: June 6, 2012

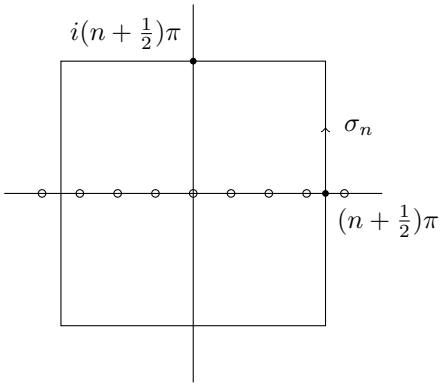
Calculate $\zeta(2n) = \sum_{k=1}^{\infty}\frac{1}{k^{2n}}$
Solution: Let $f(z) = \frac{\cot z}{z^{2n}} = \frac{\cos z}{z^{2n}\sin z}$
f has simple poles at $z = k\pi$, $0 \le k \in \mathbb{Z}$ and a multiple pole at $z = 0$.
$f(z) = \frac{g(z)}{\sin z}$ where $g(z) = \frac{\cos z}{z^{2n}}$.
For $0 \ne k \in \mathbb{Z}$,

$$\operatorname{Res}(f, k\pi) = \frac{g(k\pi)}{\cos(k\pi)} = \frac{\cos k\pi/(k\pi)^{2n}}{\cos(k\pi)} = \frac{1}{(k\pi)^{2n}}$$

At $z = 0$

$$\operatorname{Res}(f, 0) = \Big(\operatorname{Res}\frac{z\cot z}{z^{2n+1}}, 0\Big) = \text{coefficient of } z^{2n} \text{ in } z\cot z$$

Let σ_n be the square as shown.



$$g' = f \qquad \int_\alpha f = \int_\alpha g' = \big[g(z)\big]_{\alpha(t_1)}^{\alpha(t_2)}$$

We have

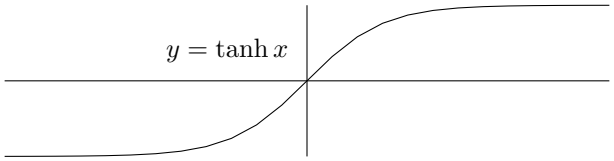
$$\int_{\sigma_n} f = 2\pi i\Big(\operatorname{Res}(0) + 2\sum_{k=1}^{n}\frac{1}{(k\pi)^{2n}}\Big)$$

If we can show that $\int f_{\sigma_n} \to 0$ as $n \to \infty$ then we get $2\sum_{k=1}^{\infty} \frac{1}{(k\pi)^{2n}} = -\operatorname{Res}(0)$.
We have

$$\begin{aligned}
|\sin(x+iy)|^2 &= |\sin x \cosh y + i \cos x \sinh y|^2 \\
&= \sin^2 x \cosh^2 y + \underbrace{\cos^2 x}_{1-\sin^2 x} \sinh^2 y \\
&= \sin^2 x(\cosh^2 y - \sinh^2 y) + \sinh^2 y \\
&= \sin^2 x + \sinh^2 y \\
|\cos(x+iy)|^2 &= \cos^2 x \cosh^2 y + \underbrace{\sin^2 x}_{1-\cos^2 x} \sinh^2 y \\
|\cot z|^2 &= \frac{\cos^2 x + \sinh^2 y}{\sin^2 x + \sinh^2 y}
\end{aligned}$$

On the vertical sides with $x = (n + \frac{1}{2})\pi$ we have

$$|\cot z|^2 = \frac{\sinh^2 y}{1 + \sinh^2 y} = \frac{\sinh^2 y}{\cosh^2 y} = \tanh^2 y \leq 1$$



On the horizontal sides with $y = (n + \frac{1}{2})\pi$

$$\begin{aligned}
|\cot z|^2 &= \frac{\cos^2 x + \sinh^2 y}{\sin^2 x + \sinh^2 y} \\
&\leq \frac{1 + \sinh^2 y}{\sinh^2 y} = \frac{\cosh^2 y}{\sinh^2 y} \\
&= \coth^2 y \leq 2
\end{aligned}$$

for large n.

$$\begin{aligned}
\therefore \left|\int_{\sigma_l} f\right| &= \left|\int_{\sigma_l} \frac{\cot z}{z^{2n}}\right| \\
&\leq \operatorname{length}(\sigma_l) \max_{z=\sigma_l(t)} \left|\frac{\cot z}{z^{2n}}\right| \\
&= 4(2l+1)\pi \cdot \frac{2}{((l+\frac{1}{2})\pi)^{2n}}
\end{aligned}$$

$\to 0$ as $l \to \infty$.

Chapter 3 (and a bit of 4) Asymptotic Formulas
We shall find asymptotic formulas for $\sum_{n \leq x} \frac{1}{n}$, $\sum_{n \leq x} \frac{1}{n^a}$ for $a > 1$, $\sum_{n \leq x} \tau(n)$, $\sum_{n \leq x} \sigma(n)$, $\sum_{n \leq x} \phi(n)$, $\sum_{p \leq x} \frac{\log p}{p}$, $\sum_{p \leq x} \frac{1}{p}$
later: $\pi(x) = \sum_{p \leq x} 1$

Terminology
For $g\colon [1, \infty) \to (0, \infty)$ we write $O(g(x))$ to denote some function $f(x)\colon [1, \infty) \to \mathbb{C}$ with the property that for some $C > 0$ and some $R > 0$

$$|f(x)| \leq Cg(x) \qquad \text{for all } x \geq R.$$

We write $o(g(x))$ to denote some function $f(x)$ with the property that

$$\lim_{n\to\infty} \frac{|f(x)|}{g(x)} = 0.$$

We write $f(x) \sim g(x)$ and say that f is *asymptotic to* g when

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Theorem: (Abel's Summation Formula)
Let $a\colon \mathbb{Z}^+ \to \mathbb{C}$, let $f\colon [1,\infty) \to \mathbb{C}$ be $\mathcal{C}^1$. Then

$$\sum_{n\le x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t)\,\mathrm{d}t$$

where $A(x) = \sum_{n\le x} a(n)$.
Proof: Let $l = \lceil x \rceil$. Then

$$\begin{aligned}\sum_{n\le x} a(n)f(n) &= a(1)f(1) + a(2)f(2) + \cdots + a(l)f(l)\\ &= A(1)f(1) + (A(2)-A(1))f(2) + \cdots + (A(l)-A(l-1))f(l)\\ &= A(l)f(l) + A(1)(f(1)-f(2)) + A(2)(f(2)-f(3)) + \cdots + A(l-1)(f(l-1)-f(l))\\ &= A(l)f(l) - \int_1^2 A(t)f'(t)\,\mathrm{d}t - \int_2^3 A(t)f'(t) - \cdots - \int_{l-1}^l A(t)f'(t)\,\mathrm{d}t\end{aligned}$$

because for $t \in [k, k+1)$ we have $A(t) = A(k)$ so

$$\int_k^{k+1} A(t)f'(t)\,\mathrm{d}t = \int_k^{k+1} A(k)f'(t) = A(k)[f(t)]_{t=k}^{k+1} = A(k)(f(k+1)-f(k))$$

$$\sum_{n\le x} a(n)f(n) = A(l)f(l) - \int_1^l A(t)f'(t)\,\mathrm{d}t$$

We have $x \in [l, l+1)$ so

$$\begin{aligned}\int_l^x A(t)f'(t)\,\mathrm{d}t &= \int_l^x A(l)f'(t)\,\mathrm{d}t\\ &= A(l)[f(t)]_{t=l}^x = A(l)f(x) - A(l)f(l)\\ \therefore \sum_{n\le x} a(n)f(n) &= A(l)f(l) - \int_1^l A(t)f'(t)\,\mathrm{d}t - \int_l^x A(l)f'(t)\,\mathrm{d}t + A(l)f(x) - A(l)f(l)\\ &= A(x)f(x) - \int_1^x A(t)f'(t)\,\mathrm{d}t\end{aligned}$$

since $A(x) = A(l)$.

PMATH 740 Lecture 17: June 8, 2012

Chapter 3 Asymptotic Formulas
Theorem: (Abel's Summation Formula)
Let $a\colon \mathbb{Z}^+ \to \mathbb{C}$, let $f\colon [1,\infty) \to \mathbb{C}$ be $\mathcal{C}^1$, let $A(x) = \sum_{n\le x} a(n)$. Then

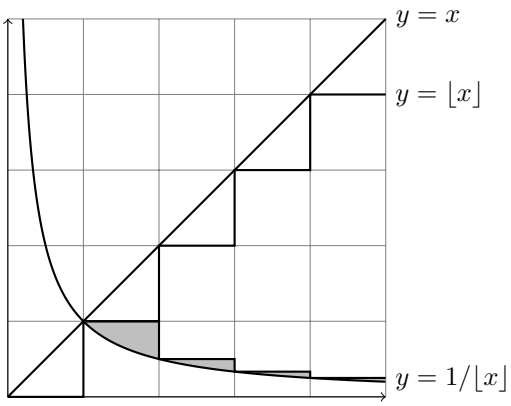
$$\sum_{n\le x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t)\,\mathrm{d}t$$

Theorem: (Euler's Summation Formula)
Let $f\colon [1,\infty) \to \mathbb{C}$ be $\mathcal{C}^1$. Then

$$\sum_{n\le x} f(n) = f(1) + \int_1^x f(t)\,\mathrm{d}t + \int_1^x \langle t\rangle f'(t)\,\mathrm{d}t - \langle x\rangle f(x)$$

where $\langle x\rangle = x - \lfloor x\rfloor$.
Proof: Let $a(n) = 1$, $A(x) = \sum_{n\le x} 1 = \lfloor x\rfloor$. Then by Abel's Summation Formula

$$\begin{aligned}
\sum_{n\le x} f(n) &= A(x)f(x) - \int_1^x A(t)f'(t)\,\mathrm{d}t \\
&= \lfloor x\rfloor f(x) - \int_1^x \lfloor t\rfloor f'(t)\,\mathrm{d}t \\
\int_1^x \underbrace{t}_{u}\underbrace{f'(t)\,\mathrm{d}t}_{\mathrm{d}v} &= \Big[tf(t) - \int f(t)\Big]_1^x \\
&= xf(x) - f(1) - \int_1^x f(t)\,\mathrm{d}t \\
\therefore \sum_{n\le x} f(n) &= \lfloor x\rfloor f(x) - \int_1^x \lfloor t\rfloor f'(t)\,\mathrm{d}t + \int_1^x tf'(t)\,\mathrm{d}t - xf(x) + f(1) + \int_1^x f(t)\,\mathrm{d}t \\
&= f(1) + \int_1^x f(t)\,\mathrm{d}t + \int_1^x \langle t\rangle f'(t)\,\mathrm{d}t - \langle x\rangle f(x)
\end{aligned}$$



Example: Euler's constant is

$$\gamma = \lim_{l\to\infty}\Big(\sum_{n=1}^{l}\frac{1}{n} - \ln l\Big) = \lim_{l\to\infty}\Big(\int_1^l \frac{1}{\lfloor x\rfloor} - \frac{1}{x}\,\mathrm{d}x\Big) = \int_1^\infty \frac{x - \lfloor x\rfloor}{x\lfloor x\rfloor}\,\mathrm{d}x$$

$$\gamma = \int_1^\infty \frac{\langle t\rangle}{t\lfloor t\rfloor}\,\mathrm{d}t$$

Note that the integral does converge since $\frac{\langle t\rangle}{t\lfloor t\rfloor} \le \frac{1}{t(t-1)}$ and $\int_2^\infty \frac{\mathrm{d}t}{t(t-1)} = \int_2^\infty \frac{1}{t-1} - \frac{1}{t}\,\mathrm{d}t = [\ln\frac{t-1}{t}]_2^\infty = -\ln\frac{1}{2} = \ln 2$.
Example: How quickly does $\sum_{n=1}^{\infty}\frac{1}{n} - \ln l$ approach γ? Find an asymptotic formula for $\sum_{n\le x}\frac{1}{n}$.

Solution: Use $f(t) = \frac{1}{t}$, $f'(t) = -\frac{1}{t^2}$ in Euler's Summation Formula to get

$$\begin{aligned}
\sum_{n\le x} \frac{1}{n} &= f(1) + \int_1^x f(t)\,\mathrm{d}t + \int_1^x \langle t\rangle f'(t)\,\mathrm{d}t - \langle x\rangle f(x) \\
&= 1 + \int_1^x \frac{1}{t}\,\mathrm{d}t - \int_1^x \frac{\langle t\rangle}{t^2}\,\mathrm{d}t - \frac{\langle x\rangle}{x} \\
&= 1 + \log x - \int_1^\infty \frac{\langle t\rangle}{t^2}\,\mathrm{d}t + \int_x^\infty \frac{\langle t\rangle}{t^2}\,\mathrm{d}t + O(\tfrac{1}{x}) \\
&= 1 + \log x - c + O(\tfrac{1}{x})^{13)} \\
\sum_{n\le x} \frac{1}{n} - \log x &= 1 - c + O(\tfrac{1}{x})
\end{aligned}$$

Take the limit as $x \to \infty$ to get

$$\gamma = 1 - c \qquad (\text{so } \int_1^\infty \frac{\langle t\rangle}{t^2}\,\mathrm{d}t = 1 - \gamma)$$

$$\therefore \sum_{n\le x} \frac{1}{n} = \log x + \gamma + O(\tfrac{1}{x})$$

Example: Find an asymptotic formula for $\sum_{n\le x} \frac{1}{n^a}$ where $1 < a \in \mathbb{R}$.
Solution: Use ESF with $f(t) = \frac{1}{t^a} = t^{-a}$, $f'(t) = -at^{-a-1} = \frac{-a}{t^{a+1}}$

$$\begin{aligned}
\sum_{n\le x} \frac{1}{n^a} &= f(1) + \int_1^x f(t)\,\mathrm{d}t + \int_1^x \langle t\rangle f'(t)\,\mathrm{d}t - \langle x\rangle f(x) \\
&= 1 + \int_1^x \frac{1}{t^a}\,\mathrm{d}t - \int_1^x \frac{a\langle t\rangle}{t^{a+1}}\,\mathrm{d}t - \frac{\langle x\rangle}{x^a} \\
&= 1 + \frac{1}{a-1} - \frac{1}{(a-1)x^{a-1}} - \int_1^\infty \frac{a\langle t\rangle}{t^{a+1}}\,\mathrm{d}t + \int_x^\infty \frac{a\langle t\rangle}{t^{a+1}} + O(\tfrac{1}{x^a})^{14)} \\
&= \frac{a}{a-1} - \frac{1}{(a-1)x^{a-1}} - c + O(\tfrac{1}{x^a})^{15)}
\end{aligned}$$

Take the limit as $x \to \infty$

$$\zeta(a) = \frac{a}{a-1} - c$$

$$\therefore \sum_{n\le x} \frac{1}{n^a} = \zeta(a) - \frac{1}{(a-1)x^{a-1}} + O(\tfrac{1}{x^a})$$

Example: Find an asymptotic formula for

$$\sum_{n\le x} \log n = \log\Big(\prod_{n\le x} n\Big) = \log(\lfloor x\rfloor!)$$

[13)] Aside:

$$\int_x^\infty \frac{\langle t\rangle}{t^2}\,\mathrm{d}t \le \int_x^\infty \frac{1}{t^2}\,\mathrm{d}t = \Big[-\frac{1}{t}\Big]_x^\infty = \frac{1}{x}$$

[14)] Aside:

$$\int_1^x \frac{1}{t^a} = \int_1^x t^{-a} = \Big[\frac{t^{-a+1}}{-a+1}\Big]_1^x = \Big[\frac{-1}{(a-1)t^{a-1}}\Big]_1^x$$

[15)] Aside:

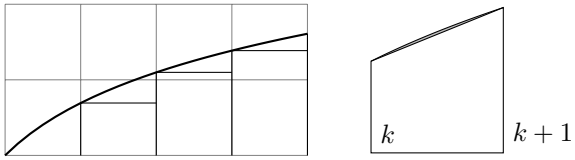
$$\int_x^\infty \frac{a\langle t\rangle}{t^{a+1}}\,\mathrm{d}t \le \int_x^\infty \frac{a}{t^{a+1}}\,\mathrm{d}t = \Big[\frac{-1}{t^a}\Big]_x^\infty = \frac{1}{x^a}$$

Solution: Use ESF with $f(t) = \log t$, $f'(t) = \frac{1}{t}$.

$$\begin{aligned}\sum_{n\le x} \log n &= f(1) + \int_1^x f(t)\,\mathrm{d}t + \int_1^x \langle t\rangle f'(t)\,\mathrm{d}t - \langle x\rangle f(x)\\ &= 0 + \int_1^x \log t\,\mathrm{d}t + \int_1^x \frac{\langle t\rangle}{t}\,\mathrm{d}t - \frac{\langle x\rangle}{x}\,^{16)}\\ &= x\log x - x + 1^{17)}\\ &= x\log x - x + O(\log x)\end{aligned}$$

Remark: If we approximate $\int_1^x \log t$ using a trapezoidal approximation, we can improve this estimate:

$$\begin{aligned}\sum_{n\le x} \log n &= x\log x - x + \tfrac{1}{2}\log x + O(1)\\ &= x\log x - x + \tfrac{1}{2}\log x + \sqrt{2\pi} + o(1)\end{aligned}$$



Example: Find an asymptotic formula for

$$\sum_{n\le x} \tau(n) = \sum_{n\le x}\sum_{d\mid n} 1$$

PMATH 740 Lecture 18: June 11, 2012

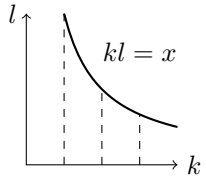
$$\sum_{n\le x} \frac{1}{n} = \log x + \gamma + O(\tfrac{1}{x})$$

$$\sum_{n\le x} \frac{1}{n^a} = \zeta(a) - \frac{1}{(a-1)x^{a-1)}} + O(\tfrac{1}{x})$$

$$\sum_{n\le x} \log n = x\log x - x + O(\log x)$$

Example: Find an asymptotic formula for $\sum_{n\le x} \tau(n)$
Solution:

$$\sum_{n\le x} \tau(n) = \sum_{n\le x}\sum_{d\mid n} 1$$



[16)] Aside: $\int_1^x \log t\,\mathrm{d}t = [t\log t - t]_1^x = x\log x + 1$
[17)] Aside: $\int_1^x \frac{\langle t\rangle}{t}\,\mathrm{d}t \le \int_1^x \frac{1}{t} = \log x$

$$\begin{aligned}\sum_{\substack{k,l\\ kl\le x}} 1 &= \sum_{k\le x}\sum_{l\le \frac{x}{k}} 1\\ &= \sum_{k\le x}\Big\lfloor \frac{x}{k}\Big\rfloor = \sum_{k\le x}\Big(\frac{x}{k} - \Big\langle \frac{x}{k}\Big\rangle\Big)\\ &= x\sum_{k\le x}\frac{1}{k} - \sum_{k\le x}\Big\langle \frac{x}{k}\Big\rangle\\ &= x(\log x + \gamma + O(\tfrac{1}{x})) + O(x)^{18)}\\ &= x\log x + \gamma x + O(1) + O(x)\\ &= x\log x + O(x)\end{aligned}$$

Example: Find a better one

Solution:
$$\begin{aligned}\sum_{n\le x}\tau(n) &= \sum_{n\le x}\sum_{d\mid n} 1\\ &= \sum_{\substack{k,l\\ kl\le x}} 1\\ &= \sum_{k^2\le x} 1 + 2\sum_{k\le\sqrt{x}}\sum_{k<l\le\frac{x}{k}} 1\\ &= \sum_{k\le\sqrt{x}} 1 + 2\sum_{k\le\sqrt{x}}\Big(\sum_{l\le\frac{x}{k}} 1 - \sum_{l\le k} 1\Big)\\ &= \lfloor\sqrt{x}\rfloor + 2\sum_{k\le\sqrt{x}}\Big(\Big\lfloor\frac{x}{k}\Big\rfloor - k\Big)\\ &= (\sqrt{x} + O(1)) + 2\sum_{k\le\sqrt{x}}\Big(\frac{x}{k} + O(1) - k\Big)\\ &= \sqrt{x} + O(1) + 2x\sum_{k\le\sqrt{x}}\frac{1}{k} - 2\sum_{k\le\sqrt{x}} k + 2O(1)\sum_{k\le\sqrt{x}} 1\end{aligned}$$

$$\begin{aligned}&\sqrt{x} + O(1) + 2x(\log\sqrt{x} + \gamma + O(\tfrac{1}{x}))\\ &\quad - 2\frac{\lfloor\sqrt{x}\rfloor(\lfloor\sqrt{x}\rfloor + 1)}{2} + O(\sqrt{x}) = \sqrt{x} + x\log x + 2\gamma x + O(\sqrt{x}) - (\sqrt{x} + O(1))(\sqrt{x} + O(1))\\ &= x\log x + 2\gamma x - x + O(\sqrt{x})\\ &= x\log x + (2\gamma - 1)x + O(\sqrt{x})\end{aligned}$$

[18)] since

$$\sum_{k\le x}\Big\langle\frac{x}{k}\Big\rangle \le \sum_{k\le x} 1 = \lfloor x\rfloor = x - \langle x\rangle = x + O(1)$$

Example: Find an asymptotic formula for $\sum_{n\le x}\sigma(n)$.

Solution:
$$\begin{aligned}
\sum_{n\le x}\sigma(n) &= \sum_{n\le x}\sum_{d|n} d \\
&= \sum_{\substack{k,l\\ kl\le x}} l = \sum_{k\le x}\sum_{l\le \frac{x}{k}} l \\
&= \sum_{k\le x} \frac{\lfloor \frac{x}{k}\rfloor(\lfloor \frac{x}{k}\rfloor+1)}{2} \\
&= \frac{1}{2}\sum_{k\le x}\Big(\frac{x}{k}+O(1)\Big)\Big(\frac{x}{k}+O(1)\Big) \\
&= \frac{1}{2}\sum_{k\le x}\Big(\frac{x^2}{k^2}+\frac{2x}{k}O(1)+O(1)\Big) \\
&= \frac{x^2}{2}\sum_{k\le x}\frac{1}{k^2} + xO(1)\sum_{k\le x}\frac{1}{k} + O(1)\sum_{k\le x}1 \\
&= \frac{x^2}{2}\Big(\zeta(2)-\frac{1}{x}+O(\frac{1}{x^2})\Big) + O(x)(\log x + O(1)) + O(x) \\
&= \frac{x^2}{2}\zeta(2) - \frac{x}{2} + O(1) + O(x\log x) \\
&= \frac{x^2}{2}\zeta(2) + O(x\log x) = \frac{\pi^2}{12}x^2 + O(x\log x)
\end{aligned}$$

Exercise: Find $\sum_{n\le x}\sigma_a(n) = \sum_{n\le x}\sum_{d|n} d^a$ for $a>1$

Example: Find an asymptotic formula for $\sum_{n\le x}\phi(n)$.

Solution:
$$\begin{aligned}
\sum_{n\le x}\phi(n) &= \sum_{n\le x}\sum_{d\mid n}\frac{\mu(d)n}{d} \quad [19)]\\
&= \sum_{\substack{k,l\\ kl\le x}}\frac{\mu(k)kl}{k} = \sum_{\substack{k,l\\ kl\le x}}\mu(k)l\\
&= \sum_{k\le x}\Big(\mu(k)\sum_{l\le \frac{x}{k}} l\Big)\\
&= \sum_{k\le x}\mu(k)\frac{\lfloor\frac{x}{k}\rfloor(\lfloor\frac{x}{k}\rfloor+1)}{2}\\
&= \frac{1}{2}\sum_{k\le x}\mu(k)\Big(\frac{x}{k}+O(1)\Big)\Big(\frac{x}{k}+O(1)\Big)\\
&= \frac{1}{2}\sum_{k\le x}\mu(k)\Big(\frac{x^2}{k^2}+\frac{x}{k}O(1)+O(1)\Big)\\
&= \frac{x^2}{2}\sum_{k\le x}\frac{\mu(k)}{k^2}+O(x)\sum\frac{\mu(k)}{k}+O(1)\sum_{k\le x}\mu(k)\\
&= \frac{x^2}{2}\Big(\sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}-\sum_{k>x}\frac{\mu(k)}{k^2}\Big)+O(x\log x)^{20)}+O(x)\\
&= \frac{x^2}{2}\Big(\frac{1}{\zeta(2)}+O(\tfrac{1}{x})\Big)^{21)}+O(x\log x)\\
&= \frac{x^2}{2}\cdot\frac{1}{\zeta(2)}+O(x)+O(x\log x)\\
&= \frac{3}{\pi^2}x^2+O(x\log x)
\end{aligned}$$

Next: $\sum\frac{\Lambda(n)}{n}=\log x+O(?)$
$\sum_{p\le x}\frac{\log p}{p}=\log x+O(?)$
$\sum_{p\le n}\frac{1}{p}=\log\log x+O(?)$

[19)] Recall:
$$N(n)=n=\sum_{d\mid n}\phi(d)$$
$$\phi(n)=\sum_{d\mid n}\frac{\mu(d)n}{d}$$

[20)] since
$$\Big|\sum_{k\le x}\frac{\mu(k)}{k}\Big|\le\sum_{k\le x}\frac{1}{k}=\log x+O(1)=O(\log x)$$
and
$$\Big|\sum_{k\le x}\mu(k)\Big|\le\sum_{k\le x}1=\lfloor x\rfloor=x-\langle x\rangle=x+O(1)=O(x)$$

[21)] since
$$\Big|\sum_{k>x}\frac{\mu(k)}{k^2}\Big|\le\sum_{k>x}\frac{1}{k^2}\le\int_{x-1}^{\infty}\frac{1}{t^2}\,\mathrm{d}t=\frac{1}{x-1}=O\Big(\frac{1}{x}\Big)$$

PMATH 740 Lecture 19: June 13, 2012

Chapter 3

$$\sum_{n\le x}\tau(n) = x\log x + (2\gamma-1)x + O(\sqrt{x})$$

$$\sum_{n\le x}\sigma(n) = \frac{\pi^2x^2}{12} + O(x\log x)$$

$$\sum_{n\le x}\phi(n) = \frac{3x^2}{\pi^2} + O(x\log x)$$

$$\pi(x) = \sum_{n\le x}\rho(n) \qquad \rho(n) = \begin{cases} 1 & \text{if } n \text{ is prime} \\ 0 & \text{otherwise} \end{cases}$$

Chapter 4

$$\sum_{n\le x}\frac{\log p}{p}$$

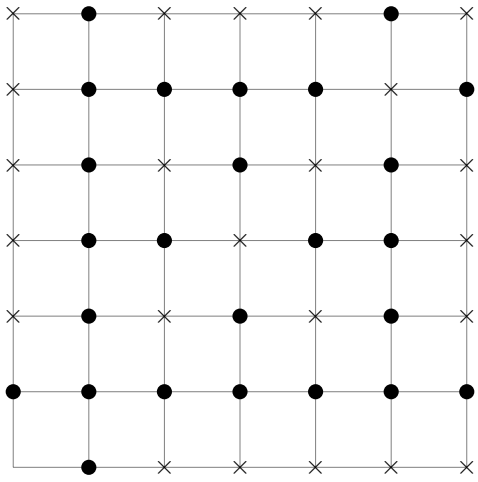
$$\sum_{n\le x}\frac{1}{p}$$

$$\frac{1}{x}\sum_{n\le x}\tau(n) \sim \log x$$

$$\frac{1}{x}\sum_{n\le x}\sigma(n) \sim \frac{\pi^2}{12}x$$

$$\frac{1}{x}\sum_{n\le x}\phi(n) \cong \frac{3}{\pi^2}x$$

Example: Find the # and the % of lattice points (a,b) visible from $(0,0)$ in the square $|a|,\ |b| \le x$.



(a,b) is visible when $\gcd(a,b) = 1$

The # of visible points (k,l) with $|a|,\ |b| \le x$ is

$$\begin{aligned} 8 + 8\sum_{k\ge 2}\phi(k) &= 8\sum_{k\ge 1}\phi(k) \\ &= 8\Big(\frac{3}{\pi^2}x^2 + O(x\log x)\Big) \\ &= \frac{24}{\pi^2}x^2 + O(x\log x) \end{aligned}$$

of (k,l) in the square $|k|,\ |l| \le x$ is

$$(2\lfloor x\rfloor + 1)^2 = (2x + O(1))^2 = 4x^2 + O(x)$$

The % of visible points is

$$\begin{aligned} \frac{\frac{24}{\pi^2}x^2 + O(x\log x)}{4x^2 + O(x)} &= \frac{\frac{24}{\pi^2} + O(\frac{\log x}{x})}{4 + O(\frac{1}{x})} \\ &\to \frac{24/\pi^2}{4} = \frac{6}{\pi^2} \text{ as } x \to \infty \end{aligned}$$

Euler's recursion formula for $\sigma(n)$

$$(1-x)(1-x^2)(1-x^3)\cdots$$

A partition of n into k parts $(a_1, a_2, \ldots, a_k)$, $1 \le a_1 \le a_2 \le \cdots \le a_k$, $\sum a_i = n$
Let $P = \{$of all partitions (of any n into any # of parts)$\}$
weight$(a_1, \ldots, a_k) = \sum a_i$

$$P = \underbrace{\{\emptyset, 1, 11, 111, \ldots\}}_{1+x+x^2+\cdots}\underbrace{\{\emptyset, 2, 22, 222, \ldots\}}_{1+x^2+x^4+\cdots}\underbrace{\{\emptyset, 3, 33, \ldots\}}_{1+x^3+x^6}, \ldots$$

$$\begin{aligned} \Phi_P &= \frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^3}\cdots \\ (1-x)(1-x^2)(1-x^3)(1-x^4)\cdots &= 1 - x^1 - x^2 - x^3 - x^4 - \cdots \\ &\quad + x^{1+2} + x^{1+3} + x^{1+4} + x^{2+3} + x^{2+4} + x^{3+4} + \cdots \\ &\quad - x^{1+2+3} - x^{1+2+4} - x^{1+3+4} - x^{2+3+4} - \cdots \\ &\quad + x^{1+2+3+4} + \cdots \end{aligned}$$

$$\therefore \prod_{k=1}^{\infty}(1-x^k) = \sum(c_n x^n)$$

where

$$c_n = (\#\text{ of parititions of } n \text{ into an even } \#\text{ of distinct parts}) - (\#\text{ of partitions of } n \text{ into an odd } \#\text{ of distinct parts})$$

$$\begin{array}{cccccccc}
1 & -x & & & & & & \\
1 & -x & -x^2 & +x^3 & & & & \\
 & & & -x^3 & +x^4 & +x^5 & -x^6 & \\
\hline
1 & -1 & -1 & 0 & 0 & 1 & 0 & 1
\end{array}
\quad
\begin{array}{ccccccc}
1 & 0 & -1 & -1 & -2 \\
-1 & 1 & 1 & 0 & 0 \\
\hline
0 & 1 & 0 & -1 & -2 \\
 & -1 & 1 & 1 & 0 \\
\hline
 & 0 & 1 & 0 & -2 \\
 & & -1 & 1 & 1 \\
\hline
 & & 0 & 1 & -1 \\
 & & & -1 & 1 \\
\hline
 & & & 0 & 0 \\
 & & & & -1 \\
\hline
 & & & & -1
\end{array}$$

$$\begin{aligned}
\prod(1-x^k) &= \sum c_n x^n \\
&= 1 - x^1 - x^2 + x^5 + x^7 - x^{12} - x^{15} + \quad + \quad - \quad -
\end{aligned}$$

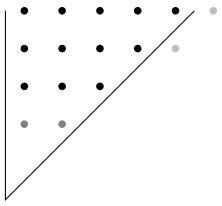
$n(3n \pm 1)/2$
Conjecture: $= \sum_{n\in\mathbb{Z}} (-1)^n x^{n(3n+1)/2}$
$1 - \sum(1-yx)(1-yx^2)(1-yx^3)$
$f(x,y) = \cdots f(xy, y)$

$\sigma(n)$

$$\begin{aligned}
f(x) &= \prod_{k=1}^{\infty}(1-x^k) \\
\log f(x) &= \sum \log(1-x^k) \\
\frac{f'}{f} &= \sum_{k=1}^{\infty} \frac{-kx^{k-1}}{1-x^k} = \frac{-1}{1-x} - \frac{2x}{1-x^2} - \frac{3x^2}{1-x^3} - \cdots \\
-\frac{xf'}{f} &= \begin{array}{ccccccccccc}
1 & +x & +x^2 & +x^3 & +x^4 & +x^5 & +x^6 & +x^7 & & +\cdots \\
 & +2x & & +2x^3 & & +2x^5 & & +2x^7 & & +\cdots \\
 & & +3x^2 & & & +3x^5 & & & +3x^8 & +\cdots \\
 & & & +4x^3 & & & & +4x^7 & & +\cdots
\end{array} \\
&= \sum \sigma(n) x^{n-1} \\
f(x) &= 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots \\
f' &= -1 - 2x + 5x^4 + 7x^6 - 12x^{11} - 15x^{14} + \cdots \\
\sum \sigma(n)x^{n-1} = -\frac{xf'}{f} &= \frac{-x - 2x^2 + 5x^6 + 7x^7 - 12x^{12} - 15x^{15} + \cdots}{1 - x - x^2 + \cdots} \\
&= (\sigma(1) + \sigma(2)x + \sigma(3)x^2 + \cdots)(1 - x - x^2 + x^5 + x^7 - \cdots) \\
&= (-1 - 2x^2 + 5x^5 - 7x^7 - 12x^{12} + \cdots)
\end{aligned}$$

This gives Euler Recursion Formula

$3 + 5 + 6 = 14$



PMATH 740 Lecture 20: June 15, 2012

A3 typos
2c)
3b) $I(n-1) \overset{\geq}{\not\leq} I(n-\frac{1}{2}) \overset{\geq}{\not\leq}$
$\overset{\pi/2}{\not\pi} = \lim(\frac{2}{1}\frac{2}{3}\cdots)$
4a) $\frac{f'(k)-f'(k+1)}{4}$
$\sum \log k = n\log n - n + \frac{1}{2}\log n + c_n$
$\overset{e^{c_n}}{\not c_n} \to \sqrt{2\pi}$

Euler's Proof of Pentagonal Number Theorem
ref Math Magazine
Vol 56 #5, Nov 1983
(by G. Andrews)
G. Polya Math & Plausible Reasoning
Vol I

Theorem:

$$\prod_{n=1}^{\infty}(1-x^n) = 1 + \sum_{n=1}^{\infty}(-1)^n(x^{n(3n-1)/2} + x^{n(3n+1)/2})$$

Sketch Proof: Let

$$\begin{aligned} f(x,y) &= 1 - \sum_{n=1}^{\infty}(1-xy)(1-x^2y)\cdots(1-x^{n-1}y)x^ny^{n+1} \\ &= \lim_{n\to\infty} f_l(x,y) \\ f_l(x,y) &= 1 - \sum_{n=1}^{l}(1-xy)(1-x^2y)\cdots(1-x^{n-1}y)x^ny^{n+1} \end{aligned}$$

verify inductively that

$$\begin{aligned} f_l(x,1) &= (1-x)(1-x^2)\cdots(1-x^l) \\ \text{so } f(x,1) &= \prod_{n=1}^{\infty}(1-x^n). \end{aligned}$$

Verify that $f(x,y)$ satisfies the recursion formula (or functional equation)

$$f(x,y) = 1 - xy^2 - x^2y^3 f(x,xy)$$

Use this (repeatedly) to show that

$$\begin{aligned} f(x,y) = 1 &+ \sum_{n=1}^{l-1}(-1)^n(x^{n(3n-1)/2}y^{3n-1} + x^{n(3n+1)/2}y^{3n}) \\ &+ (-1)^l(x^{l(3l-1)/2}y^{3l-1} + x^{l(3l+1)/2}y^{3l})f(x,xy^l) \end{aligned}$$

Let $l \to \infty$ then take $y = 1$.

$$\sum_{p \le x} \frac{\log p}{p} \quad \sum_{p \le x} \frac{1}{p} \quad \sum_{n \le x} \frac{\Lambda(n)}{n}$$

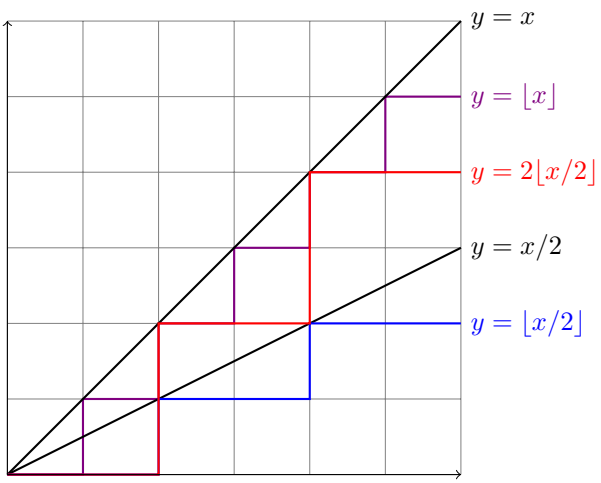
Lemma: (Shapiro) Let $a\colon \mathbb{Z}^+ \to [0, \infty)$.
If $\sum_{n \le x} a(n) \lfloor \frac{x}{n} \rfloor = x \log x + O(x)$ then $\sum_{n \le x} a(n) \frac{x}{n} = x \log x + O(x)$ so $\sum_{n \le x} \frac{a(n)}{n} = \log x + O(1)$.
Proof: Suppose $\sum_{n \le x} a(n) \lfloor \frac{x}{n} \rfloor = x \log x + O(x)$

$$\begin{aligned} \text{Then } \sum_{n \le x} a(n) \frac{x}{n} &= \sum_{n \le x} a(n) \left(\left\lfloor \frac{x}{n} \right\rfloor + \left\langle \frac{x}{n} \right\rangle \right) \\ &= \sum_{n \le x} a(n) \left\lfloor \frac{x}{n} \right\rfloor + \sum_{n \le x} a(n) \left\langle \frac{x}{n} \right\rangle \\ &= x \log x + O(x) + \sum_{n \le x} a(n) \left\langle \frac{x}{n} \right\rangle \end{aligned}$$

and $\left| \sum_{n \le x} a(n) \langle \frac{x}{n} \rangle \right| \le \sum_{n \le x} a(n)$.
So if suffices to show that $\sum_{n \le x} a(n) = O(x)$.

Let $S(x) = \sum_{n \le x} a(n)$ and $T(x) = \sum_{n \le x} a(n) \lfloor \frac{x}{n} \rfloor$. Then

$$\begin{aligned} T(x) - 2T(\tfrac{x}{2}) &= \sum_{n \le x} a(n) \left\lfloor \frac{x}{n} \right\rfloor - 2 \sum_{n \le \frac{x}{2}} a(n) \left\lfloor \frac{x}{2n} \right\rfloor \\ &= \sum_{n \le \frac{x}{2}} a(n) \Big(\underbrace{\left\lfloor \frac{x}{n} \right\rfloor - 2 \left\lfloor \frac{x}{2n} \right\rfloor}_{\in \{0,1\}} \Big) + \sum_{\frac{x}{2} < n \le x} a(n) \left\lfloor \frac{x}{n} \right\rfloor \end{aligned}$$



$$\begin{aligned} &\ge \sum_{\frac{x}{2} < n \le x} a(n) \left\lfloor \frac{x}{n} \right\rfloor \\ &= \sum_{\frac{x}{2} < n \le x} a(n) \end{aligned}$$

since for $\frac{x}{2} < n \le x$ we have

$$\frac{x}{2} < n \implies \frac{x}{n} < 2, \qquad n \le x \implies \frac{x}{n} \ge 1 \text{ so } \left\lfloor \frac{x}{n} \right\rfloor = 1$$

$$\begin{aligned}
&= \sum_{n \le x} a(n) - \sum_{n \le \frac{x}{2}} a(n) \\
&= S(x) - S(\tfrac{x}{2}) \\
\therefore S(x) - S(\tfrac{x}{2}) &= T(x) - 2(\tfrac{x}{2}) \\
&= (x \log x + O(x)) - 2(\tfrac{x}{2} \log \tfrac{x}{2} + O(\tfrac{x}{2})) \\
&= (x \log x + O(x)) - (x \log x - x \log 2 + O(x)) \\
&= O(x)
\end{aligned}$$

Choose $c > 0$ so that $S(x) - S(\frac{x}{2}) \le cx$ for large x, say $x \ge a$. We have $S(x) = \sum_{n \le x} a(n)$ for $x \ge 1$ and we set $S(x) = 0$ for $x < 1$. Modify c so that $S(x) - S(\frac{x}{2}) \le cx$ for all $x > 0$ (since $S(x)$ is bounded for $1 \le x \le n$). Then we have

$$\begin{aligned}
S(x) - S(\tfrac{x}{2}) &\le cx \\
S(\tfrac{x}{2}) - S(\tfrac{x}{4}) &\le \tfrac{cx}{2} \\
S(\tfrac{x}{4}) - S(\tfrac{x}{8}) &\le \tfrac{cx}{4} \\
&\vdots
\end{aligned}$$

eventually $S(\frac{x}{2^n}) = 0$. Add those to get

$$\begin{aligned}
S(x) &\le cx(1 + \tfrac{1}{2} + \tfrac{1}{4} + \cdots) \\
&\le 2cx \\
\therefore S(x) &= O(x)
\end{aligned}$$

Example: Find an asymptotic formula for $\sum_{n \le x} \frac{\Lambda(n)}{n}$

$$\left(\text{where } \Lambda(n) = \begin{cases} \log p & \text{when } n = p^k \text{ is a prime power} \\ 0 & \text{otherwise} \end{cases}\right)$$

Solution: [incorrect?]

$$\begin{aligned}
\sum_{n \le x} \frac{\Lambda(n)}{n} &= \sum_{p^k \le x} \frac{\log p}{p^k} \\
&= \sum_{p \le x} \sum_{\substack{k \ge 1 \\ p^k \le x}} \frac{\log p}{p^k} \\
&= \sum_{p \le x} \left(\log p \sum_{\substack{k \ge 1 \\ p^k \le x}} \frac{1}{p^k} \right)
\end{aligned}$$

Solution: Consider $\sum_{n\le x}\Lambda(n)\lfloor\frac{x}{n}\rfloor$

$$\begin{aligned}
\sum_{n\le x}\Lambda(n)\Big\lfloor\frac{x}{n}\Big\rfloor &= \sum_{p^k}\log p\Big\lfloor\frac{x}{p^k}\Big\rfloor \\
&= \sum_{p\le x}\log p\sum_{\substack{k\ge 1\\ p^k\le x}}\Big\lfloor\frac{x}{p^k}\Big\rfloor \\
&= \sum_{p\le m}\log p\sum_{k\text{ st }p^k\le m}\Big\lfloor\frac{m}{p^k}\Big\rfloor \text{ where } m=\lfloor x\rfloor \\
&= \sum_{p|m!}(\log p)e_p(m!)^{22)} \\
\exp\Big(\sum_{n\le x}\Lambda(n)\Big\lfloor\frac{x}{n}\Big\rfloor\Big) &= \prod_{p|m!}\exp(e_p(m!)\log p) \\
&= \prod_{p|m!}p^{e_p(m!)} = m! \\
\sum_{n\le x}\Lambda(n)\Big\lfloor\frac{x}{n}\Big\rfloor &= \log(m!) = \log(\lfloor x\rfloor!) \\
&= x\log x - x + \tfrac{1}{2}\log x + O(1)
\end{aligned}$$

By Shapiro's Lemma

$$\sum_{n\le x}\Lambda(n)\frac{x}{n} = x\log x + O(x)$$
$$\therefore \sum_{n\le x}\frac{\Lambda(n)}{n} = \log x + O(1)$$

Exercise: Use this to get an asymptotic formula for

$$\sum_{p\le x}\frac{\log p}{p}.$$

Challenging exercise: Get an asymptotic formula for

$$\sum_{p\le x}\frac{1}{p}.$$

PMATH 740 Lecture 21: June 18, 2012

Chapter 4

$$\sum_{p\le x}\frac{\log p}{p} \qquad \sum_{p\le x}\frac{1}{p}$$

Shapiro For $a\colon \mathbb{Z}^+\to[0,\infty)$ if $\sum a(n)\lfloor\frac{x}{n}\rfloor = x\log x + O(x)$ then $\sum a(n)\frac{x}{n} = x\log x + O(x)$

$$\therefore \sum\frac{a(n)}{n} = \log x + O(1)$$

22) since $\Big\lfloor\frac{x}{p^k}\Big\rfloor = \Big\lfloor\frac{\lfloor x\rfloor}{p^k}\Big\rfloor$

Example: $\displaystyle\sum_{n\le x}\frac{\Lambda(n)}{n}=\log x+O(1)$

Example: Find an asymptotic formula for $\sum_{p\le x}\frac{\log p}{p}$
Solution:

$$\Lambda(n)=\begin{cases}\log p & \text{when } n=p^k \text{ with } p \text{ prime}\\ 0 & \text{otherwise}\end{cases}$$

$$\begin{aligned}\sum_{n\le x}\frac{\Lambda(n)}{n}&=\sum_{p^k\le x}\frac{\log p}{p^k}\\ &=\sum_{p\le x}\sum_{\substack{k\ge 1\\ p^k\le x}}\frac{\log p}{p^k}\\ &=\sum_{p\le x}\Big(\frac{\log p}{p}+\sum_{\substack{k\ge 2\\ p^k\le x}}\frac{\log p}{p^k}\Big)\\ \therefore\sum_{n\le x}\frac{\log p}{p}&=\sum_{n\le x}\frac{\Lambda(n)}{n}-\sum_{p\le x}\sum_{\substack{k\ge 2\\ p^k\le x}}\frac{\log p}{p^k}\\ &=\log x+O(1)+\sum_{p\le x}\sum_{\substack{k\ge 2\\ p^k\le x}}\frac{\log p}{p^k}\end{aligned}$$

$$\begin{aligned}\textit{and}\ \sum_{p\le x}\sum_{\substack{k\ge 2\\ p^k\le x}}\frac{\log p}{p^k}&\le\sum_{p\le x}\sum_{k\ge 2}\frac{\log p}{p^k}\\ &=\sum_{p\le x}\log p\Big(\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\cdots\Big)\\ &=\sum_{p\le x}\frac{\log p}{p(p-1)}\\ &\le\sum_{n=1}^{\infty}\frac{\log n}{n(n-1)}\ \text{which converges}\\ \therefore\sum_{p\le x}\frac{\log p}{p}&=\log x+O(1)\end{aligned}$$

Example: Find an asymptotic formula for $\sum_{p\le x}\frac{1}{p}$.
Solution: We use Abel's Summation Formula[23] with

$$a(n)=\begin{cases}\frac{\log p}{p} & \text{when } n=p \text{ is prime}\\ 0 & \text{when } n \text{ is not prime}\end{cases}$$

[23] $\sum a(n)f(n)=A(x)f(x)-\int_1^x A(t)f'(t)\,\mathrm{d}t$

and $f(x) = \frac{1}{\log x}$ to get

$$\begin{aligned}
\sum_{n\le x}\frac{1}{p} &= \sum_{n\le x} a(n)f(n)\\
&= A(x)f(x) - \int_1^x A(t)f'(t)\,\mathrm{d}t\\
\text{where } A(x) &= \sum_{n\le x} a(n)\\
&= \sum_{p\le x}\frac{\log p}{p}\\
&= \Big(\sum_{p\le x}\frac{\log p}{p}\Big)\Big(\frac{1}{\log x}\Big) - \int_1^x \Big(\sum_{p\le t}\frac{\log p}{p}\Big)\Big(\frac{-1}{t(\log t)^2}\Big)\,\mathrm{d}t\\
&= \Big(\log x + O(1)\Big)\Big(\frac{1}{\log x}\Big) + \int_2^x \frac{\log t + g(t)}{t(\log t)^2}\,\mathrm{d}t \text{[24]}\\
&\qquad\qquad \text{where } g(t) = \Big(\sum_{p\le t}\frac{\log p}{p} - \log t\Big) = O(1)\\
&= 1 + O\Big(\frac{1}{\log x}\Big) + \int_2^x \frac{1}{t\log t}\,\mathrm{d}t + \int_2^x \frac{g(t)}{t(\log t)^2}\,\mathrm{d}t\\
&= 1 + O\Big(\frac{1}{\log x}\Big) + \Big[\log\log t\Big]_2^x + \int_2^\infty \frac{g(t)}{t(\log t)^2}\,\mathrm{d}t - \int_x^\infty \frac{g(t)}{t(\log t)^2}\,\mathrm{d}t\\
&= 1 + O\Big(\frac{1}{\log x}\Big) + \log\log x - \log\log 2 + a + O\Big(\frac{1}{\log x}\Big) \text{[25]}\\
\therefore \sum_{n\le p}\frac{1}{p} &= \log\log x + c + O\Big(\frac{1}{\log x}\Big)
\end{aligned}$$

for some constant c

$$\Big(c = 1 - \log\log 2 + a = \lim_{x\to\infty}\Big(\sum_{n\le x}\frac{1}{p} - \log\log x\Big)\Big)$$

Example: (To motivate Dirichlet Characters)
Find an asymptotic formula for $\sum_{n=k \bmod l}\binom{m}{n}$ where m, k, $l \in \mathbb{Z}^+$.

Solution: $\displaystyle\sum_{n\ge 0}\binom{m}{n} = (1+1)^m = 2^m$ [26].

Take $k = 0$. Find

$$\sum_{n=0 \bmod l}\binom{m}{n} = \binom{m}{0} + \binom{m}{l} + \binom{m}{2l} + \cdots$$

(**Answer:** $\sim \frac{1}{l}2^m$)

---

[24] note that $A(x) = 0$ for $x < 2$

[25] since if we choose b so that $|g(t)| \le b$ then

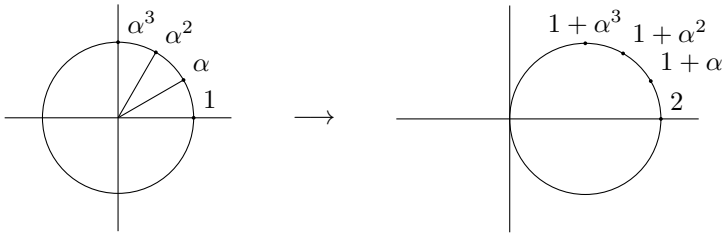
$$\Big|\int_x^\infty \frac{g(t)}{t(\log t)^2}\,\mathrm{d}t\Big| \le b\int_x^\infty \frac{\mathrm{d}t}{t(\log t)^2} = b\Big[\frac{-1}{\log t}\Big]_x^\infty = \frac{b}{\log x}.$$

[26] Aside:

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1) \qquad \sum_{\substack{p=k \bmod l\\ k\in U_l}}\frac{\log p}{p} = \frac{1}{\phi(l)}\log x + O(?)$$

Let $\alpha = e^{i2\pi/l}$. $C_l = \{1, \alpha, \alpha^2, \ldots, \alpha^{l-1}\}$, $\sum_{i=0}^{l-1} \alpha^i = 0$.

$$
\begin{aligned}
(1+1)^m &= \binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \cdots \\
(1+\alpha)^m &= \binom{m}{0} + \binom{m}{1}\alpha + \binom{m}{2}\alpha^2 + \cdots \\
(1+\alpha^2)^m &= \binom{m}{0} + \binom{m}{1}\alpha^2 + \binom{m}{2}\alpha^4 + \cdots \\
&\vdots \\
(1+\alpha^{l-1})^m &= \cdots \\
\sum_{i=1}^{l-1}(1+\alpha^i)^m &= \sum_{n=0 \bmod l} l\binom{m}{n} \\
\sum_{n=0 \bmod l} \binom{m}{n} &= \frac{1}{l}\sum_{i=0}^{l-1}(1+\alpha^i)^m \\
&= \frac{1}{l}\Big(2^m + \sum_{i=1}^{l-1}(1+\alpha^i)^m\Big)
\end{aligned}
$$



$$
\begin{aligned}
\Big|\sum_{i=1}^{l-1}(1+\alpha^i)^m\Big| &\le (l-1)|1+\alpha|^m \\
&= (l-1)\sqrt{\Big(1+\cos\frac{2\pi}{l}\Big)^2 + \Big(\sin\frac{2\pi}{l}\Big)^2}^m \\
&= (l-1)\sqrt{2+2\cos\frac{2\pi}{l}}^m \quad {}^{27)} \\
&= (l-1)\Big(2\cos\frac{\pi}{l}\Big)^m \\
&= O\Big(\Big(2\cos\frac{\pi}{l}\Big)^m\Big) \\
\therefore \sum_{n=0 \bmod l}\binom{m}{n} &= \frac{1}{l}2^m + O\Big(\Big(2\cos\frac{\pi}{l}\Big)^m\Big)
\end{aligned}
$$

To get $\sum_{n=k \bmod l}\binom{m}{n}$ find $\sum_{i=0}^{l-1}\alpha^{-ik}(1+\alpha^i)^m$. $\alpha^{-ik} = (\overline{\alpha}^k)^i$

27)

$$
\begin{aligned}
\cos^2\theta &= \frac{1+\cos 2\theta}{2} \\
4\cos^2\theta &= 2 + 2\cos 2\theta
\end{aligned}
$$

PMATH 740 Lecture 22: June 20, 2012

Midterm this Wednesday 4:30–6:00
A1, A2, A3 + $\sum \frac{\Lambda(n)}{n}$, $\sum \frac{\log p}{p}$, $\sum \frac{1}{p}$

Example: (Motivation)
Find an asymptotic formula for

$$\sum_{n=k \bmod l} \binom{m}{n}$$

where k, $l \in \mathbb{Z}^+$.
Solution: Let $\alpha = e^{i2\pi/l}$

$$\sum_{i=0}^{l-1} \alpha^i = 0$$

$$\sum_{i=0}^{l-1} \alpha^{in} = \begin{cases} l & \text{if } n = 0 \bmod l \\ 0 & \text{if } n \neq 0 \bmod l \end{cases}$$

$$\sum_{i=0}^{l-1} \alpha^{i(k-n)} = \begin{cases} l & \text{if } n = k \bmod l \\ 0 & \text{otherwise} \end{cases}$$

$$(1+\alpha^i) = \sum_n \binom{m}{n} \alpha^{in}$$

$$\alpha^{-ik}(1+\alpha^i) = \sum_n \binom{m}{n} \alpha^{i(n-k)}$$

$$\sum_{i=0}^{l-1} \alpha^{-ik}(1+\alpha^i) = \sum_n \binom{m}{n} \sum_{i=0}^{l-1} \alpha^{i(n-k)}$$

$$= l \sum_{n=k \bmod l} \binom{m}{n}$$

$$\therefore \sum_{n=l \bmod l} \binom{m}{n} = \frac{1}{l} \sum_{i=0}^{l-1} \alpha^{-ik}(1+\alpha^i)^m$$

$$\sim \frac{1}{l} 2^m$$

(the α^i are the characters of $\mathbb{Z}_l$)

$$\sum_{i=0}^{l-1} \sum_{p \leq x} \frac{\alpha^{-ik}\alpha^{ip}}{p} = l \sum_{p=k \bmod l} \frac{1}{p}$$

An n-dimensional representation of a group G is a homomorphism

$$\rho \colon G \to \mathrm{GL}(n, \mathbb{C}).$$

The *character* of ρ is the map $\chi \colon G \to \mathbb{C}$ given by

$$\chi(a) = \operatorname{trace} \rho(a).$$

Definition: A (linear) *character* of a group G is a homomorphism

$$\chi \colon G \to \mathbb{C}^*.$$

The set of characters

$$\hat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$$

is a group called the character group.
(More generally, for any group G, H, $\mathrm{Hom}(G, H)$ is a group under

$$\begin{gathered}(fg)(x) = f(x)g(x) \\ \text{with } (f^{-1})(x) = f(x)^{-1} \\ 1(x) = 1)\end{gathered}$$

Example: Let $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_l}$ and let H be an abelian group. Find $\mathrm{Hom}(G, H)$.
Solution: A homomorphism $f\colon G \to H$ is determined by the values $f(e_i)$ where $e_i = (0, \ldots, 0, \underset{i\text{th}}{1}, 0, \ldots, 0)$.
Indeed if $f(e_i) = a_i \in H$ then

$$f(k_1, \ldots, k_l) = f\Big(\sum k_i e_i\Big) = \prod f(e_i)^{k_i} = \prod a_i^{k_i}.$$

Also note that if $f(e_i) = a_i$ then

$$a_i^{n_i} = f(n_i) = f(0) = 1$$

so $\mathrm{ord}(a_i) \mid n_i$. Conversely, given $a_i \in H$ with $\mathrm{ord}(a_i) \mid n_i$ we can define $f_{a_1,\ldots,a_l}\colon G \to H$ b

$$f_{a_1,\ldots,a_l}(k_1, \ldots, k_l) = \prod_{i=1}^{l} a_i^{k_i}$$

and then f is a homomorphism

$$\therefore \mathrm{Hom}(G, H) = \{\, f_{a_1,\ldots,a_l} : a_i \in H,\, \mathrm{ord}(a_i) \mid n_i \,\}.$$

In particular for $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_l}$

$$\begin{aligned}\hat{G} &= \mathrm{Hom}(G, \mathbb{C}^*) \\ &= \{\, f_{a_1,\ldots,a_l} : a_i \in \mathbb{C}^*,\, \mathrm{ord}(a_i) \mid n_i \,\} \\ &= \{\, f_{a_1,\ldots,a_l} : a_i \in C_{n_i} \,\}\end{aligned}$$

where $C_n = \{\, z \in \mathbb{C}^* : z^n = 1 \,\}$.

$$\text{so } |\hat{G}| = \prod n_i = |G|$$

Moreover we have an isomorphism $\Phi\colon G \to \hat{G}$ given by $\Phi(e_j) = e^{i2\pi/n_j}$ so

$$\Phi(k_1, \ldots, k_l) = (e^{i2\pi k_1/n_1}, \ldots, e^{i2\pi k_l/n_l})$$

More generally (using the Classification of Finite Abelian Groups) for every finite abelian group G,

$$G \cong \hat{G}.$$

Example: The characters of $\mathbb{Z}_l$ are the homomorphisms

$$\begin{gathered}\chi_k\colon \mathbb{Z}_l \to \mathbb{C}^* \\ \chi_k(1) = e^{i2\pi k/l} \\ \chi_k(a) = e^{i2\pi ka/l}\end{gathered}$$

Theorem: (Orthogonality Relations)
Let G be a finite abelian group. Then

(1) for $a \in G$, $\sum_{\chi \in \hat{G}} = \begin{cases} |G| & \text{if } a = 1 \\ 0 & \text{otherwise} \end{cases}$

(2) for $\chi \in \hat{G}$

$$\sum_{a \in G} \chi(a) = \begin{cases} |G| & \text{if } \chi = \mathbf{1} \\ 0 & \text{otherwise} \end{cases}$$

(3) for $a, b \in G$

$$\sum_{\chi \in \hat{G}} \chi(a)\overline{\chi}(b) = \begin{cases} |a| & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases}$$

(4) for $\chi, \psi \in \hat{G}$

$$\sum_{a \in G} \chi(a)\overline{\psi}(a) = \begin{cases} |G| & \text{if } \chi = \psi \\ 0 & \text{otherwise} \end{cases}$$

Proof:

(1) Let $a \in G$.
If $a = 1$ then $\chi(a) = 1$ for all $\chi \in \hat{G}$ so $\sum_{\chi \in \hat{G}} \chi(a) = |\hat{G}| = |G|$.

(2) If $a \neq 1$ then verify that there exists $\psi \in \hat{G}$ with $\psi(a) \neq 1$

$$1 \cdot \sum_{\chi \in \hat{G}} \chi(a) = \sum_{\chi \in \hat{G}} (\psi\chi)(a)$$

(since multiplying by ψ permutes the elements of $\hat{G}$)

$$= \sum_{\chi \in \hat{G}} \psi(a)\chi(a)$$
$$= \psi(a) \sum_{\chi \in \hat{G}} \chi(a)$$
$$(1 - \psi(a)z) \sum_{\chi \in \hat{G}} \chi(a) = 0$$
$$\therefore \sum_{\chi \in \hat{G}} \chi(a) = 0$$

since $\psi(a) \neq 1$.

(3) is similar

(4) and (4) follow

Definition: Given a character $\chi \colon U_l \to \mathbb{C}^*$ we associate a map (also denoted by χ) $\chi \colon \mathbb{Z} \to \mathbb{C}^*$ defined by

$$\chi(k^{28)}) = \begin{cases} \chi(k^{29)}) & \text{if } \gcd(k, l) = 1 \text{ so } k \in U_l \\ 0 & \text{if } \gcd(k, l) \neq 1 \end{cases}$$

The map $\chi \colon \mathbb{Z} \to \mathbb{C}^*$ is called a *Dirichlet character*. Note that it is completely multiplicative and periodic.

[28)] $\in \mathbb{Z}$
[29)] $\in U_l$

PMATH 740 Lecture 23: June 22, 2012

For $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_l}$, H abelian

$$\mathrm{Hom}(G,H) = \{\, f_{a_1,\ldots,a_l} : \text{each } a_i \in H,\ a_i^{n_i} = 1 \,\}$$

$f_{a_1,\ldots,a_l}(k_1,\ldots,k_l) = \prod a_i^{k_i}$

$$\hat{G} = \mathrm{Hom}(G,\mathbb{C}^*) = \{\, f_{a_1,\ldots,a_l} : \text{each } a_i \in C_{n_i} \,\}$$

$$\begin{aligned}
\hat{G} &= \mathrm{Hom}(G,\mathbb{C}^*) \\
&= \mathrm{Hom}(G,\mathbb{S}) \qquad \mathbb{S} = \{\, z \in \mathbb{C}^* : |z| = 1 \,\} \\
&= \mathrm{Hom}\Big(G, \bigcup_{n=1}^{\infty}\Big) \qquad e^{i2\pi q} \qquad q \in \mathbb{Q}/\mathbb{Z} \\
&\cong \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})
\end{aligned}$$

$G \cong \hat{G}$ under $\Phi\colon G \to \hat{G}$ defined by

$$\begin{aligned}
\Phi(e_j) &= f_{1,\ldots,1,e^{i2\pi/n_j},1,\ldots,1} \\
\Phi(k_1,\ldots,k_l) &= f_{(e^{i2\pi k_1/n_1},\ldots,e^{i2\pi k_l/n_l})}
\end{aligned}$$

For $\chi \in \hat{U}_l$ we associate the Dirichlet character

$$\chi\colon \mathbb{Z} \to \mathbb{C}^*$$

given by

$$\chi(k^{30)}) = \begin{cases} \chi(k) & \text{if } \gcd(k,l) = 1 \text{ so } k \in U_l \\ 0 & \text{otherwise} \end{cases}$$

Notes: $\chi\colon \mathbb{Z} \to \mathbb{C}^*$ is periodic with period l.
$\chi(k)$ is a $\phi(l)^k$ root of 1 for all $k \in \mathbb{Z}$.
χ is completely multiplicative.
χ satisfies the following orthogonality relations[31)] for $n \in \mathbb{Z}$,

$$\sum_{\chi \in \hat{U}_l} \chi(n) = \begin{cases} \phi(l) & \text{if } n = 1 \bmod l \\ 0 & \text{otherwise} \end{cases}$$

for $n,\ k \in \mathbb{Z}$,

$$\sum_{\chi \in \hat{U}_l} \chi(n)\overline{\chi}(k) = \begin{cases} \phi(l) & \text{if } n = k \bmod l \\ 0 & \text{otherwise} \end{cases}$$

---

30) $\in U_l$

31) Aside: for $a \in U_l$,

$$\sum_{\chi \in \hat{U}_l} \chi(a) = \begin{cases} \phi(l) & \text{if } a = 1 \\ 0 & a \neq 1 \end{cases}$$

for $\chi \in \hat{U}_l$,

$$\sum_{a \in U_l} \chi(a) = \begin{cases} \phi(l) & \text{if } \chi = \mathbf{1} \\ 0 \end{cases}$$

for $a,\ b \in U_l$,

$$\sum_{\chi \in \hat{U}_l} \chi(a)\overline{\chi}(b) = \begin{cases} \phi(l) & \text{if } a = b \\ 0 \end{cases}$$

for $\chi \in \hat{U}_l$,

$$\sum_{k=0}^{l-1} \chi(k) = \begin{cases} \phi(l) & \text{if } \chi = \mathbf{1} \\ 0 & \text{otherwise} \end{cases}$$

for χ, $\psi \in \hat{U}_l$

Question: Does $\sum_{n=1}^{\infty} \frac{\alpha^n}{n}$ converge where $\alpha = e^{i2\pi/l}$?
Does $\sum_{n=1}^{\infty} \frac{\chi(n)}{n}$ converge?

Theorem: Let $f\colon [1,\infty) \to \mathbb{R}^+$ by $\mathcal{C}^1$ and eventually decreasing with $\lim_{x\to\infty} f(x) = 0$. Let $\chi \in \hat{U}_l$ with $\chi \neq \mathbf{1}$. Then $\sum_{n=1}^{\infty} \chi(n) f(n)$ converges and

$$\sum_{n\le x} \chi(n) f(n) = \sum_{n=1}^{\infty} \chi(n) f(n) + g(x)$$

where $|g(x)| \le \phi(l)|f(x)|$ so $g(x) = O(f(x))$.
Proof: Let $A(x) = \sum_{n\le x} \chi(n)$.
Since $\chi(n)$ is periodic and

$$A(l) = \sum_{n=1}^{\infty} \chi(n) = 0$$

$\therefore A(n)$ is periodic.
We have

$$|A(x)| = \max_{1\le k\le l} |A(k)| = \max_{1\le k\le l} |\chi(1) + \chi(2) + \cdots + \chi(k)|$$

We have $\chi(1) + \chi(2) + \cdots + \chi(k) + \chi(k+1) + \cdots + \chi(l) = 0$

$$|\chi(1) + \cdots + \chi(k)| = |\chi(k+1) + \cdots + \chi(l)|$$

$$\begin{aligned} \text{LS} &\le a = \#\text{ of } i \text{ with } 1 \le i \le k \text{ such that } \gcd(i,l) = 1 \\ \text{RS} &\le b = \#\text{ of } i \text{ with } k+1 \le i \le l \text{ with } \gcd(i,l) = 1 \\ a + b &= \phi(l) \\ \text{LS} &\le \min(a,b) \le \frac{\phi(l)}{2} \\ \therefore |A(x)| &\le \frac{\phi(l)}{2} \text{ for all } x. \end{aligned}$$

Consider the sum $\sum_{n=1}^{\infty} \chi(n) f(n)$.
For $x < y$. By Abel's Summation Formula,

$$\begin{aligned} \sum_{n\le y} \chi(n) f(n) - \sum_{n\le x} \chi(n) f(n) &= A(y)f(y) - \int_1^y A(t) f'(t)\,\mathrm{d}t - A(x)f(x) + \int_1^x A(t) f'(t)\,\mathrm{d}t \\ &= A(y)f(y) - A(x)f(x) - \int_x^y A(t) f'(t)\,\mathrm{d}t \end{aligned}$$

Each term can be made (arbitrarily) small by choosing x large and $y > x$ since

$$|A(y)f(y)| \le \frac{\phi(l)}{2}|f(y)| \le \frac{\phi(l)}{2} f(x) \to 0$$

(since f is eventually decreasing)

$$|A(x)f(x)| \le \frac{\phi(l)}{2} f(x) \to 0$$

and

$$\begin{aligned}\Big|\int_x^y A(t)f'(t)\,\mathrm{d}t\Big| &\le \int_x^y |A(t)||f'(t)|\,\mathrm{d}t\\ &\le \int_x^\infty |A(t)||f'(t)|\,\mathrm{d}t\\ &\le \frac{\phi(l)}{2}\int_x^\infty |f'(t)|\,\mathrm{d}t\\ &= \frac{\phi(l)}{2}\int_x^\infty -f'(t)\,\mathrm{d}t\\ &= \frac{\phi(l)}{2}\Big[-f(t)\Big]_x^\infty\\ &= \frac{\phi(l)}{2}f(x) \qquad (\text{since } f(t)\to 0 \text{ as } f\to\infty)\\ &\to 0\end{aligned}$$

By Cauchy's Criterion,

$$\sum_{n=1}^\infty \chi(n)f(n) \text{ converges}$$

Also, taking the limit as $y\to\infty$ gives

$$\sum_{n=1}^\infty \chi(n)f(n) - \sum_{n\le x}\chi(n)f(n) = -A(x)f(x) - \int_x^\infty A(t)f'(t)\,\mathrm{d}t$$

so

$$\sum_{n\le x}\chi(n)f(n) = \sum_{n=1}^\infty \chi(n)f(n) + g(x)$$

where

$$g(x) = A(x)f(x) + \int_x^\infty A(t)f'(t)\,\mathrm{d}t$$

and

$$\begin{aligned}|A(x)f(x)| &\le \frac{\phi(l)}{2}f(x)\\ \Big|\int_x^\infty A(t)f'(t)\,\mathrm{d}t\Big| &\le \int_x^\infty |A(t)||f'(t)|\,\mathrm{d}t\\ &\le \frac{\phi(l)}{2}\int_x^\infty -f'(t)\,\mathrm{d}t\\ &= \frac{\phi(l)}{2}f(x)\end{aligned}$$

so

$$g(x)\le \phi(l)f(x)$$

for large x.

Example: $\sum_{n=1}^\infty \frac{\chi(n)}{n}$ converges and $\sum_{n\le x}\frac{\chi(n)}{n} + g(x)$ with $|g(x)|\le \phi(l)\frac{1}{x}$
$\sum_{n=1}^\infty \frac{\chi(n)\log n}{n}$ converges

$$\sum_{n\le x}\frac{\chi(n)\log n}{n} = \sum_{n=1}^\infty \frac{\chi(n)\log n}{n} + g(x)$$

with $|g(x)| \leq \phi(l)\frac{\log x}{x}$ for large x.

$$\sum_{\substack{p\leq x \\ p=k \bmod l}} \frac{\log p}{p} = \frac{1}{\phi(l)}\log\log x + O(1)$$

$$\sum \frac{\log p}{p} \approx \sum \frac{\Lambda}{n}$$

$$\sum \frac{1}{p} \approx \sum \frac{p(n)}{n}$$

$$\sum_{d|n} \Lambda(d) = \log n$$

$$\sum_{d|n} p(d) = \#\text{ of distinct prime factors of } n$$

PMATH 740 Lecture 24: June 25, 2012

Theorem: (Dirichlet's Theorem)
Let k, $l \in \mathbb{Z}^+$ with $\gcd(k,l) = 1$.
Then there exist infinitely many primes p with $p = k \bmod l$.
Indeed,

$$\sum_{\substack{p\leq x \\ p=k \bmod l}} \frac{\log p}{p} = \frac{1}{\phi(l)}\log x + O(1)$$

Proof: Step 1. (Use Dirichlet characters)
Recall that

$$\sum_{\chi\in\hat{U}_l} \chi(p)\overline{\chi(k)} = \begin{cases} \phi(l) & \text{if } p = k \bmod l \\ 0 & \text{otherwise} \end{cases}$$

So we have

$$\begin{aligned}
\phi(l) \sum_{\substack{p\leq x \\ p=k \bmod l}} \frac{\log p}{p} &= \sum_{p\leq x}\sum_{\chi\in\hat{U}_l} \frac{\chi(p)\overline{\chi(k)}\log p}{p} \\
&= \sum_{p\leq x}\Big(\frac{\mathbf{1}(p)^{32)}\overline{\mathbf{1}(k)}\log p}{p} + \sum_{\chi\neq\mathbf{1}} \frac{\chi(p)\overline{\chi(k)}\log p}{p}\Big) \\
&= \sum_{\substack{p\leq x \\ \gcd(p,l)=1}} \frac{\log p}{p} + \sum_{p\leq x}\sum_{\chi\neq\mathbf{1}} \frac{\chi(p)\overline{\chi(k)}\log p}{p} \\
&= \sum_{p\leq x} \frac{\log p}{p} - \underbrace{\sum_{p\leq x} \frac{\log p}{p}}_{O(1)} + \sum_{\chi\neq\mathbf{1}}\sum_{p\leq x} \frac{\chi(p)\overline{\chi(k)}\log p}{p} \\
&= \log x + O(1) + \sum_{\chi\neq\mathbf{1}} \overline{\chi(k)} \sum_{p\leq x} \frac{\chi(p)\log p}{p} \\
\therefore \sum_{\substack{p\leq x \\ p=k \bmod l}} \frac{\log p}{p} &= \frac{1}{\phi(l)}\log x + \frac{1}{\phi(l)}\sum_{\chi\neq\mathbf{1}} \overline{\chi(k)} \sum_{p\leq x} \frac{\chi(p)\log p}{p} + O(1)
\end{aligned}$$

If suffices to show that $\sum_{p\le x}\frac{\chi(p)\log p}{p}=O(1)$ for each $\mathbf{1}\neq\chi\in\hat{U}_l$.

Step 2. (Write this in terms of $\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}$)

$$\begin{aligned}
\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} &= \sum_{p^k\le x}\frac{\chi(p^k)\log p}{p^k}\\
&= \sum_{p\le x}\sum_{\substack{k\ge 1\\ p^k\le x}}\frac{\chi(p^k)\log p}{p^k}\\
&= \sum_{p\le x}\frac{\chi(p)\log p}{p}+\sum_{p\le x}\sum_{\substack{k\ge 2\\ p^k\le x}}\frac{\chi(p^k)\log p}{p^k}\\
&= \sum_{p\le x}\frac{\chi(p)\log p}{p}+O(1)^{33)}\\
&\le \sum_{p\le x}\sum_{k\ge 2}\frac{\log p}{p^k}=\sum_{p\le x}\log p\Big(\underbrace{\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\cdots}_{\frac{1/p^2}{1-1/p}=\frac{1}{p(p-1)}}\Big)\\
&= \sum_{p\le x}\frac{\log p}{p(p-1)}\\
&\le \sum_{n=1}^{\infty}\frac{\log n}{n(n-1)}\ \text{which converges}\\
\therefore \sum_{p\le x}\frac{\chi(p)\log p}{p} &= \sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}+O(1)
\end{aligned}$$

It suffices to show that $\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}=O(1)$.

Step 3. (use the fact that $\sum_{d|n}\Lambda(d)=\log n$)
Recall that

$$\sum_{d|n}\Lambda(d)=\sum_{p^k|n}\log p=\sum_{p|n}e_p(n)\log p$$

$$\begin{aligned}
\exp\Big(\sum_{d|n}\Lambda(d)\Big) &= \exp\Big(\sum_{p|n}e_p(n)\log p\Big)\\
&= \prod_{p|n}\exp(e_p(n)\log p)\\
&= \prod_{p|n}p^{e_p(n)}=n\\
\therefore \sum_{d|n}\Lambda(d) &= \log n
\end{aligned}$$

---

32) $\mathbf{1}(P)=\begin{cases}1 & \text{if } \gcd(p,l)=1\\ 0 & \text{otherwise}\end{cases}$

33) because

$$\Big|\sum_{p\le x}\sum_{\substack{k\ge 2\\ p^k\le x}}\frac{\chi(p^k)\log p}{p^k}\Big|\le\sum_{p\le x}\sum_{\substack{k\ge 2\\ p^k\le x}}\frac{\log p}{p^k}$$

By Möbius inversion

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d}$$

We have

$$\begin{aligned}
\sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} &= \sum_{n\le x}\sum_{d|n} \frac{\chi(n)\mu(d)\log(\frac{n}{d})}{n} \\
&= \sum_{\substack{c,d \\ cd\le x}} \frac{\chi(cd)\mu(d)\log c}{cd} \\
&= \sum_{\substack{c,d \\ cd\le x}} \frac{\chi(c)\log c}{c} \cdot \frac{\chi(d)\mu(d)}{d} \\
&= \sum_{d\le x} \Big(\frac{\chi(d)\mu(d)}{d} \sum_{c\le x/d} \frac{\chi(c)\log c}{c} \Big)^{34)} \\
&= \sum_{d\le x} \frac{\chi(d)\mu(d)}{d} (K + y(\tfrac{x}{d}))
\end{aligned}$$

where $K = K_x = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n}$ and $|g(\frac{x}{d})| \le \phi(l)\frac{\log(x/d)}{x/d}$

$$\begin{aligned}
&= K \sum_{d\le x} \frac{\chi(d)\mu(d)}{d} + \sum_{d\le x} \frac{\chi(d)\mu(d)g(\frac{x}{d})}{d} \\
&= K \sum_{d\le x} \frac{\chi(d)\mu(d)}{d} + O(1)
\end{aligned}$$

because $\left|\sum_{d\le x} \frac{\chi(d)\mu(d)g(\frac{x}{d})}{d}\right|$

$$\begin{aligned}
&\le \sum_{d\le x} \frac{\phi(l)\log(x/d)}{x} \qquad = O(1) \\
&= \frac{\phi(l)}{x} \sum_{d\le x} (\log x - \log d) \\
&= \frac{\phi(l)}{x} \Big(\log x \sum_{d\le x} 1 - \sum_{d\le x} \log d \Big) \\
&= \frac{\phi(l)}{x} \Big(\log x(x + O(1)) - (x\log x + O(x)) \Big) \\
\therefore \sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} &= K \cdot \sum_{n\le x} \frac{\chi(n)\mu(n)}{n} + O(1)
\end{aligned}$$

where $K = K_x = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n}$ (3)

It suffices to show that $\sum_{n\le x} \frac{\chi(n)\mu(n)}{n} = O(1)$

---

[34] Recall that $K = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n}$ converges.

$$\sum_{n\le x} \frac{\chi(n)\log n}{n} = K + g(x) \qquad |g(x)| \le \phi(l)\frac{\log x}{x}$$

Step 4. (Notice that $\sum \frac{\chi(n)\mu(n)}{n}$ and $\sum \frac{\chi(n)}{n}$ are almost inverses.)
Note

$$\sum_{\substack{c,d\\ cd\le x}} \frac{\chi(c)\mu(c)}{c}\cdot\frac{\chi(d)}{d} = \sum_{n\le x}\sum_{c|n}\frac{\chi(n)}{n}\mu(c)$$
$$= \sum_{n\le x}\frac{\chi(n)}{n}\underbrace{\sum_{c|n}\mu(c)}_{=1 \text{ only when } n=1}$$
$$= \frac{\chi(1)}{1} = 1$$

We have

$$1 = \sum_{\substack{c,d\\ cd\le x}} \tfrac{\chi(c)\mu(c)}{c}\tfrac{\chi(d)}{d}$$
$$= \sum_{c\le x}\Big(\frac{\chi(c)\mu(c)}{c}\sum_{d\le x/c}\frac{\chi(d)}{d}\Big)$$
$$= \sum_{c\le x}\Big(\frac{\chi(c)\mu(c)}{c}(L+h(\tfrac{x}{c}))\Big)$$

where $L = L_x = \sum_{n=1}^{\infty}\frac{\chi(n)}{n}$ and $|h(\frac{x}{c})| \le \phi(l)\frac{c}{x}$

$$= L\cdot\sum_{c\le x}\frac{\chi(c)\mu(c)}{c} + \underbrace{\sum_{c\le x}\frac{\chi(c)\mu(c)h(\frac{x}{c})}{c}}_{O(1)}$$

PMATH 740 Lecture 25: June 27, 2012

(1)
$$\sum_{\substack{p\le x\\ p=k \bmod l}}\frac{\log p}{p} = \frac{1}{\phi(l)}\log x + \frac{1}{\phi(l)}\sum_{\chi\neq\mathbf{1}}\overline{\chi(k)}\underbrace{\sum_{p\le x}\frac{\chi(p)\log p}{p}}+O(1)$$

(2)
$$\sum_{p\le x}\frac{\chi(p)\log p}{p} = \sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}+O(1)$$

(3)
$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} = k\sum\frac{\chi(n)\mu(n)}{n}+O(1),\quad k=k_x=\sum_{n=1}^{\infty}\frac{\chi(n)\log n}{n}$$

Step 4.

$$\sum_{\substack{c,d\\ cd\le x}} \frac{\chi(c)\mu(c)}{c}\frac{\chi(d)}{d} = \sum_{n\le x}\sum_{c|n}\frac{\chi(n)}{n}\mu(k)$$

$$= \sum_{n\le x}\frac{\chi(n)}{n}\underbrace{\sum_{c|n}\mu(c)}_{=1 \text{ only when } n=1}$$

$$= \frac{\chi(1)}{1} = 1$$

$$1 = \sum_{c\le x}\sum_{d\le x/c}\frac{\chi(c)\mu(c)}{c}\frac{\chi(d)}{d}$$

$$= \sum_{c\le x}\frac{\chi(c)\mu(c)}{c}\sum_{d\le x/c}\frac{\chi(d)}{d}$$

$$= \sum_{c\le x}\frac{\chi(c)\mu(c)}{c}(L+g(x))$$

where $L = \sum_{n=1}^{\infty}\frac{\chi(n)}{n}$, $|g(x)| \le \phi(l)\frac{c}{x}$

$$= L\sum_{c\le x}\frac{\chi(c)\mu(c)}{c} + \sum_{c\le x}\frac{\chi(c)\mu(c)g(x)}{c}$$

We have

$$\Big|\sum_{c\le x}\frac{\chi(c)\mu(c)g(x)}{c}\Big| \le \sum_{c\le x}\frac{\phi(l)\frac{c}{x}}{c}$$

$$= \frac{\phi(l)}{x}\sum_{c\le x}1 = \frac{\phi(l)}{x}(x+O(1)) = O(1)$$

$$\therefore L\cdot\sum\frac{\chi(n)\mu(n)}{n} = O(1),$$

where $L = L_x = \sum_{n=1}^{\infty}\frac{\chi(n)}{n}$. It suffices to show that $L = L_x \neq 0$, for all $\mathbf{1} \neq \chi \in \hat{U}_l$. (4)

Remark: Dirichlet used the holomorphic function $L_x(z)$ defined for $\Re(z) > 1$ by

$$L_x(z) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^z}.$$

If we differentiate term by term, we get

$$L_x'(z) = -\sum_{n=1}^{\infty}\frac{\chi(n)\log n}{n^z}$$ [35)]

Step 5(a): Consider a real-valued character χ, $\mathbf{1} \neq \chi \in \hat{U}_l$

$$\chi\colon \mathbb{Z} \to \{0, \pm 1\}.$$

[35)] Aside:

$$\Big(\frac{1}{n^z}\Big)' = (e^{-z\log n})' = -\log n\, e^{-z\log n} = \frac{-\log n}{n^z}$$

Let $A(n) = \sum_{d|n} \chi(d)$, $B(x) = \sum_{n \le x} \frac{A(n)}{\sqrt{n}}$.
We show that $B(x) \to \infty$, and $B(x) = \sqrt{x}L + O(1)$, so that $L \neq 0$.

Since χ is (completely) multiplicative, A is multiplicative.
(proof: for a, b with $\gcd(a,b) = 1$, each $d \mid ab$ can be expressed uniquely as $d = kl$ with $k \mid a$, $k \mid b$, so:

$$A(ab) = \sum_{d|ab} \chi(d) = \sum_{k|a} \sum_{l|b} \chi(kl) = \sum_{k|a} \chi(k) \sum_{l|b} \chi(l) = A(a)A(b).$$

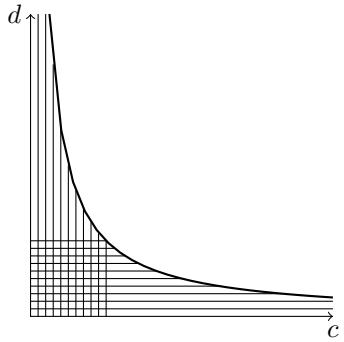
So we have $A(\prod p_i^{k_i}) = \prod A(p_i^{k_i})$
We have

$$A(p^m) = \sum_{d|p^m} \chi(d) = 1 + \chi(p) + \chi(p)^2 + \cdots + \chi(p)^m$$

If $\chi(p) = 0$, then $A(p^m) = 1$
If $\chi(p) = 1$, then $A(p^m) = 1 + m$
If $\chi(p) = -1$, then $A(p^m) = \begin{cases} 1 & \text{if } m \text{ is even} \\ 0 & \text{if } m \text{ is odd} \end{cases}$
$\therefore A(p^m) \ge 0$ for all p, m, and if m is even, $A(p^m) \ge 1$.
$\therefore A(n) \ge 0$ for all $n \in \mathbb{Z}^+$, with $A(n) \ge 1$ when n is a square.

$$\therefore B(x) = \sum_{n \le x} \frac{A(n)}{\sqrt{n}} \ge \sum_{n = m^2 \le x} \frac{A(m^2)}{m} \ge \sum_{m \le \sqrt{x}} \frac{1}{m} \to \infty, \text{ as } x \to \infty.$$

$$\textit{Also,} \qquad B(x) = \sum_{n \le x} \frac{A(n)}{\sqrt{n}} = \sum_{n \le x} \sum_{d|n} \frac{\chi(d)}{\sqrt{n}} = \sum_{\substack{c,d \\ cd \le x}} \frac{\chi(d)}{\sqrt{cd}}$$



$$= \sum_{c \le \sqrt{x}} \sum_{d \le x/c} \frac{\chi(d)}{\sqrt{cd}} + \sum_{d \le x} \sum_{c \le x/d} \frac{\chi(d)}{\sqrt{cd}} - \sum_{c \le \sqrt{x}} \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{cd}} = \cdots = \sqrt{x}L + O(1)$$

Recall: $$\sum_{n \le x} \frac{1}{\sqrt{n}} = f(1) + \int_1^x f(t)\,\mathrm{d}t + \int_1^x \langle t \rangle f'(t)\,\mathrm{d}t - \langle x \rangle f(x),$$

We have

$$L_x(1) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = L_x$$

$$L_x'(1) = -\sum \frac{\chi(n) \log n}{n} = -K_x$$

for $f(t) = t^{-1/2}$, $f'(t) = -\frac{1}{2}t^{-3/2}$, $\int f = 2t^{1/2}$.

$$\begin{aligned}
&= 1 + \int_1^x \frac{1}{\sqrt{t}}\,\mathrm{d}t - \int_1^x \frac{\langle t\rangle}{2^{3/2}}\,\mathrm{d}t - \frac{\langle x\rangle}{\sqrt{x}} \\
&= 1 + \Big[2\sqrt{t}\Big]_1^x - \int_1^\infty \frac{\langle t\rangle}{2t^{3/2}}\,\mathrm{d}t + \int_2^\infty \frac{\langle t\rangle}{2t^{3/2}}\,\mathrm{d}t - \underbrace{\frac{\langle x\rangle}{\sqrt{x}}}_{\in[0,1/\sqrt{x})} \\
&= 1 + 2\sqrt{x} - 2 - a + g(x) \\
&= 2\sqrt{x} + c + g(x),
\end{aligned}$$

where $c = -1 - \int_1^\infty \frac{\langle t\rangle}{2t^{3/2}}\,\mathrm{d}t$, and we have

$$\Big|\int_x^\infty \frac{\langle t\rangle}{2t^{3/2}}\,\mathrm{d}t\Big| \le \int_x^\infty \frac{1}{2t^{3/2}}\,\mathrm{d}t = \Big[-\frac{1}{\sqrt{t}}\Big]_x^\infty = \frac{1}{\sqrt{x}},$$

so that $|g(x)| \le \frac{1}{\sqrt{x}}$

$$(\therefore) \sum_{n\le x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + c + O\Big(\frac{1}{\sqrt{x}}\Big).$$

$$\sum_{c\le\sqrt{x}} \frac{1}{\sqrt{c}} \sum_{d\le x/c} \frac{\chi(d)}{\sqrt{d}} = \sum_{c\le x} \frac{1}{\sqrt{c}}\Big(M + h\Big(\frac{x}{c}\Big)\Big),$$

$$\text{where} \qquad M = \sum_{n=1}^\infty \frac{\chi(n)}{\sqrt{n}}, \qquad \text{and} \qquad \Big|h\Big(\frac{x}{c}\Big)\Big| \le \phi(l)\sqrt{\frac{x}{c}}$$

$$= M \sum_{c\le\sqrt{x}} \frac{1}{\sqrt{c}} + \sum_{c\le\sqrt{x}} \frac{h(\frac{x}{c})}{\sqrt{c}} = M(2x^{1/4} + O(1)) + O(1),$$

$$\text{since} \qquad \Big|\sum_{c\le\sqrt{x}} \frac{h(\frac{x}{c})}{\sqrt{c}}\Big| \le \sum_{c\le\sqrt{x}} \frac{\phi(l)\sqrt{\frac{c}{x}}}{\sqrt{c}}$$

$$= \frac{\phi(l)}{\sqrt{x}} \sum_{c\le\sqrt{x}} 1 = \frac{\phi(l)}{\sqrt{x}}(\sqrt{x} + O(1)) = O(1)$$

$$\therefore \sum_{c\le\sqrt{x}} \sum_{d\le x/c} \frac{\chi(d)}{\sqrt{cd}} = 2Mx^{1/4} + O(1).$$

$$\begin{aligned}
\sum_{d\le\sqrt{x}} \sum_{c\le x/d} \frac{\chi(d)}{\sqrt{cd}} &= \sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{c\le x/d} \frac{1}{\sqrt{c}} = \sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{d}}\Big(2\sqrt{\frac{x}{d}} + O(1)\Big) \\
&= 2\sqrt{x} \sum_{d\le\sqrt{x}} \frac{\chi(d)}{d} + \sum_{d\le x} \frac{\chi(d)}{\sqrt{d}} O(1) \\
&= 2\sqrt{x}(L + O(\tfrac{1}{\sqrt{x}})) + O(1)(M + O(\tfrac{1}{x^{1/4}})) \\
&= 2\sqrt{x}L + O(1).
\end{aligned}$$

$$\begin{aligned}
\sum_{c\le\sqrt{x}} \sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{cd}} &= \Big(\sum_{c\le\sqrt{x}} \frac{1}{\sqrt{c}}\Big)\Big(\sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{d}}\Big) \\
&= (2x^{1/4} + O(1))(M + O(\tfrac{1}{\sqrt{c}})) = 2Mx^{1/4} + O(1).
\end{aligned}$$

$$\therefore B(x) = \sum_{c\le\sqrt{x}}\sum_{d\le x/c}\frac{\chi(d)}{\sqrt{cd}} + \sum_{d\le\sqrt{x}}\sum_{c\le x/d}\frac{\chi(d)}{\sqrt{cd}} - \sum_{c\le\sqrt{x}}\sum_{d\le\sqrt{x}}\frac{\chi(d)}{cd}$$
$$= (2Mx^{1/4} + O(1)) + (2\sqrt{x}L + O(1)) - (2Mx^{1/4} + O(1))$$
$$= 2\sqrt{x}L + O(1).$$

PMATH 740 Lecture 26: June 29, 2012

$$\sum_{\substack{p\le x\\ p=k \bmod l}}\frac{\log p}{p} = \frac{1}{\phi(l)}\log x + \frac{1}{\phi(l)} + \sum_{\chi\neq\mathbf{1}}\overline{\chi(k)}\sum_{p\le x}\frac{\chi(p)\log p}{p} + O(1) \tag{1}$$

In particular, taking $k = 1$,

$$\sum_{\substack{p\le x\\ p=1 \bmod l}}\frac{\log p}{p} = \frac{1}{\phi(l)}\log x + \frac{1}{\phi(l)}\sum_{\chi\neq\mathbf{1}}\underbrace{\sum_{p\le x}\frac{\chi(p)\log p}{p}} + O(1)$$

$$\sum_{p\le x}\frac{\chi(p)\log p}{p} = \sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} + O(1) \tag{2}$$

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} = K_x\cdot\underbrace{\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}} + O(1) \tag{3}$$

$$L_x\cdot\sum_{n\le x}\frac{\chi(n)\mu(n)}{n} = O(1)$$

If $L_x \neq 0$ then $\sum_{n\le x}\frac{\chi(n)\mu(n)}{n} = O(1)$
We shall show that for $\mathbf{1}\neq\chi\in\hat{U}_l$

$$K_x\sum_{n\le x}\frac{\chi(n)\mu(n)}{n} = -\log x + O(1)$$

It follows that if $N = \#$ of $\chi\in\hat{U}_l$ with $\chi\neq\mathbf{1}$ such that $L_x = 0$ then

$$\sum_{\substack{p\le x\\ p=1 \bmod k}}\frac{\log p}{p} = \frac{1-N}{\phi(l)}\log x + O(1)$$

We can only have $N = 0$ or 1 otherwise RS $\to\infty$ but LS > 0.

Recall that if χ is real-valued then $L_x\neq 0$. Note that if χ is not real-valued then $\chi\neq\overline{\chi}$ and

$$L_x = \sum_{n=1}^{\infty}\frac{\overline{\chi}(n)}{n} = \overline{\sum_{n=1}^{\infty}\frac{\chi(n)}{n}} = \overline{L_x}$$

So we have $L_x = 0 \iff L_{\overline{\chi}} = 0$. Thus N is even and hence $N = 0$.

Final step: It remains to show that when $L_x = 0$

$$K_x\cdot\sum_{n\le x}\frac{\chi(n)\mu(n)}{n} = -\log x + O(1)$$

where

$$K_x = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n}.$$

$$\begin{aligned}
\sum_{\substack{c,d \\ cd\le x}} \frac{\chi(c)}{c}\log\Big(\frac{cd}{x}\Big)\frac{\chi(d)\mu(d)}{d} &= \sum_{n\le x}\frac{\chi(n)}{n}\log\frac{x}{n}\underbrace{\sum_{d|n}\mu(d)}_{=1 \text{ only when } =1} \\
&= \frac{\chi(1)}{1}\log\frac{1}{x} \\
&= -\log x \\
\therefore -\log x &= \sum_{d\le x}\frac{\chi(d)\mu(d)}{d}\sum_{c\le x/d}\frac{\chi(c)}{c}\log\Big(\frac{cd}{x}\Big) \\
&= \sum_{d\le x}\frac{\chi(d)\mu(d)}{d}\sum_{c\le x/d}\frac{\chi(c)}{c}\Big(\log c - \log\frac{x}{d}\Big) \\
&= \sum_{d\le x}\frac{\chi(d)\mu(d)}{d}\Big(\sum_{c\le x/d}\frac{\chi(c)\log c}{c} - \log\frac{x}{d}\sum_{c\le x/d}\frac{\chi(c)}{c}\Big) \\
&= \sum_{d\le x}\frac{\chi(d)\mu(d)}{d}\Big((K_x + g(x)) - \log\frac{x}{d}(L_x + h(x))\Big)
\end{aligned}$$

with $|g(x)| \le \phi(l)\frac{\log x/d}{x/d}$, $|h(x) \le \phi(l)\frac{1}{x/d}|$

$$= K_x\sum_{d\le x}\frac{\chi(d)\mu(d)}{d} + \sum_{d\le x}\frac{\chi(d)\mu(d)}{d}k(x)$$

where $k(x) = g(x) - \log\frac{x}{d}h(x)$, so $|k(x)| \le 2\phi(l)\frac{\log x/d}{x/d}$ and we have

$$\begin{aligned}
\Big|\sum_{d\le x}\frac{\chi(d)\mu(d)k(x)}{d}\Big| &\le \sum_{d\le x}\frac{2\phi(l)\log x/d}{x} \\
&= \frac{2\phi(l)}{x}\sum_{d\le x}(\log x - \log d) \\
&= \frac{2\phi(l)}{x}\Big(\log x\sum_{d\le x}1 - \sum_{d\le x}\log d\Big) \\
&= \frac{2\phi(l)}{x}\Big(\log x(x + O(1)) - (x\log x + O(x))\Big) \\
&= \frac{2\phi(l)}{x}O(x) \\
&= O(1)
\end{aligned}$$

This completes the proof.

$$p(n) = p_n = \text{the } n\text{th prime}$$

$$\rho(n) = \begin{cases} 1 & \text{if } n \text{ is prime} \\ 0 & \text{otherwise} \end{cases}$$

$$\pi(x) = \sum_{n \le x} \rho(n) = \#\text{ of primes } p \le x = \sum_{p \le x} 1$$

$$\psi(x) = \sum_{n \le x} \Lambda(n) = \sum_{p^k \le x} \log p \quad [36]$$

$$\vartheta(x) = \sum_{p \le x} \log p$$

$$M(x) = \sum_{n \le x} \mu(n)$$

$$A(x) = \sum_{n \le x} \frac{\mu(n)}{n}$$

Theorem: The following are equivalent

$$p(n) \sim n \log n$$

$$\lim_{x \to \infty} \frac{\pi(x) \log \pi(x)}{x} = 1$$

$$\pi(x) \sim \frac{x}{\log x} \sim \int_2^x \frac{\mathrm{d}t}{\log t}$$

$$\psi(x) \sim x$$

$$\vartheta(x) \sim x$$

$$M(x) = o(x), \text{ i.e.,}$$

$$\lim_{x \to \infty} \frac{M(x)}{x} = 0$$

$$A(x) = o(1), \text{ i.e.,}$$

$$\lim_{x \to \infty} A(x) = 0, \text{ i.e.,}$$

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0$$

Theorem:

$$a \frac{\log x}{x} \le \pi(x) \le b \frac{\log x}{x}$$

for some $a < 1$, $b > 1$

Theorem: (Bertrand's Conjecture)
For all $n \in \mathbb{Z}^+$ there exists a prime p with $n < p \le 2n$.

Unknown: For all $n \ge 2$ there exists a prime p with

$$n^2 < p < (n+1)^2.$$

PMATH 740 Lecture 27: July 4, 2012

[36] Chebyshev

Chapter 11: Dirichlet Series
A power series is a series of the form $\sum c_n z^n$ (or $\sum c_n (z-a)^n$)[37]

Definition: A *Dirichlet series* is a series of the form

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$$

where $f\colon \mathbb{Z}^+ \to \mathbb{C}$.
(such a series will converge for some values of $z \in \mathbb{C}$ and diverge for others)

Theorem: (Abscissa of Absolute Convergence)
Let $f\colon \mathbb{Z}^+ \to \mathbb{C}$.
There is a number $\sigma_a \in \mathbb{R} \cup \{\pm\infty\}$ which we call the *abscissa of absolute convergence* of the Dirichlet series $\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ such that $\sum \frac{f(n)}{n^z}$ converges absolutely for $\Re(z) > \sigma_a$ and $\sum \frac{f(n)}{n^z}$ does not converge absolutely for any z with $\Re(z) < \sigma_a$. When $\sigma_a \in \mathbb{R}$ the set of points z for which $\sum \left|\frac{f(n)}{n^z}\right|$ converges is either $\{\, z : \Re(z) > \sigma_a \,\}$ or $\{\, z : \Re(z) \geq \sigma_a \,\}$.
Proof: Note that for $z = x + iy$,

$$\begin{aligned} n^z &= e^{z \ln(n)} \\ &= e^{x \ln(n) + iy \ln(n)} \\ |n^z| &= e^{x \ln(n)} = n^x = n^{\Re(z)} \end{aligned}$$

We shall show that if $\sum_{n=1}^{\infty} \left|\frac{f(n)}{n^w}\right|$ converges then $\sum_{n=1}^{\infty} \left|\frac{f(n)}{n^z}\right|$ converges for all z with $\Re(z) \geq \Re(w)$. It follows that

$$\sigma_a = \inf\Big\{ \Re(w) : \sum_{n=1}^{\infty} \Big|\frac{f(n)}{n^w}\Big| \text{ converges} \Big\}.$$

Let $w \in \mathbb{C}$.
Suppose $\sum_{n=1}^{\infty} \left|\frac{f(n)}{n^w}\right|$ converges. Let $z \in \mathbb{C}$ with $\Re(z) \geq \Re(w)$. Say $w = a + ib$, $z = x + iy$, so $x \geq a$. Then

$$\Big|\frac{f(n)}{n^z}\Big| = \frac{|f(n)|}{n^x} \leq \frac{|f(n)|}{n^a} = \Big|\frac{f(n)}{n^w}\Big|$$

So $\sum_{n=1}^{\infty} \left|\frac{f(n)}{n^z}\right|$ converges by the Comparison Test.

Theorem: (Abscissa of Convergence)
Let $f\colon \mathbb{Z}^+ \to \mathbb{C}$. There exists a number $\sigma_c \in \mathbb{R} \cup \{\pm\infty\}$ such that $\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ converges for $\Re(z) > \sigma_c$ and $\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ diverges for $\Re(z) < \sigma_c$.

We show that if $\sum \frac{f(n)}{n^w}$ converges then $\sum \frac{f(n)}{n^z}$ for all z with $\Re(z) > \Re(w)$.
Fix $w = a + ib \in \mathbb{C}$.
Suppose $\sum_{n=1}^{\infty} \frac{f(n)}{n^w}$ converges. Let $z = x + iy \in \mathbb{C}$ with $x > a$. Write

$$S_l = \sum_{n=1}^{l} \frac{f(n)}{n^z} = \sum a(n) g(n)$$

[37] will always diverge for at least one complex value on circumference

R = radius of converge

$$\sum_{n=1}^{\infty} \frac{1}{z^n} \quad |z| = 1 \implies \Big|\frac{1}{z^n}\Big| = 1 \neq 0 \quad \therefore \text{ diverges}$$

where $a(n) = \frac{f(n)}{n^w}$, $g(t) = \frac{t^w}{t^z} = t^{w-z}$.
For $k < l$, by Abel Summation, we have

$$\begin{aligned}
|S_l - S_k| &= \Big|\sum_{n=1}^{l} a(n)g(n) - \sum_{n=1}^{k} a(n)g(n)\Big| \\
&= \Big|A(l)g(l) - \int_1^l A(t)g'(t)\,\mathrm{d}t - A(k)g(k) + \int_1^k A(t)g'(t)\,\mathrm{d}t\Big|
\end{aligned}$$

where $A(x) = \sum_{n\le x} a(n) = \sum_{n\le x} \frac{f(n)}{n^w}$

$$\begin{aligned}
&= \Big|A(l)l^{w-z} - A(k)k^{w-z} - \int_k^l A(t)(w-z)t^{w-z-1}\,\mathrm{d}t\Big| \\
&\le |A(l)|l^{a-x} + |A(k)|k^{a-x} + \int_k^l |A(t)||w-z|t^{a-x-1}\,\mathrm{d}t \\
&\le M\Big(\frac{1}{l^{x-a}} + \frac{1}{k^{x-a}} + |w-z|\Big[\frac{1}{a-x}t^{a-x}\Big]_k^l\Big)
\end{aligned}$$

where we have chosen M so that $|A(x)| \le M$ for all x (which we can do since $\sum \frac{f(n)}{n^w}$ converges)

$$\begin{aligned}
&= M\Big(\frac{1}{l^{x-a}} + \frac{1}{k^{x-a}} + \frac{|w-z|}{x-a}\Big(\frac{1}{k^{x-a}} - \frac{1}{l^{x-a}}\Big)\Big) \\
&\le M\Big(\frac{1}{k^{x-a}} + \frac{1}{k^{x-a}} + \frac{|w-z|}{x-a}\cdot\frac{1}{k^{x-a}}\Big) \\
&= M\Big(2 + \frac{|w-z|}{x-a}\Big)\cdot\frac{1}{k^{x-a}} \\
&\to 0 \text{ as } k \to \infty \text{ since } x > a
\end{aligned}$$

$\therefore \{S_l\}$ converges by Cauchy's Criterion
$\therefore \sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ converges.

Theorem: For any Dirichlet series $\sum \frac{f(n)}{n^z}$ we have

$$\sigma_a - 1 \le \sigma_c \le \sigma_a$$

Proof: We shall show that if $\sum \frac{f(n)}{n^w}$ converges then $\sum|\frac{f(n)}{n^z}|$ converges for all z with $\Re(z) > \Re(w) + 1$.

Fix $w = a + ib$.
Suppose $\sum \frac{f(n)}{n^w}$ converges.
Let $z = x + iy \in \mathbb{C}$ with $x > a + 1$.
Then

$$\begin{aligned}
\Big|\frac{f(n)}{n^z}\Big| = \frac{|f(n)|}{n^x} &= \frac{|f(n)|}{n^a}\cdot\frac{n^a}{n^x} \\
&= \Big|\frac{f(n)}{n^w}\Big|\frac{1}{n^{x-a}} \\
&\le M\cdot\frac{1}{n^{x-a}}
\end{aligned}$$

where we have chosen M so that

$$\Big|\frac{f(n)}{n^w}\Big| \le M$$

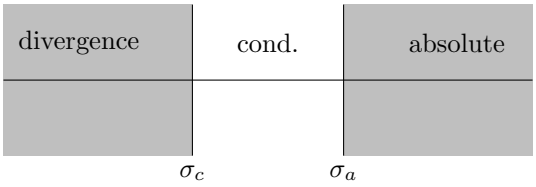
(which we can do since $\sum \frac{f(n)}{n^w}$ converges so $\big|\frac{f(n)}{n^w}\big| \to 0$)
$\therefore \sum\big|\frac{f(n)}{n^z}\big|$ converges by Comparison since $x - a > 1$ so $\sum \frac{M}{n^{x-a}}$ converges.

Example: For $\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$ we have $\sigma_a = 1$, $\sigma_c = 1$, since $\sum \left|\frac{1}{n^z}\right| = \sum \frac{1}{n^x}$ converges for $x > 1$, and $\sum \frac{1}{n^x}$ diverges when $x = 1$.

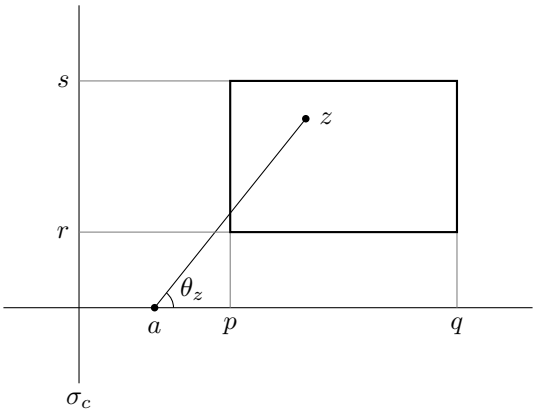
Example: For $L_x(z) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^z}$ with $\chi \in \hat{U}_l$ show that $0 \le \sigma_c \le \sigma_a = 1$.

PMATH 740 Lecture 28: July 6, 2012

$f : \mathbb{Z}^+ \to \mathbb{C}$
$\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$



Theorem: (Uniform Convergence)
For a Dirichlet series $\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ with $\sigma_c < \infty$, the series converges uniformly in compact subsets $K \subseteq \{ z : \Re(z) > \sigma_c \}$.
Proof: It suffices to prove the theorem when K is a rectangle.
Let $K = [p, q] \times [r, s]$ where $p > \sigma_c$.



Choose $a \in \mathbb{R}$ with $\sigma_c < a < p$. Let $z \in K$.
Recall that if we write $S_l = \sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ and we use Abel's Formula with $a(n) = \frac{f(n)}{n^a}$, $A(x) = \sum_{n \le x} a(n)$, $f(t) = \frac{t^a}{t^z} = t^{a-z}$, then for $k < l$

$$\begin{aligned}
|S_l - S_k| &= \Big| A(l)f(l) - A(k)f(k) - \int_k^l A(t)f'(t)\,\mathrm{d}t \Big| \\
&= \Big| \frac{A(l)}{l^{z-a}} - \frac{A(k)}{k^{z-a}} - \int_k^l A(t)(a-z)t^{a-z-1}\,\mathrm{d}t \Big| \\
&\le M\Big(\frac{1}{x^{x-a}} + \frac{1}{k^{x-a}} + |z-a| \int_k^l t^{a-x-1}\,\mathrm{d}t^{38)} \Big) \\
&\le M\Big(\frac{2}{k^{x-a}} + \frac{|z-a|}{x-a}\Big(\frac{1}{k^{x-a}} - \frac{1}{k^{x-a}} \Big) \Big) \\
&\le M\Big(2 + \frac{|z-a|}{x-a} \Big) \cdot \frac{1}{k^{x-a}}
\end{aligned}$$

where $|A(x)| \leq M$ for all x, and $z = x + iy$

$$= M(2 + \sec\theta_z) \cdot \frac{1}{k^{x-a}}$$

where θ_z is as shown

$$\leq M(2 + \sec\theta_m)\frac{1}{k^{x-a}}$$

where $\sec\theta_m = \frac{\sqrt{(p-a)^2+\max(r^2,s^2)}}{p-a}$

$$\to 0 \text{ as } k \to \infty$$

independent of z
Corollary: If we define

$$F(z) = \sum_{n=1}^{\infty} \frac{f(n)}{n^z}$$

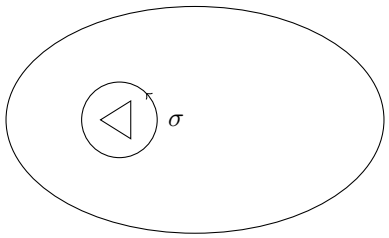
for all z with $\Re(z) > \sigma_c$ then F is holomorphic.
Proof: This follows from the fact that

if $U \subseteq \mathbb{C}$ is open

if $f_n \colon U \to \mathbb{C}$ are holomorphic in U

if $f_n \to f$ uniformly compact sets $K \subseteq U$

then f is holomorphic in U and $f_n' \to f'$
Proof: Let $a \in U$.
Choose $r > 0$ so $\bar{D}(a, r) \subseteq U$



Let α be any triangle in $D(a, r)$.
Then f is continuous and

$$\int_\alpha f = \int_\alpha \lim f_n = \lim \int_\alpha f_n = 0$$

$\therefore f$ is holomorphic in $D(a, r)$ by Morera, hence at a.

Now let $\sigma = a + re^{it}$, $0 \leq t \leq 2\pi$

---

38)

$$\int_k^l t^{a-x-1}\,\mathrm{d}t = \left[\frac{1}{a-x}t^{a-x}\right]_k^l = \frac{1}{x-a}\left(\frac{1}{k^{x-a}} - \frac{1}{l^{x-a}}\right)$$

By Cauchy's Integral Formula

$$\begin{aligned} f^{(n)}(a) &= \frac{n!}{2\pi i}\int_\sigma \frac{f(z)}{(z-a)^{n+1}}\,\mathrm{d}z \\ &= \frac{n!}{2\pi i}\int_\sigma \frac{\lim_{k\to\infty} f_k(z)}{(z-a)^{n+1}}\,\mathrm{d}z \\ &= \lim_{k\to\infty}\frac{n!}{2\pi i}\int_\sigma \frac{f_k(z)}{(z-a)^{n+1}}\,\mathrm{d}z \\ &= \lim_{k\to\infty} f_k(a) \end{aligned}$$

Theorem: (Behaviour as $\Re(z)\to\infty$)
Let $F(z)=\sum_{n=1}^\infty \frac{f(n)}{n^z}$ for $\Re(z)>\sigma_c$
If $\{z_k\}$ is a sequence with $\Re(z_k)\to\infty$ then $F(z_k)\to f(1)$ as $k\to\infty$.
Proof: Say $z_k = x_k + iy_k$ with $x_k\to\infty$.
Fix $a\in\mathbb{R}$ with $a>\sigma_a$ (so $\sum\frac{|f(n)|}{n^a}$ converges)
Choose N so $k\geq N \implies x_k\geq a$.
For all such k,

$$\begin{aligned} F(z_k) &= \sum_{n=1}^\infty \frac{f(n)}{n^{z_k}} \\ &= f(1) + \sum_{n=2}^\infty \frac{f(n)}{n^{z_k}} \end{aligned}$$

and $\left|\sum_{n=2}^\infty \frac{f(n)}{n^{z_k}}\right| \leq \sum_{n=2}^\infty \frac{|f(n)|}{n^{x_k}}$

$$\begin{aligned} &= \sum_{n=2}^\infty \frac{|f(n)|}{n^a}\frac{1}{n^{x_k-a}} \\ &\leq \frac{1}{2^{x_k-a}}\underbrace{\sum_{n=2}^\infty \frac{|f(n)|}{n^a}}_{\text{finite}} \\ &\leq \frac{1}{2^{x_k-a}}\sum_{n=1}^\infty \frac{|f(n)|}{n^a} \\ &\to 0 \text{ as } k\to\infty \end{aligned}$$

Theorem: (Uniqueness of Coefficients)
Let $F(z)=\sum_{n=1}^\infty \frac{f(n)}{n^z}$, $G(z)=\sum_{n=1}^\infty \frac{g(n)}{n^z}$ for $\Re(z)>c$.
Suppose $F(z_k)=G(z_k)$ where $\{z_k\}$ is some sequence with $\Re(z_k)\to\infty$.
Then $f(n)=g(n)$ for all n.
Proof: Let

$$H(z)=F(z)-G(z)=\sum_{n=1}^\infty \frac{h(n)}{n^z} \text{ where } h(n)=f(n)-g(n)$$

Let $z_k=x_k+iy_k$ with $x_k\to\infty$.
Suppose $F(z_k)=G(z_k)$ so $H(z_k)=0$. We need to show that $h(n)=0$ for all n. Suppose not, and let m be the smallest index with $h(m)\neq 0$. For all z with $\Re(z)>c$,

$$H(z)=\sum_{n=m}^\infty \frac{h(n)}{n^z} = \frac{h(m)}{m^z} + \sum_{n>m}\frac{h(n)}{n^z}$$

Choose $a > c+1$ (so all series converge absolutely when $\Re(z) = a$)
Choose N so $k \geq N \implies x_k > a$. For such k, $H(z_k) = 0$ so

$$\begin{aligned} 0 &= \frac{h(m)}{m^{z_k}} + \sum_{n>m} \frac{h(n)}{n^{z_k}} \\ h(m) &= -m^{z_k} \sum_{n>m} \frac{h(n)}{n^{z_k}} \\ &= -m^{z_k} \sum_{n>m} \frac{h(n)}{n^a} \cdot \frac{1}{n^{z_k - a}} \\ \therefore {}^{39)}|h(n)| &\leq m^{x_k} \sum_{n=m+1}^{\infty} \frac{|h(n)|}{n^{x_k}} \\ &\leq \frac{m^{x_k}}{m+1} \end{aligned}$$

PMATH 740 Lecture 29: July 9, 2012

$F(z_k) = G(z_k)$
$z_k = x_k + iy_k$, $x_k \to \infty$
$f(n) = g(n)$

$H = F - G$, $h = f - g$
$H(z_k) = 0$, $h(n) = 0 \ \forall n$
Let m be the smallest index with $h(m) \neq 0$

$$\begin{aligned} H(z) &= \sum_{n=m}^{\infty} \frac{h(n)}{n^z} \\ &= \frac{h(m)}{m^z} + \sum_{n=m+1}^{\infty} \frac{f(n)}{n^z} \end{aligned}$$

Since $H(z_k) = 0$

$$h(m) = -m^{z_k} \sum_{n=m+1}^{\infty} \frac{h(n)}{n^{z_k}}$$

Choose $a > 1 + c$ (so the series for F and G both converge absolutely)
Choose $N > 0$ so

$$k \geq N \implies x_k > a$$

For such k

$$\begin{aligned} |h(m)| &\leq m^{x_k} \sum_{n=m+1}^{\infty} \frac{|h(n)|}{n^{x_k}} \\ &\leq m^{x_k} \sum_{n=m+1}^{\infty} \frac{|h(n)|}{n^a} \cdot \frac{1}{n^{x_k - a}} \\ &\leq \frac{m^{x_k}}{(m+1)^{x_k - a}} \sum_{n=m+1}^{\infty} \frac{|f(n)|}{n^a} \\ &\leq \Big(\frac{m}{m+1}\Big)(m+1)^a M \to 0 \text{ as } k \to \infty \end{aligned}$$

[39] problem here?

where $M = \sum_{n=1}^{\infty} \frac{|h(a)|}{n^a}$

Theorem: (Multiplication of Dirichlet Series)
Suppose $\sum \frac{f(n)}{n^z}$ and $\sum \frac{g(n)}{n^z}$ both converge absolutely for $\Re(z) > a$. Then

$$\Big(\sum_{n=1}^{\infty} \frac{f(n)}{n^z}\Big)\Big(\sum_{n=1}^{\infty} \frac{g(n)}{n^z}\Big) = \sum_{n=1}^{\infty} \frac{h(n)}{n^z}$$

where

$$h(n) = (f * g)(n) = \sum_{\substack{k,l \\ kl=n}} f(k)g(l)$$

Proof:

$$\Big(\sum_{k=1}^{\infty} \frac{f(k)}{k^z}\Big)\Big(\sum_{l=1}^{\infty} \frac{g(l)}{l^z}\Big) = \sum_{k,l} \frac{f(k)g(l)}{(kl)^z} = \sum_{n=1}^{\infty}\Big(\frac{1}{n^z} \sum_{\substack{k,l \\ kl=n}} f(k)g(l)\Big)$$

where we have used absolute convergence to rearrange terms.

Example:

$$\begin{aligned}
\zeta(z) &= \sum_{n=1}^{\infty} \frac{1}{n^z} \\
M(z) &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^z} \\
\zeta(z)M(z) &= \sum_{k=1}^{\infty} \frac{1}{k^z} \sum_{l=1}^{\infty} \frac{\mu(l)}{l^z} \\
&= \sum_{k,l} \frac{\mu(l)}{(kl)^z} = \sum_{n=1}^{\infty} \sum_{\substack{k,l \\ kl=n}} \frac{\mu(l)}{n^z} \\
&= \sum_{n=1}^{\infty}\Big(\frac{1}{n^z} \underbrace{\sum_{d|n} \mu(d)}_{=1 \text{ only when } n=1}\Big) = 1 \\
\therefore \zeta(z)M(z) &= 1 \text{ for all } z \text{ with } \Re(z) > 1
\end{aligned}$$

(In particular $\zeta(z) \neq 0$ for $\Re(z) > 1$)

Example:

$$\begin{aligned}
\zeta^2(z) &= \sum_{k} \frac{1}{k^z} \sum_{l} \frac{1}{l^z} \\
&= \sum_{k,l} \frac{1}{(kl)^z} = \sum_{n=1}\Big(\frac{1}{n^z} \sum_{d|n} 1\Big) \\
&= \sum_{n=1}^{\infty} \frac{\tau(n)}{n^z}
\end{aligned}$$

$$\boxed{\sum_{n=1}^{\infty} \frac{\tau(n)}{n^z} = \zeta^2(z)}$$

Example:

$$\begin{aligned}\zeta(z)\zeta(z-1) &= \sum_k \frac{1}{k^z} \sum_l \frac{1}{l^{z-1}} \\ &= \sum_{k,l} \frac{l}{(kl)^z} \\ &= \sum_n \frac{1}{n^z} \sum_{l|n} l \\ &= \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^z}\end{aligned}$$

$$\boxed{\therefore \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^z} = \zeta(z)\zeta(z-1)}$$

Example:

$$\begin{aligned}\zeta(z)\zeta(z-w) &= \sum_{k,l} \frac{1}{k^z} \frac{1}{l^{z-w}} \\ &= \sum_n \frac{1}{n^z} \sum_{d|n} \frac{l^w}{=} \sum_{n=1}^{\infty} \frac{\sigma_w(n)}{n^z}\end{aligned}$$

$$\therefore \sum_{n=1}^{\infty} \frac{\sigma_w(n)}{n^z} = \zeta(z)\zeta(z-w)^{40)}$$

Example:

$$\begin{aligned}\zeta(z) \sum_{n=1}^{\infty} \frac{\phi(n)}{n^z} &= \sum_{n=1}^{\infty} \frac{1}{n^z} \sum_{d|n} \phi(d) = \sum_{n=1}^{\infty} \frac{n}{n^z} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^{z-1}} \\ &= \zeta(z-1)\end{aligned}$$

$$\boxed{\therefore \sum_{n=1}^{\infty} \frac{\phi(n)}{n^z} = \frac{\zeta(z-1)}{\zeta(z)}}$$

Exercise: Find $\zeta(z) \cdot \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^z}$

[40)] $\Re(z) > 1$ and $\Re(z-w) > 1$

Example:

$$\begin{aligned}\zeta(z)\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^z} &= \sum_{n=1}^{\infty}\Big(\frac{1}{n^z}\underbrace{\sum_{d|n}\Lambda(d)}_{\log n}\Big)\\ &= \sum_{n=1}^{\infty}\frac{\log n}{n^z}\\ &= -\zeta'(z)\end{aligned}$$

$$\boxed{\therefore \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^z} = -\frac{\zeta'(z)}{\zeta(z)}}$$

Theorem: (Euler Products)
Let $f\colon \mathbb{Z}^+ \to \mathbb{C}$.
Suppose $\sum|f(n)|$ converges. Then if f is multiplicative then

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}(1 + f(p) + f(p^2) + \cdots)$$

(note that the sums $\sum f(p^i)$ converge absolutely) and if f is completely multiplicative then

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}\frac{1}{1 - f(p)}$$

Proof: Let

$$P_l = \prod_{i=1}^{l}(1 + f(p_i) + f(p_i^2) + \cdots)$$

where p_i is the ith prime. Then (since we have absolute convergence)

$$\begin{aligned}P_l &= \sum_{\substack{0\le k_1,\\ 0\le k_2,\ldots\\ 0\le k_l}} f(p_1^{k_1})f(p_2^{k_2})\cdots f(p_l^{k_l})^{41)}\\ &= \sum_{n\in A_l} f(n)\end{aligned}$$

where $A_l = \{\, n \in \mathbb{Z}^+ : \text{if } p_i \mid n \text{ then } i \le l \,\}$

$$= \sum_{n=1}^{\infty} f(n) - \sum_{n\in B_l} f(n)$$

where $B_l = \mathbb{Z}^+ \setminus A_l = \{\, n \in \mathbb{Z}^+ : p_i \mid n \text{ for some } i > l \,\}$

$$\begin{aligned}\therefore \Big|P_l - \sum_{n=1}^{\infty} f(n)\Big| &= \Big|\sum_{n\in B_l} f(n)\Big|\\ &\le \sum_{n\in B_l}|f(n)|\\ &\le \sum_{n>p_l}|f(n)| \to 0 \text{ as } l \to \infty\end{aligned}$$

since $\sum|f(n)|$ converges

Example:

$$\begin{aligned}\zeta(z) &= \sum_{n=1}^{\infty}\frac{1}{n^z}\ ^{42)}\\ &= \prod_p\Big(1+\frac{1}{p^z}+\frac{1}{p^{2z}}+\frac{1}{p^{3z}}+\cdots\Big)\\ &= \prod_p\frac{1}{1-p^{-z}}\\ \frac{1}{\zeta(z)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^z} &= \prod_p\Big(1+\frac{\mu(p)}{p^z}+\frac{\mu(p^2)}{p^{2z}}+\cdots\Big)\\ &= \prod_p\Big(1-\frac{1}{p^z}\Big) = \prod_p(1-p^{-z})\\ \zeta^2(z) = \sum_{n=1}^{\infty}\frac{\tau(n)}{n^z} &= \prod_p\Big(1+\frac{\tau(p)}{p}+\frac{\tau(p^2)}{p}+\cdots\Big)\\ &= \prod_p\Big(1+\frac{2}{p^z}+\frac{3}{p^{2z}}+\frac{4}{p^{3z}}+\cdots\Big)\\ &= \prod_p\Big(\frac{1}{(1-p^{-z})^2}\Big)\end{aligned}$$

PMATH 740 Lecture 30: July 11, 2012

Gamma Function

Definition: For $1 < a \in \mathbb{R}$ we define

$$\Gamma(a) = \int_0^{\infty} t^{a-1}e^{-t}\,\mathrm{d}t$$

Example:

$$\Gamma(1) = \int_0^{\infty} e^{-t}\,\mathrm{d}t = \Big[-e^{-t}\Big]_0^{\infty} = 1$$

Also

$$\begin{aligned}\Gamma(a) &= \int_0^{\infty}\underbrace{t^{a-1}}_{u}\underbrace{e^{-t}}_{\mathrm{d}v}\,\mathrm{d}t\\ &= \int u\,\mathrm{d}v = uv - \int v\,\mathrm{d}u\\ &= \Big[-t^{a-1}e^{-t}\Big]_0^{\infty} + \int_0^{\infty}(a-1)t^{a-2}e^{-t}\,\mathrm{d}t\\ &= 0 + (a-1)\int_0^{\infty}t^{a-2}e^{-t}\,\mathrm{d}t\\ &= (a-1)\Gamma(a-1) \qquad \text{for } a > 2\end{aligned}$$

$$\boxed{\Gamma(a) = (a-1)\Gamma(a-1) \qquad \text{for } a > 2}$$

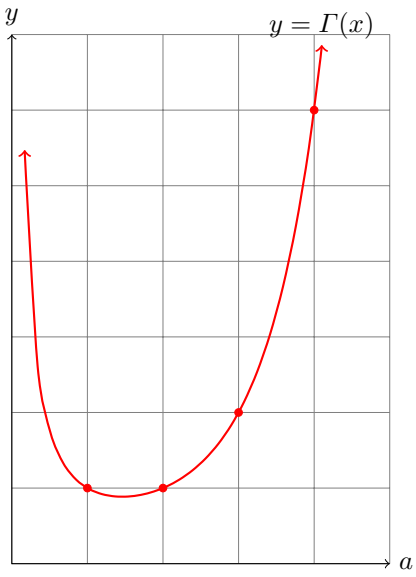
41)

$$\sum_i a_i \sum_j b_j = \sum_{i,j} a_i b_j$$

42) absolute convergence for $\Re(z) > 1$

$\Gamma(2) = 1 \cdot \Gamma(1) = 1$, $\Gamma(3) = 2\Gamma(2) = 2 \cdot 1$, $\Gamma(4) = 3\Gamma(3) = 3!$,

$$\boxed{\Gamma(n+1) = n!}$$



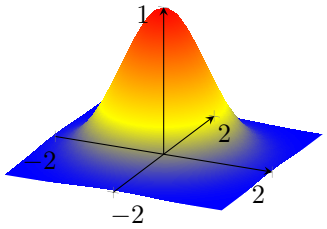
Example:

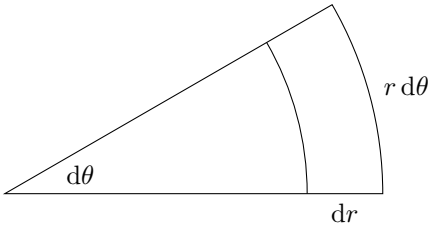
$$\begin{aligned}\Gamma(\tfrac{1}{2}) &= \int_0^\infty t^{-1/2} e^{-t}\,\mathrm{d}t \\ &= \int_{u=0}^\infty \frac{1}{u} e^{-u^2} 2u\,\mathrm{d}u \text{ [43]} \\ &= 2\int_0^\infty e^{-u^2}\,\mathrm{d}u\end{aligned}$$

Say $I = \int_0^\infty e^{-u^2}\,\mathrm{d}u$. Then

$$\begin{aligned}I^2 &= \int_0^\infty e^{-x^2}\,\mathrm{d}x \int_0^\infty e^{-y^2}\,\mathrm{d}y \\ &= \int_{y=0}^\infty \int_{x=0}^\infty e^{-x^2-y^2}\,\mathrm{d}x\,\mathrm{d}y \\ &= \int_{\theta=0}^{\pi/2} \int_{r=0}^\infty e^{-r^2} r\,\mathrm{d}r\,\mathrm{d}\theta\end{aligned}$$

[43] where $u = t^{1/2}$, $u^2 = t$, $2u\,\mathrm{d}u = \mathrm{d}t$





$$
\begin{aligned}
&= \int_{\theta=0}^{\pi/2} \left[-\tfrac{1}{2}e^{-r^2}\right]_0^{\infty} \mathrm{d}\theta \\
&= \int_0^{\pi/2} \tfrac{1}{2}\,\mathrm{d}\theta = \frac{\pi}{4} \\
\therefore I &= \int_0^{\infty} e^{-u^2}\,\mathrm{d}u = \frac{\sqrt{\pi}}{2} \\
\Gamma(\tfrac{1}{2}) &= 2I = \sqrt{\pi}
\end{aligned}
$$

The recursion formula

$$\Gamma(a) = (a-1)\Gamma(a-1)$$

gives

$$
\begin{aligned}
\Gamma(\tfrac{3}{2}) &= \tfrac{1}{2}\Gamma(\tfrac{1}{2}) = \tfrac{1}{2}\sqrt{\pi} \\
\Gamma(\tfrac{5}{2}) &= \tfrac{3}{2}\Gamma(\tfrac{3}{2}) = \tfrac{3}{2}\cdot\tfrac{1}{2}\cdot\sqrt{\pi} \\
&\vdots \\
\Gamma(\tfrac{2n+1}{2}) &= \tfrac{2n-1}{2}\cdots\tfrac{3}{2}\cdot\tfrac{1}{2}\cdot\sqrt{\pi} \\
&\boxed{\Gamma(\tfrac{2n+1}{2}) = \frac{(2n)!}{2^{2n}n!}\sqrt{\pi}}
\end{aligned}
$$

Let $U = \{\, z \in \mathbb{C} : \Re(z) > 1 \,\}$. For $z \in U$ we define

$$\Gamma(z) = \int_0^{\infty} t^{z-1}e^{-t}\,\mathrm{d}t$$

where $t^{z-1} = e^{(z-1)\ln t}$.

$$(\text{note that } |t^{z-1}| = |e^{((x-1)+iy)\ln t}| = |e^{(x-1)\ln t}| = t^{x-1})$$

This integral converges *uniformly* on compact sets $K \subseteq U$.
Proof: Let $K = [p,q] \times [r,s]$ with $p > 1$. Then

$$
\begin{aligned}
\left|\int_l^{\infty} t^{z-1}e^{-t}\,\mathrm{d}t\right| &\le \int_l^{\infty} |t^{z-1}e^{-t}|\,\mathrm{d}t \\
&= \int_l^{\infty} t^{x-1}e^{-t}\,\mathrm{d}t \qquad \text{where } z = x+iy \\
&\le \int_l^{\infty} t^{q-1}e^{-t}\,\mathrm{d}t \to 0 \qquad \text{as } l \to \infty \text{ (independent of } z)
\end{aligned}
$$

since $\int_0^{\infty} t^{q-1}e^{-t}\,\mathrm{d}t$ converges (to $\Gamma(q)$).

It follows that $\Gamma(z)$ is holomorphic in U, indeed we have:
Theorem: Let $f\colon \mathbb{R}^+ \times U \to \mathbb{C}$. Suppose

1. f is continuous
2. $f(t,z)$ is holomorphic in U for each fixed $t \in \mathbb{R}^+$
3. $\int_0^\infty f(t,z)\,\mathrm{d}t$ converges uniformly in compact subsets $K \subseteq U$.

Then the function

$$F(z) = \int_0^\infty f(t,z)\,\mathrm{d}t$$

is holomorphic in U and

$$F'(z) = \int_0^\infty \frac{\partial}{\partial z} f(t,z)\,\mathrm{d}t.$$

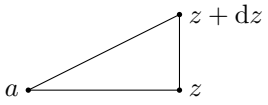
Sketch proof: Verify that $F(z)$ is continuous. For a triangle α in U,

$$\begin{aligned}
\int_\alpha F(z)\,\mathrm{d}z &= \int_\alpha \int_0^\infty f(t,z)\,\mathrm{d}t\,\mathrm{d}z \\
&= \int_0^\infty \underbrace{\int_\alpha f(t,z)\,\mathrm{d}z}_{=0}\,\mathrm{d}t, \qquad \text{by Fubini's Theorem} \\
&= \int_0^\infty 0\,\mathrm{d}t, \qquad \text{by Cauchy} \\
&= 0
\end{aligned}$$

$\therefore F(z)$ is holomorphic in U by Morera's Theorem (indeed $F(z)$ has a holomorphic antiderivative in U given by

$$G(w) = \int_\lambda F(z)\,\mathrm{d}z$$

where $a \in U$ is fixed and λ is the line from a to w.)



Also by Cauchy's Integral Formula, if $w \in U$ and σ is a circle in U about w, then

$$\begin{aligned}
F'(w) &= \frac{1}{2\pi i}\int_\sigma \frac{F(z)}{(z-w)^2}\,\mathrm{d}z \\
&= \frac{1}{2\pi i}\int_\sigma \int_0^\infty \frac{f(t,z)}{(z-w)^2}\,\mathrm{d}t\,\mathrm{d}z \\
&= \int_0^\infty \underbrace{\frac{1}{2\pi i}\int_\sigma \frac{f(t,z)}{(z-w)^2}\,\mathrm{d}z}\,\mathrm{d}t \qquad \text{(Fubini)} \\
&= \int_0^\infty \frac{\partial}{\partial z} f(t,z)\Big|_{z=w}\,\mathrm{d}t.
\end{aligned}$$

Note: We can use the recursion formula

$$\begin{aligned}
\Gamma(z) &= (z-1)\Gamma(z-1) \\
&= (z-1)(z-2)\Gamma(z-2) \\
&\vdots \\
\Gamma(z) &= (z-1)(z-2)\cdots(z-n)\Gamma(z-n)
\end{aligned}$$

equivalently

$$\Gamma(z+n) = (z+n-1)\cdots(z+1)(z)\Gamma(z)$$
$$\text{or} \qquad \Gamma(z) = \frac{\Gamma(z+n)}{(z)(z+1)(z+2)\cdots(z+(n-1))}$$

We use this to define $\Gamma(z)$ for $\Re(z) > -n+1$,

$$z \neq 0,\ -1,\ -2,\ \ldots,\ -(n-1).$$

Since $n \in \mathbb{Z}^+$ is arbitrary, we can use this to *define* $\Gamma(z)$ for all $z \in \mathbb{C}$ except $z = 0,\ -1,\ -2,\ \ldots$ with simple poles at these points.

Theorem: (Euler's Reflection Formula)
For all $z \neq k\pi$ for $k \in \mathbb{Z}$,

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}.$$

PMATH 740 Lecture 31: July 13, 2012

$\Gamma(z)$ is holomorphic in $\mathbb{C} \setminus \{0, -1, -2, \ldots\}$ with simple poles at $z = 0,\ -1,\ -2,\ \ldots$.

Theorem: (Euler's Reflection Formula for Γ)
For $z \in \mathbb{C} \setminus \mathbb{Z}$ we have

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}$$

Proof: For $z = a \in \mathbb{R}$ with $0 < a < 1$,

$$\begin{aligned}\Gamma(a)\Gamma(1-a) &= \int_0^\infty t^{a-1}e^{-t}\,\mathrm{d}t \int_0^\infty t^{-a}e^{-t}\,\mathrm{d}t \\ &= \int_{u=0}^\infty u^{2a-2}e^{-u^2}\cdot 2u\,\mathrm{d}u \int_0^\infty v^{-2a}e^{-v^2}\cdot 2v\,\mathrm{d}v\end{aligned}$$

where $u = v = \sqrt{t}$, $u^2 = v^2 = t$, $2u\,\mathrm{d}u = 2v\,\mathrm{d}v = \mathrm{d}t$

$$\begin{aligned}&= 4\int_{v=0}\int_{u=0} u^{2a-1}v^{1-2a}e^{-u^2-v^2}\,\mathrm{d}u\,\mathrm{d}v \\ &= 4\int_{\theta=0}^{\pi/2}\int_{r=0}^\infty (\tan\theta)^{1-2a}e^{-r^2}r\,\mathrm{d}r\,\mathrm{d}\theta\end{aligned}$$

where $r^2 = u^2 + v^2$, $\tan\theta = \frac{v}{u}$

$$= \int_{\theta=0}^{\pi/2} 2(\tan\theta)^{1-2a}\,\mathrm{d}\theta \int_{r=0}^\infty 2re^{-r^2}\,\mathrm{d}r.$$

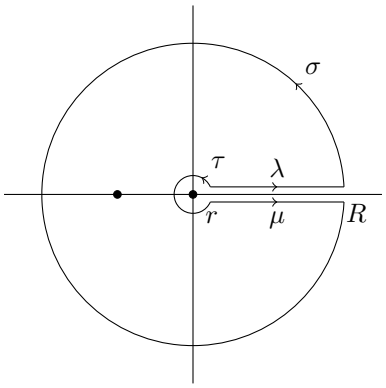
We have

$$\int_{r=0}^\infty 2re^{-r^2}\,\mathrm{d}r = \left[-e^{-r^2}\right]_0^\infty = 1$$

To find $\int_0^{\pi/2} 2(\tan\theta)^{1-2a}\,\mathrm{d}\theta$ we let $x = \tan^2\theta$, $\mathrm{d}x = 2\tan\theta\sec^2\theta\,\mathrm{d}\theta$. Then

$$\int_0^{\pi/2} 2(\tan\theta)^{1-2a}\,\mathrm{d}\theta = \int_{\theta=0}^{\pi/2} \frac{2\tan\theta}{(\tan^2\theta)^a}\cdot\frac{\sec^2\theta}{\sec^2\theta}\,\mathrm{d}\theta = \int_{x=0}^\infty \frac{\mathrm{d}x}{x^a(x+1)}$$

To find $I = \int_0^\infty \frac{x^{-a}}{x+1}\,\mathrm{d}x$ we integrate $f(z) = \frac{z^{-a}}{z+1}$ along the loop $\alpha = \lambda \cdot \sigma \cdot \mu^{-1} \cdot \tau^{-1}$,



where $\lambda(t) = t = te^{i0}$ (with $\log(\lambda(t)) = \ln t + i0$) for $r \le t \le R$

$\mu(t) = t = te^{i2\pi}$ (so $\log(\mu(t)) = \ln t + i2\pi$) for $r \le t \le R$

$\sigma(t) = Re^{it}$ for $0 \le t \le 2\pi$ $(R > 1)$

$\tau(t) = re^{it}$ for $0 \le t \le 2\pi$ $(0 < r < 1)$

By Cauchy's Residue Theorem,

$$\begin{aligned}\int_\alpha f &= 2\pi i \operatorname{Res}(f, -1)\\ &= 2\pi i(-1)^{-a}\\ &= 2\pi i e^{-a\log(-1)}\\ &= 2\pi i e^{-a(\ln 1 + i\pi)}\\ &= 2\pi i e^{-i\pi a}\end{aligned}$$

Also

$$\int_\alpha f = \int_\lambda f + \int_\sigma f - \int_\mu f - \int_\tau f$$

and

$$\int_\lambda f = \int_r^R f(\lambda(t))1\,\mathrm{d}t = \int_r^R \frac{t^{-a}}{t+1}\,\mathrm{d}t \to I \text{ as } r \to 0,\ R \to \infty$$

$$\begin{aligned}
\int_\mu f &= \int_r^R f(\mu(t))\,\mathrm{d}t \\
&= \int_r^R \frac{t^{-a}e^{-i2\pi a}}{t+1}\,\mathrm{d}t \quad (44) \\
&= e^{-i2\pi a}\int_r^R \frac{t^{-a}}{t+1}\,\mathrm{d}t \\
&\to e^{-i2\pi a} I \text{ as } r \to 0,\ R \to \infty
\end{aligned}$$

$$\begin{aligned}
\Big|\int_\sigma f\Big| &\le \text{length}(\sigma) \max_{z \text{ on } \sigma} |f(z)| \\
&= 2\pi R \cdot \max_{0\le t\le 2\pi} \Big|\frac{(Re^{it})^{-a}}{Re^{it}+1}\Big| \quad (45) \\
&= 2\pi R \max_{0\le t\le 2\pi} \Big|\frac{R^{-a}}{Re^{it}+1}\Big| \\
&= 2\pi R \frac{R^{-a}}{R-1} \to 0 \text{ as } R \to \infty
\end{aligned}$$

and

$$\begin{aligned}
\Big|\int_\tau f\Big| &\le \text{length}(\tau) \max_{z \text{ on } \tau} |f(z)| \\
&= 2\pi r \max_{0\le t\le 2\pi} \Big|\frac{r^{-a}}{re^{it}+1}\Big| \\
&= 2\pi r \frac{r^{-a}}{1-r} \\
&= \frac{2\pi r^{1-a}}{1-r} \to 0 \text{ as } r \to 0
\end{aligned}$$

$$2\pi i e^{-i\pi a} = \int_\alpha f = \int_\lambda f + \int_\sigma f - \int_\mu f - \int_\tau f$$

Take the limit as $r \to 0$, $R \to \infty$ to get

$$2\pi i e^{-i\pi a} = I + 0 - e^{-i2\pi a} I + 0$$
$$\therefore I = \frac{2\pi i e^{-i\pi a}}{1 - e^{-i2\pi a}} = \frac{2\pi i}{e^{i\pi a} - e^{-i\pi a}} = \frac{\pi}{\sin(\pi a)} \quad 46)$$
$$\therefore \Gamma(a)\Gamma(1-a) = I = \frac{\pi}{\sin(\pi a)}$$

for $a \in \mathbb{R}$ with $0 < a < 1$. By the Identity Theorem

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}$$

for all $z \in \mathbb{C} \setminus \mathbb{Z}$.

Note: $\Gamma(z)$ is holomorphic in $\mathbb{C} \setminus \{0, -1, -2, \ldots\}$ with simple poles at $z = 0$, -1, -2, ...
$\Gamma(1-z)$ is holomorphic in $\mathbb{C} \setminus \{1, 2, 3, \ldots\}$ with simple poles at $z = 1$, 2, 3, ...
$\frac{\pi}{\sin \pi z}$ is holomorphic in $\mathbb{C} \setminus \mathbb{Z}$ with simple poles at $z \in \mathbb{Z}$ and *no zeros*.
$\therefore \Gamma(z)$ has no zeros in $\mathbb{C} \setminus \mathbb{Z}$. Also $\Gamma(z) \neq 0$ for $z = 1$, 2, 3, ... (otherwise a zero of $\Gamma(z)$ at k would cancel the pole of $\Gamma(1-z)$ so that $\frac{\pi}{\sin \pi z} = \Gamma(z)\Gamma(1-z)$ would be holomorphic at $z = k$).
Thus $\frac{1}{\Gamma(z)}$ is holomorphic in all of $\mathbb{C}$ (it's entire) with zeros at $z = 0$, -1, -2, ... (and no other zeros).

Theorem: $\zeta(z)$ is holomorphic in $\mathbb{C} \setminus \{1\}$ with a simple pole at 1 of residue 1.
Proof: Note that for $n \in \mathbb{Z}^+$,

$$\int_0^\infty t^{z-1} e^{-nt} \, \mathrm{d}t = \int_{s=0}^\infty \left(\frac{s}{n}\right)^{z-1} e^{-s} \frac{1}{n} \, \mathrm{d}s$$

where $s = nt$

$$= \int_0^\infty \frac{1}{n^z} \cdot s^{z-1} e^{-s} \, \mathrm{d}s$$
$$= \frac{1}{n^z} \Gamma(z)$$
$$\therefore \zeta(z) = \sum_{n=1}^\infty \frac{1}{n^z}$$
$$= \sum_{n=1}^\infty \frac{1}{\Gamma(z)} \int_0^\infty t^{z-1} e^{-nt} \, \mathrm{d}t$$

We want to show that

$$\zeta(z) - \frac{1}{z-1}$$

---

44)
$$(\mu(t))^{-a} = e^{-a \log \mu(t)}$$
$$= e^{-a(\ln t + i2\pi)}$$
$$= e^{-a \ln t} e^{-ai2\pi}$$
$$= t^{-a} e^{-i2\pi a}$$

45)
$$(Re^{it})^{-a} = e^{-a \log(Re^{it})}$$
$$= e^{-a(\ln R + it)}$$
$$= e^{-a \ln R} e^{-iat}$$

46) $\sin z = \frac{e^{iz} - e^{-iz}}{2i}$

is entire. We have

$$\begin{aligned}\zeta(z)-\frac{1}{z-1}&=\sum_{n=1}^{\infty}\frac{1}{\Gamma(z)}\int_0^\infty t^{z-1}e^{-nt}\,\mathrm{d}t-\frac{\Gamma(z-1)}{\Gamma(z)}\text{ 47)}\\&=\frac{1}{\Gamma(z)}\Big(\int_0^\infty t^{z-1}\sum_{n=1}^{\infty}e^{-nt}\,\mathrm{d}t-\int_0^\infty t^{z-2}e^{-t}\,\mathrm{d}t\Big)\\&=\frac{1}{\Gamma(z)}\int_0^\infty t^{z-1}\Big(\frac{e^{-t}}{1-e^{-t}}\Big)\text{ 48)}-t^{z-2}e^{-t}\,\mathrm{d}t\end{aligned}$$

$$\boxed{\zeta(z)-\frac{1}{z-1}=\frac{1}{\Gamma(z)}\int_0^\infty t^{z-1}\Big(\frac{1}{e^t-1}-\frac{1}{te^t}\Big)\,\mathrm{d}t}$$

PMATH 740 Lecture 32: July 16, 2012

Theorem: $\zeta(z)$ can be extended to be holomorphic in $\mathbb{C}\setminus\{1\}$ with a simple pole of residue 1 at 1.
Proof:

$$\int_0^\infty t^{z-1}e^{-nt}\,\mathrm{d}t=\cdots=\frac{1}{n^z}\Gamma(z)$$

For $\Re(z)>1$,

$$\begin{aligned}\zeta(z)&=\sum_{n=1}^{\infty}\frac{1}{n^z}=\sum_{n=1}^{\infty}\frac{1}{\Gamma(z)}\int_0^\infty t^{z-1}e^{-nt}\,\mathrm{d}t\\&=\frac{1}{\Gamma(z)}\int_0^\infty t^{z-1}\frac{e^{-t}}{1-e^{-t}}\,\mathrm{d}t\\\zeta(z)&=\frac{1}{\Gamma(z)}\int_0^\infty t^{z-1}\Big(\frac{1}{e^t-1}\Big)\,\mathrm{d}t\end{aligned}$$

for $\Re(z)>1$.

We wish to show that $\zeta(z)-\frac{1}{z-1}$ is holomorphic in $\mathbb{C}$

$$\begin{aligned}\zeta(z)-\frac{1}{z-1}&=\frac{1}{\Gamma(z)}\int_0^\infty t^{z-1}\Big(\frac{1}{e^t-1}\Big)\,\mathrm{d}t-\frac{\Gamma(z-1)}{\Gamma(z)}\\&=\frac{1}{\Gamma(z)}\Big(\int_0^\infty t^{z-1}\Big(\frac{1}{e^t-1}\Big)\,\mathrm{d}t-\int_0^\infty t^{z-2}e^{-t}\,\mathrm{d}t\Big)\end{aligned}$$

$$\boxed{\zeta(z)-\frac{1}{z-1}=\frac{1}{\Gamma(z)}\underbrace{\int_0^\infty t^{z-1}g(t)\,\mathrm{d}t}_{\text{holomorphic for }\Re(z)>0}}$$

where $g(t)=\big(\frac{1}{e^t-1}-\frac{1}{te^t}\big)$.

Note that for $t\in\mathbb{C}$, $\frac{1}{e^t-1}$ is holomorphic in $\mathbb{C}\setminus\{\,i2\pi k:k\in\mathbb{Z}\,\}$ and $\frac{1}{te^t}$ is holomorphic in $\mathbb{C}\setminus\{0\}$, and near

47) $\Gamma(z)=(z-1)\Gamma(z-1)$
48)

$$\sum_{n=1}^{\infty}e^{-nt}=e^{-t}+e^{-2t}+e^{-3t}+\cdots=\frac{e^{-t}}{1-e^{-t}}$$

$t = 0$,

$$\frac{1}{e^t - 1} = \frac{1}{t + \frac{1}{2}t^2 + \cdots} = \frac{1}{t} - \frac{1}{2!} + O(t)$$
$$\frac{1}{te^t} = \frac{1 - t + \frac{1}{2!}t^2}{t} = \frac{1}{t} - 1 + O(t)$$
$$\therefore g(t) = \frac{1}{e^t - 1} - \frac{1}{te^t} = \frac{1}{2} + O(t)$$

so $g(t)$ is holomorphic in $\mathbb{C} \setminus \{\, i2\pi k : 0 \neq k \in \mathbb{Z} \,\}$ (in particular $g(t)$ is holomorphic in $D(0, 2\pi)$).

Aside:

$$\zeta(z) - \frac{1}{z-1} = \frac{1}{\Gamma(z)} \int_0^\infty t^{z-1} g(t)\, \mathrm{d}t^{49)}$$

integrate by parts using $u = g(t)$, $\mathrm{d}v = t^{z-1}\,\mathrm{d}t$, $v = \frac{1}{z}t^z$

$$\zeta(z) - \frac{1}{z-1} = \frac{1}{\Gamma(z)} \Big(\Big[\frac{1}{z} t^z g(t) \Big]_{\substack{\to 0}}^\infty - \int_0^\infty \frac{1}{z} t^z g'(t)\, \mathrm{d}t \Big)$$
$$= \frac{-1}{z\Gamma(z)} \int_0^\infty t^z g'(t)\, \mathrm{d}t = \frac{1}{\Gamma(z)} \int_0^\infty t^z g'(t)\, \mathrm{d}t$$

Suppose, inductively, that for $n \in \mathbb{Z}^+$

$$\zeta(z) - \frac{1}{z-1} = \frac{(-1)^n}{\Gamma(z+n)} \int_0^\infty t^{z+n-1} g^{(n)}(t)\, \mathrm{d}t$$

and that $g^{(n)}(t)$ is of the form

$$g^{(n)}(t) = \frac{p_n(e^t)}{(e^t - 1)^{n+1}} - \frac{q_n(t)}{t^{n+1}e^t}$$

for some polynomials p_n, q_n of degree $\leq n$.

Then we have

$$\frac{\mathrm{d}}{\mathrm{d}t}\Big(\frac{p_n(e^t)}{(e^t-1)^{n+1}} \Big) = \frac{p_n'(e^t)e^t(e^t-1)^{n+1} - p_n(e^t)(n+1)(e^t-1)^n e^t}{(e^t-1)^{2n+2}}$$
$$= \frac{p_n'(e^t)e^t(e^t-1) - p_n(e^t)(n+1)e^t}{(e^t-1)^{n+2}}$$
$$\coloneqq \frac{p_{n+1}(e^t)}{(e^t-1)^{n+2}}$$
$$\frac{\mathrm{d}}{\mathrm{d}t}\Big(\frac{q_n(t)}{t^{n+1}e^t} \Big) = \overset{\text{exercise}}{\cdots} = \frac{q_{n+1}(t)}{t^{n+2}e^t}$$

$\therefore g^{(n+1)}(t)$ is of the required form.

We integrate by parts using $u = g^{(n)}(t)$, $\mathrm{d}v = t^{z+n-1}\,\mathrm{d}t$, $v = \frac{1}{z+n}t^{z+n}$

$$= \frac{(-1)^n}{\Gamma(z+n)} \Big(\Big[\frac{1}{z+n} t^{z+n} g^{(n)}(t) \Big]_{\substack{\to 0}}^\infty - \int_0^\infty \frac{1}{z+n} t^{z+n} g^{(n+1)}(t)\, \mathrm{d}t \Big)$$
$$\zeta(z) - \frac{1}{z-1} = \frac{(-1)^{n+1}}{\Gamma(z+n+1)} \int_0^\infty t^{z+n} g^{(n+1)}(t)\, \mathrm{d}t$$

[49)] $g(t) = \frac{1}{e^t-1} - \frac{1}{te^t}$

By induction we have

$$\boxed{\zeta(z) - \frac{1}{z-1} = \frac{(-1)^n}{\Gamma(z+n)} \int_0^\infty t^{z+n-1} g^{(n)}(t)\,\mathrm{d}t \qquad \text{where} \qquad g(t) = \frac{1}{e^t - 1} - \frac{1}{te^t}}$$

for all $0 \leq n \in \mathbb{Z}$ and for $\Re(z) > 1$.

We can use this formula to extend the definition of $\zeta(z)$ to include all $z \in \mathbb{C}$ with $\Re(z) > -n$, $z \neq 1$. Since n is arbitrary we can define $\zeta(z)$ for all $z \in \mathbb{C}$, $z \neq 1$.

We see that $\zeta(z)$ has a simple pole of residue 1 at 1 and that it has zeros at

$$z = 0, -1, -2, \ldots.$$

Exercise: Note that

$$\int_0^\infty t^{z-1} e^{-(n+a)t}\,\mathrm{d}t = \frac{1}{(n+a)^z}\Gamma(z)$$

Fix $l \in \mathbb{Z}^+$. For $n \in \mathbb{Z}^+$ we can write n uniquely as $n = q \cdot l + r$ with $q \geq 0$, $1 \leq r \leq l$ so

$$\begin{aligned} L_\chi(z) &= \sum_{n=1}^\infty \frac{\chi(n)}{n^z} \\ &= \sum_{r=1}^l \sum_{q=0}^\infty \frac{\chi(ql+r)}{(ql+r)^z} \\ &= \sum_{r=1}^l \sum_{q=0}^\infty \frac{\chi(r)}{l^z(q+\frac{r}{l})^z} \\ &= \sum_{r=1}^l \frac{\chi(r)}{l^2} \sum_{q=0}^\infty \frac{1}{(q+\frac{r}{l})^z} \\ &= \sum_{r=1}^l \frac{\chi(r)}{l^z} \zeta_{r/l}(z) \end{aligned}$$

where for $0 < a < 1$

$$\zeta_a(z) = \sum_{n=0}^\infty \frac{1}{(n+a)^z}$$

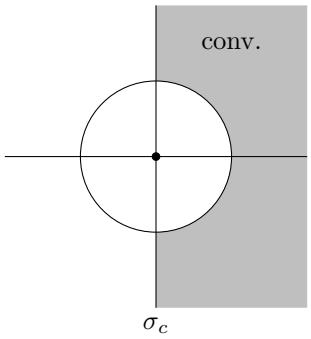
$\zeta_a(z)$ is called the *Hurwitz zeta function.*

Show that $\zeta_a(z)$ is holomorphic in $\mathbb{C} \setminus \{1\}$ with a simple pole of residue 1 at.

What does this imply about $L_{\mathbf{1}}(z)$ and $L_\chi(z)$ for $\chi \neq \mathbf{1}$?

Theorem: (Landau's Convergence Theorem)
Let $\sum_{n=1}^\infty \frac{f(n)}{n^z}$ be a Dirichlet series with real non-negative coefficients $f(n) \geq 0$. If σ_c is finite then the series is *singular* at σ_c (this means that we cannot extend $F(z) = \sum_{n=1}^\infty \frac{f(n)}{n^z}$ to be holomorphic in any disc

$D(\sigma_c, r)$).



PMATH 740 Lecture 33: July 18, 2012

$$\zeta(z) - \frac{1}{z-1} = \underbrace{\frac{1}{\Gamma(z+n)}}_{50)} \underbrace{\int_0^\infty t^{z+n-1} g^{(n)}(t)\,\mathrm{d}t}_{51)}$$

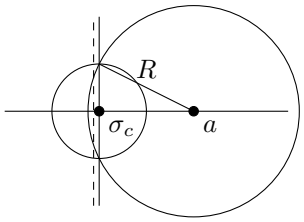
We can see that $\zeta(z) - \frac{1}{z-1}$ can be extended to be holomorphic for $\Re(z) > -n$.
Also, we can see that $\zeta(z)$ has zeros at $0, -1, -2, \ldots$
In fact $\zeta(z)$ has zeros at $z = -2, -4, -6, \ldots$.

Riemann Xi function

$$\xi(z) = \frac{z(z-1)\Gamma(\frac{z}{2})}{2\pi^{z/2}}\zeta(z)?$$

This is entire with $\xi(z) = \xi(1-z)$.

Theorem: (Landau's Convergence Theorem)
Let $\sum \frac{f(n)}{n^z}$ be a Dirichlet series with real non-negative coefficients $f(n) \geq 0$ and with finite abscissa σ_c. Then $F(z) = \sum_{n=1}^\infty \frac{f(n)}{n^z}$ is singular at σ_c.
Proof: Suppose for a contradiction, that $F(z)$ can be extended to be holomorphic in $D(\sigma_c, r)$. Let $a = 1 + \sigma_c$.



[50] holomorphic in $\mathbb{C}$ (with zeros at $-n, -n-1, \ldots$)
[51] holomorphic for $\Re(z) > -n$

Choose $R > 0$ so that $F(z)$ is holomorphic in $D(a, R)$ and $R > a - \sigma_c$. For z with $\Re(z) > \sigma_c$

$$\begin{aligned} F(z) &= \sum_{n=1}^{\infty} \frac{f(n)}{n^z} \\ F'(z) &= \sum_{n=1}^{\infty} \frac{-(\log n) f(n)}{n^z} \\ &\vdots \\ F^{(k)}(z) &= \sum_{n=1}^{\infty} \frac{(-1)^k (\log n)^k f(n)}{n^z} \end{aligned}$$

For $z \in D(a, R)$ we have

$$\begin{aligned} F(z) &= \sum_{k=0}^{\infty} \frac{F^{(k)}(a)}{k!} (z-a)^k \\ &= \sum_{k=0}^{\infty} \underbrace{\sum_{n=1}^{\infty} \frac{(-1)^k (\log n)^k f(n)}{k! n^a}}_{\text{converges}} (z-a)^k \end{aligned}$$

Aside:

$$\begin{aligned} F(z) &= \sum \frac{f(n)}{n^z} = \frac{f(n)}{n^{z-a} \cdot n^a}{}^{52)} \\ &= \sum_{n=1}^{\infty} \frac{f(n)}{n^a} e^{(a-z)\log n} \\ &= \sum_{n=1}^{\infty} \frac{f(n)}{n^a} \sum_{k=0}^{\infty} \frac{(\log n)^k}{k!} (a-z)^k \end{aligned}$$

In particular, this converges for some values $z \in \mathbb{R}$ with $z < \sigma_c$. Then all the terms in the series

$$\sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(\log n)^k f(n)}{k! n^a} (a-z)^k$$

are non-negative so we can interchange summation to get

$$F(z) = \sum_{n=1}^{\infty} \sum_{k=0}^{\infty} \frac{(\log n)^k f(n)}{k! n^a} (a-z)^k = \cdots = \sum_{n=1}^{\infty} \frac{f(n)}{n^z}.$$

Thus the original Dirichlet series converges for some $z \in \mathbb{R}$ with $z < \sigma_c$, and this is not possible.

Theorem: $\zeta(z) \neq 0$ for $\Re(z) \geq 1$.
Proof: We already know that $\zeta(z) \neq 0$ for $\Re(z) > 1$ (since for $\Re(z) > 1$ we have

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}, \; M(z) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^z}$$

and

$$\zeta(z) \cdot M(z) = \sum_{k,l} \frac{1}{k^z} \cdot \frac{\mu(l)}{l^z} = \sum_{n=1}^{\infty} \frac{1}{n^z} \sum_{d|n} \mu(d) = 1$$

52) $\frac{1}{n^{z-a}} = e^{-(z-a)\log n}$

so $\zeta(z) \neq 0$ for $\Re(z) > 1$.)[53]
It remains to show that $\zeta(z) \neq 0$ for $\Re(z) = 1$.

Suppose, for a contradiction, $\zeta(1+ia) = 0$ where $0 \neq a \in \mathbb{R}$. Since $\zeta(\overline{z}) = \overline{\zeta(z)}$ we also have $\zeta(1-ia) = 0$.

Note that the function $\zeta(z)\zeta(z+ia)$ is holomorphic in all of $\mathbb{C}$ since the zero of $\zeta(z+ia)$ cancels the pole of $\zeta(z)$ at $z = 1$ and the zero of $\zeta(z)$ cancels the pole of $\zeta(z+ia)$ at $z = 1-ia$.

Similarly $\zeta(z)\zeta(z-ia)$ is holomorphic in $\mathbb{C}$. Let $F(z) = \zeta(z)^2\zeta(z+ia)\zeta(z-ia)$ which is holomorphic in $\mathbb{C}$. We calculate the coefficients for the Dirichlet series of $F(z)$. For $\Re(z) > 1$

$$\begin{aligned} F(z) &= \zeta(z)^2\zeta(z+ia)\zeta(z-ia) \\ &= \prod_p \Big(\frac{1}{1-p^{-z}}\Big)^2 \prod_p \Big(\frac{1}{1-p^{-z-ia}}\Big) \prod_p \Big(\frac{1}{1-p^{-z+ia}}\Big). \end{aligned}$$

Using the principal branch of the logarithm on the right, and some branch on the left[54]

$$\begin{aligned} \log F(z) &= -\sum_p 2\log(1-p^{-z}) + \log(1-p^{-z-ia}) + \log(1-p^{-z+ia}) \\ &= \sum_p \sum_{k=1}^{\infty} \Big(\frac{2}{kp^{kz}} + \frac{1}{kp^{kz+ika}} + \frac{1}{kp^{kz-ika}}\Big) \\ &= \sum_p \sum_{k\geq 1} \frac{1}{kp^{kz}} \Big(2 + p^{-ika} + p^{ika}\Big) \\ &= \sum_p \sum_{k\geq 1} \frac{2}{kp^{kz}} (1 + \cos(ka\log p))^{55} \\ &= \sum_{n=p^k} \frac{2\Lambda(n)(1+\cos(a\log n))}{\log n \cdot n^z} \\ &= \sum_n \frac{g(n)}{n^z} \end{aligned}$$

where $g(n) = \frac{2\Lambda(n)(1+\cos(a\log n))}{\log n}$

$$\therefore F(z) = e^{\sum_{n=1}^{\infty} \frac{g(n)}{n^z}} = \sum_{k=0}^{\infty} \frac{1}{k!} \Big(\sum_{n=1}^{\infty} \frac{g(n)}{n^z}\Big)^k$$

If we expand this, we will find that the coefficients of $F(z)$ are real and non-negative.

$$F(z) = \zeta(z)^2\zeta(z+ia)\zeta(z-ia)$$

is holomorphic in $\mathbb{C}$ and $F(z) = \sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ with each $f(n) \geq 0$ so by Landau's Theorem σ_c is not finite so $\sigma_c = -\infty$ so $\sum \frac{f(n)}{n^z}$ converges absolutely for all $z \in \mathbb{C}$.

PMATH 740 Lecture 34: July 20, 2012

[53] $\zeta(z) = \prod_p \frac{1}{1-p^{-z}}$, $M(z) = \prod_p (1-p^{-z})$

[54] Aside:

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots \qquad -\log(1-x) = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \cdots$$

[55] Aside:

$$p^{-ika} + p^{ika} = e^{-ika\log p} + e^{ika\log p} = 2\cos(ka\log p)$$

for $n = p^k$, $\log n = k\log p = k\Lambda(n)$, $\frac{1}{k} = \frac{\Lambda(n)}{\log n}$

$\zeta(z) \neq 0$ for $\Re(z) \geq 1$.
We supposed that $\zeta(1+ia) = 0$.
It follows that $F(z) = \zeta(z)^2\zeta(z+ia)\zeta(z-ia)$ is entire, and for $\Re(z) > 1$, $F(z) = \sum_{n=1}^{\infty} f(n)/n^z$ with each $f(n) \geq 0$.

By Landau's Theorem, $F(z) = \sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ converges absolutely for all $z \in \mathbb{C}$.

For all $z \in \mathbb{C}$,

$$F(z) = \sum_n \frac{f(n)}{n^z} = \prod_p \Big(\frac{1}{1-p^{-z}}\Big)^2 \Big(\frac{1}{1-p^{-z-ia}}\Big)\Big(\frac{1}{1-p^{-z+ia}}\Big)$$

If we expand and group together the terms involving products of 2,

$$\sum_{n=2^k} \frac{f(n)}{n^z} = \Big(\frac{1}{1-2^{-z}}\Big)^2 \Big(\frac{1}{1-2^{-z-ia}}\Big)\Big(\frac{1}{1-2^{-z+ia}}\Big)$$

In particular, for $z = x > 0$, we have

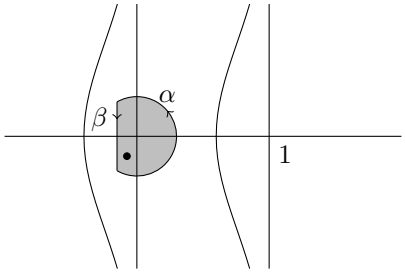
$$\begin{aligned} F(x) &= \sum_{n=1}^{\infty} \frac{f(n)}{n^x} \geq \sum_{n=2^k} \frac{f(n)}{n^k} = \frac{1}{(1-2^{-x})^2} \cdot \frac{1}{(1-2^{-x-ia)}} \cdot \frac{1}{(1-2^{-x+ia)}} \\ &= \frac{1}{(1-2^{-x})^2} \frac{1}{|1-2^{-(x+ia)}|^2} \geq \frac{1}{(1-2^{-x})^2} \cdot \frac{1}{(1+|2^{-(x+ia)}|)^2} \\ &= \frac{1}{(1-4^{-x})^2} \to \infty, \text{ as } x \to 0^+. \end{aligned}$$

This contradicts the fact that $F(z)$ is holomorphic in $\mathbb{C}$ (hence continuous at 0).

Theorem: (Newman's Convergence Theorem)
Let $\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ be a Dirichlet series with $|f(n)| \leq 1$ for all n. Suppose $\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ converges for $\Re(z) > 1$. Suppose the function

$$F(z) = \sum_{n=1}^{\infty} \frac{f(n)}{n^z}$$

(which is holomorphic for $\Re(z) > 1$) extends to be holomorphic on some open set U which contains $\{ z : \Re(z) \geq 1 \}$. Then $\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ converges for $\Re(z) \geq 1$.
Proof: Fix w with $\Re(w) = 1$. Note that $G(z) = F(w+z)$ is holomorphic in $V = U - w = \{ z = u - w : u \in U \}$.



Let $R > 1$ and let $r \in (0, \frac{1}{2})$ be small enough so that the set

$$D = \overline{D}(0, R) \cap \{ z : \Re(z) \geq -r \}$$

is contained in V. Let γ be the loop which goes once (counterclockwise) around ∂D. Let α be the part of γ in $\Re(z) \geq 0$ and let β be the part in $\Re(z) \leq 0$.

We integrate the function

$$F(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)$$

along γ for $l \in \mathbb{Z}^+$.

Note that by Cauchy's Integral Formula

$$\int_\gamma \frac{F(w+z)l^z}{z}\,\mathrm{d}z = 2\pi i \cdot F(w+0)l^0 = 2\pi i F(w)$$

and

$$\int_\gamma \frac{F(w+z)l^z z}{R^2}\,\mathrm{d}z = 0$$

so

$$\begin{aligned}
2\pi i F(w) &= \int_\gamma F(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z \\
&= \int_\alpha F(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z + \int_\beta F(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z \\
&= \int_\alpha S_l(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z + \int_\alpha E_l(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z + \int_\beta F(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z
\end{aligned}$$

where for $\Re(z) > 0$ we have $F(w+z) = \sum_{n=1}^{\infty} \frac{f(n)}{n^{w+z}}$ and we write

$$S_l(w+z) = \sum_{n=1}^{l} \frac{f(n)}{n^{w+z}}$$

$$E_l(w+z) = \sum_{n=l+1}^{\infty} \frac{f(n)}{n^{w+z}}$$

$$2\pi i F(w) = 2\pi i S_l(w) - \int_{-\alpha} S_l(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z + \int_\alpha E_l(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z + \int_\beta F(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z$$

since $\int_{(\alpha)(-\alpha)} S_l(w+z)l^z\big(\frac{1}{z}+\frac{z}{R^2}\big)\,\mathrm{d}z = 2\pi i S_l(w)$, as above.

$$\therefore 2\pi i(F(w)-S_l(w)) = \int_\alpha S_l(w-z)l^{-z}\Big(-\frac{1}{z}-\frac{z}{R^2}\Big)\,\mathrm{d}z + \int_\alpha E_l(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z + \int_\beta F(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z$$

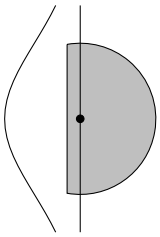
since

$$\int_{-\alpha} g(z)\,\mathrm{d}z = \int_{t_1}^{t_2} g(-\alpha(t))\cdot(-\alpha'(t))\,\mathrm{d}t = -\int_\alpha g(-z)\,\mathrm{d}z$$

$$2\pi i(F(w)-S_l(w)) = A + B$$

$$\text{where } A = \int_\alpha (E_l(w+z)l^z - S_l(w-z)l^{-z})\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z$$

$$B = \int_\beta F(w+z)l^z\Big(\frac{1}{z}+\frac{z}{R^2}\Big)\,\mathrm{d}z.$$



For $z = x + iy$ on α (so $|z| = R$) with $x > 0$

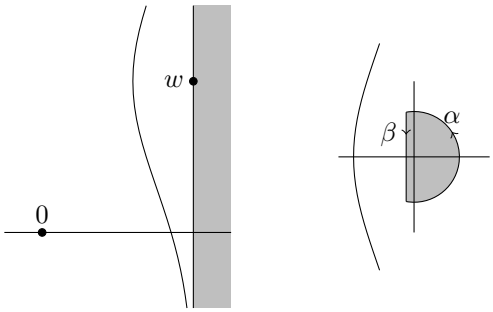
$$\begin{aligned}
\Big|\frac{1}{z} + \frac{z}{R^2}\Big| &= \Big|\frac{\overline{z} + z}{R^2}\Big| = \frac{2x}{R^2} \\
|E_l(w+z)| &= \Big|\sum_{n=l+1}^{\infty} \frac{f(n)}{n^{w+z}}\Big| \le \sum_{n=l+1}^{\infty} \frac{|f(n)|}{|n^{w+z}|} \\
&\le \sum_{n=l+1}^{\infty} \frac{1}{n^{1+x}} \le \int_l^{\infty} \frac{1}{t^{1+x}}\,\mathrm{d}t \\
&= \Big[\frac{-1}{xt^x}\Big]_l^{\infty} = \frac{1}{xl^x} \\
|S_l(w-z)| &= \Big|\sum_{n=1}^{l} \frac{f(n)}{n^{w-z}}\Big| \\
&\le \sum_{n=1}^{l} \frac{1}{n^{1-x}} \\
&= l^{x-1} + \sum_{n=1}^{l-1} n^{x-1} \\
&\le l^{x-1} + \int_0^l t^{x-1}\,\mathrm{d}t \\
&= l^{x-1} + \Big[\frac{t^x}{x}\Big]_0^l \\
&= l^{x-1} + \frac{l^x}{x} \\
&= l^x\Big(\frac{1}{l} + \frac{1}{x}\Big)
\end{aligned}$$

So we have

$$\begin{aligned}
|A| &\le \pi R \max_{x+iy \text{ on } \alpha}\Big(\frac{1}{xl^x} l^x + l^x\Big(\frac{1}{l} + \frac{1}{x}\Big) l^{-x}\Big)\Big(\frac{2x}{R^2}\Big) \\
&= \pi R \max\Big(\frac{2}{x} + \frac{1}{l}\Big)\Big(\frac{2x}{R^2}\Big) \\
&= \pi R \max\Big(\frac{4}{R^2} + \frac{2x}{lR^2}\Big) \\
&= \pi R\Big(\frac{4}{R^2} + \frac{2}{lR}\Big) = \frac{4\pi}{R} + \frac{2\pi}{l}
\end{aligned}$$

PMATH 740 Lecture 35: July 23, 2012

Newman's Convergence Theorem
$\sum \frac{f(n)}{n^z}$, $|f(n)| \le 1$



$$S_l(w) = \sum_{n=1}^{\infty} \frac{f(n)}{n^w}$$

$$\int_\gamma F(w+z) l^z \big(\frac{1}{z} + \frac{z}{R^2}\big)$$

$$2\pi i (F(w) - S_l(w)) = A + B$$

$$A = \int_\alpha (E_l(w+z) l^z - S_l(w-z) l^{-z}) \Big(\frac{1}{z} + \frac{z}{R^2}\Big)\, \mathrm{d}z$$

$$A \le \frac{?}{R} + \frac{?}{l}$$

$$B = \int_\beta F(w+z) l^z \Big(\frac{1}{z} + \frac{z}{R^2}\Big)\, \mathrm{d}z$$

for z on β with $|z| = R$

$$\Big|\frac{1}{z} + \frac{z}{R^2}\Big| = \Big|\frac{\overline{z} + z}{R^2}\Big| = \Big|\frac{2x}{R^2}\Big| = \frac{-2x}{R^2}$$

where $x = \Re(z)$, also β can be given by

$$\beta(t) = -t \pm i\sqrt{R^2 - t^2},\ 0 \le t \le r$$

$$\beta'(t) = -1 \pm i \frac{t}{\sqrt{R^2 - t^2}}$$

$$|\beta'(t)|^2 = 1 + \frac{t^2}{R^2 - t^2} = \frac{R^2}{R^2 - t^2} \le \frac{R^2}{R^2 - r^2} \le \frac{1}{1 - \frac{1}{4}}$$

for z with $\Re(z) = -r$

$$\Big|\frac{1}{z} + \frac{z}{R^2}\Big| = \Big|\frac{1}{z}\Big(1 + \frac{z^2}{R^2}\Big)\Big| \le \frac{1}{r}\Big(1 + \frac{R^2}{R^2}\Big) = \frac{2}{r}$$

$$\therefore |B| \le 2 \int_0^r M \cdot l^{-t} \cdot \frac{2t}{R^2} \cdot N\, \mathrm{d}t + 2RMl^{-r}\frac{2}{r}$$

where $M = \max_{z \text{ on } \beta} |F(w+z)|$, $N = \max_{0 \le t \le r} |\beta'(t)| \le \frac{2}{\sqrt{3}}$

$$\begin{aligned} &= \frac{4MN}{R^2} \int_0^r \frac{t}{l^t}\, \mathrm{d}t + \frac{4RM}{rl^r} \\ &= \frac{4MN}{R^2} \Big[-\frac{t}{\log l \cdot l^t} - \frac{1}{(\log l)^2 l^t}\Big]_0^r + \frac{4RM}{rl^r} \quad 56) \\ &\le \frac{4MN}{R^2 (\log l)^2} + \frac{4RM}{rl^r} \to 0 \text{ as } l \to \infty \end{aligned}$$

Theorem: (Prime Number Theorem)

(1) $\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0$

(2) $\sum_{n \le x} \mu(n) = o(x)$, i.e., $\lim_{x \to \infty} \frac{1}{x} \sum_{n \le x} \mu(n) = 0$

(3) $\psi(x) \sim x$, i.e., $\lim_{x \to \infty} \frac{\psi(x)}{x} = 1$ where $\psi(x) = \sum_{n \le x} \Lambda(n) = \sum_{p^k \le x} \log(p)$

---

56)

$$\int \underbrace{t}_{u} \underbrace{l^{-t}\, \mathrm{d}t}_{\mathrm{d}v} = \frac{-t}{\log l \cdot l^t} + \int \frac{l^{-t}}{\log l}$$

$\mathrm{d}v = e^{-t \log l}$, $v = -\frac{1}{\log l} l^{-t}$

(4) $\vartheta(x) \sim x$, i.e., $\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1$ where $\vartheta(x) = \sum_{p\le x} \log p$

(5) $\pi(x) \sim \frac{x}{\log x}$, i.e., $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$ where $\pi(x) = \sum_{p\le x} 1 = \sum_{n\le x} \rho(n)$

(6) $p_n = p(n) \sim n \log n$ where $\rho(n)$ is the nth prime.

Proof: NCT $\Longrightarrow$ (1)
For $\Re(z) > 1$, $\zeta(z)M(z) = 1$ where $\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$, $M(z) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^z}$

$$\Big(\sum_{k=1}^{\infty} \frac{1}{k^z} \sum_{l=1}^{\infty} \frac{\mu(l)}{l^z} = \sum_{n=1}^{\infty} \frac{1}{n^z} \sum_{d|n} \mu(d) = 1\Big)$$

$\zeta(z)$ is holomorphic in $\mathbb{C} \setminus \{1\}$ with a pole at 1.
$\zeta(z) \neq 0$ for $\Re(z) \ge 1$
The zero set $Z = \{\, z \in \mathbb{C} : \zeta(z) = 0 \,\}$ is a closed set in $\mathbb{C}$

$$F(z) = \begin{cases} 1/\zeta(z) & \text{for } 1 \neq z \in \mathbb{C} \setminus Z \\ 0 & \text{if } z = 1 \end{cases}$$

is holomorphic in $U = \mathbb{C} \setminus Z$.
U is open and includes $\Re(z) \ge 1$.
Since $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^z} = F(z)$ for $\Re(z) > 1$ and $F(z)$ is holomorphic in U
$\therefore$ by NCT $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^z} = F(z)$ for $\Re(z) \ge 1$.
In particular, when $z = 1$ we get $\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = F(1) = 0$

Proof: (1) $\Longrightarrow$ (2) (We need to show that

$$\frac{1}{x} \sum_{n\le x} \mu(n) \to 0 \text{ as } x \to \infty)$$

By Abel's Summation Formula, using $a(n) = \frac{\mu(n)}{n}$, $f(t) = t$ we have

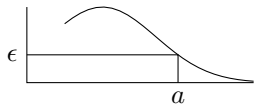
$$\sum_{n\le x} \mu(n) = \sum_{n\le x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t)\,\mathrm{d}t = A(x)x - \int_1^x A(t)\,\mathrm{d}t$$

$$\frac{1}{x} \sum_{n\le x} \mu(n) = A(x) - \frac{1}{x} \int_1^x A(t)\,\mathrm{d}t$$

where $A(x) = \sum_{n\le x} \frac{\mu(n)}{n} \to 0$ as $x \to \infty$ by (1).
It suffices to show that

$$\frac{1}{x} \int_1^x A(t)\,\mathrm{d}t \to 0 \text{ as } x \to \infty$$

(given that $A(t) \to 0$)



Given $\epsilon > 0$ choose $a \ge 1$ so $|A(t)| \le \epsilon$ for $t \ge a$.

Then for $x \geq a$,

$$\begin{aligned}\Big|\frac{1}{x}\int_1^x A(t)\,\mathrm{d}t\Big| &\leq \Big|\frac{1}{x}\int_1^a A(t)\,\mathrm{d}t\Big| + \Big|\frac{1}{x}\int_a^x A(t)\,\mathrm{d}t\Big| \\ &\leq \frac{1}{x}\underbrace{\int_1^a |A(t)|\,\mathrm{d}t}_{\text{constant}} + \frac{x-a}{x}\epsilon \\ &\to \epsilon \text{ as } x \to \infty\end{aligned}$$

(2) $\implies$ (3) (we need to show that

$$\lim_{x\to\infty}\frac{\psi(x)}{x} = 1, \text{ i.e., } \lim_{x\to\infty}\frac{1}{x}\sum_{n\leq x}\Lambda(n) = 1)$$

Recall that $\Lambda(n)$ are the coefficients in the Dirichlet series for $-\frac{\zeta'(z)}{\zeta(z)}$

$$\Big(\sum_{n=1}^{\infty}\frac{1}{n^z}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^z} = \sum_{n=1}^{\infty}\frac{1}{n^z}\sum_{d|n}\Lambda(d) = \sum_{n=1}^{\infty}\frac{\log n}{n^z} = -\zeta'(z)\Big)$$

We need to show

$$\frac{1}{x}\sum_{n\leq x}\Lambda(n) \to 1$$

or equivalently

$$\frac{1}{x}\sum_{n\leq x}(\Lambda(n) - 1) \to 0$$

$\Lambda(n) - 1$ are the coefficients of the Dirichlet series for $-\frac{\zeta'(z)}{\zeta(z)} - \zeta(z)$

$$\begin{aligned}-\frac{\zeta'(z)}{\zeta(z)} - \zeta(z) &= \frac{1}{\zeta(z)}(-\zeta'(z) - \zeta^2(z)) \\ &= \sum_{n=1}^{\infty}\frac{\mu(n)}{n^z}\Big(\sum_{n=1}^{\infty}\frac{\log n}{n^z} - \sum_{n=1}^{\infty}\frac{\tau(n)}{n^z}\Big) \\ &= \sum_{n=1}^{\infty}\frac{1}{n^z}\sum_{\substack{k,l\\kl=n}}\mu(k)(\log l - \tau(l)) \\ \therefore \Lambda(n) - 1 &= \sum_{\substack{k,l\\kl=n}}\mu(k)(\log l - \tau(l))\end{aligned}$$

We need to show that:

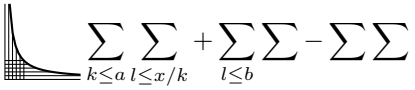
$$\begin{aligned}\frac{1}{x}\sum_{n\leq x}\Big(\sum_{\substack{k,l\\kl=n}}\mu(k)(\log l - \tau(l))\Big) &\to 0 \\ \text{i.e., } \frac{1}{x}\sum_{\substack{k,l\\kl\leq x}}\mu(k)(\log l - \tau(l)) &\to 0\end{aligned}$$

Exercise:

$$\sum_{l\le x}\log l = x\log x - x + O(\log x)$$

$$\sum \tau(l) = x\log x + (2\gamma-1)x + O(\sqrt{x})$$

$$\sum \log l - \tau(l) = -2\gamma x + O(\sqrt{x})$$



PMATH 740 Lecture 36: July 25, 2012

Prime Number Theorem

(1) $\sum_{n=1}^{\infty}\frac{\mu(n)}{n} = 0$

(2) $\sum_{n\le x}\mu(n) = o(x)$

(3) $\psi(x)\sim x$

(4) $\vartheta(x)\sim x$

(5) $\pi(x)\sim\frac{x}{\log x}$

(6) $p(n)\sim n\log n$

(2) $\implies$ (3)
MST

$$\frac{1}{x}\psi(x)\to 1$$

$$\frac{1}{x}\sum_{n\le x}\Lambda(n)\to 1$$

$$\frac{1}{x}\sum_{n\le x}(\Lambda(n)-1)\to 0$$

$\Lambda(n)-1$ are the coefficients of the Dirichlet series

$$\begin{aligned}-\frac{\zeta'(z)}{\zeta(z)} - \zeta(z) &= \frac{1}{\zeta(z)}(-\zeta'(z)-\zeta^2(z))\\ &= \sum_{n=1}^{\infty}\frac{\mu(n)}{n^z}\Big(\sum_{n=1}^{\infty}\frac{\log n}{n^z} - \sum_{n=1}^{\infty}\frac{\tau(n)}{n^z}\Big)\\ &= \sum_{n=1}^{\infty}\frac{1}{n^z}\sum_{\substack{k,l\\ kl=n}}\mu(k)(\log l-\tau(l))\\ \Lambda(n)-1 &= \sum_{\substack{k,l\\ kl=n}}\mu(k)(\log l-\tau(l))\end{aligned}$$

we need to show

$$\frac{1}{x}\sum_{n\le x}(\Lambda(n)-1)\to 0$$

$$\frac{1}{x}\sum_{n\le x}\sum_{\substack{k,l\\ kl=n}}\mu(k)(\log l-\tau(l))\to 0 \text{ as } x\to\infty$$

Recall that

$$\sum_{l\le x}\log l = x\log x - x + O(\log x)$$

$$\sum_{l\le x}\tau(l) = x\log x + (2\gamma-1)x + O(\sqrt{x})$$

$$\text{so } \sum_{l\le x}(\log l - \tau(l)) = -2\gamma x + O(\sqrt{x})$$

It suffices to show that

$$\frac{1}{x}\sum_{\substack{k,l\\ kl\le x}}\mu(k)((\log l - \tau(l) + 2\gamma) - 2\gamma) \to 0$$

Note that

$$\frac{1}{x}\sum_{\substack{k,l\\ kl\le x}}\mu(k)(-2\gamma) = -\frac{2\gamma}{x}\sum_{n\le x}\underbrace{\sum_{d|n}\mu(d)} = -\frac{2\gamma}{x} \to 0$$

So we need to show that

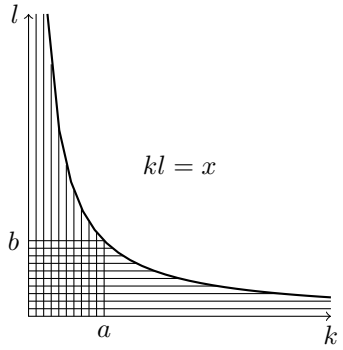
$$\frac{1}{x}\sum_{\substack{k,l\\ kl\le x}}\mu(k)g(l) \to 0$$

where $g(x) = \log l - \tau(l) + 2\gamma$.
We use $\frac{1}{x}\sum_{n\le x}\mu(n) \to 0$ (part (2)) and $\sum_{l\le x} g(l) = O(\sqrt{x})$,
Choose $C > 0$ so

$$\left|\sum_{l\le x} g(l)\right| \le C\sqrt{x}$$

For a, $b \ge 1$ with $ab = x$ we have

$$\frac{1}{x}\sum_{\substack{k,l\\ kl\le x}}\mu(k)g(l) = \frac{1}{x}\sum_{k\le a}\sum_{l\le x/k}\mu(k)g(l) + \frac{1}{x}\sum_{l\le b}\sum_{k\le x/l}\mu(k)g(l) - \frac{1}{x}\sum_{k\le a}\sum_{l\le b}\mu(k)g(l)$$



We have

$$\begin{aligned}\Big|\frac{1}{x}\sum_{k\le a}\Big(\mu(k)\sum_{l\le x/k}g(l)\Big)\Big| &\le \frac{1}{x}\sum_{k\le a}\Big|\sum_{l\le x/k}g(l)\Big| \le \frac{1}{x}\sum_{k\le a}c\sqrt{\frac{x}{k}}\\ &= \frac{c}{\sqrt{x}}\sum_{k\le a}\frac{1}{\sqrt{k}}\\ &= \frac{c}{\sqrt{x}}\Big(2\sqrt{a}+O(1)\Big)^{57)}\\ &= \frac{c}{\sqrt{x}}\Big(2\sqrt{\frac{x}{b}}+O(1)\Big)\\ &= \frac{2c}{\sqrt{b}}+O\Big(\frac{1}{\sqrt{x}}\Big) < \epsilon + O\Big(\frac{1}{\sqrt{x}}\Big)\end{aligned}$$

where we choose b large enough so $\frac{2c}{\sqrt{b}} < \epsilon$

$$\Big|\frac{1}{x}\sum_{l\le b}g(l)\sum_{k\le x/l}\mu(k)\Big| \le \frac{1}{x}\sum_{l\le b}|g(l)|\Big|\sum_{k\le x/l}\mu(k)\Big| = \sum_{l\le b}\frac{|g(l)|}{l}\Big|\frac{1}{x/l}\sum_{k\le x/l}\mu(k)\Big| < \epsilon$$

for all $x \ge r$ where r is chosen so that

$$\frac{|g(l)|}{l}\Big|\frac{1}{x/l}\sum_{k\le x/l}\mu(k)\Big| < \frac{\epsilon}{b}$$

for each $l \le b$ (which we can do by part (c))

$$\begin{aligned}\Big|\frac{1}{x}\sum_{k\le a}\mu(k)\sum_{l\le b}g(l)\Big| &= \frac{1}{x}\Big|\sum_{k\le x/b}\mu(k)\Big|\Big|\sum_{l\le b}g(l)\Big|\\ &= \frac{1}{b}\Big|\frac{1}{x/b}\sum_{k\le x/b}\mu(k)\Big|\cdot c\sqrt{b}\\ &< \epsilon \text{ for all } x \ge 3\end{aligned}$$

where s is chosen large enough.

(3) $\implies$ **(4)** [we have $\frac{\psi(x)}{x} \to 1$ we must show $\frac{\vartheta(x)}{x} \to 1$]

$$\begin{aligned}\vartheta(x) &= \sum_{p\le x}\log p\\ \psi(x) &= \sum_{p^k\le x}\log p = \sum_{p\le x}\sum_{\substack{k\ge 1\\ p^k\le x}}\log p\\ &= \sum_{p\le x}\log p + \sum_{p\le x}\sum_{\substack{k\ge 2\\ p^k\le x}}\log p\\ &= \vartheta(x) + \sum_{2\le k\le \log_2 x}\sum_{p\le x^{1/k}}\log p\\ &= \vartheta(x) + \sum_{2\le k\le \log_2 x}\vartheta(x^{1/k})\end{aligned}$$

[57)] by Euler's Sum Formula

Note that

$$\vartheta(x) = \sum_{p \le x} \log p \le \sum_{p \le x} \log x \le x \log x$$

So we have

$$\begin{aligned}
\psi(x) - \vartheta(x) &= \sum_{2 \le k \le \log_2 x} \vartheta(x^{1/k}) \\
0 \le \psi(x) - \vartheta(x) &\le \sum_{2 \le k \le \log_2 x} x^{1/k} \log x^{1/k} \\
&\le \sum_{2 \le k \le \log_2 x} x^{1/2} \log x^{1/2} \le \log_2 x \cdot x^{1/2} \cdot \log x^{1/2} \\
0 \le \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} &\le \frac{\log_2 x \cdot \log x^{1/2}}{x^{1/2}} = \frac{(\log x)^2}{2 \log 2\sqrt{x}} \to 0 \text{ as } x \to \infty \\
\therefore \left(\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \right) &\to 0
\end{aligned}$$

and $\frac{\psi(x)}{x} \to 1$ so $\frac{\vartheta(x)}{x} \to 1$.

(4) $\implies$ (5) [we have $\vartheta(x) \sim x$, i.e., $\sum_{p \le x} \log p \sim x$; we need to show $\pi(x) \sim \frac{x}{\log x}$, i.e., $\sum_{p \le x} 1 \sim \frac{x}{\log x}$]
We use Abel's Summation Formula with

$$a(n) = \begin{cases} \log p & \text{if } n = p, \text{ prime} \\ 0 & \text{otherwise} \end{cases}$$

so $A(x) = \sum_{n \le x} a(n) = \sum_{p \le x} \log p = \vartheta(x)$ and $f(t) = \frac{1}{\log t}$ so $f'(t) = \frac{-1}{t(\log t)^2}$ to get

$$\begin{aligned}
\pi(x) &= \sum_{p \le x} 1 = \sum_{n \le x} a(n) f(n) \\
&= A(x) f(x) - \int_1^x A(t) f'(t) \, \mathrm{d}t \\
&= \frac{\vartheta(x)}{x} + \int_1^x \frac{\vartheta(t)}{t(\log t)^2} \, \mathrm{d}t \\
\frac{\pi(x) \log x}{x} &= \frac{\vartheta(x)}{x} + \frac{\log x}{x} \int_1^x \frac{\vartheta(t)}{t(\log t)^2} \, \mathrm{d}t
\end{aligned}$$

and using l'Hôpital's Rule

$$\begin{aligned}
\lim_{x \to \infty} \frac{\int_1^x \frac{\vartheta(t) \, \mathrm{d}t}{t(\log t)^2} \; 58)}{\frac{x}{\log x} \; 59)} &= \lim_{x \to \infty} \frac{\frac{\vartheta(x)}{x(\log x)^2}}{\frac{\log x - 1}{(\log x)^2}} \\
&= \lim_{x \to \infty} \frac{\vartheta(x)/x}{\log x - 1} \\
&= 0
\end{aligned}$$

(5) $\implies$ **(6)** [MST $p(n) \sim n \log n$]

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$$
$$\lim_{x\to\infty} (\log \pi(x) + \log\log x - \log x) = 0$$
$$\lim_{x\to\infty} \Big(\frac{\log \pi(x)}{\log x} + \frac{\log\log x}{\log x}^{60)} - 1 \Big) = 0$$
$$\lim_{x\to\infty} \frac{\log \pi(x)}{\log x} = 1$$
$$\therefore \frac{\log \pi(x)}{\log x} \frac{\pi(x)\log x}{x}^{61)} \to 1$$
$$\therefore \frac{\pi(x)\log \pi(x)}{x} \to 1$$

Take $x = p(n)$ so $\pi(x) = n$

$$\frac{n \log n}{p(n)} \to 1.$$

[58)] $\to \infty$
[59)] $\to \infty$
[60)] $\to 0$
[61)] by (5)