PMATH 740: ANALYTIC NUMBER THEORY

HEESUNG YANG

1. September 14: some basics

For the sake of completeness, we are going to review some basics first.

Definition 1. For $n \in \mathbb{N} = \{1, 2, 3, \dots\}$, let p_n be the *n-th prime*. That is, $p_1 = 2, p_2 = 3, \dots$.

Theorem 1 (Euclid)**.** *There are infinitely many primes.*

Proof. Suppose that there are only finitely many primes, say $p_1, \dots, p_n$. Consider

$$m := p_1 p_2 \dots p_n + 1 \geq 2.$$

By the fundamental theorem of arithmetic, m is a product of primes. Thus $p_k \mid m$ for some $k \in \mathbb{N}$ with $1 \leq k \leq n$. Then $p_k \mid (m - p_1 p_2 \dots p_n) = 1$. Then $p_k \mid 1$, which is a contradiction. □

Remark 1. There are many different ways to prove Theorem 1 – for instance, using topology. See Furstenberg's work (doi:10.2307/2307043).

Definition 2. For $x \in \mathbb{R}$, let

$$\pi(x) := \#\{p \leq x : p \text{ prime}\}.$$

By Theorem 1, we have $\pi(x) \to \infty$ as $x \to \infty$. Our goal is understand how "large" $\pi(x)$ is.

Proposition 2. *For $n \in \mathbb{N}$, we have $p_n \leq 2^{2^n}$.*

Proof. We prove this result by induction. For $k = 1$, clearly $p_1 = 2 \leq 2^{2^1} = 4$. Suppose that the result holds for $1 \leq k \leq n$. We have seen in the proof of Theorem 1 that

$$p_{n+1} \leq p_1 p_2 \cdot p_n + 1.$$

Thus by the induction hypothesis, it follows

$$p_{n+1} \leq 2^{2^1} 2^{2^2} \cdots 2^{2^n} + 1 = 2^{2^{n+1}-2} + 1 \leq 2^{2^{n+1}}.$$

By induction, the result follows. □

Corollary 3. *For $x \in \mathbb{R}$ with $x \geq 2$, we have $\pi(x) \geq \log \log x$.*

Date: 2 December 2015.

First proof. Clearly the result holds for $2 \leq x < 4$. For $x \geq 4$, let $s \in \mathbb{N}$ satisfy

$$2^{2^5} \leq x \leq 2^{2^6}.$$

By Proposition 2, we have $p_s \leq 2^{2^s} \leq x$. Thus $\pi(x) \geq s$. By taking logarithms twice, we see that

$$\begin{aligned} x &< 2^{2^{s+1}} \\ \Rightarrow \log x &< 2^{s+1} \log 2 \\ \Rightarrow \frac{\log\left(\frac{\log x}{\log 2}\right)}{\log 2} &< s+1. \end{aligned}$$

It follows that

$$\pi(x) \geq s > \frac{\log\left(\frac{\log x}{\log 2}\right)}{\log 2} - 1 > \log\log x.$$

The last inequality is left as an exercise (*Hint*: $\log 2 < 1$ and calculus). □

Second proof. Note that for all primes p, we have

$$\frac{p-1}{p} \geq \frac{1}{2} \Leftrightarrow \left(1 - \frac{1}{p}\right)^{-1} \leq 2.$$

Thus for $x \geq 2$, we have

$$2^{\pi(x)} \geq \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \geq \sum_{n \leq x} \frac{1}{n} \geq \int_1^x \frac{du}{u} \log x.$$

Thus

$$\pi(x) \geq \frac{\log\log x}{\log 2} \geq \log\log x,$$

as required. □

Conjecture (Fermat; proved to be false)**.** *The numbers of the form* $2^{2^n} + 1$ *for* $n \in \mathbb{N} \cup \{0\}$ *are primes.*

Definition 3. The numbers of the form $F_n := 2^{2^n} + 1$ are the *Fermat numbers.*

Remark 2. Fermat's conjecture is false. Indeed, F_n is a prime for $n = 0, 1, 2, 3, 4$. However, F_5 is not, since $641 \mid F_5$ (proved by Euler in 1732). Also, it is known that $F_6, \ldots, F_{21}$ are composite.

Claim 1. $F_n \mid (F_m - 2)$.

Proof. We have $F_m - 2 = 2^{2^{n+k}} - 1$. Write $x = 2^{2^n}$. Then

$$\frac{F_m - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1 \in \mathbb{N}.$$

The claim now follows. □

Theorem 4 (Pólya)**.** *For* $m, n \in \mathbb{N}$ *with* $n < m$*, we have* $(F_n, F_m) = 1$.

Proof. Let $m = n + k$ for some $k \in \mathbb{N}$, and let $d = (F_n, F_m)$. Since $d \mid F_n$ and $d \mid F_m$, by Claim 1 we have $d \mid (F_m - 2)$. Thus $d \mid 2$ so d is either 1 or 2. But since $2 \nmid F_n$, indeed $d = 1$, as desired. □

Remark 3. From Theorem 4, we obtain another proof of Theorem 1 and Proposition 2.

2. September 16

Theorem 5. *For $x \geq 2$, we have*

$$\pi(x) \geq \frac{\log x}{2 \log 2}.$$

Also, for $n \geq 1$, we have $p_n \leq 4^n$.

Proof. Let $2 = p_1, p_2, \ldots, p_j$ be the primes less than or equal to x. For $n \in \mathbb{N}$ with $n \geq x$, write $n = n_1^2 m$ with $n_1 \in \mathbb{N}$ and m square-free. That is, $m = p_1^{e_1} \cdots p_j^{e_j}$ such that $e_i \in \{0, 1\}$ for each $i = 1, 2, \ldots, j$. Thus, there are at most 2^j possible values for m. and at most $\sqrt{x}$ possible values for n. Thus it follows that $2^j \sqrt{x} \geq x$, or

$$2^j \geq \sqrt{x}. \tag{1}$$

But then recall that $j = \pi(x)$, so indeed we have (from (1)) that $\pi(x) \log 2 \geq \log x/2$. Hence the first claim follows.

Also, take $x = p_n$. Then $j = n = \pi(p_n)$. So again from (1), we have $2^n \geq \sqrt{p_n}$, or equivalently $4^n \geq p_n$. □

In 1896, Hadamard and de la Vallée Poussin proved independently the prime number theorem. More precisely, they showed that (conjectured by Gauss),

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

Let $n \in \mathbb{N}$ and p a prime. Then the exact power dividing $n!$ is

$$\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Claim 2. *We have*

$$\prod_{p \leq 2n} p^{r_p} \equiv 0 \pmod{N},$$

where $N = \binom{2n}{n}$, where $r_p \in \mathbb{N} \cup \{0\}$ satisfies $p^{r_p} \leq 2n < p^{r_p + 1}$.

Proof. Note that the exact power of p dividing $(2n)!$ is

$$\sum_{k=1}^{r_p} \left\lfloor \frac{2n}{p^k} \right\rfloor,$$

and the exact power of p dividing n is

$$\sum_{k=1}^{r_p} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Thus the exact power of p dividing $\binom{2n}{n}$ is

$$\sum_{k=1}^{r_p} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \leq r_p,$$

since

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \leq 1.$$

The claim now follows. □

Theorem 6. *For $x \geq 2$, we have*

$$\left(\frac{3 \log 2}{8} \right) \frac{x}{\log x} < \pi(x) < (6 \log 2) \frac{x}{\log x}.$$

Proof (Erdős). Consider first a lower bound for $\pi(x)$. Note that the binomial coefficient

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \in \mathbb{N}.$$

From Claim 2, we have

$$\binom{2n}{n} \leq \prod_{p \leq 2n} p^{r_p} \leq (2n)^{\pi(2n)}.$$

Note that

$$\binom{2n}{n} = \frac{(2n)(2n-1) \cdots (n+2)(n+1)}{1 \cdot 2 \cdot \cdots \cdot n} = \frac{n+1}{1} \cdot \frac{n+2}{2} \cdot \cdots \cdot 2 \geq 2^n.$$

By the above two inequalities,

$$2^n \leq (2n)^{\pi(2n)}.$$

Hence,

$$\pi(2n) \geq \frac{n \log 2}{\log(2n)} = \left(\frac{\log 2}{2} \right) \frac{2n}{\log(2n)}.$$

Note that $x(\log x)^{-1}$ is increasing for $x \geq e$. For $x \geq 6$, let $n \in \mathbb{N}$ satisfy $\frac{3}{4}x < 2n \leq x$. Then

$$\pi(x) \geq \pi(2n) \geq \left(\frac{\log 2}{2} \right) \left(\frac{2n}{\log(2n)} \right) \geq \left(\frac{\log 2}{2} \right) \frac{\frac{3}{4}x}{\log\left(\frac{3}{4}x\right)} \geq \frac{3 \log 2}{8} \cdot \frac{x}{\log x}.$$

Also, we can check that the lower bound holds for $2 \leq x \leq 6$. We now consider an upper bound. Note that

$$\prod_{n < p \leq 2n} p \,\Bigg|\, \binom{2n}{n}.$$

Therefore $\prod_{n < p \leq 2n} p < (1+1)^{2n} = 2^{2n}$. On the other hand, we have the following lower bound:

$$\prod_{n < p \leq 2n} p \geq n^{\pi(2n) - \pi(n)}.$$

It follows that

$$n^{\pi(2n) - \pi(n)} \leq 2^{2n}.$$

Thus,

$$\pi(2n)\log n - \pi(n)\log n < (\log 2)2n.$$

In other words,

$$\pi(2n)\log n - \pi(n)\log\left(\frac{n}{2}\right) < (\log 2)2n + (\log 2)\pi(n) < (3\log 2)n.$$

Take $n = 2^k$. Then

$$\begin{aligned}
\pi(2^{k+1})\log 2^k - \pi(2^k)\log 2^{k-1} &< (3\log 2)2^k \\
\pi(2^k)\log 2^{k-1} - \pi(2^{k-1})\log 2^{k-2} &< (3\log 2)2^{k-1} \\
&\vdots \\
\pi(8)\log 4 - \pi(4)\log 2 &< (3\log 2)4,
\end{aligned}$$

so upon adding those inequalities we see that

$$\pi(2^{k+1})\log 2^k < (3\log 2)(2^k + 2^{k-1} + \cdots + 4) + 2\log 2 < (3\log 2)2^{k+1}.$$

Thus

$$\pi(2^{k+1}) < (3\log 2)\left(\frac{2^{k+1}}{\log 2^k}\right).$$

So for $x \geq 2$, let $k \in \mathbb{N}$ with $2^k < x \leq 2^{k+1}$. Then $\pi(x) \leq \pi(2^{k+1})$. Hence for $x \geq e$,

$$\pi(x) \leq (3\log 2)\frac{2^{k+1}}{\log 2^k} \leq (6\log 2)\left(\frac{2^k}{\log 2^k}\right) \leq (6\log 2)\frac{x}{\log x}.$$

Also, we can check that the upper bound holds for $2 \leq x \leq e$. □

3. September 18

In 1845, Bertrand showed that there is always a prime p in the interval $[n, 2n]$ for $n \in \mathbb{N}$ provided that $n < 6 \cdot 10^6$. He conjectured that this is always holds. Chebyshev proved this in 1850.

Proposition 7. *For $n \in \mathbb{N}$, we have $\prod_{p \leq n} p \leq 4^n$.*

Proof. We prove this result by induction. The claim holds when $n = 1$ and $n = 2$. Suppose that the result holds for $1 \leq k \leq n-1$. Since for $n > 2$, if n is even then

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p.$$

Thus we can consider only when n is odd. Write $n = 2m+1$ and consider $\binom{2m+1}{m}$. We have

$$\prod_{m+1 < p \leq 2m+1} p \;\Bigg|\; \binom{2m+1}{m}.$$

Note that $\binom{2m+1}{m}$ and $\binom{2m+1}{m+1}$ occur in the binomial expansion of $(1+1)^{2m+1}$ and $\binom{2m+1}{m} = \binom{2m+1}{m+1}$. Thus $\binom{2m+1}{m} \leq \frac{2^{2m+1}}{2} = 4^m$. By our induction hypothesis, we see

$$\prod_{p \leq 2m+1} p = \left(\prod_{p \leq m+1} p\right)\left(\prod_{m+1 < p \leq 2m+1} p\right) \leq 4^{m+1} \cdot 4^m = 4^{2m+1},$$

as required. □

For $\alpha \in \mathbb{N} \cup \{0\}$, we write $p^\alpha \| b$ to mean that $p^\alpha | b$ but $p^{\alpha+1} \nmid b$.

Proposition 8. *If $n \geq 3$ and p is a prime with $\frac{2}{3}n < p \leq n$ then $p \nmid \binom{2n}{n}$.*

Proof. Since $n \geq 3$, if p satisfies $\frac{2n}{3} < p \leq n$, then $p > 2$. Thus p and $2p$ are the only multiples of p with $p \leq 2n$ and so $p^2 \| (2n)!$. Since $\frac{2n}{3} < p \leq n$, we have $p \| n!$. Hence $p^2 \| (n!)^2$. The result follows upon noting that $\binom{2n}{n} = \frac{(2n)!}{n!n!}$. □

4. September 21: Chebyshev's theorem

Theorem 9 (Chebyshev)**.** *For $n \in \mathbb{N}$ there exists a prime p with $n < p \leq 2n$.*

Proof (Erdős). Note that the result holds for $n = 1, 2, 3$. Suppose that the result is false for some $n \in \mathbb{N}$ with $n \geq 4$. Let p be a prime dividing $\binom{2n}{n}$ and $p^{\alpha_p} \| \binom{2n}{n}$. By our assumption, $p \leq n$. Also, by 8, we have $p \leq \frac{2}{3}n$. Let r_p be defined in the proof of Theorem 6, i.e., $p^{r_p} \leq 2n < p^{r_p+1}$. We have seen in the proof of Theorem 6 that $\alpha_p \leq r_p$. Thus $p^{\alpha_p} \leq p^{r_p} \leq 2n$. If $\alpha_p \geq 2$, then $p^2 \leq 2n$, i.e., $p \leq \sqrt{2n}$. By Proposition 7, we have

$$\binom{2n}{n} \leq \left(\prod_{\substack{p \leq \frac{2}{3}n \\ \alpha_p \leq 1}} p \right) \left(\prod_{\substack{p \leq \frac{2}{3}n \\ \alpha_p \geq 2}} p^{\alpha_p} \right) \leq 4^{\frac{2}{3}n} (2n)^{\pi(\sqrt{2n})} \leq 4^{\frac{2}{3}n} (2n)^{\sqrt{2n}}.$$

Note that $\binom{2n}{n}$ is the largest $(2n+1)$ terms in the binomial expression of

$$(1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{2n}{2n}.$$

Therefore,

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}.$$

Combining the above inequalities, we have

$$\frac{4^n}{2n+1} \leq 4^{\frac{2}{3}n} (2n)^{\sqrt{2n}},$$

so we have

$$4^{\frac{n}{3}} \leq (2n)^{\sqrt{2n}} (2n+1) \leq (2n)^{\sqrt{2n}+2}.$$

Taking logarithms, we find that

$$\frac{n}{3} \log 4 < (\sqrt{2n} + 2) \log(2n).$$

By calculus (exercise!) one can show that the above inequality is false for $n \geq 512$. This implies that the statement of the theorem holds for $n \geq 512$. By checking all cases for $n < 512$, we see that the result holds for all $n \in \mathbb{N}$. □

5. September 21: Möbius function and von Mangoldt function

Notation: let f and g be functions from $\mathbb{N}$ or $\mathbb{R}_+$ to $\mathbb{R}$, and suppose that g maps to $\mathbb{R}_+$.

Definition 4. The *big-O notation* $f = O(g)$ means that there exist $c, C \in \mathbb{R}_+$ such that for $x > c$ we have $|f(x)| \leq Cg(x)$. The *little-O notation* $f = o(g)$ means that

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

Finally, $f(x) \sim g(x)$ (i.e., "f *is asymptotic to* g") means

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

Example 1. $20x = O(x), \sin x = O(1), \int_x^\infty \frac{1}{u^2}\,du = O(x^{-1}), x = o(x^2), \sin(x) = o(\log x), \frac{x}{(\log x)^2} = o\left(\frac{x}{\log x}\right)$; $x + 1 \sim x, x + \sqrt{x} \sim x$. Also, recall the prime number theorem:

$$\pi(x) \sim \frac{x}{\log x}.$$

Definition 5. The *Möbius function* μ is defined by

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes and is square-free} \\ 0 & \text{otherwise.} \end{cases}$$

Example 2. 12 is not square-free, so $\mu(12) = 0$. On the other hand, $\mu(15) = \mu(3 \cdot 5) = (-1)^2 = 1$ and $\mu(30) = \mu(2)\mu(3)\mu(5) = (-1)^3 = -1$.

Definition 6. Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the unique factorization of n into distinct prime powers. Then $N := p_1 p_2 \cdots p_r$ is called the *radical* of n.

Proposition 10. $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$.

Proof. If $n = 1$, then the result is immediate from the definition of $\mu(n)$. If $n > 1$, let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the unique factorization of n into distinct prime powers, and let N be the radical of n. Since $\mu(d) = 0$ unless d is square-free, we have

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

Note that the divisors of N are in one-to-one correspondence with the subsets of $\{p_1, \ldots, p_r\}$. Thus the latter sum contains 2^r summands. The number of k-element subsets is $\binom{r}{k}$ and the corresponding divisor d of such a set satisfied $\mu(d) = (-1)^k$. Therefore

$$\sum_{d|N} \mu(d) = \sum_{k=0}^{r} (-1)^k \binom{r}{k} = (1-1)^r = 0,$$

so the claim follows. □

6. September 23

Remark 4. Some analogous relations between $\mathbb{Z}$ and $\mathbb{F}_q[t]$:

	$\mathbb{Z}$	$\mathbb{F}_q[t]$
units	$\{\pm 1\}$	$\mathbb{F}_q$
norm	$\lvert a\rvert$ =absolute value	$\lvert f\rvert = q^{\deg f}$
unique factorization	every positive integer > 1 is a product of primes	every monic polynomial of degree ≥ 1 is a product of monic irreducible polynomials

$$\begin{aligned}\sum_{\substack{f\in\mathbb{F}_q[t]\\ f \text{ monic}}} T^{\deg f} &= \prod_{\substack{v\in\mathbb{F}_q[t]\\ v \text{ monic irred}}} (1+T^{\deg v}+T^{2\deg v}+\cdots)\\ &= \prod_{\substack{v\in\mathbb{F}_q[t]\\ v \text{ monic irred}}} (1-T^{\deg v})^{-1}\\ &= \prod_{d=1}^{\infty}(1-T^{-d})^{-N_d}.\end{aligned}$$

Proposition 11 (Möbius inversion formula)**.** *$f(n) = (1*g)(n) = \sum_{d|n} g(d)$ if and only if $g(n) = (\mu * f)(n) = \sum_{d|n}\mu(d)f(n/d)$.*

Proof. ($\Leftarrow$) Suppose that $g(n) = \sum_{d|n}\mu(d)f(n/d)$. Then we have

$$\begin{aligned}\sum_{d|n} g(d) &= \sum_{d|n}\sum_{e|d}\mu(e)f\left(\frac{d}{e}\right)\\ &= \sum_{est=n}\mu(e)f(s) \quad \left(\text{let } s=\frac{d}{e}\right)\\ &= \sum_{s|n} f(s)\underbrace{\sum_{e|\frac{n}{s}}\mu(e)}_{(*)}.\end{aligned}$$

The claim follows upon noting that $(*)$ is 1 if $n = s$ and 0 otherwise.

($\Rightarrow$) Suppose $f(n) = \sum_{d|n} g(d)$. Then we have

$$\begin{aligned}\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right) &= \sum_{d|n}\mu(d)\sum_{e|\frac{n}{d}} g(e)\\ &= \sum_{des=n}\mu(d)g(e) = \sum_{e|n} g(e)\sum_{d|\frac{n}{e}}\mu(d) = g(n).\end{aligned}$$

□

Definition 7. For $n \in \mathbb{N}$, the *von Mangoldt function*, denoted by $\Lambda(n)$ is defined by

$$\Lambda(n) = \begin{cases}\log p & \text{if } n = p^k \text{ for some } k\in\mathbb{N}\\ 0 & \text{otherwise}\end{cases}.$$

Also for $x \in \mathbb{R}$, we define

$$\theta(x) = \sum_{p \le x} \log p = \log \left(\prod_{p \le x} p \right)$$
$$\psi(x) = \sum_{\substack{p^k \le x \\ \text{for some } k \in \mathbb{N}}} \log p = \sum_{n \le x} \Lambda(n).$$

Note that

$$\psi(x) = \sum_{p \le x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p.$$

Also $p^2 \le x$ is equivalent to $p \le x^{1/2}$; similarly, $p^3 \le x$ is equivalent to $p \le x^{1/3}$ and so forth. Thus we have $\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \cdots$. Since $2^m \le p^m \le x$ we see that $\theta(x^{1/m}) = 0$ provided that $m > \frac{\log x}{\log 2}$. Thus

$$\psi(x) = \sum_{k=1}^{\lfloor \frac{\log x}{\log 2} \rfloor} \theta(x^{1/k}).$$

Since

$$\theta(x) = \sum_{p \le x} \log p \le x \log x,$$

we see that

$$\sum_{k=2}^{\lfloor \frac{\log x}{\log 2} \rfloor} \theta(x^{1/k}) \le \sum_{k=2}^{\lfloor \frac{\log x}{\log 2} \rfloor} x^{1/k} \log(x^{1/k}) \le x^{1/2} \sum_{k=2}^{\lfloor \frac{\log x}{\log 2} \rfloor} \frac{1}{k} \log x = O(x^{1/2} (\log x)^2).$$

Therefore

$$\psi(x) = \theta(x) + O(x^{1/2} (\log x)^2). \tag{2}$$

But what we don't know at this point is whether $\theta(x)$ is the dominant term, which is what we want. We have seen in Theorem 6 that $\pi(x) \le c_1 \frac{x}{\log x}$ for some $c_1 > 0$. Thus

$$\theta(x) = \sum_{p \le x} \log p \le \pi(x) \log x \le c_1 x.$$

Combine this with (2), we see that $\psi(x) \le c_2 x$ for some $c_2 > 0$. Also, we have seen in the proof of Theorem 6 that

$$2^n \le \binom{2n}{n} \text{ and } \binom{2n}{n} \Big| \prod_{p \le 2n} p^{r_p}$$

with $p^{r_p} \le 2n < p^{r_p+1}$. It follows that

$$n \log 2 = \log(2^n) \le \log \binom{2n}{n} \le \sum_{p \le 2n} \left\lfloor \frac{\log 2n}{\log p} \right\rfloor \log p \le \psi(2n).$$

For $x \ge 2$, let $n \in \mathbb{N}$ with $2n \le x < 2n + 2$. Then we have

$$\psi(x) \ge \psi(2n) \ge n \log 2 > \frac{x - 2}{2} \log 2.$$

Thus there exists $c_3 > 0$ such that $\psi(x) > c_3 x$. Again, combine this with (2), we see that $\theta(x) > c_4 x$ for some $c_4 > 0$.

7. September 25

Theorem 12. $\pi(x) \sim \frac{\theta(x)}{\log x} \sim \frac{\psi(x)}{\log x}$.

Remark 5. By Theorem 12, to prove that $\pi(x) \sim \frac{x}{\log x}$ it suffices to show that $\pi(x) \sim \theta(x) \sim x$.

Proof of Theorem 12. We have seen that $\psi(x) = \theta(x) + O(x^{1/2}(\log x)^2)$. Since $\theta(x) > c_4 x$ it follows that

$$\frac{\theta(x)}{\log x} \sim \frac{\psi(x)}{\log x}.$$

Thus it suffices to show that $\pi(x) \sim \frac{\theta(x)}{\log x}$. Note that

$$\theta(x) = \sum_{p \le x} \log p \text{‘} \pi(x) \log x.$$

Thus

$$\pi(x) \ge \frac{\theta(x)}{\log x},$$

that is,

$$\frac{\pi(x)}{\frac{\theta(x)}{\log x}} \ge 1.$$

Note that for any $\delta > 0$, we have

$$\theta(x) = \sum_{p \le x} \log p \ge \log(x^{1-\delta}) \sum_{x^{1-\delta} \le p \le x} 1 \ge (1-\delta) \log x (\pi(x) - \pi(x^{1-\theta})).$$

Thus

$$\begin{aligned} \theta(x) + (1-\delta)\log x(x^{1-\theta}) &\ge (1-\delta)(\log x)\pi x \\ \frac{\theta(x)}{(1-\delta)\log x} + x^{1-\delta} &\ge \pi(x) \\ \frac{1}{1-\delta} + \frac{x^{1-\delta}\log x}{\theta(x)} &\ge \frac{\pi(x)\log x}{\theta(x)}. \end{aligned}$$

Given any $\varepsilon > 0$, we can choose $\delta > 0$ so that $\frac{1}{1-\delta} < 1 + \frac{\varepsilon}{2}$. Since $\theta(x) > c_4 x$ for some $c_4 > 0$ there exists $x_0 \in \mathbb{R}$ such that for $x > x_0$, $\frac{x^{1-\delta}\log x}{\theta(x)} < \frac{\varepsilon}{2}$. Thus for $x > x_0$, we have

$$\frac{\pi(x)\log x}{\theta(x)} < 1 + \varepsilon.$$

Since

$$1 \le \frac{\pi(x)\log x}{\theta(x)} < 1 + \varepsilon,$$

by choosing ε to be arbitrarily close to 0 the result follows. □

The following summation formula by Abel is useful:

Proposition 13 (Abel's summation formula)**.** *Let $\{a_n\}_{n=1}^{\infty}$ be a sequence of complex numbers. Let f be a function from $\{x \in \mathbb{R} : x \geq 1\}$ to $\mathbb{C}$. For $x \in \mathbb{R}$, we write*

$$A(x) := \sum_{n \leq x} a_n.$$

If f has a continuous first derivative for $x \geq 1$, then

$$\sum_{n \leq x} a_n f(n) = A(x)f(x) - \int_1^x A(u)f'(u)\,du.$$

Proof. Let $N = \lfloor x \rfloor$. Then

$$\begin{aligned}\sum_{n \leq N} a_n f(n) &= A(1)f(1) + (A(2) - A(1))f(2) + \cdots + (A(N) - A(N-1))f(N) \\ &= A(1)(f(1) - f(2)) + \cdots + A(N-1)(f(N-1) - f(N)) + A(N)f(N).\end{aligned}$$

Note that for $i \in \mathbb{N}$ and $u \in \mathbb{R}$ with $i \leq u < i+1$, we have $A(u) = A(i)$. Thus

$$A(i)(f(i) - f(i+1)) = \int_i^{i+1} A(u)f'(u)\,du.$$

It follows that

$$\sum_{n \leq N} a_n f(n) = -\int_1^N A(u)f'(u)\,du + A(N)f(N). \tag{3}$$

Also, for $x \geq u \geq N$, we have $A(u) = A(N)$. Thus

$$\int_N^x A(u)f'(u)\,du - A(x)(f(x) - f(N)) = A(x)f(x) - A(N)f(N).$$

or equivalently

$$0 = A(x)f(x) - A(N)f(N) - \int_N^x A(u)f'(u)\,du. \tag{4}$$

Combine (3) and (4), then we get

$$\sum_{n \leq x} a_n f(n) = \sum_{n \leq N} a_n f(n) = A(x)f(x) - \int_1^x A(u)f'(u)\,du,$$

as required. □

Definition 8. Given $x \in \mathbb{R}$, we denote $\{x\}$ the *fractional part* of x. That is, $\{x\} := x - \lfloor x \rfloor$. The *Euler-Mascheroni constant* (or *Euler's constant*) γ is

$$\gamma = 1 - \int_1^{\infty} \frac{\{u\}}{u^2}\,du \; (= 0.57721\ldots).$$

Theorem 14. $\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O(x^{-1})$.

Proof. Take $a_n = 1$ and $f(u) = u^{-1}$. Then

$$A(x) = \sum_{n \leq x} 1 = \lfloor x \rfloor.$$

By Abel's summation formula,

$$\begin{aligned}
\sum_{n\le x}\frac{1}{n} &= \frac{\lfloor x\rfloor}{x}+\int_1^x \frac{\lfloor u\rfloor}{u^2}\,du\\
&= \frac{x-\lfloor x\rfloor}{x}+\int_1^x \frac{u-\{u\}}{u^2}\,du\\
&= 1+O(x^{-1})+\int_1^x \frac{1}{u}\,du-\int_1^x \frac{\lfloor u\rfloor}{u^2}\,du\\
&= 1+O(x^{-1})+\log x-\left(\int_1^\infty \frac{\lfloor u\rfloor}{u^2}\,du-\int_x^\infty \frac{\lfloor u\rfloor}{u^2}\,du\right)\\
&= \log x+\gamma+O(x^{-1})+\int_x^\infty \frac{\lfloor u\rfloor}{u^2}\,du\\
&\le \log x+\gamma+O(x^{-1})+\int_x^\infty \frac{1}{u^2}\,du.
\end{aligned}$$

Note that $\int_x^\infty \frac{1}{u^2}\,du \le \frac{1}{x}$ so the integrand is indeed $O(x^{-1})$. The result follows. □

8. September 30

Let's recall the Abel summation formula:

$$\sum_{n\le x} a_n f(n) = A(x)f(x)-\int_1^x A(u)f'(u)\,du$$

where $A(x)=\sum_{n\le x} a_n$.

Theorem 15. *We have*

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

Proof. Let $a_n=1$ and $f(n)=\log n$. By Abel's summation, we have

$$\begin{aligned}
\sum_{n\le x}\log n &= \lfloor x\rfloor\log x-\int_1^x \frac{\lfloor(\rfloor\, u)}{u}\,du\\
&= (x-\{x\})\log x-\int_1^x \frac{u-\{u\}}{u}\,du\\
&= x\log x+O(\log x)-(x-1)+\int_1^x \frac{\{u\}}{u}\,du\\
&= x\log x-x+O(\log x).
\end{aligned}$$

Furthermore,

$$\begin{aligned}\sum_{n\le x}\log n = \log(\lfloor x\rfloor!) &= \sum_{p\le x}\left(\sum_{k=1}^{\infty}\left\lfloor\frac{x}{p^k}\right\rfloor\right)\log p\\ &= \sum_{p^k\le x}\left\lfloor\frac{x}{p^k}\right\rfloor\log p = \sum_{n\le x}\left\lfloor\frac{x}{n}\right\rfloor\Lambda(n)\\ &= \sum_{n\le x}\left(\frac{x}{n}-\left\{\frac{x}{n}\right\}\right)\Lambda(n) = x\sum_{n\le x}\frac{\Lambda(n)}{n}+O\left(\sum_{n\le x}\Lambda(n)\right).\end{aligned}$$

Since $\sum_{n\le x}\Lambda(n)=\psi(x)=O(x)$, it follows that

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

so

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

or $\sum_{n\le x}\frac{\Lambda(n)}{n}=\log x+O(1)$, as desired. □

Theorem 16. $\displaystyle\sum_{p\le x}\frac{\log p}{p}=\log x+O(1).$

Proof. By Theorem 15, we have

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

Note that

$$\begin{aligned}\sum_{m\ge 2}\sum_{p^m\le x}\frac{\log p}{p^m} &\le \sum_{p}\left(\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)\log p\\ &= \sum_{p}\frac{\log p}{p(p-1)} \le \sum_{n=2}^{\infty}\frac{\log n}{n(n-1)} = O(1).\end{aligned}$$

Combining the above two inequalities, it follows $\sum_{p\le x}\frac{\log p}{p}=\log x+O(1)$. □

Theorem 17. *There exists $\beta \in \mathbb{R}$ such that*

$$\sum_{p \le x} \frac{1}{p} = \log\log x + \beta + O((\log x)^{-1}).$$

Proof. Let

$$a_n = \begin{cases} \frac{\log p}{p} & \text{if } n = p \text{ is a prime} \\ 0 & \textit{otherwise.} \end{cases}$$

Write

$$A(x) = \sum_{n \le x} a_n.$$

By the Abel summation formula, we have

$$\sum_{p \le x} \frac{1}{p} = \frac{A(x)}{\log x} + \int_1^x \frac{A(u)}{u(\log u)^2}\, du.$$

By Theorem 16, we can write $A(x) = \sum_{p \le x} \frac{\log p}{p} = \log x + \gamma(x)$, where

$$\gamma(x) := \sum_{p \le x} \frac{\log p}{p} - \log x = O(1).$$

Also, we note that $A(u) = 0$ for $1 \le u < 2$. Thus

$$\begin{aligned} \sum_{p \le x} \frac{1}{p} &= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{\log u + \gamma(u)}{u(\log u)^2}\, du \\ &= 1 + \int_2^x \frac{1}{u \log u}\, du + \int_2^x \frac{\gamma(u)}{u(\log u)^2}\, du + O\left(\frac{1}{\log x}\right). \end{aligned}$$

It follows that

$$\begin{aligned} \sum_{p \le x} \frac{1}{p} &= 1 + (\log\log x - \log\log 2) + \int_2^x \frac{\gamma(u)}{u(\log u)^2}\, du + O\left(\frac{1}{\log x}\right) \\ &= \log\log x + (1 - \log\log 2) + \int_2^\infty \frac{\gamma(u)}{u(\log u)^2}\, du - \underbrace{\int_x^\infty \frac{\gamma(u)}{u(\log u)^2}\, du}_{=O(\frac{1}{\log x})} + O\left(\frac{1}{\log x}\right) \\ &= \log\log x + \beta + O\left(\frac{1}{\log x}\right), \end{aligned}$$

where $\beta = 1 - \log\log 2 + \int_2^\infty \frac{\gamma(u)}{u(\log u)^2}\, du$ is a constant. □

Definition 9. The constant β is called *Merten's constant*.

Remark 6. One can show that there is a relationship between β and γ. More specifically,

$$\beta = \gamma + \left(\sum_p \log\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right) = 0.261497\ldots,$$

where γ is the Euler-Mascheroni constant.

9. September 30: Riemann ζ-function

For $s \in \mathbb{C}$, consider the series

$$\sum_{n=1}^{\infty} \frac{1}{n^s},$$

which converges absolutely if $\mathrm{Re}(s) > 1$.

Definition 10. For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, the *Riemann zeta-function* is defined by

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Remark 7. Note that

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right).$$

Since a typical term in the above product is of the form

$$\frac{1}{p_1^{a_1 s} \cdots p_k^{a_k s}} = \frac{1}{(p_1^{a_1} \cdots p_k^{a_k})^s} = \frac{1}{n^s},$$

(where $n = p_1^{a_1} \cdots p_k^{a_k}$), by the fundamental theorem of arithmetic for $\mathrm{Re}(s) > 1$ we have

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s).$$

Definition 11. The product $\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ is called the *Euler product representation for* $\zeta(s)$.

10. October 2

Theorem 18. *The following are true:*

(1) For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, we have

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{\infty} \frac{\{u\}}{u^{s+1}}\, du.$$

Therefore it follows

$$\lim_{s \to 1^+} (s-1)\zeta(s) = 1.$$

(2) $\zeta(s)$ has analytic continuation to $\mathrm{Re}(s) > 0$ with $s \neq 1$. It is analytic except for a simple pole at $s = 1$.

Proof. For (a), apply Abel's summation formula with $a_n = 1$ and $f(x) = x^{-s}$. Then we have

$$\sum_{n \leq x} \frac{1}{n^s} = \frac{\lfloor x \rfloor}{x^s} + s \int_1^x \frac{\lfloor u \rfloor}{u^{s+1}}\, du.$$

By letting $x \to \infty$ we see that for $\mathrm{Re}(s) > 1$,

$$\begin{aligned}\zeta(s) &= 0 + s\int_1^\infty \frac{\lfloor u \rfloor}{u^{s+1}}\,du \\ &= s\int_1^\infty \frac{u - \{u\}}{u^{s+1}}\,du \\ &= s\int_1^\infty \frac{1}{u^s}\,du - s\int_1^\infty \frac{\{u\}}{u^{s+1}}\,du \\ &= \frac{s}{s-1} - s\int_1^\infty \frac{\{u\}}{u^{s+1}}\,du.\end{aligned}$$

Therefore $(s-1)\zeta(s) = s - s(s-1)\int_1^\infty \frac{\{u\}}{u^{s+1}}\,du$. Since $\{u\} = O(1)$, the above integral converges for $\mathrm{Re}(s) > 0$. It follows that $\lim\limits_{s\to 1^+}(s-1)\zeta(s) = 1$.

As for part (b), we see that from the identity theorem for analytic functions, since $\int_1^\infty \frac{\{u\}}{u^{s+1}}\,du$ converges for $\mathrm{Re}(s) > 0$, $\zeta(s)$ has an analytic continuation to $\mathrm{Re}(s) > 0$ with $s \neq 1$. □

Theorem 19. *$\zeta(s)$ has no zero in the region $\mathrm{Re}(s) \geq 1$.*

Proof. If $\mathrm{Re}(s) > 1$ we will show in Assignment #2 that $\zeta(s) \neq 0$. Recall that $|u| < 1$, we have

$$-\log(1-u)) = \sum_{n=1}^\infty \frac{u^n}{n}.$$

Thus

$$\log\zeta(s) = \log\left(\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}\right) = \sum_p \sum_{n=1}^\infty \frac{1}{n}\cdot\frac{1}{p^{ns}}.$$

Write $s = \sigma + it$ with $\sigma, t \in \mathbb{R}$. Then

$$p^{-int} = e^{-int\log p} = \cos(-nt\log p) + i\sin(-nt\log p) = \cos(nt\log p) - i\sin(nt\log p).$$

Thus $\mathrm{Re}(p^{-int}) = \cos(nt\log p)$. It follows that

$$\mathrm{Re}(\log\zeta(\sigma+it)) = \sum_p \sum_{n=1}^\infty \frac{p^{-\sigma n}\cos(nt\log p)}{n}.$$

Note that for $\theta \in \mathbb{R}$,

$$0 \leq 2(1+\cos\theta)^2 = 2 + 4\cos\theta + 2\cos^2\theta + 3 + 4\cos\theta + \cos(2\theta).$$

Thus

$$\sum_p \sum_{n=1}^\infty \frac{p^{-\sigma n}}{n}(3 + 4\cos(nt\log p) + \cos(2nt\log p)) \geq 0.$$

This implies that

$$\mathrm{Re}(3\log\zeta(\sigma) + 4\log(\sigma+it) + \log(\sigma+2it)) \geq 0.$$

Particularly, for $\sigma > 1$ and $t \in \mathbb{R}$, we have

$$|\zeta(\sigma)|^3|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)| \geq 1. \qquad (*)$$

Recall that $\lim_{s\to 1^+}(s-1)\zeta(s)=1$. Hence

$$\lim_{\sigma\to 1^+}|\zeta(\sigma)|=\lim_{\sigma\to 1^+}|(\sigma-1)^{-1}|.$$

Suppose that $1+it_0$ is a zero of $\zeta(s)$ of order $m\geq 1$, i.e., when $\sigma+it\to 1+it_0$ we have

$$\zeta(\sigma+it)=((\sigma+it)-(1+it_0))g\sigma+it)$$

for some function g with $g(1+it_0)\neq 0$. Since $\zeta(s)$ has a pole at $s=1, t_0\neq 0$. Also, by taking $t=t_0$ we have

$$\lim_{\sigma\to 1^+}|\zeta(\sigma+it_0)|=C_1$$

for some constant $C_1\neq 0$. Hence

$$\lim_{\sigma\to 1^+}|\zeta(\sigma+it_0)|=\lim_{\sigma\to 1^+}|C_1(\sigma-1)^m|.$$

Also, since $1+2it_0$ is not a pole of $\zeta(s)$ there exists C_2 such that

$$\lim_{\sigma\to 1^+}|\zeta(\sigma+2it_0)|\ C_2.$$

Since $m\geq 1$, we have

$$\lim_{\sigma\to 1^+}|\zeta(\sigma)|^3\cdot|\zeta(\sigma+it_0)|^4\cdot|\zeta(\sigma+2it_0)|=\lim_{\sigma\to 1^+}|(\sigma-1)^{-3}\cdot c_1^4(\sigma-1)^{4m}\cdot c_2|=0,$$

but this contradicts $(*)$. Therefore $\zeta(s)$ has no zeros in $\mathrm{Re}(s)>1$. □

11. October 5

We proved last class that:

(1) the analytic continuation of $\zeta(s)$ to $\mathrm{Re}(s)>0$
(2) the non-vanishing of $\zeta(s)$ on $\mathrm{Re}(s)=1$.

These are the main ingredients to prove the prime number theorem.

Theorem 20 (Donald J. Newman)**.** *Let $a_n\in\mathbb{C}$ with $|a_n|\leq 1$ for $n\in\mathbb{N}$. Consider the series*

$$\sum_{n=1}^{\infty}\frac{a_n}{n^s},$$

which converges to an analytic function, say $F(s)$ for $\mathrm{Re}(s)>1$. If $F(s)$ can be analytically continued to $\mathrm{Re}(s)\geq 1$, then the series converges to $F(s)$ for $\mathrm{Re}(s)\geq 1$.

Proof. Let $w\in\mathbb{C}$ with $\mathrm{Re}(w)\geq 1$. Thus $F(z+w)$ is analytic for $\mathrm{Re}(z)\geq 0$. Choose $R\geq 1$ and let $\delta=\delta(R)>0$ so that $F(z+w)$ is analytic on the region. Define

$$\widetilde{\Gamma}:=\{z\in\mathbb{C}:\mathrm{Re}(z)\geq-\delta,|z|\leq R\}.$$

Let M denote the maximum of $|F(z+w)|$ on $\widetilde{\Gamma}$, and let Γ denote the contour obtained by following the boundary of $\widetilde{\Gamma}$ counterclockwise.

Let A be the part of Γ with $\mathrm{Re}(z)>0$ and B the remainder part of Γ. For $N\in\mathbb{N}$, consider the function

$$F(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right),$$

which is analytic on $\widetilde{\Gamma}$, except a (possible) simple pole at $z = 0$. Then by Cauchy's residue theorem, we see

$$\begin{aligned} 2\pi i F(w) &= \int_{\Gamma} F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz \\ &= \int_{A} F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz + \int_{B} F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz. \end{aligned} \tag{5}$$

We see that on A, $F(z+w)$ is equal to its series.

Split the series as

$$S_N(z+w) = \sum_{n=1}^{N} \frac{a_n}{n^{z+w}}$$

and

$$R_N(z+w) = F(z+w) - S_N(z+w).$$

Note that $S_N(z+w)$ is analytic for $z \in \mathbb{C}$. Let C be the contour given by the path $|z| = R$, taken in counterclockwise direction. Thus by Cauchy's residue theorem, we have

$$2\pi i S_N(w) = \int_{C} S_N(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz.$$

Note that $C = A \cup (-A) \cup \{iR, -iR\}$. Thus

$$2\pi i S_N(w) = \int_{A} S_N(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz + \int_{-A} S_N(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz.$$

By changing variable z to $-z$ in the above integral, we see that

$$\int_{-A} S_N(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz = \int_{A} S_N(-z+w) N^{-z} \left(\frac{1}{z} + \frac{z}{R^2}\right) dz.$$

Thus

$$2\pi i S_N(w) = \in_A \left(S_N(z+w) N^z + S_N(-z+w) N^{-z}\right) \left(\frac{1}{z} + \frac{z}{R^2}\right) dz.$$

Combining this with (5), we have

$$\begin{aligned} 2\pi i (F(w) - S_N(w)) = &\int_{A} (R_N(z+w) N^z - S_N(-z+w) N^{-z}) \left(\frac{1}{z} + \frac{z}{R^2}\right) dz \\ &+ \int_{B} F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz \end{aligned}$$

We now need to show that $S_N(w) \to F(w)$ as $N \to \infty$. Write $z = x + iy$ with $x, y \in \mathbb{R}$. Then for $z \in A$, we have $|z| = R$ and thus

$$\frac{1}{z} + \frac{z}{R^2} = \frac{2x}{R^2}.$$

Since $|n^z| = n^x$ we have

$$|R_N(z+w)| \leq \sum_{n=N+1}^{\infty} \frac{1}{n^{\mathrm{Re}(z+w)}} \leq \sum_{n=N+1}^{\infty} \frac{1}{n^{x+1}} \leq \int_{N}^{\infty} \frac{1}{u^{x+1}}\, du = \frac{1}{xN^x}.$$

Also, we have

$$|S_N(-z+w)| \le \sum_{n=1}^{N} \frac{1}{n^{-x+1}} \le N^{x-1} + \sum_{n=1}^{N} u^{x-1}\,du \le N^{x-1} + \frac{N^x}{x}.$$

Therefore $|S_N(-z+w)| \le N^x\left(\frac{1}{N}+\frac{1}{x}\right)$. Combining the above estimates, we have

$$\begin{aligned}
&\left|\int_A (R_N(z+w)N^z - S_N(-z+w)N^{-z})\left(\frac{1}{z}+\frac{z}{R^2}\right)dz\right| \\
&\le \int_A \left(\frac{1}{xN^x}N^x + N^x\left(\frac{1}{N}+\frac{1}{x}\right)N^{-x}\right)\frac{2x}{R^2}\,dz \\
&= \int_A \left(\frac{2}{x}+\frac{1}{N}\right)\frac{2x}{R^2}\,dz \le \int_A \left(\frac{4}{R^2}+\frac{2x}{NR^2}\right)dz \\
&\le \left(\frac{4}{R^2}+\frac{2}{NR^2}\right)\pi R \quad (\because x \in R) \\
&= \frac{4\pi}{R^2}+\frac{2\pi}{N}.
\end{aligned}$$

We now estimate the integral over B. Divide B into two parts: $\mathrm{Re}(z) = -\delta$ and $-\delta < \mathrm{Re}(z) \le 0$. For $z \in B$ with $\mathrm{Re}(z) = -\delta$ since $|z| \le R$ we have

$$\left|\frac{1}{z}+\frac{z}{R^2}\right| = \left|\frac{1}{z}\right|\left|\frac{\bar{z}}{z}+\frac{\bar{z}z}{R}\right| \le \frac{1}{\delta}\left(1+\frac{|z|^2}{R^2}\right) \le \frac{2}{\delta}.$$

Let

$$S_N(z+w) = \sum_{n=1}^{N} \frac{a_n}{n^{z+w}},$$

where $\mathrm{Re}(w) \ge 1$. We have shown that

$$2\pi i(F(w) - S_N(w)) = \underbrace{\int_A (*)\,dz}_{\le \frac{4\pi}{R}+\frac{2\pi}{N}} + \int_B F(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz. \tag{6}$$

Divide B into two parts: $\mathrm{Re}(z) = -\delta$ and $-\delta < \mathrm{Re}(z) < 0$. For $z \in B$, $\left|\frac{1}{z}+\frac{z}{R^2}\right| \le 2\delta^{-1}$. Since $|F(z+w)| \le M$ for $z \in B$, we have

$$\begin{aligned}
\left|\int_B F(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz\right| &\le \int_{-R}^{R} MN^{-\delta}\frac{2}{\delta}\,dz + 2\left|\int_{-\delta}^{0} MN^x\frac{2x}{R^2}\,dx\right| \\
&\le \frac{4MR}{\delta N^\delta} + \frac{4M}{R^2}\underbrace{\left|\int_{-\delta}^{0} xN^x\,dx\right|}_{\left(\frac{1}{\log N}-\frac{1}{N^\delta \log x}\right)(ex)} \\
&\le \frac{4MR}{\delta N^\delta} + \frac{4M\delta}{R^2\log N}.
\end{aligned} \tag{7}$$

Combining (**??**) and (7) gives us

$$|2\pi i(F(w) - S_N(w))| \le \frac{4\pi}{R} + \frac{2\pi}{N} + \frac{4MR}{\delta N^\delta} + \frac{4M\delta}{R^2\log N},$$

or equivalently

$$|F(w) - S_N(w)| \leq \frac{2}{R} + \frac{1}{N} + \frac{MR}{\delta N^\delta} + \frac{2M\delta}{R^2 \log N}.$$

Given $\varepsilon > 0$, choose $R = \frac{3}{\varepsilon}$. Then for N sufficiently large, we have $|F(w) - S_N(w)| < \varepsilon$. It implies that $S_N(w) \to F(w)$ as $N \to \infty$, as required. □

12. October 7

Theorem 21. *Let μ be the Möbius function. Then*

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0.$$

Proof. Fro $\mathrm{R}e(s) > 1$, we have

$$\frac{1}{\zeta(s)} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

We have seen in Theorems 18 and 19 that the function $(s-1)\zeta(s) = f(s)$ is analytic and nonzero in $\mathrm{R}e(s) \geq 1$. Thus

$$\frac{1}{\zeta(s)} = \frac{s-1}{f(s)},$$

which is analytic in $\mathrm{R}e(s) \geq 1$. In particular, it converges at $s = 1$. Since $\zeta(s)$ has a (simple) pole at $s = 1$, then $\zeta(s)^{-1}$ has a zero at $s = 1$. It follows that

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = \frac{1}{\zeta(1)} = 0,$$

as required. □

Theorem 22. $\sum_{n \leq x} \mu(n) = o(x)$.

Proof. Take $a_n := \mu(n)/n$ and $f(u) = u$. Then

$$A(x) = \sum_{n \leq x} \frac{\mu(n)}{n} = o(1)$$

by Theorem 21. Now the theorem follows immediately from the Abel summation formula: note that

$$\sum_{n \leq x} \mu(n) = xA(x) - \int_1^x A(u)\, du = o(x).$$ □

Definition 12. We say $(x_1, \ldots, x_n) \in \mathbb{R}^n$ is a *lattice point* if $x_i \in \mathbb{Z}$ for all $i = 1, 2, \ldots, n$.

Theorem 23. *Let $d(n)$ be the number of positive divisors of n. We have then*

$$\sum_{m=1}^{n} d(m) = \sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor = n \log n + (2\gamma - 1)n + O(\sqrt{x}),$$

where γ is the Euler-Mascheroni constant.

Proof. Let $D_n := \{(x,y) \in \mathbb{R}^2 : x > 0, y > 0, xy \le n\}$. Let $(x,y) \in D_n$ be a lattice point. Note that each lattice point in D_n satisfies $xy = m$ for some $m \in \mathbb{N}$ with $1 \le m \le n$. Thus $\sum_{m=1}^{n}$ is the number of lattice points in D_n. Note that each fixed $x \in \{1, \dots, n\}$, there are $\left\lfloor \frac{n}{x} \right\rfloor$ many y with $xy \le n$. Hence

$$\sum_{m=1}^{n} d(m) = \sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor.$$

Divide the lattice points in D_n into three disjoint regions:

$$D_{n,1} := \{(x,y) \in \mathbb{N}^2, xy \le n, x < y\}$$
$$D_{n,2} := \{(x,y) \in \mathbb{N}^2, xy \le n, x > y\}$$
$$D_{n,3} := \{(x,y) \in \mathbb{N}^2, xy \le n, x = y\}.$$

We have $|D_{n,1}| = |D_{n,2}|$. Let $(x,y) \in D_{n,1}$. Then $x^2 < xy \le n$, or $x < \sqrt{n}$. Also, for a fixed x, the number of y satisfying $xy \le n$ and $y > x$ is $\left\lfloor \frac{n}{x} \right\rfloor - \lfloor x \rfloor$. Also, $|D_{n,3}| = \lfloor \sqrt{n} \rfloor$. Also,

$$\begin{aligned}
\sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor &= 2 \sum_{x=1}^{\lfloor \sqrt{n} \rfloor} \left(\left\lfloor \frac{n}{x} \right\rfloor - \lfloor x \rfloor \right) + \lfloor \sqrt{n} \rfloor \\
&= 2 \sum_{x=1}^{\lfloor \sqrt{n} \rfloor} \left(\frac{n}{x} - x + O(1) \right) + \lfloor \sqrt{n} \rfloor \\
&= 2n(\log \lfloor \sqrt{n} \rfloor + \gamma + O(n^{-1/2})) - 2 \left(\frac{\lfloor \sqrt{n} \rfloor (\lfloor \sqrt{n} \rfloor + 1)}{2} \right) + O(\sqrt{n}),
\end{aligned}$$

with the last equality following from Theorem 14.

Since $\lfloor \sqrt{n} \rfloor = \sqrt{n} - \{\sqrt{n}\}$ and $\log(1-r) = O(r)$ for $0 < r < 1$ we have

$$\begin{aligned}
\log(\lfloor \sqrt{n} \rfloor) = \log(\sqrt{n} - \{\sqrt{n}\}) &= \log \left(\sqrt{n} \left(1 - \frac{\{\sqrt{n}\}}{\sqrt{n}} \right) \right) \\
&= \log \sqrt{n} + \log \left(1 - \frac{\{\sqrt{n}\}}{\sqrt{n}} \right) = \log \sqrt{n} + O(n^{-1/2}).
\end{aligned}$$

Combining all the estimates presented here, we get

$$\begin{aligned}
\sum_{m=1}^{n} d(m) = \sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor &= 2n(\log \sqrt{n} + \gamma + O(n^{-1/2})) - n + O(\sqrt{n}) \\
&= n \log n + (2\gamma - 1)n + O(\sqrt{n}).
\end{aligned}$$

□

13. October 9

Proposition 24. *Given a function $f : \mathbb{R}_+ \to \mathbb{C}$, let*

$$F(x) = \sum_{n \le x} f\left(\frac{x}{n}\right).$$

Then

$$f(x) = \sum_{n \le x} \mu(n) F\left(\frac{x}{n}\right).$$

Proof. By Proposition 10, we have

$$\begin{aligned} f(x) &= \sum_{n\le x}\left(\sum_{k\mid n}\mu(k)\right) f\left(\frac{x}{n}\right) \\ &= \sum_{kl\le x}\mu(k) f\left(\frac{x}{kl}\right) \\ &= \sum_{k\le x}\mu(k)\left(\sum_{l\le \frac{x}{k}} f\left(\frac{x}{kl}\right)\right) = \sum_{k\le x}\mu(k)F\left(\frac{x}{k}\right). \end{aligned}$$

□

Theorem 25 (Prime number theorem)**.** $\pi(x) \sim \frac{x}{\log x}$.

Proof. By Theorem 12, it suffices to prove that

$$\psi(x) = \sum_{p^k\le x}\log p \sim x.$$

Let

$$F(x) := \sum_{n\le x}\left(\psi\left(\frac{x}{n}\right) - \left\lfloor\frac{x}{n}\right\rfloor + 2\gamma\right).$$

By Proposition 24, we have

$$\psi(x) - \lfloor x\rfloor + 2\gamma = \sum_{n\le x}\mu(n)F\left(\frac{x}{n}\right),$$

that is,

$$\psi(x) = x + O(1) + \sum_{n\le x}\mu(n)F\left(\frac{x}{n}\right).$$

Our goal is to show that

$$\sum_{n\le x}\mu(n)F\left(\frac{x}{n}\right) = o(x).$$

We have

$$F(x) = \sum_{n\le x}\psi\left(\frac{x}{n}\right) - \sum_{n\le x}\left\lfloor\frac{x}{n}\right\rfloor + 2\gamma\lfloor x\rfloor. \tag{8}$$

Note also that

$$\begin{aligned}\sum_{n\le x}\psi\left(\frac{x}{n}\right) &= \sum_{n\le x}\sum_{m\le\frac{x}{n}}\Lambda(m)\\ &= \sum_{m\le x}\Lambda(m)\left(\sum_{n\le\frac{x}{m}}1\right)\\ &= \sum_{m\le x}\Lambda(m)\left\lfloor\frac{x}{m}\right\rfloor\\ &= \sum_{\substack{p\le x\\ p\text{ prime}}}\log p\left(\left\lfloor\frac{x}{p}\right\rfloor+\left\lfloor\frac{x}{p^2}\right\rfloor+\cdots\right)\\ &= \log(\lfloor x\rfloor!)=\sum_{n\le x}\log n.\end{aligned}$$

Note that the sum $\left\lfloor\frac{x}{p}\right\rfloor+\left\lfloor\frac{x}{p^2}\right\rfloor+\cdots$ ends at $\left\lfloor\frac{x}{p^k}\right\rfloor$ where $p^k\,\|\,x$.

We have seen in the proof of Theorem 15 that

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

from which it follows

$$\sum_{n\le x}\psi\left(\frac{x}{n}\right) = x\log x - x + O(\log x). \tag{9}$$

By Theorem 23,

$$\sum_{n=1}^{\lfloor x\rfloor}\left\lfloor\frac{\lfloor x\rfloor}{n}\right\rfloor = \lfloor x\rfloor\log\lfloor x\rfloor + (2\gamma-1)\lfloor x\rfloor + O(x^{1/2}).$$

Note that

$$\sum_{n=1}^{\lfloor x\rfloor}\left\lfloor\frac{\lfloor x\rfloor}{n}\right\rfloor \le \sum_{n=1}^{\lfloor x\rfloor}\left\lfloor\frac{x}{n}\right\rfloor \le \sum_{n=1}^{\lfloor x\rfloor}\left\lfloor\frac{\lfloor x\rfloor+1}{n}\right\rfloor.$$

Therefore

$$\sum_{n=1}^{\lfloor x\rfloor}\left\lfloor\frac{x}{n}\right\rfloor = x\log x + (2\gamma-1)x + O(x^{1/2}). \tag{10}$$

Combining (8), (9), and (10) gives

$$F(x) = (x\log x - x + O(\log x)) - (x\log x + (2\gamma-1)x + O(x^{1/2})) + (2\gamma x + O(1)) = O(x^{1/2}).$$

Hence there is a constant $c > 0$ such that for $x \geq 1$, we have $|F(x)| < cx^{1/2}$. Suppose $t \in \mathbb{N}$ and $t \geq 2$. Then

$$\begin{aligned}\left|\sum_{n\leq \frac{x}{t}} \mu(n)F\left(\frac{x}{n}\right)\right| &\leq \sum_{n\leq \frac{x}{t}} \left|F\left(\frac{x}{n}\right)\right| \leq \sum_{n\leq \frac{x}{t}} c\left(\frac{x}{n}\right)^{1/2} \\ &\leq cx^{1/2}\left(1+\int_1^{x/t}\frac{du}{u^{1/2}}\right) \leq cx^{1/2}\left(1+2\left(\frac{x}{t}\right)^{1/2}-2\right) \leq 2\frac{cx}{\sqrt{t}}.\end{aligned} \tag{11}$$

Observe that F is a step function. In particular, if $a \in \mathbb{Z}$ with $a \leq x < a+1$ then $F(x) = F(a)$. Thus

$$\sum_{\frac{x}{t}<n\leq x} \mu(n)F\left(\frac{x}{n}\right) = F(1)\sum_{\frac{x}{2}<n\leq x}\mu(n) + F(2)\sum_{\frac{x}{3}<n\leq \frac{x}{2}}\mu(n) + \cdots + F(t-1)\sum_{\frac{x}{t}<n\leq \frac{x}{t-1}}\mu(n).$$

So we have

$$\begin{aligned}\left|\sum_{\frac{x}{t}<n\leq x} \mu(n)F\left(\frac{x}{n}\right)\right| &\leq \sum_{k=1}^{t-1}|F(k)|\left|\sum_{\frac{x}{k+1}<n\leq \frac{x}{k}}\mu(n)\right| \\ &\leq \left(\sum_{k=1}^{t-1}|F(k)|\right)\max_{2\leq i\leq t}\left|\sum_{\frac{x}{i}<n\leq \frac{x}{i-1}}\mu(n)\right| \\ &\leq \sum_{i=1}^{t} ci^{1/2}\cdot\max_{2\leq i\leq t}\left|\sum_{\frac{x}{i}<n\leq \frac{x}{i-1}}\mu(n)\right| = o(t^{3/2}\cdot x).\end{aligned}$$

Hence for any given $\varepsilon > 0$, choose $t = t(\varepsilon)$ so that $\frac{2c}{t^{1/2}} < \frac{\varepsilon}{2}$. Then by (11),

$$\left|\sum_{n\leq \frac{x}{t}} \mu(n)F\left(\frac{x}{n}\right)\right| < \frac{\varepsilon x}{2}.$$

Now, for (some fixed) ε and t, we can choose x sufficiently large so that $o(t^{3/2}x) \leq \frac{\varepsilon x}{2}$. Also, since

$$\left|\sum_{\frac{x}{t}<n\leq x} \mu(n)F\left(\frac{x}{n}\right)\right| < \frac{\varepsilon}{2}x,$$

from the two aforementioned inequalities we have

$$\left|\sum_{n\leq x} \mu(n)F\left(\frac{x}{n}\right)\right| = o(x). \qquad \square$$

14. October 14 & 16

Remark 8. In 1896, Hadamard and de la Vallée Poussin proved that

$$\pi(x) \sim \frac{x}{\log x}.$$

Let

$$\mathrm{Li}(x) := \int_2^x \frac{1}{\log t}\,dt \sim \frac{x}{\log x}\sum_{k=0}^{\infty}\frac{k!}{(\log x)^k}$$
$$= \frac{x}{\log x} + \frac{x}{(\log x)^2} + \frac{2x}{(\log x)^3} + \cdots.$$

In 1899, de la Vallée Poussin proved that as $x \to \infty$, there exists $a > 0$ such that

$$\pi(x) = \mathrm{Li}(x) + O(xe^{-a\sqrt{\log x}}).$$

Remark 9. The main ingredient in the proof of the prime number theorem (Theorem 25) is that

$$\sum_{n\le x}\mu(n) = o(x),$$

which is a consequence of the analytic continuation and non-vanishing of $\zeta(s)$ at $\mathrm{Re}(s) = 1$. The Riemann hypothesis (RH) states that the 'non-trivial zeroes' of $\zeta(s)$ all have real part $\frac{1}{2}$. In 1901, Helge von Koch proved that RH is true if and only if

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x).$$

Remark 10. We proved in Assignment #1 that

$$N_n = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}.$$

Thus we have

$$N_n = \frac{q^n}{n} + O\left(\frac{q^{n/k}}{n}\right).$$

In other words, the "Riemann hypothesis in $\mathbb{F}_q[t]$" is true.

Definition 13. For $n \in \mathbb{N}$, let $\omega(n)$ denote the number of distinct prime factors of n, and let $\Omega(n)$ denote the number of prime factors of n counted with multiplicity.

Example 3. If $n = 2^3 \cdot 3^5 \cdot 5^2$, then $\omega(n) = 3$ and $\Omega(3) = 3 + 5 + 2 = 10$.

For $k \in \mathbb{N}$ and $x \in \mathbb{R}$, define

$$\tau_k(x) = \#\{n \le x : \Omega(n) = k\}$$
$$\pi_k(x) = \#\{n \le x : \omega(n) = \Omega(n) = k\},$$

i.e., squarefree with k prime factors. Note that $\pi(x) = \pi_1(x) = \tau_1(x)$.

Theorem 26 (Landau (1900))**.** *For $k \in \mathbb{N}$, $\pi_k(x) \sim \tau_k(x) \sim \frac{1}{(k-1)!}\cdot\frac{x}{\log x}\cdot(\log\log x)^{k-1}$.*

Proof. Define

$$L_k(x) = \sum_{p_1 \cdots p_k \le x}{}' \frac{1}{p_1 p_2 \dots p_k}$$

$$\Pi_k(x) = \sum_{p_1 \cdots p_k \le x}{}' 1$$

$$\Theta_k(x) = \sum_{p_1 \cdots p_k \le x}{}' \log(p_1 \dots p_k),$$

where $\sum'$ signifies that the sum is taken over all k-tuples of primes $(p_1, \dots, p_k)$ with $p_1 p_2 \cdots p_k \le x$. Note that different k-tuples may correspond to the same product $p_1 \dots p_k$.

For $n \in \mathbb{N}$, let

$$c_n = c_n(k) = \#\{k\text{-tuples}(p_1, \dots, p_k) : p_1 p_2 \cdots p_k = n\}.$$

Then $\Pi_k(x) = \sum\limits_{n \le x} c_n$ and $\Theta_k(x) = \sum\limits_{n \le x} c_n \log n$. Note that

$$c_n = \begin{cases} 0 & \text{if } n \text{ is not a product of } k \text{ primes} \\ k! & \text{if } n \text{ is squarefree and } \omega(n) = \Omega(n) = k. \end{cases}$$

Also, $0 < c_n < k!$ if $\Omega(n) = k$ and n is not squarefree. It follows that

$$k!\pi_k(x) \le \Pi_k(x) \le k!\tau_k(x) \tag{12}$$

For $k \ge 2$, note that

$$\tau_k(x) - \pi_k(x) = \#\{n \le x : \Omega(n) = k \text{ and } n \text{ is not squarefree}\}.$$

Thus

$$\tau_k(x) - \pi_k(x) = \sum_{\substack{p_1 p_2 \dots p_k \le x \\ p_i = p_j \text{ for some } i \ne j}}{}' 1 \le \binom{k}{2} \sum_{p_1 p_2 \dots p_{k-1} \le x}{}' 1 = \binom{k}{2} \Pi_{k-1}(x) \tag{13}$$

By (12) and (13), to prove that

$$\pi_k(x) \sim \tau_k(x) \sim \frac{1}{(k-1)!} \cdot \frac{x}{\log x} (\log \log x)^{k-1},$$

it suffices to show that

$$\Pi_k(x) \sim k \frac{x (\log \log x)^{k-1}}{\log x} \tag{$\dagger$}$$

for all $k \in \mathbb{N}$. Let $a_n = c_n$ and $f(u) = \log u$. By Abel's summation

$$\Theta_k(x) = \sum_{n \le x} c_n \log n = \Pi_k(x) \log x - \int_1^x \frac{\Pi_k(u)}{u}\, du.$$

Observe that

$$\Pi_k(x) \le k!\tau_k(x) \le k!x.$$

Thus $\Pi_k(u) = O(u)$. it follows that

$$\Theta_k(x) = \Pi_k(x) \log x + O(x).$$

Thus to prove (†), it suffices to show that for all $k \in \mathbb{N}$,

$$\Theta_k(x) \sim kx(\log\log x)^{k-1}.$$

We will prove this by induction on k. For $k = 1$, by the prime number theorem we have $\theta_1(x) = \theta(x) \sim x$ (by the prime number theorem). Assume now that $\Theta_k(x) \sim kx(\log\log x)^{k-1}$. Consider Θ_{k+1}. Note that for $k \geq 1$, we have

$$\left(\sum_{p \leq x^{1/k}} \frac{1}{p}\right)^k \leq L_k(x) \leq \left(\sum_{p \leq x} \frac{1}{p}\right)^k.$$

By Theorem 17,

$$\left(\sum_{p \leq x} \frac{1}{p}\right)^k \sim (\log\log x)^k$$

and

$$\left(\sum_{p \leq x^{1/k}} \frac{1}{p}\right)^k \sim (\log\log x^{1/k})^k = (\log\log x - \log k)^k \sim (\log\log x)^k.$$

Thus $L_k(x) \sim (\log\log x)^k$. It follows that

$$\Theta_{k+1}(x) - (k+1)x(\log\log x)^k = \Theta_{k+1}(x) - (k+1)xL_k(x) + o(x(\log\log x)^k).$$

Note that

$$\begin{aligned} k\log(p_1 p_2 \dots p_k p_{k+1}) &= \log(p_1^k p_2^k \cdots p_k^k p_{k+1}^k) \\ &= \sum_{i=1}^{k+1} \log(p_1 p_2 \cdots \hat{p_i} \cdots p_k p_{k+1}), \end{aligned}$$

where $p_1 p_2 \cdots \hat{p_i} \cdots p_k p_{k+1}$ denotes the product of all $p_1, \dots p_{k+1}$ with p_i being omitted (or equivalently, the above sum is over all k-subsets of $\{1, 2, \dots, k+1\}$). Thus we have

$$\begin{aligned} k\Theta_{k+1}(x) &= \sum_{p_1 \cdots p_{k+1} \leq x}{}' k \cdot \log(p_1 \cdots p_{k+1}) \\ &= \sum_{p_1 \cdots p_{k+1} \leq x}{}' \sum_{i=1}^{k+1} \log(p_1 p_2 \cdots \hat{p_i} \cdots p_k p_{k+1}) \\ &= (k+1) \sum_{p_1 \leq x} \sum_{p_2 \cdots p_{k+1} \leq \frac{x}{p_1}}{}' \log(p_2 \cdots p_{k+1}) \\ &= (k+1) \sum_{p_1 \leq x} \Theta_k\left(\frac{x}{p_1}\right). \end{aligned}$$

Next, we put $L_0(x) = 1$, and note

$$L_k(x) = \sum_{p_1 \cdots p_k \leq x}{}' \frac{1}{p_1 \cdots p_k} = \sum_{p \leq x} \frac{1}{p_1} L_{k=1}\left(\frac{x}{p_1}\right).$$

Therefore by the above two estimates,

$$\Theta_{k+1}(x) - (k+1)xL_k(x) = (k+1)\sum_{p_1 \le x}\left(\frac{1}{k}\Theta_k\left(\frac{x}{p_1}\right) - \frac{x}{p_1}L_{k-1}\left(\frac{x}{p_1}\right)\right)$$

by the induction hypothesis. So we have

$$\Theta_k(y) - kyL_{k-1}(y) = o(y(\log\log y)^{k-1}).$$

Thus given $\varepsilon > 0$, there exists $x_0 = x_0(\varepsilon, k)$ such that for $y \ge x_0$ we have

$$|\Theta_k(y) - kyL_{k-1}(y)| \le \varepsilon y(\log\log y)^{k-1}.$$

Further, there exists $c = c(\varepsilon, k) > 0$ such that for $y \le x_0$,

$$|\Theta_k(y) - kyL_{k-1}(y)| \le C.$$

Thus for x sufficiently large (note: $\frac{x}{p_1} > x_0 \Leftrightarrow \frac{p_1}{<}\frac{x}{x_0}$).

$$\begin{aligned}
|\Theta_{k+1}(x) - (k+1)xL_k(x)| &\le \frac{k+1}{k}\left(\sum_{p_1 < \frac{x}{x_0}} \varepsilon\frac{x}{p_1}\left(\log\log\frac{x}{p_1}\right)^{k-1} + \sum_{\frac{x}{x_0} \le p_1 \le x} c\right) \\
&\le 2\varepsilon x(\log\log x)^{k-1}\sum_{p_1 < \frac{x}{x_0}}\frac{1}{p_1} + 2cx \\
&\le 4\varepsilon x(\log\log x)^k + 2cx \\
&\le 5\varepsilon x(\log\log x)^k.
\end{aligned}$$

Thus $\Theta_{k+1}(x) - (k+1)xL_k(x) = o(x(\log\log x)^k)$, from which we conclude that

$$\Theta_{k+1}(x) \sim (k+1)x(\log\log x)^k. \qquad \square$$

15. October 19

Theorem 27. *The following statements hold:*

$$\sum_{n\le x}\omega(n) = x\log\log x + \beta x + o(x)$$
$$\sum_{n\le x}\Omega(n) = x\log\log x + \tilde{\beta}x + o(x),$$

where β is Merten's constant and $\tilde{\beta} = \beta + \sum_p \frac{1}{p(p-1)}$.

Proof. Let $S(x) := \sum_{n\le x}\omega(n)$ and $T(x) := \sum_{n\le x}\Omega(n)$. By Theorem 17, we have

$$\begin{aligned}
S(x) &= \sum_{n\le x}\sum_{p|n} 1 = \sum_{p\le x}\left\lfloor\frac{x}{p}\right\rfloor = x\sum_{p\le x}\frac{1}{p} + O(\pi(x)) \\
&= x(\log\log x + \beta + o(1)) + O(\pi(x)) = x\log\log x + \beta x + o(x).
\end{aligned}$$

Note that

$$T(x) - S(x) = \sum_{\substack{p^m \le x \\ m \ge 2}} \left\lfloor \frac{x}{p^m} \right\rfloor = \sum_{\substack{p^m \le x \\ m \ge 2}} \frac{x}{p^m} + O\left(\sum_{\substack{p^m \ge x \\ m \ge 2}} 1 \right).$$

Note also that $2^m \le p^m \le x$ and thus $m \le \log x / \log 2$. Also, $p^2 \le p^m \le x$ implies that $p \le \sqrt{x}$. Thus

$$\begin{aligned} T(x) - S(x) &= x \sum_{\substack{p^m \le x \\ m \ge 2}} \frac{1}{pm} + O(x^{1/2} \log x) \\ &= x \left(\sum_p \left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots \right) - \sum_{\substack{p^m > x \\ m \ge 2}} \frac{1}{p^m} \right) + O(x^{1/2} \log x). \end{aligned}$$

Note also that

$$\sum_{\substack{p^m > x \\ m \ge 2}} \frac{1}{p^m} \le \sum_{n \ge x} \left(\frac{1}{n^2} + \frac{1}{n^3} + \cdots \right) = O(x^{-1}) = o(1).$$

Therefore

$$T(x) - S(x) = x \left(\sum_p \frac{1}{p(p-1)} + o(1) \right) + O(x^{1/2} \log x).$$

By our estimate of $S(x)$ we have

$$T(x) = x \log \log x + \underbrace{\left(\beta + \sum_p \frac{1}{p(p-1)} \right)}_{\tilde{\beta}} x + o(x),$$

as required. □

Definition 14. Let $A \subseteq \mathbb{N}$. For $n \in \mathbb{N}$, let

$$A(n) := A \cap \{1, 2, \ldots, n\}.$$

Then the *upper asymptotic density* of A, denotes $\bar{d}(A)$, is defined by

$$\bar{d}(A) := \limsup_{n \to \infty} \frac{|A(n)|}{n}.$$

Similarly, we define $\underline{\mathrm{d}}(A)$ the *low asymptotic density* of A by

$$\underline{d}(A) = \liminf_{n \to \infty} \frac{|A(n)|}{n}.$$

If $\bar{d}(A) = \underline{d}(A)$, we say A has an *asymptotic density*, and we say $d(A) = \bar{d}(A) = \underline{d}(A)$.

Example 4. If P is the set of primes, then $\underline{d}(A) = \bar{d}(A)) = 0$. If $A := \{n \in \mathbb{N}, 5 \mid n\}$, then $\underline{d}(A) = \bar{d}(A) = \frac{1}{5}$. If $B = \{n \in \mathbb{N}, n \text{ not of the form } k^2 + 1 \text{ for some } k \in \mathbb{N}\}$, then $\underline{d}(B) = \bar{d}(B) = 1$.

Example 5. Let $D = \{a \in \mathbb{N} : (2k)! < a < (2k+1)! \text{ for some } k \in \mathbb{N}\}$. Then for $n = (2k+1)!$ any a satisfying $(2k)! < a < (2k+1)!$ will be counted. Thus

$$1 \geq \frac{D((2k+1)!)}{(2k+1)!} \geq \frac{(2k+1)! - (2k)!}{(2k+1)!} = \frac{2k}{2k+1}.$$

Thus as $k \to \infty$ we have

$$\frac{D((2k+1)!)}{(2k+1)!} \to 1.$$

Hence $\bar{d}(D) = 1$. On the other hand, if $n = (2k)!$, then we only count a up to $(2k-1)!$. Thus

$$0 \leq \frac{D((2k)!)}{(2k)!} \leq \frac{(2k-1)!}{(2k)!} = \frac{1}{2k}.$$

Hence as $k \to \infty$ we have as $k \to \infty$

$$\frac{D((2k)!)}{(2k)!} \to 0.$$

So $\underline{d}(D) = 0$. Therefore D has no asymptotic density.

Definition 15. Let $f(n)$ and $F(n)$ be functions from $\mathbb{N}$ to $\mathbb{R}_+$. We say that $f(n)$ has *normal order* $F(n)$ if for any $\varepsilon > 0$ the set

$$A(\varepsilon) = \{n \in \mathbb{N} : (1-\varepsilon)F(n) < f(n) < (1+\varepsilon)F(n)\}$$

has the property that $\underline{d}(A(\varepsilon)) = 1$.

Definition 16. Let $f(n)$ and $F(n)$ be functions from $\mathbb{N}$ to $\mathbb{R}_+$. We say that $f(n)$ has *average order* $F(n)$ if

$$\sum_{i=1}^{n} f(i) \sim \sum_{i=1}^{n} F(i).$$

Example 6. Let

$$f(n) = \begin{cases} 1 & \text{if } n \neq k! \text{ for all } k \in \mathbb{N} \\ n & \text{if } n = k!. \end{cases}$$

Then f has normal order 1, but not average order 1. Similarly, if

$$g(n) = \begin{cases} 2 & \text{if } n \equiv 1 \pmod 2 \\ 0 & \text{if } n \equiv 0 \pmod 2, \end{cases}$$

then g has average order 1 but does not have normal order 1. The third example is

$$h(n) = \begin{cases} \log n + (\log n)^{1/2} & \text{if } n \equiv 1 \pmod 2 \\ \log n - (\log n)^{1/2} & \text{if } n \equiv 0 \pmod 2. \end{cases}$$

$h(n)$ has both normal and average order $\log n$.

From Theorem 27, we see that $\omega(n)$ and $\Omega(n)$ have average $\log\log n$. Note that $\sum_{n \leq x} \log\log n \sim x \log\log x$). We will prove next class that they have normal order $\log\log n$.

16. October 21

We proved last time that

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

Also note that

$$\sum_{n\le x}\log\log n = \sum_{n\le x^{1/2}}\log\log n + \sum_{x^{1/2}<n\le x}\log\log n = O(x^{1/2}\log\log x) + \sum_{x^{1/2}<n\le x}\log\log n.$$

Note that

$$\sum_{x^{1/2}<n\le x}\log\log n \ge (\log\log x - \log 2)\sum_{x^{1/2}<n\le x} 1 = x\log\log x + O(x^{1/2}\log\log x)$$

$$\sum_{x^{1/2}<n\le x}\log\log n \le \log\log x \sum_{x^{1/2}<n\le x} 1 = x\log\log x + O(x^{1/2}\log\log x).$$

Thus

$$\sum_{n\le x}\log\log n = x\log\log x + O(x^{1/2}\log\log x).$$

Thus the average order of $\omega(n)$ is $\log\log n$.

Theorem 28. *We have*

$$\sum_{n\le x}(\omega(n) - \log\log x)^2 = O(x\log\log x).$$

Proof. Note that

$$\sum_{n\le x}(\omega(n) - \log\log x)^2 = \sum_{n\le x}\omega^2(n) - 2\log\log x\sum_{n\le x}\omega(n) + \underbrace{(\log\log x)^2\sum_{n\le x}1}_{x(\log\log x)^2 + O((\log\log x)^2)}.$$

By Theorem 27, we have

$$2\log\log x\sum_{n\le x}\omega(n) = 2x(\log\log x)^2 + O(x\log\log x).$$

We now consider the sum of $\omega^2(n)$. W ehave

$$\begin{aligned}\sum_{n\le x}\omega^2(n) &= \sum_{n\le x}\left(\left(\sum_{p|n}1\right)\left(\sum_{q|n}1\right)\right) = \sum_{n\le x}\left(\sum_{\substack{pq|n\\ p\ne q}}1 + \sum_{p|n}1\right)\\ &= \sum_{\substack{pq\le x\\ p\ne q}}\sum_{\substack{n\le x\\ pq|n}}1 + \sum_{n\le x}\omega(n) = \sum_{\substack{pq\le x\\ p\ne q}}\left\lfloor\frac{x}{pq}\right\rfloor + O(x\log\log x)\\ &= x\sum_{\substack{pq\le x\\ p\ne q}}\frac{1}{pq} + O(x) + O(x\log\log x).\end{aligned}$$

Also we have

$$\sum_{\substack{pq\le x\\ p\neq q}}\frac{1}{pq}=\sum_{pq\le x}\frac{1}{pq}-\sum_{p^2\le x}\frac{1}{p^2}=\sum_{pq\le x}\frac{1}{pq}+O(1).$$

Observe that

$$\left(\sum_{p\le x^{1/2}}\frac{1}{p}\right)^2\le\sum_{pq\le x}\frac{1}{pq}\le\left(\sum_{p\le x}\frac{1}{p}\right)^2.$$

By Theorem 17, we have

$$\left(\sum_{p\le x}\frac{1}{p}\right)^2=(\log\log x)^2+O(\log\log x)$$

and

$$\left(\sum_{p\le x^{1/2}}\frac{1}{p}\right)^2=(\log\log x^{1/2}+O(1))^2=(\log\log x-\log 2+O(1))^2=(\log\log x)^2+O(\log\log x).$$

Therefore

$$\sum_{pq\le x}\frac{1}{pq}=(\log\log x)^2+O(\log\log x).$$

Combining the above estimates gives

$$\sum_{n\le x}\omega^2(n)=x(\log\log x)^2+O(x\log\log x).$$

It follows that

$$\begin{aligned}\sum_{n\le x}(\omega(n)-\log\log x)^2&=\sum_{n\le x}\omega^2(n)-2\log\log x\sum_{n\le x}\omega(n)+(\log\log x)^2\sum_{n\le x}1\\&=x(\log\log x)^2+O(x\log\log x)-2x(\log\log x)^2+x(\log\log x)^2\\&=O(x\log\log x).\end{aligned}$$

□

Corollary 29. *Let $\delta>0$. Then*

$$\#\{n\le x:|\omega(n)-\log\log n|>(\log\log n)^{1/2+\delta}\}$$

is $o(x)$. Thus the normal order of $\omega(n)$ is $\log\log n$.

Proof. The number of $n\le x^{1/2}$ is $o(x)$. Also, for $x^{1/2}<n\le x$ we have $\log\log x\ge\log\log n>\log\log x-\log 2$. Thus to prove the corollary it suffices to show that

$$E(x):=\#\{n\le x:|\omega(n)-\log\log x|>(\log\log x)^{1/2+\delta}\}=o(x).$$

By Theorem 28, we have

$$E(x)\cdot(\log\log x)^{1+2\delta}\le\sum_{n\le x}(\omega(n)-\log\log x)^2=O(x\log\log x).$$

So it follows that

$$E(x)=O\left(\frac{x\log\log x}{(\log\log x)^{1+2\delta}}\right)=o(x),$$

as required. □

Corollary 30. *The normal order of* $\Omega(n)$ *is* $\log\log n$.

Proof. By Theorem 27, we have

$$\sum_{n\le x}(\Omega(n)-\omega(n)) = O(x).$$

Thus $\#\{n \le x : \Omega(n)-\omega(n) > (\log\log n)^{1/2+\delta}\}$. Then the results follows from Corollary 29. □

Remark 11. Since the average order of $\omega(n)$ is $\log\log n$, which is asymptotic to $\log\log x$ for almost all n, we can view $\sum_{n\le x}(\omega(n)-\log\log x)^2$ as the square of the standard deviation of $\omega(n)$. On Assignment #3 we shall prove that actually

$$\sum_{n\le x}(\omega(n)-\log\log x)^2 \sim x\log\log x.$$

Thus the standard variation of $\omega(n)$ is about $\sqrt{\log\log n}$.

Definition 17. Let

$$G(\gamma) := \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\gamma} e^{-\frac{t^2}{2}}\,dt.$$

Then $G(\gamma)$ is called the *Gaussian normal distribution.*

Remark 12. In 1934, Erdős and Kac proved that

$$\frac{1}{x}\#\left\{n\le x : \frac{\omega(n)-\log\log n}{\sqrt{\log\log n}} \le \gamma\right\} = G(\gamma).$$

17. October 23

Recall that the normal order of $\omega(n)$ and $\Omega(n)$ is $\log\log n$. Let $d(n)$ be the number of positive divisors of n. If $n = p_1^{a_1}\cdots p_r^{a_r}$ with $a_1,\dots,a_r \in \mathbb{N}$ and $p_1,\dots,p_r$ distinct primes then $\omega(n) = r$ and $\Omega(n) = a_1+\cdots+a_r$ and $d(n) = (a_1+1)\cdots(a_r+1)$.

Theorem 31. *For* $\varepsilon > 0$*, define the set*

$$S(\varepsilon) := \{n\in\mathbb{N}, 2^{(1-\varepsilon)\log\log n} < d(n) < 2^{(1+\varepsilon)\log\log n}\}.$$

Then $S(\varepsilon)$ *has asymptotic density* 1.

Proof. Note that for $a\in\mathbb{N}$, we have $2 \le 1+a \le 2^a$. Thus we have

$$2^{\omega(n)} \le d(n) \le 2^{\Omega(n)}.$$

Then the result follows from Corollaries 29 and 30. □

Remark 13. Recall that

$$\sum_{n\le x} d(n) \sim x\log x.$$

Thus the average order of $d(n)$ is $\log n$. However, by the above theorem, for almost all n, $d(n)$ satisfies

$$(\log n)^{\log 2-\varepsilon} < d(n) < (\log n)^{\log 2+\varepsilon}$$

for any $\varepsilon > 0$.

18. October 23: Quadratic reciprocity

Definition 18. For $n \in \mathbb{N}$, the Euler-totient function is defined by

$$\varphi(n) = \#\{1 \leq m \leq n : (m, n) = 1\}.$$

Theorem 32 (Euler's theorem)**.** *Let $a \in \mathbb{N}$ and $(a, n) = 1$. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. Let $c_1, c_2, \ldots, c_{\varphi(n)}$ be a reduced residue system mod n. Since $(a, n) = 1$, the set $\{ac_1, \ldots, ac_{\varphi(n)}\}$ is also a reduced residue system mod n. Thus

$$\begin{aligned} c_1 c_2 \cdots c_{\varphi(n)} &\equiv (ac_1)(ac_2)\cdots(ac_{\varphi(n)}) \pmod{n} \\ c_1 c_2 \cdots c_{\varphi(n)} &\equiv a^{\varphi(n)}(c_1 c_2 \cdots c_{\varphi(n)}) \pmod{n} \\ a^{\varphi(n)} &\equiv 1 \pmod{n}. \end{aligned}$$

□

Corollary 33 (Fermat's little theorem)**.** *Let p be a prime. Then for any $a \in \mathbb{Z}$ with $p \nmid a$ we have $a^{p-1} \equiv 1 \pmod{p}$.*

Theorem 34 (Wilson's theorem)**.** *Let p be a prime. Then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Consider the polynomial $x^{p-1} - 1$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. By Corollary 33, $1, 2, \ldots, p-1$ are its roots.Thus in $(\mathbb{Z}/p\mathbb{Z})[x]$ we have

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

Consider the constant coefficients on both sides; we see that $-1 \equiv (-1)(-2)\cdots(-(p-1)) = (-1)^{p-1}(p-1)! \pmod{p}$. If $p = 2$ then the result holds since $-1 \equiv 1 \pmod{2}$. Otherwise if p is odd then $(-1)^{p-1} = 1$ so the result follows. □

Definition 19. Let p be a prime and let $a \in \mathbb{Z}$ with $(a, p) = 1$. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ by the rule

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{otherwise.} \end{cases}$$

If $\left(\frac{a}{p}\right) = 1$ then a is a *quadratic residue mod p*. Otherwise, then a is a *quadratic non-residue mod p*.

Theorem 35 (Euler's criterion)**.** *Let p be an odd prime and let $a \in \mathbb{Z}$ with $(a, p) = 1$. Then*

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

Proof. The congruence $x^2 \equiv 1 \pmod{p}$ has at most two solutions mod p. Two cases:

(1) Suppose that there is a solution, say b. Then $\left(\frac{a}{p}\right) = 1$. Since $b^2 \equiv a \pmod{p}$, we have

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}.$$

Thus $a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$.

(2) Suppose that there is no solution. In this case, $\left(\frac{a}{p}\right) = -1$. Since $(a,p) = 1$, for each fixed $r \in (\mathbb{Z}/p\mathbb{Z})^*$, there exists a *unique* $s \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $rs \equiv a \pmod{p}$. Since $x^2 \equiv a \pmod{p}$ has no solution, we see that $r \neq s$. Split elements in $(\mathbb{Z}/p\mathbb{Z})^*$ into $\frac{p-1}{2}$ pairs (r,s) with $r \neq s$ and $rs \equiv a \pmod{p}$. Thus

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

But Theorem 34 says $a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}$, so the claim follows. □

19. October 26

Theorem 36. *Let p be an odd prime and let $a, b, \in \mathbb{Z}$. Then*

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

Also,

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

Note that if $a \in \mathbb{Z}$ and $p \,|\, a$, then we extend the definition of the Legendre symbol by letting $\left(\frac{a}{p}\right) = 0$.

Proof. The statement holds if $p \,|\, ab$ (i.e., $p \,|\, a$ or $p \,|\, b$). Thus we may assume $p \nmid a$ and $p \nmid b$. By Euler's criterion we have

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Since $\left(\frac{ab}{p}\right), \left(\frac{a}{p}\right), \left(\frac{b}{p}\right) \in \{-1, 1\}$ and p is an odd prime, the result follows. Again, by Euler's criterion we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Since $\left(\frac{-1}{p}\right) \in \{-1, 1\}$ and p is an odd prime, it follows that

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

as required. □

Theorem 37 (Gauss's lemma)**.** *Let p be an odd prime and $a \in \mathbb{Z}$ with $(a,p) = 1$. Let μ be the number of integers from $\left\{a, 2a, \ldots, \left(\frac{p-1}{2}\right)a\right\}$ whose residues mod p of least absolute value (i.e., in $\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$) are negative. Then*

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

Example 7. If $p = 5$ and $a = 2$ then we have $\{2, 4\}$, or equivalent $\{2, -1\}$. Therefore $\mu = -1$.

Proof. We first replace the integers $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ by their residues of least absolute value. Denote the negative ones by $-s_1, -s_2, \ldots, -s_\mu$ and the positive ones by $r_1, \ldots, r_{\frac{p-1}{2}-\mu}$. Since $1 \leq r_i, s_j \leq \frac{p-1}{2}$, no two r_i's are equal and no two s_j's are equal. We further claim that $r_i \neq s_j$ for all i, j. To see this, note that if $m_1 a \equiv r_i \pmod{p}$ and $m_2 a \equiv -s_j \pmod{p}$ with $r_i = s_j$, then $(m_1 + m_2)a \equiv 0 \pmod{p}$. Since $(a, p) = 1$, it follows that $p \mid m_1 + m_2$. But this is a contradiction since $1 \leq m_1, m_2 \leq \frac{p-1}{2}$. Since $r_i \neq r_j$ and $s_i \neq s_j$ and $r_i \neq s_j$ for all $i \neq j$, we see that $s_1, \ldots, s_\mu, r_1, \ldots, r_{\frac{p-1}{2}-\mu}$ is a rearrangement of $1, 2, \ldots, \frac{p-1}{2}$. Thus

$$\begin{aligned} a \cdot 2a \cdot \cdots \cdot \left(\frac{p-1}{2}\right) a &\equiv 1 \cdot 2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right) \cdot (-1)^\mu \pmod{p} \\ \Leftrightarrow a^{\frac{p-1}{2}} &\equiv (-1)^\mu \pmod{p} \\ \Leftrightarrow \left(\frac{a}{p}\right) &= (-1)^\mu, \end{aligned}$$

by Euler's criterion (and also that $(-1)^\mu, \left(\frac{a}{p}\right) \in \{\pm 1\}$ and p is odd). □

Corollary 38. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof. Consider the set $\{2, 4, 6, \ldots, \frac{p-1}{2} \cdot 2\}$. Note that

$$2r \leq \frac{p-1}{2} \Leftrightarrow r \leq \frac{p-1}{4}.$$

Thus the number of integers on the set whose residues of least absolute value is negative is equal to

$$\mu = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor.$$

Note that if $p \equiv \pm 1 \pmod{8}$ then μ is even; if $p \equiv \pm 3 \pmod{8}$ then μ is odd. By Gauss's lemma, we have $\left(\frac{2}{p}\right) = (-1)^\mu$. Thus w is a quadratic residue if $p \equiv \pm 1 \pmod{8}$ and is a quadratic non-residue if $p \equiv \pm 3 \pmod{8}$. □

20. October 28

Theorem 39 (Law of quadratic reciprocity)**.** *If p, q are distinct odd primes, then*

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

Example 8. $\left(\frac{13}{17}\right) = (-1)^{\frac{13-1}{2} \cdot \frac{17-1}{2}} \left(\frac{17}{13}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1.$

Example 9. We claim that 5 is a quadratic residue mod p if and only if $p \equiv \pm 1 \pmod{10}$. Indeed, note that

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right),$$

and that

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{10} \\ -1 & \text{if } p \equiv \pm 3 \pmod{10}. \end{cases}$$

Proof. By Gauss's lemma, we have $\left(\frac{p}{q}\right) = (-1)^{\mu}$ and $\left(\frac{q}{p}\right) = (-1)^{\nu}$, where μ is the number of integers from $\{p, 2p, \cdots, \left(\frac{q-1}{2}\right)p\}$ whose residue mod q of least absolute value is negative and ν is the number of integers from $\{q, 2q, \ldots, \left(\frac{p-1}{2}\right)q\}$ whose residue mod p of least absolute value is negative. Thus to prove the claim, it suffices to show that

$$\mu + \nu \equiv \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \pmod{2}.$$

We claim that

Claim 3. *For $x \in \mathbb{Z}$ with $1 \leq x \leq \frac{q-1}{2}$ there exists a unique $y \in \mathbb{Z}$ such that $-\frac{q}{2} < xp - qy < \frac{q}{2}$. Furthermore, $y \geq 0$ (note that $xp - qy$ is the residue mod q of the least absolute value of xp).*

Proof of Claim 3. Note that

$$-\frac{q}{2} < xp - yq < \frac{q}{2} \Leftrightarrow -\frac{xp}{q} - \frac{1}{2} < -y < -\frac{xp}{q} + \frac{1}{2}. \qquad (\star)$$

Thus y is uniquely determined. Also, we note that if $y < 0$ then $xp - yq \geq q$. Since $xp - yq \in \left(-\frac{q}{2}, \frac{q}{2}\right)$ we see that $y \geq 0$. □

Note that if $y = 0$ there is no contribution from $xp - yq$ to μ since $xp > 0$. Also, if $x = \frac{q-1}{2}$, then from $(\star)$, we have

$$y < \frac{xp}{q} + \frac{1}{2} = \frac{\left(\frac{q-1}{2}\right)p}{q} + \frac{1}{2} = \frac{p}{2}\left(\frac{q-1}{q}\right) + \frac{1}{2} < \frac{p+1}{2},$$

since $y \in \mathbb{Z}, y \leq \frac{p-1}{2}$. Thus the number μ corresponds to the number of combinations of x and y from the sequences (A) $1, 2, \ldots, \frac{q-1}{2}$ and (B) $1, 2, \ldots, \frac{p-1}{2}$ respectively such that $\frac{-q}{2} < xp - yq < 0$ or equivalently $0 < yq - xp < \frac{q}{2}$. Similarly, ν is the number of combinations of x and y from the sequences (A) and (B) respectively, for which $-\frac{p}{2} < yq - xp < 0$. So for any other pairs (x, y) with x from (A) and y from (B), either $yq - xp < -\frac{p}{2}$ or $yq - xp > \frac{q}{2}$.

Let ρ be the number of pairs (x, y) for which $yq - xp < -\frac{p}{2}$ and λ be the number of pairs (x, y) for which $yq - xp > \frac{q}{2}$. Then

$$\left(\frac{q-1}{2}\right)\left(\frac{p-1}{2}\right) = \nu + \mu + \rho + \lambda.$$

As x and y run through (A) and (B) respectively,

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

run through (A) and (B) respectively but in reserve order. Note that $yq - xp < -\frac{p}{2}$ if and only if

$$\begin{aligned} y'q - x'p &= \left(\frac{p+1}{2} - y\right) q - \left(\frac{q+1}{2} - x\right) p \\ &= \frac{q-p}{2} - (yq - xp) > \frac{q}{2}. \end{aligned}$$

Then $\rho = \lambda$. It follows that

$$\left(\frac{q-1}{2}\right)\left(\frac{p-1}{2}\right) = \mu + \nu + 2\lambda \equiv \mu + \nu \pmod 2. \qquad \square$$

21. October 30

Example 10. The equation $x^4 - 17y^4 = 2w^2$ has no integral solution. Suppose otherwise, that is there exist $x, y, w \in \mathbb{Z}$ such that $x^4 - 17y^4 = 2w^2$. Without loss of generality, we can assume $(x, y) = 1$. Thus x and w are coprime. Note that if p is an odd prime which divides w, since $x^4 \equiv 17y^4 \pmod p$, i.e., $17 \equiv (x^2y^{-2})^2 \pmod p$ we have $\left(\frac{17}{p}\right) = 1$. By the law of quadratic reciprocity,

$$\left(\frac{p}{17}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{p}\right) = 1.$$

Thus an odd prime p dividing w is a quadratic residue mod 17. Also by Corollary 38 we have

$$\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = 1,$$

so 2 is a quadratic residue mod 17. By the above arguments, we see that any prime (either 2 or p) dividing w is a quadratic residue mod 17. Therefore we have $w \equiv t^2 \pmod{17}$ for some $t \in \mathbb{Z}$. Note that $17 \nmid w$ and that $17 \nmid t$. Now, since $x^4 - 17y^4 = 22^p$, it follows that $x^f \equiv 2t^4 \pmod{17}$. Thus $2 \equiv x^4t^{-4} \pmod{17}$, that is there exists $r \in \mathbb{Z}$ such that $2 \equiv r^4 \equiv 17$, which is a contradiction. One can generalize it to $x^4 - ay^4 = bw^2$, i.e., determining with what kind of a and b would this will work.

Example 11. Is the congruence $3x^2 + 7x - 42 \equiv 0 \pmod{391}$ solvable? First, multiply both sides by 12 to get $36x^2 + 84x - 516 \equiv 0 \pmod{391}$, or $(6x + 7)^2 \equiv 565 \pmod{391}$. Thus it suffices to consider $y^2 \equiv 174 \pmod{391}$. Note that $391 = 17 \cdot 23$. We see that $y^2 \equiv 174 \pmod{17} \Leftrightarrow y^2 \equiv 4 \pmod{17}$ which has a solution. Also, note that $y^2 \equiv 174 \pmod{391} \Leftrightarrow y^2 \equiv 13 \pmod{23}$. By the law of quadratic reciprocity, we have

$$\left(\frac{13}{23}\right) = (-1)^{\frac{23-1}{2}\cdot\frac{13-1}{2}}\left(\frac{23}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{5}\right) = (-1)(-1) = 1.$$

Thus $y^2 \equiv 13 \pmod{23}$ has a solution. Since $y^2 \equiv 13 \pmod{17}$ and $y^2 \equiv 13 \pmod{23}$, by the Chinese remainder theorem, $y^2 \equiv 174 \pmod{391}$ has a solution.

Example 12. What is $\left(\frac{713}{1009}\right)$?

Note that $713 = 23 \cdot 31$. Then by Theorem 36, we have

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right).$$

By the law of quadratic reciprocity, it follows

$$\left(\frac{23}{1009}\right) = (-1)^{\frac{23-1}{2}\cdot\frac{1009-1}{2}}\left(\frac{1009}{23}\right) = \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \left(\frac{5}{23}\right)$$
$$= (-1)^{\frac{5-1}{2}\cdot\frac{23-1}{2}}\left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Similar argument yields

$$\left(\frac{31}{1009}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = 1\cdot(-1) = -1.$$

Hence

$$\left(\frac{713}{1009}\right) = (-1)(-1) = 1.$$

Remark 14. In the above calculation, we are given the fact that $713 = 23\cdot 31$. However, it is not always easy to find the prime factorization of an integer a. Yet, it is possible to evaluate $\left(\frac{a}{p}\right)$ without knowing the prime factorization of a. The idea is to 'flip' the Legendre symbol to $\left(\frac{p}{a}\right)$ even when a is not a prime.

Definition 20. Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}$ be odd. If $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, we define the *Jacobi symbol* to be

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{\alpha_i}.$$

Theorem 40 (Generalized law of quadratic reciprocity)**.** *Let $a, b \in \mathbb{N}$ be odd. Then*

(1) $\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \pmod 4 \\ -1 & \text{if } b \equiv 3 \pmod 4. \end{cases}$

(2) $\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } b \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$

(3) $\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{if } a \equiv 1 \pmod 4 \text{ or } b \equiv 1 \pmod 4 \\ -\left(\frac{b}{a}\right) & \text{if } a \equiv b \equiv 3 \pmod 4. \end{cases}$

Proof. Exercise! □

Example 13. Now compute $\left(\frac{713}{1009}\right)$ using the generalized law of quadratic reciprocity. Since $713 \equiv 1 \pmod 4$ and $713 \equiv 1 \pmod 8$, we have

$$\left(\frac{713}{1009}\right) = \left(\frac{1009}{713}\right) = \left(\frac{296}{713}\right) = \left(\frac{2^3\cdot 37}{713}\right) = \left(\frac{37}{713}\right).$$

Now, since $37 \equiv 1 \pmod 4$ and $37 \equiv 5 \pmod 8$, we have

$$\left(\frac{37}{713}\right) = \left(\frac{713}{37}\right) = \left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -\left(\frac{5}{37}\right).$$

Since $5 \equiv 1 \pmod 4$, we have

$$\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Therefore $\left(\frac{713}{1009}\right) = 1$.

22. November 2: primitive roots

We recall the Euclidean algorithm: for $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = (a, b)$.

Theorem 41 (Chinese remainder theorem)**.** *Let $m_1, \ldots, m_t \in \mathbb{Z}$ with $(m_i, m_j) = 1$ for all $i \neq j$, and let $m = m_1 \cdots m_t$. Let $b_1, \ldots, b_t \in \mathbb{Z}$. Then the simultaneous congruences*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_t \pmod{m_t} \end{aligned}$$

has a unique solution modulo m.

Proof. Let $n_i = m/m_i$ $(1 \leq i \leq t)$. Then $(m_i, n_i) = 1$. Then there exist $r_i, s_i \in \mathbb{Z}$ such that $r_i n_i + s_i m_i = 1$ $(1 \leq i \leq t)$. Let $e_i = r_i n_i$. Then $e_i \equiv 0 \pmod{m_j}$ and $e_i \equiv 1 \pmod{m_j}$ for $i \neq j$. Consider now

$$x_0 = \sum_{i=1}^{t} b_i e_i.$$

Then $x_0 \equiv b_i \pmod{m_i}$ for each $1 \leq i \leq t$. That is, it is a solution of the simultaneous congruences. To prove the uniqueness of x_0, suppose that $x_1 \equiv b_i \pmod{m_i}$ for all $1 \leq i \leq t$. Then $m_i \,|\, (x_1 - x_0)$ $(1 \leq i \leq t)$. Since $(m_i, m_j) = 1$ for $i \neq j$ and $m = m_1 \ldots m_t$, we have $m \,|\, (x_1 - x_0)$, i.e., $x_1 \equiv x_0 \pmod{m}$. □

For $n \in \mathbb{Z}$, let $(\mathbb{Z}/n\mathbb{Z})^*$ denote the invertible elements in $\mathbb{Z}/n\mathbb{Z}$. That is, they are the congruence classes $(r + n\mathbb{Z})$ for which there exists $(s + n\mathbb{Z})$ with $(r + n\mathbb{Z})(s + n\mathbb{Z}) = 1 + n\mathbb{Z}$. This is equivalent to saying that $(r, n) = 1$.

Theorem 42. *Let $m_1, \ldots, m_t \in \mathbb{N}$ with $(m_i, m_j) = 1$ for $i \neq j$, and let $m = m_1 m_2 \ldots m_t$. Then*

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}$$

as rings. Also,

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_t\mathbb{Z})^*$$

as groups.

Proof. Let $\psi : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ defined by $\psi(n) \mapsto (n + m_1\mathbb{Z}, \ldots, n + m_t\mathbb{Z})$. It is a straightforward verification that ψ is a ring homomorphism. Note that ψ is surjective and $\ker \psi = m\mathbb{Z}$, by the Chinese remainder theorem. Thus by the first isomorphism theorem for rings, the first claim follows. Now let $\lambda : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_t\mathbb{Z})^*$ be defined by $\lambda(r + m\mathbb{Z}) = (r + m_1\mathbb{Z}, \ldots, r + m_t\mathbb{Z})$. Note that $(r, m) = 1$ if and only if $(r, m_i) = 1$ for all $1 \leq i \leq t$. Thus the map is well-defined. It is straightforward to verify λ is a group homomorphism. It is also bijective by the Chinese remainder theorem. □

Corollary 43. *Let $m_1, \ldots, m_t \in \mathbb{N}$ with $(m_i, m_j) = 1$ for $i \neq j$, and let $m = m_1 m_2 \ldots m_t$. Then $\varphi(m) = \varphi(m_1)\varphi(m_2) \cdots \varphi(m_t)$.*

Proof. Note that $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$ and $\varphi(m_1)\cdots\varphi(m_t) = |(\mathbb{Z}/m_1\mathbb{Z})^*|\cdots|(\mathbb{Z}/m_t\mathbb{Z})^*| = |(\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_t\mathbb{Z})^*|$. So now the result follows from Theorem 42. □

Corollary 44. *Let $m = p_1^{a_1}\cdots p_t^{a_t}$, where $p_1 \dots p_t$ are distinct primes and $a_1, \dots, a_t \in \mathbb{N}$. Then*

$$\varphi(m) = m\prod_{i=1}^{t}\left(1 - \frac{1}{p_i}\right).$$

Proof. Take $m_i = p_i^{a_i}$, where $1 \le i \le t$ in Corollary 43. Note that $\varphi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i-1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right)$. So it follows that

$$\varphi(m) = \prod_{i=1}^{t}\varphi(p_i^{a_i}) = p_1^{a_1}\cdots p_t^{a_t}\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_t}\right) = m\prod_{i=1}^{t}\left(1 - \frac{1}{p_i}\right). \qquad \square$$

Proposition 45. *Let p be a prime. If $d\,|\,(p-1)$, then $x^d \equiv 1 \pmod p$ has exactly d solutions mod p.*

Proof. Write $p - 1 = dk$ with $k \in \mathbb{N}$. Then

$$\frac{x^{p-1} - 1}{x^d - 1} = \frac{(x^d)^k - 1}{x^d - 1} = (x^d)^{k-1} + \cdots + x^d + 1 = g(x) \in (\mathbb{Z}/p\mathbb{Z})[x].$$

By Fermat's little theorem, $x^{p-1} - 1$ has $p - 1$ distinct roots in $\mathbb{Z}/p\mathbb{Z}$. This $(x^d - 1)g(x)$ factors into linear factors in $(\mathbb{Z}/p\mathbb{Z})[x]$ and the result follows. □

Theorem 46. *$(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group.*

Proof. For each divisor d of $p-1$, let $\lambda(d)$ denote the number of elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order d. By Prop 45, there are exactly d elements whose order divides d. Thus

$$d = \sum_{c|d}\lambda(c).$$

By the Möbius inversion formula, we have

$$\lambda(d) = \sum_{c|d}\frac{\mu(c)}{c}d = d\sum_{c|d}\frac{\mu(c)}{c} = d\prod_{p|d}\left(1 - \frac{1}{p}\right) = \varphi(d).$$

Thus there are $\varphi(p-1)$ elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order $p - 1$. In particular, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. □

Remark 15. For a general $n \in \mathbb{N}$, the group $(\mathbb{Z}/n\mathbb{Z})^*$ is *not* always cyclic. For example, $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$, but none of the elements have order 4.

23. November 4

Definition 21. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. We say a is a *primitive root modulo n* if $a + n\mathbb{Z}$ generates $(\mathbb{Z}/n\mathbb{Z})^*$.

Example 14. w is a primitive root mod 5 but is not a primitive root module 7, since $2^3 \equiv 1 \pmod 7$.

Remark 16. We have seen in the proof of Theorem 46 that for a prime p, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. Thus there exists a primitive root mod p. In fact, we see from the proof of the theorem, there are $\varphi(p-1)$ primitive root modulo p. Note that if $a \in \mathbb{N}$ is a square, then it is a quadratic residue mod p. Thus a is not a primitive root mod p.

Conjecture (Artin's primitive root conjecture)**.** *If $a \in \mathbb{N}$ is not a perfect square, then a isa primitive root mod p for infinitely many primes p.*

Remark 17. The conjecture still remain open, but some progress has been made. In 1967, Hooley proved that the conjecture is true under the assumption of the generalized Riemann hypothesis (GRH). In 1980's, using sieve theory, Gupta, K. Murty, R. Murty, and Heath-Brown showed unconditionally that given any non-square $a, b, c \in \mathbb{N}$, then at least one of them is a primitive root mod p for infinitely many primes p. For example, one of $2, 3, 5$ is a primitive root mod p for infinitely many primes p. However, the result is not constructive, and thus we do not know which one satisfies the condition.

Proposition 47. *Let p be a prime and $l \in \mathbb{N}$. If $a \equiv b \pmod{p^l}$, then $a^p \equiv b^p \equiv p^{l+1}$.*

Proof. Write $a = b + cp^l$ for some $c \in \mathbb{Z}$. Then

$$a^p = (b+cp^l)^p = b^p + \binom{p}{1} b^{p-1} cp^l + \binom{p}{2} b^{p-2} (cp^l)^2 + \cdots + \binom{p}{p} (cp^l)^p.$$

Since $p^{l+1} \,|\, \binom{p}{1} b^{p-1} cp^l$ and $p^{l+1} \,|\, p^{il}$ for $2 \le i \le p$, it follows that $a^p \equiv b^p \pmod{p^{l+1}}$. □

Proposition 48. *Let p be an odd prime and $l \in \mathbb{N}$ with $l \ge 2$. Then for $a \in \mathbb{Z}$, we have $(1+ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \pmod{p^l}$.*

Proof. We prove the result by induction on l. The result is immediate for $l = 2$. Suppose that the result holds for some $l \in \mathbb{N}$ with $l \ge 2$. And we prove it for $l+1$. By Proposition 47 and the induction hypothesis, we have

$$(1+ap)^{p^{l-1}} \equiv ((1+ap)^{p^{l-2}})^p \equiv (1+ap^{l-1})^p \equiv 1 + \binom{p}{1} ap^{l-1} + \cdots + \binom{p}{p} (ap^{l-1})^p \pmod{mod p^{l+1}}.$$

Note that for $l \ge 2$ and $k \ge 3$, we have

$$2(l-1) + 1 \le 3(l-1) \le k(l-1).$$

It follows that

$$p^{2(l-1)+1} \,|\, (ap^{l-1})^k$$

for $k = 3, \ldots, p$. Also, we note that

$$\binom{p}{2} (ap^{l-1})^2 = \frac{p(p-1)}{2} (ap^{l-1})^2 = \frac{p-1}{2} ap^{2(l-1)+1}.$$

Since $\frac{p-1}{2} \in \mathbb{Z}$ as p is odd, it follows that

$$p^{2(l-1)+1} \left| \binom{p}{2} (ap^{l-1})^2 \right. .$$

Note that $2(l-1)+1 \geq l+1$ for $l \geq 2$. Thus $p^{l+1} \,|\, p^{2(l-1)+1}$. Thus we have

$$\begin{aligned}(1+ap)^{p^{l-1}} &\equiv 1 + \binom{p}{1}ap^{l-1} + \binom{p}{2}(ap^{l-1})^2 + \cdots + \binom{p}{p}(ap^{l-1})^p \\ &\equiv 1 + \binom{p}{1}ap^{l-1} \equiv 1 + ap^l \pmod{p^{l+1}}.\end{aligned}$$

By induction, the result follows. □

24. November 6

Proposition 49. *If p is an odd prime, $l \in \mathbb{N}$ with $l \geq 2$ and $a \in \mathbb{Z}$ with $(a,p) = 1$, then $1 + ap$ has order p^{l-1} in $(\mathbb{Z}/p^l\mathbb{Z})^*$.*

Proof. Note that the group $(\mathbb{Z}/p^l\mathbb{Z})^*$ is of order $p^l - p^{l-1} = p^{l-1}(p-1)$. By Proposition 48, we have

$$(1+ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \pmod{p^l}.$$

Since $(a,p) = 1$, we have $(1+ap)^{p^{l-2}} \not\equiv 1 \pmod{p^l}$. Then by Proposition 48 again,

$$(1+ap)^{p^{l-1}} \equiv 1 + ap^l \pmod{p^{l+1}}.$$

Thus $(1+ap)^{p^{l-1}} \equiv 1 \pmod{p^l}$. It follows that $(1+ap)$ has order p^{l-1} in $(\mathbb{Z}/p^l\mathbb{Z})^*$. □

Theorem 50. *Let p be an odd prime and $l \in \mathbb{N}$ with $l \geq 2$. Then $(\mathbb{Z}/p^l\mathbb{Z})^*$ is a cyclic group.*

Proof. By Theorem 46, there exists a primitive root modulo p. Note that

$$(g+p)^{p-1} = g^{p-1} + \binom{p-1}{1}g^{p-2}p + \binom{p-1}{2}g^{p-3}p^2 + \cdots + \binom{p-1}{p-1}p^{p-1}.$$

If we assume that $g^{p-1} \equiv 1 \pmod{p^2}$ then

$$(g+p)^{p-1} \equiv 1 + \binom{p-1}{1}g^{p-2}p \pmod{p^2}.$$

Since $p \nmid (p-1)$ and $(g,p) = 1$ we see that

$$(g+p)^{p-1} \not\equiv 1 \pmod{p^2}.$$

Thus at least one of g^{p-1} and $(g+p)^{p-1}$ is not congruent to $1 \pmod{p^2}$. Without loss of generality, we may assume that $g^{p-1} \not\equiv 1 \pmod{p^2}$.

We claim that if $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a primitive root modulo p. We note that once we prove this claim, we are home free. Time to prove this claim. Suppose that g has order m in $(\mathbb{Z}/p^l\mathbb{Z})^*$. Since $|(\mathbb{Z}/p^l\mathbb{Z})^*| = p^l - p^{l-1} = p^{l-1}(p-1)$, we have $m \nmid p^{l-1}(p-1)$. Write $m = dp^s$ where $d \,|\, (p-1)$ and $0 \leq s \leq l-1$. By Fermat's little theorem, we have $g^p \equiv g \pmod{p}$. Thus $g^{p^s} \equiv g \pmod{p}$. Thus, $g^{p^s} \equiv g \pmod{p}$ for $s \in \mathbb{N}$. Since $g^m \equiv 1 \pmod{p^l}$ and thus $g^m \equiv 1 \pmod{p}$, we have

$$g^d \equiv (g^{p^s})^d \equiv g^m \equiv 1 \pmod{p}.$$

Since g is a primitive root mod p, we have $(p-1) \,|\, d$. Thus $d = (p-1)$. Since $g^{p-1} \equiv 1 \pmod{p}$ and $g^{p-1} \not\equiv 1 \pmod{p^2}$, there exists $a \in \mathbb{Z}$ with $(a,p) = 1$ such that $g^{p-1} \equiv 1 + ap \pmod{p^2}$. By Proposition (49), $1+ap$ has order p^{l-1} in $(\mathbb{Z}/p^l\mathbb{Z})^*$. Thus g has order $(p-1)p^l$, which implies that $(\mathbb{Z}/p^l\mathbb{Z})^*$ is cyclic. □

25. November 9

Theorem 51. *Let $l \in \mathbb{N}$.*

(1) If $l = 1, 2$ then $(\mathbb{Z}/2^l\mathbb{Z})^*$ is cyclic.

(2) For $l \geq 3$, $(\mathbb{Z}/2^l\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{l-2}\mathbb{Z}$. In particular, we have

$$(\mathbb{Z}/2^l\mathbb{Z})^* = \{(-1)^a 5^b + 2^l\mathbb{Z} : a \in \{0,1\}, b \in \{0,1,\ldots,2^{l-2}-1\}\}.$$

Proof. It is straightforward to verify that $(\mathbb{Z}/2\mathbb{Z})^*$ and $(\mathbb{Z}/4\mathbb{Z})^*$ are cyclic. Thus we focus on the second part.

Claim 4 (Claim 1)**.** *For $l \geq 3$, $5^{2^{l-3}} \equiv 1 + 2^{l-1} \pmod{2^l}$.*

Proof of Claim 1. We prove the claim by induction on l. For $l = 3$, we have $5 \equiv 1 + 2^2 \pmod{2^3}$ as required. Suppose that the above congruence holds for some $l \in \mathbb{N}$ with $l \geq 3$ and we prove it for $l + 1$. Write $5^{2^{l-3}} \equiv 1 + 2^{l-1} + k2^l$ for some $k \in \mathbb{Z}$. It follows that

$$\begin{aligned} 5^{2^{l-2}} &= (1 + 2^{l-1} + k2^l)^2 \\ &= 1 + (2^{l-1})^2 + (k2^l)^2 + 2 \cdot 2^{l-1} + 2 \cdot k2^l + 2 \cdot 2^{l-1}k2^l \\ &= 1 + 2^l + k2^{l+1} + 2^{2l-2} + k2^{2l} + k^2 2^{2l}. \end{aligned}$$

Note that $2(l-1) \geq l + 1$ for $l \geq 3$. Thus we have

$$5^{2^{l-2}} \equiv 1 + 2^l \pmod{2^{l+1}}.$$

By induction, the claim holds. From the above proof, we see that $5^{2^{l-3}} \not\equiv 1 \pmod{2^l}$ and $5^{2^{l-2}} \equiv 1 \pmod{2^l}$. Thus 5 has order 2^{l-2} in $(\mathbb{Z}/2^l\mathbb{Z})^*$. □

Claim 5 (Claim 2)**.** *For $l \geq 3$, the numbers*

$$(-1)^a 5^b \text{ with } a \in \{0,1\} \text{ and } b \in \{0,1,\ldots,2^{l-2}-1\}$$

are distinct modulo 2^l.

Proof of Claim 2. Suppose that $(-1)^{a_1}5^{b_1} \equiv (-1)^{a_2}5^{b_2} \pmod{2^l}$ with $0 \leq a_i \leq 1$ and $0 \leq b_i < 2^{l-2} (i = 1, 2)$. Then $(-1)^{a_1}5^{b_1} \equiv (-1)^{a_2}5^{b_2} \pmod 4$. Since $5 \equiv 1 \pmod 4$, we see that $(-1)^{a_1} \equiv (-1)^{a_2} \pmod 4$. Thus $a_1 = a_2$. We now have $5^{b_1} \equiv 5^{b_2} \pmod{2^l}$. Since 5 has order 2^{l-2} in $(\mathbb{Z}/2^l\mathbb{Z})^*$ and $0 \leq b_i \leq 2^{l-2}$, it follows that $b_1 = b_2$. □

Since $(\mathbb{Z}/2^l\mathbb{Z})^* = \{(-1)^a 5^b : a \in \{0,1\}, b \in \{0,1,\ldots,2^{b-2}-1\}\}$ it follows that

$$(\mathbb{Z}/2^l\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2^{l-2}\mathbb{Z}.$$

□

26. November 9

Theorem 52. *The group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic (i.e. it has a primitive root) if and only if $n = 1, 2, 4, p^l, 2p^l$ with p being an odd prime and $l \in \mathbb{N}$.*

Proof. Let $n = 2^{l_0}p_1^{l_1} \cdots p_r^{l_r}$ where $l_0 \in \mathbb{N} \cup \{0\}$ and $l_1, \ldots, l_r \in \mathbb{N}$, and p_i distinct odd primes. Then by Theorem 42,

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/2^{l_0}\mathbb{Z})^* \times \prod_{i=1}^{r} (\mathbb{Z}/p_i^{l_i}\mathbb{Z})^*.$$

By Theorem 46, $(\mathbb{Z}/p_i^{l_i}\mathbb{Z})^*$ is cyclic for $1 \le i \le r$. By Theorem 51, $(\mathbb{Z}/2^{l_0}\mathbb{Z})^*$ is cyclic for $0 \le l_0 \le 2$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{l_0-2}\mathbb{Z}$ for $l \ge 3$. Thus, the order of any element of $(\mathbb{Z}/n\mathbb{Z})^*$ is a divisor of $\lambda(n) := \operatorname{lcm}(b, \varphi(p_1^{l_1}), \ldots, \varphi(p_r^{l_r}))$, where

$$b = \begin{cases} \varphi(2^{l_0}) & \text{if } 0 \le l_0 \le 2 \\ \frac{1}{2}\varphi(2^{l_0}) & \text{if } l_0 \ge 3. \end{cases}$$

Note that $2 \,|\, \varphi(p_i^{l_i})$ for all $1 \le i \le r$. It thus follows that

$$\lambda(n) < \varphi(2^{l_0})\varphi(p_1^{l_1}) \cdots \varphi(p_r^{l_r})$$

except in the cases $n = 1, 2, 4, p^l, 2p^l$. Since $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic if and only if $\lambda(n) = \varphi(2^{l_0})\varphi(p_1^{l_1}) \cdots \varphi(p_r^{l_r})$, the result follows. □

Definition 22. The number

$$\lambda(n) = \operatorname{lcm}(b, \varphi(p_1^{l_1}), \varphi(p_2^{l_2}), \ldots, \varphi(p_r^{l_r}))$$

is called the *universal exponent* of n.

Theorem 53. *For $n \in \mathbb{N}$, let $\lambda(n)$ be the universal exponent. Then for any $a \in \mathbb{Z}$ with $(a, n) = 1$ we have*

$$a^{\lambda(n)} \equiv 1 \pmod{n}.$$

Remark 18. Euler's theorem states that for any $a \in \mathbb{Z}$ with $(a, n) = 1$, then we have

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

The above theorem gives a strengthening of Euler's theorem.

Remark 19. Given a prime p, one can ask for an upper bound for the smallest positive integer b which is a primitive root mod p. Hua proved that $b < 2^{\omega(p-1)+1}\sqrt{p}$.

Theorem 54. *If p is a prime of the form $4q + 1$ with q an odd prime, then 2 is a primitive root mod p.*

Proof. Let m be the order of 2 mod p. By Fermat's little theorem, $m \,|\, (p-1)$ and thus $m \,|\, 4q$. It follows that $m = 1, 2, 4, 2q, 4q$. Since p is a prime of the form $4q + 1$ with q an odd prime, we have $p = 13$ or $p > 20$. Thus $m \neq 1, 2, 4$. Also, by Euler's criterion we have

$$2^{2q} \equiv 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}.$$

On the other hand, by Corollary 38, since q is odd we have

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(4q+1)^2-1}{8}} = (-1)^{2q^2+q} = -1.$$

Thus $2^{2q} \equiv -1 \pmod{p}$. That is, $m \neq q, 2q$. It follows that $m = 4q = p - 1$, i.e., 2 is a primitive root mod p. □

Let $k, l \in \mathbb{N}$ with $(k, l) = 1$. Dirichlet's theorem states that there are infinitely many primes p with $p \equiv l \pmod{k}$. To prove this theorem, we will introduce later the notion of L functions. However, for many pairs (k, l), we can prove Dirichlet's theorem by elementary means. For example on Assignment #1, we show that there are infinitely many primes p with $p \equiv 5 \pmod{6}$.

27. November 11 & 13

Theorem 55. *Let $n \in \mathbb{N}$. There are infinitely many primes p with $p \equiv 1 \pmod{n}$.*

Proof. This proof is due to Birkhoff and Vandiver (1904). Let $a \in \mathbb{N}$ with $a > 2$ and $\zeta_n = e^{2\pi i/n}$. Consider $\Phi_n(a)$, the n-th cyclotomic polynomial evaluated at a, i.e.,

$$\Phi_n(a) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (a - \zeta_n^j).$$

We recall that $\Phi_n(x) \in \mathbb{Z}[x]$ and $x^n - 1 = \prod_{d|n} \Phi_d(x)$. We claim that:

Claim 6. *If p is a prime dividing $\Phi_n(a)$ then $p \mid n$ or $p \equiv 1 \pmod{n}$.*

Proof of the claim. Note that $p \mid (a^n - 1)$ and thus $p \nmid a$. Two cases:

(1) If $p \nmid (a^d - 1)$ for all $d \mid n$ with $d \neq n$. Then the order of a mod p is n. By Fermat's little theorem, $n \mid (p-1)$ and $p \equiv 1 \pmod{n}$.
(2) Suppose that $p \mid (a^d - 1)$ for some $d \mid n$ with $d \neq n$. Note that $\Phi_n(x) \mid \frac{x^n-1}{x^d-1}$ (in $\mathbb{Z}[x]$). Since $p \mid \Phi_n(a)$, it follows that $p \mid \frac{a^n-1}{a^d-1}$.

We have

$$a^n = (1 + (a^d - 1)^{\frac{n}{d}} = 1 + \frac{n}{d}(a^d - 1) + \binom{n/d}{2}(a^d - 1)^2 + \cdots + .$$

Thus

$$\frac{a^n - 1}{a^d - 1} = \frac{n}{d} + \binom{n/d}{2}(a^d - 1) + \cdots .$$

Since $p \mid \frac{a^n-1}{a^d-1}$ and $p \mid (a^d - 1)$, we conclude that $p \mid \frac{n}{d}$. Thus we have $p \mid n$. This completes the proof of the claim. □

We are now ready to prove the theorem. Suppose that there are only finitely many primes $p_1, \ldots, p_r$ such that $p_j \equiv 1 \pmod{n}$ for all $1 \leq j \leq r$. Write $\Phi_n(x) = x^{\varphi(n)} + \cdots + \pm 1$. Consider then $\Phi_n(np_1p_2 \cdots p_r m)$. We see that $(\Phi(np_1 \ldots p_r m), n) = 1$. Also, since $p_j \nmid \Phi_n(np_1 \ldots p_r m)(1 \leq j \leq r)$. Letting $m \to \infty$, we see that for m sufficiently large we have $\Phi_n(np_1 \ldots p_r m) \geq 2$. Thus it has a prime divisor p, which is not equal to $p_1, \ldots, p_r$. By the claim we have either $p \equiv 1 \pmod{n}$ or $p \mid n$. Since $(\Phi_n(np_1 \ldots p_r m), n) = 1$, we have $p \nmid n$. Thus $p \equiv 1 \pmod{n}$. However $p \notin \{p_1, \ldots, p_r\}$, and this leads to a contradiction. □

Definition 23. Let G be a finite abelian group. A *character of G* is a homomorphism $\chi : G \to \mathbb{C}^*$. The set of characters of G forms a group under the operation

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g)\chi_2(g).$$

This group is called the *dual group of G* and is denoted by $\widehat{G} := \{\chi : G \to \mathbb{C}^* \text{ homomorphism}\}$. The identity of $\widehat{G}$ is the *principal character* χ_0, where $\chi_0(g) = 1$ for all $g \in G$. Note that if $|G| = n$ then $g^n = e$ (the identity element) for all $g \in G$. It follows that $(\chi(g))^n = 1$ and thus $\chi(g)$ is an n-th root of unity.

Theorem 56. *Let G be a finite abelian group. Then*

(1) $|G| = |\widehat{G}|$
(2) $G \cong \widehat{G}$

(3) We have

$$\sum_{\chi\in\widehat{G}}\chi(g)=\begin{cases}|G| & \text{if } g=e\\ 0 & \text{otherwise.}\end{cases}$$

and

$$\sum_{g\in G}\chi(g)=\begin{cases}|G| & \text{if } \chi=\chi_0\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Suppose that $|G|=n$. Since G is a finite abelian group, we have

$$G\cong\mathbb{Z}/n_1\mathbb{Z}\times\cdots\times\mathbb{Z}/n_r\mathbb{Z}.$$

Thus there exist $g_1,\ldots,g_r\in G$ such that $g_j^{h_j}=e(1\le j\le r)$ and every element $g\in G$ has a unique representation in the form $g=g_1^{a_1}\cdots g_r^{a_r}$ with $0\le a_j\le h_j(1\le j\le r)$. Note that any character χ is determined by its action on $g_1,\ldots,g_r$. Since $(\chi(g_j))^{h_j}=1$, we see that $\chi(g_j)$ is an h_j-th root of unity. Thus there are at most $h_1\ldots h_r$ characters. On the other hand, if w_j is a h_j-th root of unity, we can define $\chi(g_j)=w_j$ for $(1\le j\le r$ and extend it multiplicatively to all elements of G. Thus there are at least $h_1\ldots h_j$ characters. It follows therefore that $|\widehat{G}|=|G|$.

For the second part, let χ_j be the character defined by $\chi_j(g_j)=e^{2\pi i/h_j}$ and $\chi_j(g_k)=1$ for $j\ne k$. Define $\varphi:G\to\widehat{G}$ by

$$\varphi(g_1^{a_1}\cdots g_r^{a_r})=\chi_1^{a_1}\cdots\chi_r^{a_r}.$$

One can check that φ is a group homomorphism. Also, since

$$\chi_1^{a_1}\cdots\chi_r^{a_r}(g_j)=e^{2\pi i a_j/h_j},$$

we see that $\chi_1^{a_1}\cdots\chi_r^{a_r}=\chi_0$ if and only if $a_j=h_j$ for all $1\le j\le r$. And this corresponds to $g_1^{h_1}\cdots g_r^{h_r}=e$, the identity of G. Thus φ is injective. Finally, since G is finite and $|\widehat{G}|=|G|$, we see that φ is surjective also. Hence $\widehat{G}\cong G$ as desired.

For the last part, we start by letting

$$S(g)=\sum_{\chi\in\widehat{G}}\chi(g).$$

If $g=e$ then $\chi(e)=1$ for all $\chi\in\widehat{G}$. Thus

$$S(e)=|\widehat{G}|=|G|.$$

We now assume that $g\ne e$. By (2), there exists a character $\chi_1\in\widehat{G}$ such that $\chi_1(G)\ne-1$. Also, since $\widehat{G}\cong G$, if $\chi\in\widehat{G}$ with $\chi\ne\chi_0$ then there exists $\chi^{-1}\in\widehat{G}$ such that $\chi\chi^{-1}=\chi_0$. In particular, if χ runs through all the elements of $\widehat{G}$, so does $\chi_1\chi$. Thus we have

$$S(g)=\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}(\chi_1\chi)(g)=\chi_1(g)\sum_{\chi\in\widehat{G}}\chi(g)=\chi_1(g)S(g).$$

Since $(1-\chi_1(g)\ne0$, it follows that $S(g)=0$ as required. □

Let $T(\chi) := \sum_{g\in G} \chi(g)$. Then if $\chi = \chi_0$ then $\chi_0(g) = 1$ for all $g \in G$ so $T(\chi_0) = |G|$. If $\chi \neq \chi_0$ then there exists $g_1 \in G$ such that $\chi(g_1) \neq 1$. Thus $T(\chi) = 0$, since

$$T(\chi) = \sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(g_1 g) = \chi(g_1) \sum_{g\in G} \chi(g) = \chi(g_1) T(\chi).$$

Let $k \in \mathbb{N}$ with $k \geq 2$. Let χ be a character on $(\mathbb{Z}/k\mathbb{Z})^*$. We extend the definition of χ to $\mathbb{Z}$, also denoted by χ, by putting

$$\chi(a) = \begin{cases} \chi(a + k\mathbb{Z}) & \text{if } (a,k) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Definition 24. We call such χ defined above a *character mod k*.

Theorem 57. *Let χ be a character mod k.*

(1) If $(n,k) = 1$ then $\chi(n)$ is a $\varphi(k)$-th root of unity.

(2) The function χ is completely *multiplicative. That is, $\chi(mn) = \chi(m)\chi(n)$ for* all *$m, n \in \mathbb{Z}$.*

(3) χ is periodic modulo k, that is, $\chi(n + k) = \chi(n)$ for all $n \in \mathbb{Z}$.

(4) We have that

$$\sum_{\chi \ char \ mod \ k} \chi(n) = \begin{cases} \varphi(k) & \text{if } n \equiv 1 \pmod{k} \\ 0 & \text{otherwise.} \end{cases}$$

and

$$\sum_{n=1}^{k} \chi(n) = \begin{cases} \varphi(k) & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases}$$

(5) Let $\overline{\chi}$ denote the conjugate character to χ, i.e., $\overline{\chi}(n) = \overline{\chi(n)}$ for all $n \in \mathbb{Z}$. Let χ' be a character mod k. Then for $(m,k) = 1$ we have

$$\sum_{\chi \ char \ mod \ k} \chi(n)\overline{\chi}(m) = \begin{cases} \varphi(k) & \text{if } n \equiv m \pmod{k} \\ 0 & \text{otherwise.} \end{cases}$$

and

$$\sum_{n=1}^{k} \chi(n)\chi'(n) = \begin{cases} \varphi(k) & \text{if } \chi' = \overline{\chi} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The first four parts follow either from definition or Theorem 56. So we focus on (5) only. Note that $\overline{\chi}(m)\chi(m) = 1 = \chi(m)\chi(m^{-1})$, where m^{-1} is the multiplicative inverse of m modulo k. Thus $\overline{\chi}(m) = \chi(m^{-1})$. It follows that

$$\sum_{\chi \text{ char mod } k} \chi(n)\overline{\chi}(m) = \sum_{\chi} \chi(n)\chi(m^{-1}) = \sum_{\chi} \chi(nm^{-1}).$$

By Theorem 56(3), the last sum is $\varphi(k)$ if and only if $nm^{-1} \equiv 1 \pmod{k}$, or equivalently $n \equiv m \pmod{k}$; and 0 otherwise.

Also, we note that if $\chi' = \overline{\chi}$, then $\chi\chi' = \chi_0$. Otherwise, $\chi\chi'$ is a non-principal character. Thus the second result also follows, again from Theorem 56(3). $\square$

We now describe the group of characters mod k. By multiplicity, it is enough to discuss the characters mod p^l for a prime p.

(1) Assume first that p is an odd prime and let g be a primitive root mod p^l. For $n \in \mathbb{Z}$ with $(n,p)=1$, there exists a unique $\nu \in \mathbb{Z}$ with $1 \le \nu \le \varphi(p^l)$ such that $n \equiv g^\nu \pmod{p^l}$. For $d \in \mathbb{Z}$ with $1 \le d \le \varphi(p^l)$, we define the character $\chi^d(n)$ by

$$\chi^d(n) = \exp\left(\frac{2\pi i d\nu}{\varphi(p^l)}\right).$$

We get in this way $\varphi(p^l)$ different characters mod p^l, and this gives the complete list of characters mod p^l.

(2) Consider characters mod 2^l. If $l=1$ then we only have the principal character. If $l=2$, then we have the principal chracter and the character χ_4 which is defined by

$$\chi_4(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

If $l \ge 3$, then $(\mathbb{Z}/2^l\mathbb{Z})^*$ is not cyclic. However, we have seen in Theorem 51 that for each $n \in \mathbb{Z}$ with $(2,n)=1$, i.e., $n + 2^l\mathbb{Z} \in (\mathbb{Z}/2^l\mathbb{Z})^*$, there exists a unique integer pair (a,b) with $0 \le a \le 1$ and $0 \le b \le 2^{l-2}$ such that $n \equiv (-1)^a 5^b \pmod{2^l}$. Thus for $d \in \mathbb{Z}$ with $1 \le d \le \varphi(2^l)$

$$\chi^d(n) = \begin{cases} \exp\left(\frac{2\pi i d a}{2} + \frac{2\pi i d b}{2^{l-2}}\right) & \text{if } n \equiv 1 \pmod 2 \\ 0 & \text{otherwise.} \end{cases}$$

We get in this way $\varphi(2^l)$ different characters mod 2^l and this gives the complete list of characters mod 2^l.

28. November 16: L-functions and Dirichlet's theorem

Let $k \in \mathbb{N}$ with $k \ge 2$ and χ be a character mod k. For $\mathrm{Re}(s) > 1$, define

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

Let χ_0 be the principal character.

Theorem 58. *The following hold:*

(1) If $\chi \neq \chi_0$ then $L(s,\chi)$ has an analytic continuation to $\mathrm{Re}(s) > 0$.

(2) If $\chi = \chi_0$ then $L(s,\chi_0)$ has an analytic continuation to $\mathrm{Re}(s) > 0$ with $s \neq 1$. At $s=1$, $L(s,\chi_0)$ has a simple pole with residue $\frac{\varphi(k)}{k}$.

Proof. Let $A(x) := \sum_{n \le x} \chi(n)$ and

$$E(\chi) := \begin{cases} 1 & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases}$$

Also, notice that

$$\sum_{n=1}^{k} \chi(n) = \begin{cases} \varphi(k) & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases}$$

By Theorem 57(4), we have

$$A(x) = \begin{cases} \left\lfloor \frac{x}{k} \right\rfloor \varphi(k) + T(x) & \text{if } \chi = \chi_0 \\ \left\lfloor \frac{x}{k} \right\rfloor \cdot 0 + T(x) & \text{otherwise,} \end{cases}$$

with $|T(x)| \leq \varphi(k)$.

It follows that

$$A(x) = E(\chi)\frac{\varphi(k)}{k}x + R(x),$$

where $|R(x)| \leq 2\varphi(k)$. Let $f(n) = n^{-s}$. By Abel's summation, we have

$$\begin{aligned} \sum_{n \leq x} \frac{\chi(n)}{n^s} &= \frac{A(x)}{x^s} + s\int_1^x \frac{A(u)}{u^{s+1}}\,du \\ &= E(\chi)\frac{\varphi(k)}{k} \cdot \frac{1}{x^{s-1}} + \frac{R(x)}{x^s} + sE(\chi)\frac{\varphi(k)}{k}\left(-\frac{u^{s+1}}{s-1}\Big|_1^x\right) + s\int_1^x \frac{R(u)}{u^{s+1}}\,du \\ &= E(\chi)\frac{\varphi(k)}{k}(x^{1-s} + \frac{s}{1-s}(x^{1-s}-1)) + \frac{R(x)}{x^s} + s\int_1^x \frac{R(u)}{u^{s+1}}\,du. \end{aligned} \tag{14}$$

Now we prove each claim. As for (1), if $\chi \neq \chi_0$ then we have $E(\chi) = 0$. We see from (14) that

$$\sum_{n \leq x} \frac{\chi(n)}{n^s} = \frac{R(x)}{x^s} + s\int_1^x \frac{R(u)}{u^{s+1}}\,du.$$

By letting $x \to \infty$, since $|R(x)| \leq 2\varphi(k)$ for $\mathrm{Re}(s) > 0$ we have

$$L(s,\chi) = s\int_1^\infty \frac{R(u)}{u^{s+1}}\,du.$$

Since the integral converges for $\mathrm{Re}(s) > 0$, it follows that $L(s,\chi)$ has an analytic continuation to $\mathrm{Re}(s) > 0$.

We move on to (2). If $\chi = \chi_0$ then $E(\chi) = 1$. Thus by (14) we have

$$\sum_{n \leq x} \frac{\chi(n)}{n} = \frac{\varphi(k)}{k}\left(x^{1-s} + \frac{s}{1-s}(x^{1-s}-1)\right) + \frac{R(x)}{x^s} + s\int_1^x \frac{R(u)}{u^{s+1}}\,du.$$

Consider $\mathrm{Re}(s) > 1$. By letting $x \to \infty$, we have

$$L(s,\chi_0) = \frac{\varphi(k)}{k} \cdot \frac{s}{s-1} + s\int_1^\infty \frac{R(u)}{u^{s+1}}\,du.$$

Since the integral converges for $\mathrm{Re}(s) > 0$, the function $L(s,\chi_0)$ has an analytic continuation to $\mathrm{Re}(s) > 0$ except at a simple pole at $s = 1$ with residue $\frac{\varphi(k)}{k}$. □

Definition 25. Let $\{\lambda_n\}_{n=1}^\infty$ be a strictly increasing sequence of positive real numbers. For $z \in \mathbb{C}$, a *Dirichlet series* attached to $\{\lambda_n\}_{n=1}^\infty$ is a series of the form

$$\sum_{n \geq 1} a_n e^{-\lambda_n z}$$

where $\{a_n\}_{n\geq 1}$ is a sequence of complex numbers.

Theorem 59. *If the Dirichlet series* $\sum_{n\geq 1} a_n e^{-\lambda_n z}$ *converges for* $z = z_0$ *then it converges uniformly for* $\mathrm{Re}(z - z_0) > 0$ *and* $|\arg(z - z_0)| < a$ *with* $a < \frac{\pi}{2}$.

Proof. Without loss of generality, we may assume $z_0 = 0$. Since $\sum_{n\geq 1} a_n$ converges, for any $\varepsilon > 0$ there exists $N = N(\varepsilon) \in \mathbb{N}$ such that if $l, m > N$ then

$$\sum_{n=l}^{m} |a_n| < \varepsilon.$$

Let $A_{l,m} = \sum_{n=l}^{m} a_n$. By taking the convention that $A_{l,l-1} = 0$, we have

$$\begin{aligned}\sum_{n=l}^{m} a_n e^{-\lambda_n z} &= \sum_{n=l}^{m} (A_{l,n} - A_{l,n-1}) e^{-\lambda_n z} \\ &= \sum_{n=l}^{m-1} A_{l,n}(e^{-\lambda_n z} + e^{-\lambda_{n+1} z}) + A_{l,m} e^{-\lambda_m z}.\end{aligned}$$

Thus for $\mathrm{Re}(z) \geq 0$, we have

$$\left| \sum_{n=l}^{m} a_n e^{-\lambda_n z} \right| \leq \varepsilon \left(\sum_{n=l}^{m-1} |e^{-\lambda_n z} - e^{-\lambda_{n+1} z}| + 1 \right)$$

Note that $e^{-\lambda_n z} - e^{-\lambda_{n+1} z} = z \int_{\lambda_n}^{\lambda_{n+1}} e^{-tz}\, dt$. Also, for $z = x + iy$ with $x, y \in \mathbb{R}$ we have $|e^{-tz}| = e^{-tx}$. Thus we have

$$\begin{aligned}|e^{-\lambda_n z} - e^{-\lambda_{n+1} z}| &\leq |z| \int_{\lambda_n}^{\lambda_{n+1}} e^{-tx}\, dt \\ &\leq \frac{|z|}{x}(e^{-\lambda_n x} - e^{-\lambda_{n+1} x}).\end{aligned}$$

Therefore we have

$$\left| \sum_{n=l}^{m} a_n e^{-\lambda_n z} \right| \leq \varepsilon \left(\frac{|z|}{x}(e^{-\lambda_l x} - e^{-\lambda_m x}) + 1 \right).$$

Note that for $|\arg(z)| < \alpha$, we have $\frac{|z|}{x} < c$ for some $c = c(\alpha)$. Also, we have $|e^{-\lambda_l x} - e^{-\lambda_m x}| \leq 2$. It follows that

$$\left| \sum_{n=l}^{m} a_n e^{-\lambda_n z} \right| < (2c + 1)\varepsilon.$$

Therefore the Dirichlet series converges for $\mathrm{Re}(z) \geq 0$ and $|\arg(z)| \leq \alpha$, as desired. $\square$

29. November 18 & 20

Theorem 60. *If*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$$

be a Dirichlet series with $a_n \in \mathbb{R}$ and $a_n \geq 0$ for all $n \in \mathbb{N}$. Suppose that the series converges for $\mathrm{Re}(z) > \sigma_0$ with $\sigma_0 \in \mathbb{R}$. Suppose also that $f(z)$ can be analytically continued in a neighbourhood $\sum n^{-s}$ of σ_0. Then there exists a real number $\varepsilon > 0$ such that $\sum_{n\geq 1} a_n e^{-\lambda_n z}$ for $\mathrm{Re}(z) > \sigma_0 - \varepsilon$.

Proof. Without loss of generality, we may assume that $\sigma_0 = 0$. Since $f(z)$ is analytic in a neighbourhood of 0, by Theorem 59, it is analytic for $\mathrm{Re}(z) > 0$. Since $f(z)$ is analytic for $\mathrm{Re}(z) > 0$, and is also analytic in a neighbourhood of 0, there exists $\varepsilon > 0$ such that f is analytic in $|z - 1| \leq 1 + \varepsilon$. Note that for $\mathrm{Re}(z) > 0$,

$$f^{(m)}(z) = \sum_{n=1}^{\infty} a_n (-\lambda_n)^m e^{-\lambda_n z}.$$

This implies that $f^{(m)}(1) = \sum a_n (-\lambda_n)^m e^{-\lambda_n}$. Thus the Taylor series expansion of $f(z)$ around 1 in $|z - 1| \leq 1 + \varepsilon$ is of the form

$$\sum_{m=0}^{\infty} \frac{f^{(m)}(1)}{m!} (z-1)^m.$$

We now consider $f(z)$ at the point $z = -\varepsilon$. We have

$$\begin{aligned} f(-\varepsilon) &= \sum_{m=0}^{\infty} \left(\sum_{n=1)}^{\infty} a_n (-\lambda_n)^m e^{-\lambda_n} \right) \frac{(-1-\varepsilon)^m}{m!} \\ &= \sum_{m=0}^{\infty} \left(\sum_{n=1}^{\infty} a_n \lambda_n^m e^{-\lambda_n} \right) \frac{(1+\varepsilon)^m}{m!}. \end{aligned}$$

Since $a_n \geq 0$ and all other terms are positive, we can switch the order of summation and obtain

$$\begin{aligned} f(-\varepsilon) &= \sum_{n=1}^{\infty} a_n e^{-\lambda_n} \left(\sum_{m=0}^{\infty} \frac{(\lambda_n)^m (1+\varepsilon)^m}{m!} \right) \\ &= \sum_{n=1}^{\infty} a_n e^{-\lambda_n} \cdot e^{\lambda_n (1+\varepsilon)} = \sum_{n=1}^{\infty} a_n e^{\lambda_n \varepsilon} = \sum_{n=1}^{\infty} a_n e^{(-\lambda_n)(-\varepsilon)}. \end{aligned}$$

Thus the series $\sum a_n e^{-\lambda_n z}$ converges to $f(z)$ at $z = -\varepsilon$. By Theorem 59 it converges to $f(z)$ for $\mathrm{Re}(z) > -\varepsilon$. □

Theorem 61. *For $k \in \mathbb{N}$ with $k \geq 2$, let χ be a character mod k. Then*

(1) $L(s, \chi)$ is non-zero for $\mathrm{Re}(s) > 1$
(2) If $\chi \neq \chi_0$, then $L(1, \chi)$ is non-zero.

Proof. (1) Note that $L(s,\chi)$ converges absolutely for $\mathrm{Re}(s) > 1$. Since χ is completely multiplicative, $L(s,\chi)$ has a Euler product representation for $\mathrm{Re}(s) > 1$ which is

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

for $\mathrm{Re}(s) > 1$. Since

$$\sum_p \left|\frac{\chi(p)}{p^s}\right|$$

converges for $\mathrm{Re}(s) > 1$, it follows that $L(s,\chi)$ is non-zero for $\mathrm{Re}(s) > 1$.

(2) We recall that for $|u| < 1$, we have

$$-\log(1-u) = \sum_{n=1}^{\infty} \frac{u^n}{n}.$$

Thus for $\mathrm{Re}(s) > 1$ we have

$$\begin{aligned}\log L(s,\chi) &= \log\left(\prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}\right) \\ &= \sum_p -\log\left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_p \sum_{n=1}^{\infty} \frac{\chi(p^s)}{np^{ns}}.\end{aligned}$$

Let $l \in \mathbb{Z}$ with $(l,k) = 1$. By summing over all characters mod k we have

$$\begin{aligned}\sum_{\chi \text{ char mod } k} \overline{\chi}(l) \log L(s,\chi) &= \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}} \sum_{\chi \text{ char mod } k} \overline{\chi}(l)\chi(p^n) \\ &= \varphi(k) \sum_{n=1}^{\infty} \sum_{p^n \equiv l \pmod k} \frac{1}{np^{ns}},\end{aligned}$$

by Theorem 57(5). By taking $l = 1$ and exponentiating both sides, we have

$$\prod_{\chi \text{ char mod } k} L(s,\chi) = \exp\left(\varphi(k) \sum_{n=1}^{\infty} \sum_{p^n \equiv 1 \pmod k} \frac{1}{np^{ns}}\right).$$

Thus if $s \in \mathbb{R}$ with $s > 1$, then we have

$$\prod_{\chi \text{ char mod } k} L(s,\chi) \geq 1.$$

We now split into cases depending on if χ is a real character or not.

(1) Suppose that $L(1,\chi) = 0$ where χ is a non-real character. Since $L(s,\overline{\chi}) = \overline{L(s,\chi)}$ for $s \in \mathbb{R}$ with $s > 1$, we have $L(1,\overline{\chi}) = \overline{L(1,\chi)} = 0$.

We also recall that for $s \in \mathbb{R}$ with $s > 1$, we have

$$\prod_{\chi \text{ char mod } k} L(s, \chi) > 1. \tag{15}$$

We have seen in Theorem 58 that $L(s, \chi_0)$ has a simple pole at $s = 1$ and $L(s, \chi)$ does not have a pole at $s = 1$ for any $\chi \neq \chi_0$. Thus as $s \to 1^+$ on the real line, we have

$$\prod_{\chi \text{ char mod } k} L(s, \chi) = O((s-1)^{-1}(s-1)^2 = O(s-1),$$

which contradicts (15). Thus $L(1, \chi) \neq 0$ for χ a non-real character.

(2) Now suppose that $L(1, \chi) = 0$ with χ a real character. For $\mathrm{Re}(s) > 1$, define

$$g(s) := \frac{\zeta(s)L(s, \chi)}{\zeta(2s)}.$$

Consider the Euler product representation of $g(s)$ for $\mathrm{Re}(s) > 1$ we have

$$\begin{aligned} g(s) &= \prod_p \frac{1 - p^{-2s}}{(1 - p^{-s})(1 - \chi(p)p^{-s})} = \prod_p \frac{1 + p^{-s}}{1 - \chi(p)p^{-s}} \\ &= \prod_p (1 + p^{-s}) \left(\sum_{l=0}^{\infty} \chi(p^l) p^{-ls} \right) = \prod_p \left(1 + \sum_{l=1}^{\infty} (\chi(p^{l-1}) + \chi(p^l)) p^{-ls} \right) \\ &= \prod_p \left(1 + \sum_{l=1}^{\infty} b(p^l) p^{-ls} \right), \end{aligned}$$

where $b(p^l) = \chi(p^{l-1}) + \chi(p^l) \quad (l \geq 1)$. Since χ is a real character, we have $\chi(p) \in \{0, \pm 1\}$. Since χ is multiplicative, we have

$$b(p^l) = \chi(p^{l-1}) + \chi(p^l) = \begin{cases} 0 & \text{if } \chi(p) = 0 \text{ or } -1 \\ 2 & \text{if } \chi(p) = 1. \end{cases}$$

In all cases, we have $b(p^l) \geq 1$ for all $l \geq 1$. Thus

$$g(s) = 1 + \sum_{n=2}^{\infty} \frac{a_n}{n^s}, \tag{16}$$

with $a_n \in \mathbb{R}_{\geq 0}$ for all $n \geq 2$. Since the zero of $L(1, \chi)$ eliminates the pole of $\zeta(s)$ at $s =!$ and since $\zeta(2s)$ is non-zero and analytic for $\mathrm{Re}(s) > \frac{1}{2}$, it follows that $g(s)$ has an analytic continuation to $\mathrm{Re}(s) > \frac{1}{2}$. By Theorem 60, we conclude that the series defining g converges to g for $\mathrm{Re}(s) > \frac{1}{2}$. As $s \to \frac{1}{2}^+$ on the real axis, since $\zeta(2s)$ has a pole at $s = \frac{1}{2}$ we see that $g(s) = O\left(s - \frac{1}{2}\right)$. But this contradicts (16) as $g(s) \geq 1$ for $\mathrm{Re}(s) > \frac{1}{2}$. Thus $L(1, \chi) \neq 0$ for χ real characters. $\square$

30. November 23

Theorem 62. *Let $l, k \in \mathbb{Z}$ with $k \geq 2$ and $(l,k) = 1$. Then the series*

$$\sum_{p \equiv l \pmod{k}} p^{-1}$$

diverges. This implies that there are infinitely many primes p with $p \equiv l \pmod{k}$.

Remark 20. For $x \in \mathbb{R}$, let

$$\pi(x; k, l) = \#\{p \leq x : p \text{ is a prime and } p \equiv l \pmod{k}\}.$$

Then using similar method used by Newman for his proof of the prime number theroem, one can prove that

$$\pi(x; k, l) \sim \frac{1}{\varphi(k)} \cdot \frac{x}{\log x}.$$

This was proved by Valleé-Poussin. In the case when k is "small", the Siegel-Walfisz theorem gives a refinement of the above result. More precisely, define

$$\psi(x; k, l) = \sum_{\substack{n \leq x \\ n \equiv l \pmod{k}}} \Lambda(n)$$

If $k \leq (\log x)^N$ for some $N \in \mathbb{N}$, then

$$\psi(x; k, l) = \frac{x}{\varphi(k)} + O(x \exp(-C_N (\log x)^{1/2})),$$

where the constant C_N depends on N.

Proof. We have seen in the proof of Theorem 61 that

$$\frac{1}{\varphi(k)} \sum_{\chi \text{ char mod } k} \overline{\chi}(l) \log L(s, \chi) = \sum_{n=1}^{\infty} \sum_{p^n \equiv l \pmod{k}} \frac{1}{np^{ns}}. \tag{17}$$

We recall that

$$E(\chi) = \begin{cases} 1 & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

As $s \to 1^+$ on the real axis, by Theorems 58 and 61, we see that $(s-1)^{E(\chi)} L(s, \chi)$ tends to a finite non-zero limit. Thus $E(\chi) \log(s-1) + \log L(s, \chi)$ tends to a limit. It follows that as $s \to 1^+$ on the real axis, we have

$$\log L(s, \chi) = -E(\chi) \log(s-1) + O(1).$$

Thus we have

$$\begin{aligned} \frac{1}{\varphi(k)} \sum_{\chi \text{ char mod } k} \overline{\chi}(l) \log L(s, \chi) &= \frac{1}{\varphi(k)} \log L(s, \chi_0) + \frac{1}{\varphi(k)} \sum_{\substack{\chi \text{ char mod } k \\ \chi \neq \chi_0}} \overline{\chi}(l) \log L(s, \chi) \\ &= -\log(s-1) + O(1). \end{aligned}$$

Combining this with (17) we have

$$\sum_{n=1}^{\infty} \sum_{p^n \equiv l \pmod{k}} \frac{1}{np^{ns}} = -\frac{1}{\varphi(k)} \log(s-1) + O(1).$$

Thus

$$\sum_{p \equiv l \pmod{k}} p^{-s} + \sum_{n=2}^{\infty} \sum_{p^n \equiv l \pmod{k}} \frac{1}{np^{ns}} = -\frac{1}{\varphi(k)} \log(s-1) + O(1).$$

Note that for $\mathrm{Re}(s) \geq 1$ and $s \in \mathbb{R}$,

$$\begin{aligned}
\sum_{n=2}^{\infty} \sum_{p^n \equiv l \pmod{k}} \frac{1}{np^{ns}} &\leq \frac{1}{2} \sum_{n=2}^{\infty} \sum_{p^n \equiv l \pmod{k}} \frac{1}{p^{ns}} \\
&= \frac{1}{2} \sum_{m=2}^{\infty} \left(\frac{1}{m^{2s}} + \frac{1}{m^{3s}} + \cdots \right) \\
&\leq \frac{1}{2} \sum_{m=2}^{\infty} \frac{1}{m^{2s}} \left(\frac{1}{1 - \frac{1}{m^s}} \right) \\
&\leq \sum_{m=2}^{\infty} \frac{1}{m^{2s}} \leq \sum_{m=2}^{\infty} \frac{1}{m^2} \leq \frac{\pi^2}{6}.
\end{aligned}$$

Thus

$$\sum_{p \equiv l \pmod{k}} \frac{1}{p^s} = -\frac{1}{\varphi(k)} \log(s-1) + O(1).$$

As $s \to 1^+$ on the real axis the quantity $-\frac{1}{\varphi(k)} \log(s-1) \to \infty$. It follows that $\sum_{p \equiv l \pmod{k}} p^{-1}$ diverges. □

31. November 23: Waring's problem

In 1770, Edward Waring asserted without proof that every natural number is a sum of at most 4 squares, 9 cubes, 19 biquadrates and so on. Waring's problem states that: for $k \in \mathbb{N}$ with $k \geq 2$, there exists a number $s = s(k)$ such that every natural number is a sum of at most s k-th powers of natural numbers, i.e., $n = x_1^k + \cdots + x_s^k$ with $x_i \in \mathbb{N} \cup \{0\}$ $(1 \leq i \leq s)$.

Let $g(k)$ denote the least s such that the above statement holds. Then Waring's problem states that $g(k) < \infty$. In 1770, Lagrange proved that $g(2) = 4$. By 1909, only known cases were $k = 2, 3, 4, 5, 6, 7, 8, 10$. In 1909, by a combinatorial method, Hilbert proved that $g(k) < \infty$ for every $k \geq 2$. By the work of Vinogradov, we now have an *almost* complete solutions to $g(k)$.

Consider the integer

$$n = 2^k \left\lfloor \left(\frac{3}{2} \right)^k \right\rfloor - 1 < 3^k.$$

The most efficient representation for n is to use $\left(\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1\right)$ many 2^k and

$$n = 2^k \left(\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 \right) + 1^k(2^k - 1).$$

Thus we obtain a result of Euler that

$$g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2.$$

Indeed, the equality holds for all but finitely many k. In fact, the equality holds when

$$2^k \{ \left(\frac{3}{2}\right)^k \} + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor \leq 2^k.$$

In 1957, Mahler showed that the above inequality holds for all but finitely many k.

Let $G(k)$ be the least s such that for n sufficiently large we can write $n = x_1^k + \cdots + x_s^k$.

In the following, we will establish $g(2) = 4$. Observe that as x runs over $\mathbb{Z}/8\mathbb{Z}$ we have $x^2 \equiv 0, 1, 4 \pmod 8$. Since $x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \pmod 8$ we see that $g(2) \geq 4$.

32. November 25

Recall that for $k \in \mathbb{N}$ with $k \geq 2$, let $g(k)$ denote the least integer s such that for all $n \in \mathbb{N}$ we have

$$n = x_1^k + x_2^k + \cdots + x_s^k$$

with $x_i \in \mathbb{N} \cup \{0\}$. Our goal is to prove that $g(2) = 4$.

Theorem 63. *If p is an odd prime then there exists integers x, y such that $1 + x^2 + y^2 = mp$ where $m \in \mathbb{Z}$ with $1 \leq m \leq p - 1$.*

Proof. Consider the sets

$$S_1 = \left\{ x^2 + p\mathbb{Z} : x \in \mathbb{Z}, 0 \leq x \leq \frac{p-1}{2} \right\}.$$

and

$$S_2 = \left\{ -1 - y^2 + p\mathbb{Z} : y \in \mathbb{Z}, 0 \leq y \leq \frac{p-1}{2} \right\}.$$

Note that $x_1^2 \equiv x_2^2 \pmod p$ if and only if $x_1 \equiv \pm x_2 \pmod p$. Since $0 \leq x \leq \frac{p-1}{2}$, all elements in S_1 are distinct, and so are S_2. Since $|S_1| = |S_2| = \frac{p+1}{2}$, we have $S_1 \cap S_2 \neq \emptyset$. Thus there exist $x, y \in \mathbb{Z}$ with $0 \leq x, y \leq \frac{p-1}{2}$ such that $x^2 \equiv -1 - y^2 \pmod p$, or $1 + x^2 + y^2 \equiv 0 \pmod p$. Thus $1 + x^2 + y^2 = mp$ for some $m \in \mathbb{Z}$. We also have $0 < m < \frac{1+x^2+y^2}{p} \leq \frac{1+\left(\frac{p-1}{2}\right)^2+\left(\frac{p-1}{2}\right)^2}{p} < p$. □

Theorem 64 (Lagrange)**.** *We have $g(2) = 4$. That is, every natural number can be written as a sum of at most four squares.*

Proof. We have the Lagrange identity

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2\\ &\quad+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\ &\quad+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2\\ &\quad+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2.\end{aligned}$$

We see that the product of two members which are representable as a sum of four squares is also representable as a sum of four squares. Thus it suffices to prove that every prime can be written as a sum of four squares. Note that $2=1^2+1^2+0^2+0^2$. Let p be an odd prime. By Theorem 63, there exist $x_1,x_2,x_3,x_4\in\mathbb{Z}$ such that $x_1^2+x_2^2+x_3^2+x_4^2=mp$ with $1\le m\le p-1$. Let m_0 be the smallest natural number such that m_0p is a sum of four squares. It remains to show that $m_0=1$. Suppose that m_0 is even. Note that

$$(x_1+x_2+x_3+x_4)^2=x_1^2+x_2^2+x_3^2+x_4^2+2\sum_{1\le i<j\le 4}x_ix_j.$$

Since $x_1^2+x_2^2+x_3^2+x_4^2=m_0p$ is even, we see that $x_1+x_2+x_3+x_4$ is even also. Thus either x_1,x_2,x_3,x_4 are all even, all odd, or only two of them are even (without loss of generality, let's say x_1 and x_2 are even). In all cases, we see that

$$x_1+x_2,x_1-x_2,x_3+x_4,x_3-x_4$$

are all even. So it follows that

$$\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2=\frac{x_1^2+x_2^2+x_3^2+x_4^2}{2}=\frac{m_0}{2}p.$$

But this contradicts the minimality of m_0. Hence m_0 is odd. Suppose now that $m_0>1$. Since $x_1^2+x_2^2+x_3^2+x_4^2=m_0p$ and $1\le m_0\le p-1$, not all of x_1,x_2,x_3,x_4 are divisible by m_0, for otherwise we would have $m_0^2\,|\,m_0p$, which is impossible since this would imply $m_0\,|\,p$. Thus there exist $b_1,b_2,b_3,b_4\in\mathbb{Z}$ such that $y_i=x_i-b_im_0$ and $|y_i|<\frac{m_0}{2}$ $(1\le i\le 4)$ and not all the y_i's are zero. Then $0<y_1^2+y_2^2+y_3^2+y_4^2<4\left(\frac{m_0}{2}\right)^2=m_0^2$ and $y_1^2+y_2^2+y_3^2+y_4^2\equiv 0 \pmod{m_0}$. Thus there exist $m_1\in\mathbb{N}$ with $m_1<m_0$ such that

$$y_1^2+y_2^2+y_3^2+y_4^2=m_0m_1.$$

We recall that $x_1^2+x_2^2+x_3^2+x_4^2=m_0p$. Multiply the above two equalities together. By the Lagrange identity, there exist $z_1,z_2,z_3,z_4\in\mathbb{Z}$ such that

$$z_1^2+z_2^2+z_3^2+z_4^2=m_0^2m_1p,$$

where $z_1=x_1y_1+x_2y_2+x_3y_3+x_4y_4$ and etc. Since

$$z_1=\sum_{i=1}^4 x_i(x_i-b_im_0)=\sum_{i=1}^4 x_i^2+m_0K$$

for some $K\in\mathbb{Z}$. Since $x_1^2+x_2^2+x_3^2+x_4^2=m_0p$ we have $m_0\,|\,z_1$. Similarly, we see that z_2,z_3,z_4 are all divisible by m_0. Let $t_i=z_i/m_0$ $(1\le i\le 4)$. Then

$$t_1^2+t_2^2+t_3^2+t_4^2=m_1p$$

and $1\le m_1<m_0$, which contradicts the minimality of m_0. Thus $m_0=1$ for all odd primes p. Thus we see that all primes are representable as a sum of four squares. $\square$

Theorem 65. $g(4) \leq 53$.

Proof. We have the identity

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 = &(a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4 \\ &+(a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4 \\ &+(a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4. \end{aligned}$$

Combining the above identity with Theorem 64, we see that every integer of the form $6x^2$ can be expressed as a sum of 12 fourth powers. Note that every natural number can be written in the form $6k+r$ with $k \in \mathbb{N} \cup \{0\}$ and $0 \leq r \leq 5$. Then by Theorem 64 we can write k as a sum of four squares, say $k = x_1^2+x_2^2+x_3^2+x_4^2$. Then $6k = 6x_1^2+6x_2^2+6x_3^2+6x_4^2$.

Since each term in the above sum is a sum of 12 fourth powers, $6k$ can be expressed as a sum of 48 fourth powers. Finally, we note that $r = 1^4+\cdots+1^4$ (r times). Since $0 \leq r \leq 5$, it follows that $6k+r$ is a sum of 53 fourth powers as needed. □

33. November 27: Hardy-Littlewood circle method

We recall that the number $g(k)$ is determined by "small" numbers of special form. Thus a more interesting question is to estimate $G(k)$, defined to be the least integer $s = s(k)$ such that every *sufficiently large* integer is the sum of at most k-powers of natural numbers. Clearly, we have $G(k) \leq g(k)$. Also, a conjecture states that $G(k) = \max\{k+1, \Gamma_0(k)\}$ where $\Gamma_0(k)$ is the least integers s such that for every prime p and $m \in \mathbb{N}$, we have $n = x_1^k+\cdots+x_s^k$ has a soultion in mod p^m where $(x_1, p) = 1$. For large k, Wooley proved in 1992 that $G(k) \leq k\log k + O(k\log\log k)$.

One can consider a more refined question: for fixed $k \in \mathbb{N}$ with $k \geq 2$, let

$$R_s(n) = R_{s,k}(n) = \#\{n : x_1^k+\cdots+x_s^k, x_i \in \mathbb{N}, 1 \leq i \leq s\}.$$

Note that if the above equality holds, then $x_i \leq n^{1/k}$. Also the sum $x_1^k+\cdots+x_s^k$ ranges from s to sn. Thus we expect that $R_s(n)$ is of size

$$(n^{1/k})^s \cdot (sn-s)^{-1} \asymp n^{s/k-1}.$$

Note that $(n^{1/k})^s$ denotes the choices for $x_1, \ldots, x_s$ and $(sn-s)^{-1}$ the probability that their sum is n. That is, we expect $R_s(n) \sim C(s,k;n)n^{s/k-1}$ for some appropriate constant $C > 0$.

Let $\widetilde{G}(k)$ be the least integer $s = s(k)$ such that the above asymptotic formula holds for every sufficiently large integer n. Note that for $G(k)$, we only need $R_s(n) > 0$. Thus we have $G(k) \leq \widetilde{G}(k)$. To estimate $R_s(n)$, we apply the exponential function. For $\alpha \in \mathbb{R}$, let $e(\alpha) = e^{2\pi i\alpha}$. We have

$$e(\alpha)e(\beta) = e(\alpha+\beta).$$

Moreover, for $h \in \mathbb{Z}$ we have the following orthogonal relation

$$\int_0^1 e(\alpha h)\,d\alpha = \begin{cases} 1 & \text{if } h = 0 \\ 0 & \text{if } h \in \mathbb{Z}\setminus\{0\}. \end{cases}$$

Define $p = n^{1/k}$ and

$$f(\alpha) = \sum_{1 \leq x \leq p} e(\alpha x^k).$$

It follows that

$$\begin{aligned}\int_0^1 f(\alpha)^s e(-n\alpha)\,d\alpha &= \int_0^1 \left(\sum_{x\le p} e(\alpha x^k)\right)^s e(-n\alpha)\,d\alpha \\ &= \sum_{x_1\le p}\cdots\sum_{x_s\le p}\int_0^1 e(\alpha x_1^k)\cdots e(\alpha x_s^k)e(-n\alpha)\,d\alpha \\ &= \sum_{x_1\le p}\cdots\sum_{x_s\le p}\underbrace{\int_0^1 e(\alpha(x_1^k+\cdots+x_s^k-n))\,d\alpha}_{(*)} = R_s(n).\end{aligned}$$

Note that $(*)$ is 1 if $n = x_1^k+\cdots+x_s^k$ and 0 otherwise. Note that as α runs between 0 and 1, $e(\alpha)$ runs through the unit circl. This is why we call this approach the circle method.

34. November 30

Define $\widetilde{G}(k)$ the least integer $s = s(k)$ such that the expected asymptotic formula holds for every sufficiently large n.

Conjecture. $\widetilde{G}(k) = \max\{k+1, \Gamma_0(n)\}$ *where* $\Gamma_0(k)$ *is the least integer* s *such that for every prime* p *and* $m\in\mathbb{N}$*, we have*

$$n = x_1^k+\cdots+x_s^k$$

has a solution in mod p^m *with* $(x_1,p)=1$*.*

For $\alpha\in\mathbb{R}$, let $e(\alpha) := e^{2\pi i\alpha}$. Let $p = n^{1/k}$ and $f(\alpha) = \sum_{1\le x\le p} e(\alpha x^k)$. We have seen

$$R_s(n) = \int_0^1 f(\alpha)^s e(-n\alpha)\,d\alpha.$$

Idea is to divide $[0,1)$ into two parts: major arc $\mathfrak{M}$ and minor arc $\mathfrak{m}$, where $\mathfrak{M}$ contains $\alpha\in[0,1)$ that are "close" to a rational number of "small" denominators and $\mathfrak{m} = [0,1)\setminus\mathfrak{M}$.

Consider $\alpha = \frac{a}{q}$ with $(a,q)=1$. Write $x = yq+r$ with $1\le r\le q$. We have

$$\begin{aligned}e\left(\frac{a}{q}\right) &= \sum_{1\le x leq p} e\left(\frac{a}{q}x^k\right) = \sum_{r=1}^{q}\sum_{\frac{1-r}{q}\le y\le\frac{p-r}{q}} e\left(\frac{a}{q}(yq+r)^k\right) \\ &= \sum_{r=1}^{q}\sum_{\frac{1-r}{q}\le y\le\frac{p-r}{q}} e\left(\frac{ar^k}{q}\right) \sim \frac{p}{q}\sum_{r=1}^{q} e\left(\frac{ar^k}{q}\right).\end{aligned}$$

We need $q\le p$ for the $\sim$ part to be true. To extend the above estimate to $\alpha[0,1)$ that is close enough to $\frac{a}{q}$, we note that

$$f\left(\frac{a}{q}+cp^{-k}\right) = \sum_{x\le p} e\left(\left(\frac{a}{q}+cp^{-k}\right)x^k\right) = \sum_{x\le p} e\left(\frac{a}{q}x^k\right)e(cp^{-k}x^k).$$

To approximate $f\left(\frac{a}{q}+cp^{-k}\right)$ by $f\left(\frac{a}{q}\right)$, we need $e(cp^{-k}x^k)$ to be "close" to 1. Since $p^{-k}x^k\le 1$, it suffices to choose to be "small". This motivates the following definition of the major arcs.

Definition 26. Let $\delta \in \mathbb{R}$ with $0 < \delta < \frac{1}{5}$, and let $a, q \in \mathbb{N} \cup \{0\}$. We define the *major arcs* to be

$$\mathfrak{M} := \bigcup_{\substack{0 \le a < q \le p^\delta \\ (a,q)=1}} \mathfrak{M}(q,a)$$

where

$$\mathfrak{M}(q,a) = \left\{ \alpha \in [0,1) : \left| \alpha - \frac{a}{q} \right| \le p^{\delta - k} \right\}.$$

The remaining portion $\mathfrak{m} = [0,1) \setminus \mathfrak{M}$ is the *minor arcs*. One can show that

$$\int_{\mathfrak{M}} f(\alpha)^s e(-n\alpha)\, d\alpha \sim C(s,k,n) k^{\frac{s}{k}-1}.$$

A trivial bound for $f(\alpha)$ is

$$|f(\alpha)| = \left| \sum_{x \le p} e(\alpha x^k) \right| \le p.$$

Suppose that we can show $\sup\limits_{\alpha \in \mathfrak{m}} |f(\alpha)| \ll p^{1-\nu}$ where $\nu = \nu(k) > 0$. Then it follows that

$$\left| \int_{\mathfrak{m}} f(\alpha)^s e(-n\alpha)\, d\alpha \right| \le \left(\sup_{\alpha \in \mathfrak{m}} |f(\alpha)| \right)^s \int_{\mathfrak{m}} 1\, d\alpha \ll (p^{1-\nu})^s.$$

Here, we want to get $\ll p^{s-k-\lambda}$ for some $\lambda > 0$. For this, it suffices to have $s\nu > k + \lambda$. Thus $(p^{1-\nu})^s \ll p^{s-k-\nu} \ll n^{\frac{s}{k}-1-\frac{\nu}{k}}$. Now we need to show $s\nu > k + \lambda$. Write $s = 2r + 1$. We see that

$$\begin{aligned} \int_{\mathfrak{m}} f(\alpha)^s\, d\alpha &\ll \sup_{\alpha \in \mathfrak{m}} |f(\alpha)| \int_0^1 |f(\alpha)|^{2r}\, d\alpha \\ &= \sup_{\alpha \in \mathfrak{m}} |f(\alpha)| \#\{x_1^k + \cdots + x_r^k = y_1^k + \cdots + y_r^k, x_i, y_i \in p\} \\ &\sim p^{1-\nu} \cdot p^{2r-k}. \end{aligned}$$

We need to find r sufficiently large, namely $r \sim k^2$.

35. December 2

Let $a, q \in \mathbb{N} \cup \{0\}$. Suppose that $0 < a < q$ and $(a,q) = 1$. For $\alpha \in \mathfrak{M}(q,a) \subseteq \mathfrak{M}$ we have $q \le p^\delta (0 < \delta < \frac{1}{5})$ and

$$\left| \alpha - \frac{p}{q} \right| \le p^{\delta - k}.$$

Write $\alpha = \frac{a}{q} + \beta$. Then

$$\begin{aligned} f(\alpha) &= \sum_{1 \le x \le p} e(\alpha x^n) \\ &= \sum_{r=1}^{q} \sum_{\frac{1-r}{q} \le y \le \frac{p-r}{q}} e\left(\left(\frac{a}{q} + \beta\right)(qy+r)^k\right) \\ &= \sum_{r=1}^{q} e\left(\frac{ark}{q}\right) \sum_{\frac{1-r}{q} \le y \le \frac{p-r}{q}} e(\beta(qy+r)^k). \end{aligned}$$

Since $e(\_)$ is smooth, we have

$$\begin{aligned} \sum_{\frac{1-r}{q} \le y \le \frac{p-r}{q}} e(\beta(qy+r)^k) &\sim \int_{\frac{1-r}{q}}^{\frac{p-r}{q}} e(\beta(zq+r)^k)\, dz \\ &\sim \int_{-\frac{r}{q}}^{\frac{p-r}{q}} e(\beta(zq+r)^k)\, dz \\ &\sim \frac{1}{q} \int_0^p e(\beta\gamma^k)\, d\gamma, \end{aligned}$$

where $\gamma := zq + r$ and $d\gamma = q\, dz$.

Define $S(q,a) := \sum_{r=1}^{q} e\left(\frac{ark}{q}\right)$ and $v(\beta) = \int_0^p e(\beta\gamma^k)\, d\gamma$. Then one can show that for $\alpha \in \mathfrak{M}(q,a) \subseteq \mathfrak{M}$,

$$f(\alpha) = \frac{1}{q} S(q,a) v\left(\alpha - \frac{a}{q}\right) + p^{2\delta}.$$

Since $f(\alpha) \sim q^{-1} S(q,a)$ we have

$$\begin{aligned} \int_{\mathfrak{M}} f(\alpha)^s e(-n\alpha)\, d\alpha &= \sum_{1 \le q \le p^\delta} \sum_{a=0}^{q-1} \int_{\left|\alpha - \frac{a}{q}\right| = |\beta| \le p^{\delta-k}} f(\alpha)^s e\left(-\frac{n\alpha}{q}\right) e(-n\beta)\, d\beta \\ &\sim \sum_{1 \le q \le p^\delta} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} (q^{-1} S(q,a))^s e\left(-\frac{na}{q}\right) \int_{|\beta| \le p^{r-k}} v(\beta)^s e(-n\beta)\, d\beta. \end{aligned}$$

For $Q > 0$, define

$$\mathfrak{S}_s(n,Q) = \sum_{1 \le q \le Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} (q^{-1} S(q,a))^s e\left(-\frac{na}{q}\right)$$

and

$$J_s(n,Q) = \sum_{-Q}^{Q} v(\beta) e(-n\beta)\, d\beta.$$

Then one can show that

$$\int_{\mathfrak{M}} f(\alpha)^s e(-n\alpha)\, d\alpha = \mathfrak{S}_s(n, p^\delta) J_s(n, p^{\delta-k}) + O(p^{s-k-u})$$

for some $u > 0$.

Define the singular series

$$\mathfrak{S}_s(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} (q^{-1}S(q,a))^e \left(-\frac{na}{q}\right)$$

and the singular integral

$$J_s(n) = \int_{-\infty}^{\infty} v(\beta)^s e(-n\beta)\, d\beta.$$

One can show that for $s > 2^k$ there exists $w > 0$ so that

$$\int_{\mathfrak{M}} f(\alpha)^s e(-n\alpha)\, d\alpha = \mathfrak{S}_s(n)J_s(n) + O(p^{s-k-w}).$$

One can also show that for $s \geq 2$ we have

$$J_s(n) = \frac{\Gamma\left(1+\frac{1}{k}\right)^s}{\Gamma\left(\frac{s}{k}\right) n^{\frac{s}{k}-1}},$$

where Γ is the gamma function defined by

$$\Gamma(x) := \int_0^{\infty} t^{x-1}e^{-t}\, dt.$$

It remains to show that $1 \ll \mathfrak{S}_s(n) \ll 1$. One can show that

$$\mathfrak{S}_s(n) = \prod_{p \text{ prime}} \sigma(p),$$

where

$$\sigma(p) := \sum_{n=0}^{\infty} A(p^k, n)$$

and

$$A(q,n) = \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} (q^{-1}S(q,a))^s e\left(-\frac{na}{q}\right).$$

Indeed, $\sigma(p)$ corresponds to the p-adic solutions of $x_1^k + \cdots + x_s^k = n$. More precisely, if we let $M_n(q) = \#\{m_1^k + \cdots + M_s^k \equiv n \pmod q, 1 \leq m_i \leq q\}$, then we have $\sigma(p) = \lim_{h\to\infty} p^{h(1-s)}M_n(p^h) > 0$. It follows therefore that

$$\int_{\mathfrak{M}} f(\alpha)^s e(-n\alpha)\, d\alpha = \mathfrak{S}_s(n)\frac{\Gamma\left(1+\frac{1}{k}\right)^s}{\Gamma(s/k)} n^{\frac{s}{k}-1} + O(n^{\frac{s}{k}-1-w})$$

for some $w > 0$.

Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada N2L 3G1

E-mail address: hsyang@uwaterloo.ca