PMATH 440/640 ANALYTIC NUMBER THEORY

---

1. Lecture: Monday, September 11, 2000

NO TEXT
References:

- Introduction to Analytic Number Theory. Tom Apostol, Springer-Verlag, 1976
- An Introduction to the Theory of Numbers. G. H. Hardy and E. M. Wright, Oxford University Press (5th ed, 1979)

Marks:

- Final Exam 65%
- Midterm 25%
- Assignments 10%

Is there a formula for nth prime p_n?

$$p_1 = 2, p_2 = 3, \ldots$$

Yes, but such a formula is complicated.
For example, is there a polynomial $f \in \mathbb{Z}[x]$ for which $f(n) = p_n$?

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$
$$f(a_0) = a_n {a_0}^n + \cdots + a_1 a_0 + a_0$$

so $a_0 \mid f$.
Suppose q is prime and $f(n) = q$. Then $q \mid f(n + kq)$ for each $k \in \mathbb{Z}^+$. So, in particular, we see that if $f(m)$ is prime for each positive integer m, then f is a constant. In particular, $f(x) = q$ for some prime q.
The polynomial $n^2 + n + 41$ is prime for $n = 0, 1, \ldots, 39$.
Further, $(n - 40)^2 + (n - 40) + 41$ is prime for $0 \leq n \leq 79$.

These examples are connected with the fact that the ring of algebraic integers of the field $\mathbb{Q}(\sqrt{-163})$ is a Unique Factorization Domain. (Note that 163 is the largest squarefree integer D such that $\mathbb{Q}(\sqrt{-D})$ is a U.F.D.)

By using ideas of Matijàsevic which were used to prove Hilbert's 10th problem, one can find a polynomial $f \in \mathbb{Z}[a, b, \ldots, z]$ such that the set of positive values assumed by f as the variables run over the non-negative integers is the set of prime numbers.

Is $n^2 + 1$ a prime for infinitely many n?
Almost surely yes. The best result in this direction is that $n^2 + 1$ is a P_2 for infinitely many integers n. A P_2 is an integer which is the product of at most 2 primes.

There is no polynomial of degree > 1 which is known to be prime infinitely often.
On the other hand, we can deal with degree 1. Let k and ℓ be coprime positive integers. Then $kn + \ell$ is prime for infinitely many positive integers n. This is *Dirichlet's Theorem.*

Theorem 1 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. Assume that there are finitely many primes $p_1, \ldots, p_n$ say, and consider

$$m = p_1 \cdots p_n + 1$$

Then m can be written as a product of primes, and so $p_k \mid m$ for some k with $1 \le k \le n$.
Then $p_k \mid m - p_1 \cdots p_n$, so $p_k \mid 1$, which is a contradiction. □

Definition. For any real number x, let $\pi(x)$ denote the number of primes $\le x$.
We can estimate $\pi(x)$ from below using Euclid's proof. In particular, we'll show that p_k, the kth prime, satisfies

$$p_k \le 2^{2^k} \text{ for } k = 1, \ldots, n$$

We prove this by induction.
The result holds for $k = 1$, since $2 = p_1 \le 2^2 = 4$.
Assume the result holds for $1 \le j \le k$.
Then, by Euclid's argument, $p_k \le p_1 \cdots p_{k-1} + 1$ and so by our inductive assumption,

$$p_k \le 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{k-1}} + 1 \le 2^{2^k - 1} + 1 \le 2^{2^k}$$

---

2. Lecture: Wednesday, September 13, 2000

Thus, given $x \ge 2$ let s be the integer satisfying

$$2^{2^s} \le x \le 2^{2^{s+1}} \tag{1}$$

Then, since $p_k \le 2^{2^k}$ for $k = 1, 2, \ldots$ then we have $\pi(x) \ge s$.
By (1), $\frac{\log x}{\log 2} < 2^{s+1}$, hence

$$\frac{\log(\frac{\log x}{\log 2})}{\log(2)} < s + 1$$

and so $\pi(x) \ge \lfloor \log \log x \rfloor$.

Another way of proving such a lower bound for $\pi(x)$ is the following.
Suppose $x \ge 2$. Then

$$2^{\pi(x)} \ge \prod_{p \le x} \left(1 - \frac{1}{p}\right) = \prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \ge \sum_{n \le x} \frac{1}{n} \ge \int_1^{\lfloor x \rfloor + 1} \frac{du}{u} \ge \log x$$

Hence

$$\pi(x) \ge \frac{\log \log x}{\log 2} \ge \log \log x$$

Fermat (1601-1655) conjectured that the numbers of the form $2^{2^n}+1$ for $n=0,1,2,\ldots$ are prime. He checked it for $n=0,1,2,3,4$.
These are known as the *Fermat numbers* and are denoted by F_n, so

$$F_n = 2^{2^n}+1$$

Euler in 1732 proved that $641 \mid F_5$. It is known that $F_6,\ldots,F_{21}$ are composite. Quite likely $F_{22},\ldots$ are composite.
Almost certainly only finitely many Fermat numbers are prime.

Theorem 2 (Polya)**.** *If n and m are positive integers with $1 \le n < m$ then $(F_n, F_m) = 1$.*

Proof. Let $m = n+k$ with $k \ge 1$. We first show that $F_n \mid F_m - 2$.
We have $F_m - 2 = (2^{2^{n+k}}+1) - 2 = 2^{2^{n+k}} - 1$.
Put $x = 2^{2^n}$. Then

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

Thus we have $F_n \mid F_m - 2$.
Suppose that $d \mid F_n$ and $d \mid F_m$. Then $d \mid 2$ but $2 \nmid F_n$ and so $d = \pm 1$. The result follows. □

Thus we obtain another proof of Euclid's Theorem and we see that

$$p_n < 2^{2^n}$$

Theorem 3. *For $x \ge 2$,*

$$\pi(x) \ge \frac{\log \lfloor x \rfloor}{2\log(2)}$$

and for $n \ge 1$,

$$p_n < 4^n$$

Proof. Let $x \ge 1$ with $x \in \mathbb{Z}$. Let $2 = p_1, \ldots, p_j$ be the primes $\le x$.
For each integer n with $n \le x$ we can write $n = {n_1}^2 m$ where n is a positive integer and m is squarefree, so not divisible by the square of a prime. Therefore,

$$m = {p_1}^{\epsilon_1} \cdots {p_j}^{\epsilon_j}$$

where ϵ_i is in $\{0,1\}$ for each $i = 1,\ldots,j$.
Thus, there are at most 2^j possible values for m.
There are at most $\sqrt{x}$ possible values for n_2.
Therefore,

$$2^j \sqrt{x} \ge x$$

and so

$$2^j \ge \sqrt{x} \tag{2}$$

Since $j = \pi(x)$ we see that

$$\pi(x)\log 2 \ge \frac{\log x}{2}$$

amd the first part follows.
Now take $x = p_n$ so that $\pi(p_n) = n$.
By (1), $2^n \geq \sqrt{p_n}$ and so $4^n \geq p_n$. □

In 1896 Hadamard and de la Vallée Poussin proved independently the *Prime Number Theorem*. That is, they proved that

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

The result had been conjectured by Gauss.

Remark. Let n be a positive integer and let p be a prime. Then the exact power of p dividing $n!$ is

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

---

3. Lecture: Friday, September 15, 2000

Theorem 4. *For $x \geq 2$,*

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

Proof. (Argument due to Erdős). Let us first prove the lower bound for $\pi(x)$.
Note that $\binom{2n}{n}$ is an integer and that

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \mid \prod_{p<2n} p^{r_p} \tag{1}$$

where r_p satisfies the inequality $p^{r_p} \leq 2n < p^{r_p+1}$.
To see this note 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 dividing $n!$ is

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

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

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

In particular, by (1),

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

Note that $\binom{2n}{n}$ and so $2^n \leq (2n)^{\pi(2n)}$ hence

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

Note that $\frac{x}{\log x}$ is increasing for $x \geq e$ and so for $x \geq 6$, let n be such that $2n \leq x \leq 2n+2$, then

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

We can then check that the result holds for $6 \leq x \leq 2n$.

Now the upper bound. Note that

$$\prod_{n \leq p \leq 2n} p \mid \binom{2n}{n}$$

Thus

$$\prod_{n \leq p \leq 2n} p < (1+1)^{2n} = 2^{2n}$$

On the other hand,

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

Therefore,

$$\pi(2n)\log(n) - \pi(n)\log(n/2) < \log(2)2n + \log(2)\pi(n) < (3\log 2)n$$

Take $n = 2^k$. Then

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

Therefore,

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

and so

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

Thus, given $x \geq 2$ choose k so that $2^k \leq x \leq 2^{k+1}$.
Then $\pi(x) \leq \pi(2^{k+1})$. Therefore,

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

for $x > e$. We check for $2 \leq x \leq e$. □

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

4. Lecture: Monday, September 18, 2000

Theorem 5. *For all $n \in \mathbb{Z}^+$,*

$$\prod_{p \le n} p < 4^n$$

Proof. We'll prove the result by induction. The claim is certainly true for $n = 1$ or $n = 2$.

Suppose the result is true for $1 \le k \le n-1$. We first remark that we can restrict our attention to the case where n is odd, since if n is even, and $n > 2$, then

$$\prod_{p \le n} p = \prod_{p \le n-1} p$$

and the result follows by induction.

We write $n = 2m+1$, and we consider $\binom{2m+1}{m}$. In particular,

$$\prod_{m+1 < p \le 2m+1} p \mid \binom{2m+1}{m}$$

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,

$$\binom{2m+1}{m} \le \frac{1}{2}(2^{2m+1}) = 4^m \tag{1}$$

Now,

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

by our inductive assumption and (1). The result now follows by induction. □

Theorem 6. *If $n \ge 3$ and p is a prime with $\frac{2}{3}n < p \le n$ then $p \not| \binom{2n}{n}$.*

Proof. Since $n \ge 3$ we see that if p is in the range $\frac{2}{3}n < p \le n$ then $p > 2$. Then p and $2p$ are the only multiples of p with $p \le 2n$ and so

$$p^2 \,||\, (2n)!$$

(Here $p^2 \,||\, b$ means $p^3 \not| b$ and $p^2 \mid b$.)
Further, $p \,||\, n!$, hence $p^2 \,||\, (n!)^2$ since $\frac{2}{3}n < p \le n$.
Since $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ we see that $p \not| \binom{2n}{n}$. □

Theorem 7. *For each positive integer n, there is a prime p with $n < p \le 2n$.*

Proof. (This proof due to Erdős).
Note that the result holds for $n = 1, 2, 3$. Assume the result is false for some integer n with $n \geq 4$. Then, by Theorem 6, every prime p which divides $\binom{2n}{n}$ is $\leq \frac{2}{3}n$.
Let p be such a prime and suppose that $p^\alpha \mid\mid \binom{2n}{n}$. Then, as in the proof of Theorem 4, $\alpha \leq r_p$, so $p^\alpha \leq p^{r_p} \leq 2n$.
If $\alpha \geq 2$ then $p^2 \leq p^\alpha \leq 2n$, so $p \leq \sqrt{2n}$. Thus

$$\binom{2n}{n} \leq \left(\prod_{p \leq n} p\right) (2n)^{\pi(\sqrt{2n})} \leq \left(\prod_{p \leq \frac{2}{3}n} p\right) (2n)^{\sqrt{2n}}$$

since $\pi(x) \leq x$.
Further, by Theorem 5,

$$\binom{2n}{n} \leq 4^{2n/3}(2n)^{\sqrt{2n}} \tag{2}$$

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

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1} \tag{3}$$

By (1) and (2),

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

Taking logarithms, we find that

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

Notice that if $n = 512$ the inquality is false.

By calculus, the claim holds for $n \geq 512$.
Finally, $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 557$ are all primes and so the result is general. □

---

5. Lecture: Wednesday, September 20, 2000

What can we say about differences between consecutive primes?

Let $(2 = p_1, p_2, \ldots)$ be the sequence of primes. By Theorem 7, $p_{n+1} \leq 2p_n$ or $p_{n+1} - p_n \leq p_n$.
By probabalistic reasoning, Cramer was in 1936 led to conjecture that

$$\limsup_{n \to \infty} \left(\frac{p_{n+1} - p_n}{(\log p_n)^2}\right) \leq 1$$

The best upper bound for $p_{n+1} - p_n$ is due to Baker and Harman. They proved that, for n sufficiently large, $p_{n+1} - p_n < {p_n}^{0.535}$.

What about small gaps between consecutive primes? We conjecture that $p_{n+1}-p_n = 2$ for infinitely many integers n. If we assume the primes are *randomly* distributed and an integer x is prime with probability $\frac{1}{\log x}$ then we could expect x and $x+2$ to be prime with probability $\frac{1}{(\log x)^2}$.
Thus we expect about $\frac{x}{(\log x)^2}$ primes p with $p+2$ prime and $p \leq x$. A more careful heuristic suggests that there are about $C\frac{x}{(\log x)^2}$ such primes p with $C > 0$ and $C \neq 1$. In the 60's, Chen proved that there are more than $0.6\frac{x}{(\log x)^2}$ primes p with $p \leq x$ such that $p+2$ is a P_2, provided that x is sufficiently large.

Surprisingly, it is not known that

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0$$

The best result in this direction is due to Maier who proved in 1988 that

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} < \frac{1}{4}$$

In 1955 Ricci proved that the set of accumulation points of $\{\frac{p_{n+1}-p_n}{\log p_n} : n \in \mathbb{Z}^+\}$ has positive measure. The only point of accumulation that is actually known is ∞.
In the 1930's Erdős proved that for infinitely many integers n,

$$p_{n+1}-p_n > c_1 \log p_n \frac{\log\log p_n}{(\log\log\log p_n)^2}$$

for a positive constant c_1.

In 1938 Rankin added a factor of $\log\log\log\log p_n$.

Conclusion: We have much work to do. We don't even know many primes. In fact,

$$\sum_{p \text{ is a known prime}} \frac{1}{p} < 4$$

Primes of the form $2^p - 1$ where p is a prime are known as *Mersenne primes* and they are easy to test for primality. The largest prime known is the Mersenne prime

$$2^{6,972,593} - 1 \text{ (Hajratwala 1999)}$$

6. Lecture: Friday, September 22, 2000

Let $a_1, \ldots, a_n$ be distinct positive integers. For $m \in \mathbb{Z}^+$ we define $\nu(m)$ to be the number of distinct residue classes modulo m occupied by the integers $a_1, \ldots, a_k$.

Thus

$$\nu(m) = \text{the cardinality of } \{a_i + m\mathbb{Z} : i = 1, \ldots, k\}$$

In 1923, Hardy and Littlewood conjectured that if $\nu(p) < p$) for all primes p then there exist infinitely many integers n such that the integers $n+a_1, n+a_2, \ldots, n+a_k$ are all primes. (e.g. $a_1 = 0, a_2$ gives the twin prime conjecture). The conjecture is known as the *k-tuple conjecture*.

Hardy and Littlewood also conjectured

$$\pi(x+y) - \pi(y) \leq \pi(x) \text{ for all } x > 1, y > 1$$

Hensley and Richards proved, about 30 years ago that these conjectures are incompatible. At least one is false.

Definition. We introduce the symbols $O, o, \sim$.
Let f and g be functions from $\mathbb{Z}^+$ or $\mathbb{R}^+$ to $\mathbb{R}$, and suppose g maps to $\mathbb{R}^+$.

(i) $f = O(g)$ means that there exist positive numbers c_1 and c_2 such that for $x > c_1$, $|f(x)| \leq c_2 g(x)$.
(ii) $f = o(g)$ means that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$.
(iii) $f \sim g$ means that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$. (read: f is asymptotic to g.)

Observe $20x = O(x)$, $\sin(x) = O(1)$, $x = O(x^2)$, $x = o(x^2)$, $\sin(x) = o(\log x)$, $x+1 \sim x$, $x+\sqrt{x} \sim x$.

By the Prime Number Theorem,

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

or equivalently,

$$\pi(x) = \frac{x}{\log x} + o(\tfrac{x}{\log x})$$

Let $\epsilon > 0$. Then the number of primes in $[x, (1+\epsilon)x]$ is

$$\pi((1+\epsilon)x) - \pi(x) = \frac{(1+\epsilon)x}{\log((1+\epsilon)x)} - \frac{x}{\log x} + o(\tfrac{x}{\log x})$$

Note

$$\frac{(1+\epsilon)x}{\log((1+\epsilon)x)} = \frac{(1+\epsilon)x}{\log x + \log(1+\epsilon)} = \frac{(1+\epsilon)x}{(\log x)(1+\frac{\log(1+\epsilon)}{\log x})} = \frac{(1+\epsilon)x}{\log x} + o((\tfrac{x}{\log x}))$$

Therefore,

$$\pi((1+\epsilon)x) - \pi(x) = \frac{(1+\epsilon)x}{\log x} - \frac{x}{\log x} + o(\tfrac{x}{\log x}) = \frac{\epsilon x}{\log x} + o(\tfrac{x}{\log x})$$

Note that we can take $\epsilon = 1$. Then $\pi(2x) - \pi(x) = \frac{x}{\log x} + o(\frac{x}{\log x})$.
But $\pi(x) = \frac{x}{\log x} + o(\frac{x}{\log x})$. (Should this be worrying?)

Definition. For any integer n we define $\Lambda(n)$ by the rule

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

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

$$\theta(x) = \sum_{p \leq x} \log p = \log\left(\prod_{p \leq x} p\right)$$

and

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

Notice that

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

Also observe that since $p^2 \leq x$ is equivalent to $p \leq \sqrt{x}$, $p^3 \leq x$ is equivalent to $p \leq \sqrt[3]{x}$, then we have

$$\psi(x) = \theta(x) + \theta(\sqrt{x}) + \theta(x^{1/3}) + \cdots$$

Note that $\theta(x^{\frac{1}{m}}) = 0$ provided $m > \frac{\log x}{\log 2}$.
Thus

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

Observe that $\theta(x) = O(x \log x)$, hence

$$\sum_{k \geq 2} \theta(x^{\frac{1}{k}}) = O(x^{\frac{1}{2}} (\log x)^2)$$

Therefore,

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

7. Lecture: Monday, September 25, 2000

By Theorem 4, $\theta(x) < c_1 x$ and so by (1), $\psi(x) < c_2 x$. Further, by the proof of Theorem 4,

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

so that for $x \geq 2$, we have $\psi(x) > c_3 x$, hence $\theta(x) > c_4 x$. Here c_1, c_2, c_3, c_4 are positive constants.

What is the link between $\theta(x), \psi(x)$, and $\pi(x)$?
Note that $\theta(x) \leq \pi(x) \log x$, thus

$$\pi(x) \geq \frac{\theta(x)}{\log x} > c_4 \frac{x}{\log x} \tag{1}$$

Theorem 8.

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

Proof. Since $\psi(x) = \theta(x) + O(x^{1/2}(\log x)^2)$ and $\theta(x) > c_4 x$, we see that $\theta(x) \sim \psi(x)$. In particular, $\frac{\theta(x)}{\log x} \sim \frac{\psi(x)}{\log x}$ and so it suffices to show that $\pi(x) \sim \frac{\theta(x)}{\log x}$.

By (1), $\pi(x) \geq \frac{\theta(x)}{\log x}$, so

$$\liminf_{x \to \infty} \frac{\pi(x) \log x}{\theta(x)} \geq 1$$

We need an upper bound for $\pi(x)$ in terms of $\theta(x)$.
Note that for any $\delta > 0$, we have

$$\theta(x) = \sum_{p \leq x} \log p \geq \left(\log(x^{(1-\delta)}) \sum_{x^{1-\delta} \leq p \leq x} 1 \right) \geq (1-\delta)(\log x)(\pi(x) - \pi(x^{(1-\delta)}))$$

Thus,

$$\theta(x) + (1-\delta) x^{(1-\delta)} \log x \geq (1-\delta)(\log x)\pi(x)$$

so

$$\frac{\theta(x)}{(1-\delta)\log x} + x^{(1-\delta)} \geq \pi(x)$$

Therefore,

$$\frac{1}{1-\delta} + \frac{x^{(1-\delta)} \log x}{\theta(x)} \geq \frac{\pi(x) \log x}{\theta(x)}$$

Given $\epsilon > 0$, we can choose $\delta > 0$ so that $\frac{1}{1-\delta} < 1 + \frac{\epsilon}{2}$ and then choose x_0 so that if $x > x_0$,

$$\frac{x^{(1-\delta)} \log x}{\theta(x)} < \frac{\epsilon}{2}$$

since $\theta(x) > c_1 x$ for $x \geq 2$.
Then, for $x > x_0$,

$$1 \leq \frac{\pi(x)\log x}{\theta(x)} < 1 + \epsilon$$

and so our result follows. □

Lemma 1 (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 introduce*

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

If f' is continuous for $x \geq 1$,

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

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

$$\sum_{n \leq N} a_n f(n) = A(1)f(1) + (A(2) - A(1))f(2) + \cdots + (A(N) - A(N-1))f(N)$$

$$= A(1)(f(1) - f(2)) + A(2)(f(2) - f(3)) + \cdots + A(N-1)(f(N-1) - f(N)) + A(N)f(N)$$

Next observe that if i is a positive integer and t is a real number with $i \leq t < i+1$ then $A(t) = A(i)$. Thus

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

Accordingly,

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

This gives us the result when x is an integer.
Finally note that $A(t) = A(N)$ for $x \geq t \geq N$. Hence

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

and so our result follows. □

---

8. Lecture: Wednesday, September 27, 2000

Definition. We define *Euler's constant* γ by

$$\gamma = 1 - \int_1^{\infty} \frac{t - \lfloor t \rfloor}{t^2} dt$$

Note $\gamma = 0.57721....$

It is not known but it is conjectured that γ is irrational and indeed that γ is transcendental.

Theorem 9.

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

Proof. Take $a_n=1$ and $f(t)=\frac{1}{t}$.
Then $A(x)=\sum_{n\le x}a_n=\sum_{n\le x}1=\lfloor x\rfloor$.

By Abel's summation formula,

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

□

Theorem 10.

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

Proof. Apply Abel's summation formula with $a_n=1$ and $f(n)=\log n$. Then

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

Also we have

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

$$= \sum_{n\le x} \frac{x}{n}\Lambda(n) - \sum_{n\le x}\left(\frac{x}{n} - \left\lfloor \frac{x}{n}\right\rfloor\right)\Lambda(n)$$
$$= x\sum_{n\le x}\frac{\Lambda(n)}{n} - O(\textstyle\sum_{n\le x}\Lambda(n))$$

But $\displaystyle\sum_{n\le x}\Lambda(n) = \psi(x) = O(x)$ and so

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

By (1),

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

hence

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

Thus

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

□

Theorem 11.

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

Proof. Note that

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

But,

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

The result follows. □

Theorem 12. *There exists a real number β_1 such that*

$$\sum_{p\le x}\frac{1}{p} = \log\log x + \beta_1 + O(\tfrac{1}{\log x})$$

Proof. We apply Lemma 1 with

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

and with $f(n) = \frac{1}{\log n}$.

Then on putting $A(x) = \sum_{n \le x} a_n$, 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 11, we have

$$A(x) = \sum_{p \le x} \frac{\log p}{p} = \log x + O(1)$$

Therefore,

$$\sum_{p \le x} \frac{1}{p} = 1 + O(\tfrac{1}{\log x}) + \int_2^x \frac{\log u + \tau(u)}{u(\log u)^2} du$$

where $\tau(u) = O(1)$.
Thus,

$$\sum_{p \le x} \frac{1}{p} = 1 + O(\tfrac{1}{\log x}) + \log\log x - \log\log 2 + \int_2^x \frac{\tau(u)}{u(\log u)^2} du$$

$$= \log\log x + 1 - \log\log 2 + \int_2^\infty \frac{\tau(u)}{u(\log u)^2} du - \int_x^\infty \frac{\tau(u)}{u(\log u)^2} du + O(\tfrac{1}{\log x})$$

$$= \log\log x + \beta_1 + O(\tfrac{1}{\log x})$$

In fact, $\beta_1 = \gamma + (\sum_p \log(1 - \frac{1}{p}) + \frac{1}{p}) = 0.261497....$ □

---

9. Lecture: Wednesday, September 29, 2000

To prove the Prime Number Theorem we introduce the *Riemann zeta function*, $\zeta(s)$.

Definition. For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, we define $\zeta(s)$ by

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

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

The series $\sum_{n=1}^\infty \frac{1}{n^s}$ converges absolutely for $\mathrm{Re}(s) > 1$ and we have the *Euler product representation* for $\mathrm{Re}(s) > 1$ given by

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

To see this, note that

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

and a typical term is

$$\frac{1}{{p_1}^{\alpha_1 s}\cdots {p_k}^{\alpha_k s}} = \frac{1}{({p_1}^{\alpha_1}\cdots {p_k}^{\alpha_k})^s}$$

and by the Fundamental Theorem of Arithmetic (1) holds.

Notice that (1) allows us to give another proof that there are infinitely many primes.
If there were only finitely many, then $\prod_p (1-\frac{1}{p^s})^{-1}$ is bounded as we let s tend to 1 from above on the real line, whereas $\sum_{n=1}^{\infty}\frac{1}{n}$ diverges. This argument goes back to Euler.

Theorem 13. *$\zeta(s)$ can be analytically continued to $\mathrm{Re}(s)>0$ with $s\neq 1$. It is analytic except at the point $s=1$ where it has a simple pole with residue 1.*

Proof. For $\mathrm{Re}(s)>1$ we have $\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$.
By Lemma 1, with $a_n=1$ and $f(x)=\frac{1}{x^s}$, we find that

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

Letting $x\to\infty$ we find that

$$\begin{aligned}
\zeta(s) &= 0 + s\int_1^{\infty}\frac{\lfloor u\rfloor}{u^{s+1}}du \\
&= s\int_1^{\infty}\frac{u-(u-\lfloor u\rfloor)}{u^{s+1}}du \\
&= s\int_1^{\infty}u\frac{du}{u^{s+1}} - s\int_1^{\infty}\frac{u-\lfloor u\rfloor}{u^{s+1}}du \\
&= s\left(\frac{u^{1-s}}{1-s}\Big|_1^{\infty}\right) - s\int_1^{\infty}\frac{u-\lfloor u\rfloor}{u^{s+1}}du \\
&= \frac{s}{s-1} - s\int_1^{\infty}\frac{u-\lfloor u\rfloor}{u^{s+1}}du
\end{aligned}$$

for $\mathrm{Re}(s)>1$. Note that

$$\int_1^{\infty}\frac{u-\lfloor u\rfloor}{u^{s+1}}du$$

converges for $\mathrm{Re}(s)>0$ and represents an analytic function.

Therefore, $\frac{s}{s-1} - s\int_1^{\infty}\frac{u-\lfloor u\rfloor}{u^{s+1}}du$ represents an analytic function for $\mathrm{Re}(s)>0, s\neq 1$ and so gives an analytic continuation of $\zeta(s)$ to the region.
Note that $\frac{s}{s-1}$ has a simple pole of residue 1 at $s=1$.

□

Theorem 14. *$\zeta(s)$ has no zeroes in the region* $\mathrm{Re}(s) \geq 1$.

Proof. If $\mathrm{Re}(s) > 1$, then since $\prod_p (1 - \frac{1}{p^s})^{-1}$ converges, then $\zeta(s) \neq 0$.
Recall $s = \sigma + it$ with $\sigma, t \in \mathbb{R}$.
Let $\sigma > 1$. For all $t \in \mathbb{R}$,

$$\log^*(\zeta(\sigma + it)) = \sum_p \log\left(\left(1 - \frac{1}{p^s}\right)^{-1}\right) = -\sum_p \sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{1}{p^s}\right)$$

where log denotes the principal branch of the logarithm and $\log^*$ denotes some branch of the logarithm. We now consider the real part of both sides of the above equality to get

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

since

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

So $\mathrm{Re}(p^{-int}) = \cos(nt\log p)$.

We appeal to the inequality

$$\begin{aligned} 0 \leq 2(1+\cos\theta)^2 &= 2(1 + 2\cos\theta + \cos^2\theta) \\ &= 2 + 4\cos\theta + 2\cos^2\theta \\ &= 3 + 4\cos\theta + (2\cos^2\theta - 1) \\ &= 3 + 4\cos\theta + \cos(2\theta) \end{aligned}$$

We then deduce

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

hence that

$$\log|\zeta(\sigma)|^3 + \log|\zeta(\sigma + it)|^4 + \log|\zeta(\sigma + 2it)| \geq 0$$

In particular,

$$|\zeta(\sigma)|^3 \cdot |\zeta(\sigma + it)| \cdot |\zeta(\sigma + 2it)| \geq 1 \tag{2}$$

for $\sigma > 1$ and $t \in \mathbb{R}$.

Suppose that $1 + it_0$ is a zero of $\zeta(s)$.
Then $t_0 \neq 0$ since $\zeta(s)$ has a pole at $s = 1$.
Note that as $\sigma \to 1$ from the right, then

$$|\zeta(s)| = O((\sigma - 1)^{-1})$$

since 1 is a simple pole of $\zeta(s)$. Also since $1 + it_0$ is a zero of $\zeta(s)$, then $|\zeta(\sigma + it_0)| = O(\sigma - 1)$ as $\sigma \to 1$ from the right.

Finally, $|\zeta(\sigma + 2it_0)| = O(1)$ as $\sigma \to 1$ from the right, since $1 + i2t_0$ is not a pole of $\zeta(s)$. Therefore,

$$|\zeta(\sigma)|^3 \cdot |\zeta(\sigma + it)| \cdot |\zeta(\sigma + 2it)| = O((\sigma - 1)^{-3})O((\sigma - 1)^4)O(1) = O(\sigma - 1)$$

Thus $|\zeta(\sigma)|^3 \cdot |\zeta(\sigma + it)| \cdot |\zeta(\sigma + 2it)|$ tends to 0 as $\sigma \to 1$ which contradicts (1).
Therefore,$\zeta(s)$ has no zero on $\mathrm{Re}(s) = 1$ and the result follows. □

10. Lecture: Monday, October 2, 2000

11. Lecture: Wednesday, October 4, 2000

Theorem 15 (Donald J. Newman)**.** *Suppose $a_n \in \mathbb{C}$ with $|a_n| \leq 1$ for $n = 1, 2, \ldots$. Form the series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$.*
The series converges to the analytic function $F(s)$ for $\mathrm{Re}(s) > 1$.
If $F(s)$ can be analytically continued to $\mathrm{Re}(s) \geq 1$ then $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ 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 determine $\delta = \delta(R) > 0$ so that $F(z+w)$ is analytic on the region $\{z : -\delta \leq \mathrm{Re}(z) \text{ and } |z| \leq R\}$.

Let M denote the maximum of $|F(z+w)|$ on the region.

Let Γ denote the contour obtained by following the outside of the region in a counterclockwise path. Let A be the part of Γ in $\mathrm{Re}(z) \geq 0$ and B be the remainder of Γ.

By Cauchy's residue theorem, for any $N \in \mathbb{Z}^+$,

$$2\pi i F(w) = \int_{\Gamma} F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz \tag{1}$$

Now on A, $F(z+w)$ is equal to its series and we may split the series as $S_N(z+w) = \sum_{n=1}^{N} \frac{a_N}{n^{z+w}}$ and $R_N(z+w) = F(z+w) - S_N(z+w)$.

Again by Cauchy's residue theorem,

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

where C is the contour given by the path $|z| = R$ taken in counterclockwise direction. (Note that $S_N(z+w)$ is analytic for $z \in \mathbb{C}$.)

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

Thus

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

In the second integral change, change variables $z \to -z$. We see that

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

Therefore,

$$2\pi i S_N(w) = \int_A (S_N(z+w)N^z + S_N(w-z)N^{-z}) \left(\frac{1}{z} + \frac{z}{R^2}\right) dz \tag{3}$$

From (1) and (3),

(4)

$$2\pi i(F(w) - S_N(w)) = \int_A (R_N(z+w)N^z - S_N(w-z)N^{-z}) \left(\frac{1}{z} + \frac{z}{R^2}\right) dz + \int_B F(z+w)N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz$$

We want to show that $S_N(w) \to F(w)$ as $N \to \infty$.
So let's get down to it.

Observe that if we write $z = x + iy$ with $x, y, \in \mathbb{R}$ then for $z \in A$,

$$\frac{1}{z} + \frac{z}{R^2} = \frac{2x}{R^2} \tag{5}$$

$$|R_N(z+w)| \leq \sum_{n=N+1}^{\infty} \frac{1}{n^{x+1}} \leq \int_N^{\infty} \frac{1}{u^{x+1}} du = \frac{1}{xN^x} \tag{6}$$

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

So

$$|S_N(w-z)| \leq N^x(\frac{1}{N} + \frac{1}{x}) \tag{7}$$

Therefore from (5), (6), (7),

$$\begin{aligned} &\left| \int_A (R_N(z+w)N^z - S_N(w-z)N^{-z}) \left(\frac{1}{z} + \frac{z}{R^2}\right) dz \right| \\ &\leq \left| \int_A \left(\frac{1}{x}\frac{N^x}{N^x} + N^x \left(\frac{1}{N} + \frac{1}{x}\right) N^{-x} \right) \frac{2x}{R^2} dz \right| \\ \leq \int_A \left(\frac{2}{x} + \frac{1}{N}\right) \frac{dx}{R^2} dz &= \int_A \left(\frac{4}{R^2} + \frac{2x}{NR^2}\right) dz \leq \int_A \left(\frac{4}{R^2} + \frac{2}{NR}\right) dz \\ &= \pi R \left(\frac{4}{R^2} + \frac{2}{NR}\right) = \frac{4\pi}{R} + \frac{2\pi}{N} \end{aligned}$$

We now estimate the integral over B. Observe that

$$\left|\frac{1}{z} + \frac{z}{R^2}\right| = \left|\frac{1}{z}\right| \left|\frac{\overline{z}}{z} + \frac{z\overline{z}}{R}\right| \leq \frac{1}{\delta}\left(1 + \frac{|z|^2}{R^2}\right) \leq \frac{2}{\delta}$$

for $\mathrm{Re}(z) = -\delta$, $|z| \leq R$.

Therefore since $|F(z+w)|$ is at most M we see that

$$\begin{aligned}\left|\int_B F(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz\right| &\le \int_{-R}^{R} M\frac{2}{\delta}N^{-\delta}dz + 2\left|\int_{-\delta}^{0} MN^x\frac{2x}{R^2}2dx\right| \\ &\le \frac{4MR}{\delta N^\delta} + \frac{8M}{R^2}\left|\int_{-\delta}^{0} xN^x dx\right| \\ &\le \frac{4MR}{\delta N^\delta} + \frac{8M\delta}{R^2}\left(\frac{1}{\log N} - \frac{1}{N^\delta \log N}\right) \\ &\le \frac{4RM}{\delta N^\delta} + \frac{8M\delta}{R^2\log N}\end{aligned}$$

Thus

$$|2\pi i(F(w)-S_N(w))| \le \frac{4\pi}{R} + \frac{2\pi}{N} + \frac{4RM}{\delta N^\delta} + \frac{8M\delta}{R^2\log N}$$

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

Given $\epsilon > 0$, choose $R = \frac{3}{\epsilon}$. Then for N sufficiently large, $|F(w) - S_N(w)| < \epsilon$.

Thue $S_N(w) \to F(w)$ as $N \to \infty$.
The result follows. □

---

12. Lecture: Friday, October 6, 2000

Definition. We now introduce the *Möbius function* $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ under the rule that $\mu(1) = 1$ and $\mu(n) = (-1)^r$ if n is the product of r distinct primes and $\mu(n) = 0$ otherwise.
E.g. $\mu(12) = 0, \mu(15) = 1, \mu(30) = -1$.

Notice that for $\mathrm{Re}(s) > 1$,

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

Theorem 16. (i) *Let $n \in \mathbb{Z}^+$,*

$$\sum_{k \mid n} \mu(k) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

(ii) *Let $f : \mathbb{R}^+ \to \mathbb{C}$ and define $F : \mathbb{R}^+ \to \mathbb{C}$ by $F(x) = \sum_{n \le x} f(\frac{x}{n})$. Then $f(x) = \sum_{n \le x} \mu(n) F(\frac{x}{n})$.*
(iii) *Let $f : \mathbb{Z}^+ \to \mathbb{C}$ and define $F : \mathbb{Z}^+ \to \mathbb{C}$ by $F(n) = \sum_{d \mid n} f(d)$. Then $f(n) = \sum_{d \mid n} \mu(d) F(\frac{n}{d})$.*

Proof. (i) If $n = 1$ the result is obvious.
If $n > 1$ we can write $n = {p_1}^{\ell_1} \cdots {p_r}^{\ell_r}$ with $p_1, \ldots, p_r$ distinct primes and $\ell_1, \ldots, \ell_r$ positive integers.
Then $\sum_{k \mid n} \mu(k) = \sum_{k \mid m} \mu(k)$ where $m = p_1 \cdots p_r$.
But notice that

$$\sum_{k \mid m} \mu(k) = 1 - \binom{r}{1} + \binom{r}{2} + \cdots + (-1)^r \binom{r}{r} = (1-1)^r = 0$$

(ii) By (i),

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

(iii) Again by (i),

$$f(n) = \sum_{c \mid n} \left(\sum_{d \mid \frac{n}{c}} \mu(d) \right) f(c) = \sum_{cd \mid n} \mu(d) F(c)$$
$$= \sum_{d \mid n} \mu(d) \sum_{c \mid \frac{n}{d}} f(c) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right)$$

□

Theorem 17.

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

Proof. For $\mathrm{Re}(s) > 1$ we have $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(s)}{n^s}$.
It follows from Theorems 13 and 14 that $(s-1)\zeta(s)$ is analytic and non-zero in $\mathrm{Re}(s) \ge 1$, hence $\frac{1}{\zeta(s)}$ is analytic in $\mathrm{Re}(s) \ge 1$.

By Theorem 15, $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ converges to $\frac{1}{\zeta(s)}$ for $\mathrm{Re}(s) \ge 1$. In particular, it converges at $s = 1$. But $\zeta(s)$ has a pole at $s = 1$ so $\frac{1}{\zeta(1)} = 0$.

□

Theorem 18.

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

Proof. Apply Lemma 1 with $a_n = \frac{\mu(n)}{n}$ and $f(x) = x$. Then

$$\sum_{n \le x} \mu(n) = A(x)x - \int_1^x A(u)du$$

where

$$A(t) = \sum_{n \le t} \frac{\mu(n)}{n} \tag{1}$$

By Theorem 17, $A(t) = o(1)$, so

$$A(x)x = o(x) \tag{2}$$

and

$$\int_1^x A(u)du = o(x) \tag{3}$$

The result follows from (1),(2),(3). □

13. Lecture: Wednesday, October 11, 2000

For any positive integer n, let $d(n)$ denote the number of positive integers which divide n.

Theorem 19.

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

where γ is Euler's constant.

Proof. Let D_n be the region in the upper right hand quadrant not containing the x or y axes and under and including the hyperbola $xy = n$.
That is, $D_n = \{(x, y) \in \mathbb{R}^2 : x > 0, y > 0, xy \leq n\}$.

Every lattice point in D_n, in other words every point with integer coordinates in D_n, is contained in a hyperbola $xy = s$ for some s with $1 \leq s \leq n$.

Thus $\sum_{s=1}^{n} d(s)$ is the number of lattice points in D_n. Notice that this is equivalent to $\sum_{m=1}^{n} \left\lfloor \frac{n}{m} \right\rfloor$ since we may count the number of lattice points with x coordinates $1, 2, \ldots, n$.

Observe that to estimate the number of lattice points in D_n we first remark that the number above the line $x = y$ is the same as the number below.

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

By Theorem 9,

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

Since $\lfloor \sqrt{n} \rfloor = \sqrt{n} - \{\sqrt{n}\}$ where $\{x\}$ denotes the fractional part of x for any $x \in \mathbb{R}$, we have

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

Thus, from (1), we have

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

as required. □

14. Lecture: Friday, October 13, 2000

Theorem 20 (Prime Number Theorem)**.**

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

Proof. By Theorem 8 it suffices to prove that $\psi(x) \sim x$. Put

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

By Möbius inversion, Theorem 16 (ii), we have

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

It remains to show that $\sum_{n \le x} \mu(n) F\left(\frac{x}{n}\right) = o(x)$.

To do this we first estimate $F(x)$. We have

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

also

$$\sum_{n \le x} \psi\left(\frac{x}{n}\right) = \sum_{n \le x} \sum_{m \le \frac{x}{n}} \Lambda(m) = \sum_{n \le x} \Lambda(n) \left(\sum_{m \le \frac{x}{n}} 1 \right)$$

$$= \sum_{n \le x} \Lambda(n) \left\lfloor \frac{x}{m} \right\rfloor = \sum_{p^k \le x} \log p \left\lfloor \frac{x}{p^k} \right\rfloor$$

$$= \sum_{p \le x} \left(\left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \cdots \right) \log p = \log(\lfloor x \rfloor !) = \sum_{n \le x} \log n$$

and as in the proof of Theorem 10,

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

hence

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

Further, by Theorem 19,

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

Note that

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

Thus

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

Therefore,

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

Thus there is a positive constant c such that

$$|F(x)|<cx^{1/2}\text{ for }x\ge1$$

Let t be an integer larger than 1. Then

$$\left|\sum_{n\le\frac{x}{t}}\mu(n)F\left(\frac{x}{n}\right)\right|\le\sum_{n\le\frac{x}{t}}\left|F\left(\frac{x}{n}\right)\right|\le\sum_{n\le\frac{x}{t}}c\frac{x}{n}^{1/2}$$

$$\le cx^{1/2}\left(1+\int_1^{\frac{x}{2}}\frac{du}{u^{1/2}}\right)\le cx^{1/2}\left(1+2u^{1/2}\Big|_1^{\frac{x}{t}}\right)$$

$$\le cx^{1/2}\left(1+2\left(\frac{x}{t}\right)^{1/2}-2\right)\le2\frac{cx}{t^{1/2}}\tag{1}$$

Observe that F is a step function.
In particular, if a is an integer and $a\le x<a+1$ then $F(x)=F(a)$. Therefore,

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

Thus

$$\left|\sum_{\frac{x}{t}<n\le x}\mu(n)F\left(\frac{x}{n}\right)\right|\le|F(1)|\left|\sum_{\frac{x}{2}<n\le x}\mu(n)\right|+\cdots+|F(t-1)|\left|\sum_{\frac{x}{t}<n\le\frac{x}{t-1}}\mu(n)\right|$$

so

$$\left|\sum_{\frac{x}{t}<n\le x}\mu(n)F\left(\frac{x}{n}\right)\right|\le(|F(1)|+\cdots+|F(t-1)|)\max_{2\le i\le t}\left|\sum_{\frac{x}{t}<n\le\frac{x}{t-1}}\mu(n)\right|$$

But

$$\sum_{\frac{x}{i}<n\le\frac{x}{i-1}}\mu(n)=\sum_{n\le\frac{x}{i-1}}\mu(n)-\sum_{\frac{x}{i}<n}\mu(n)=o(x)$$

Therefore,

$$\left| \sum_{\frac{x}{t} < n \leq x} \mu(n) F\left(\frac{x}{n}\right) \right| = o(x)$$

Thus given $\epsilon > 0$ choose t so that $\frac{2c}{t^{1/2}} < \frac{\epsilon}{2}$. Then for x sufficiently large,

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

And so by (1),

$$\left| \sum_{n \leq x} \mu(n) F\left(\frac{x}{n}\right) \right| < \frac{\epsilon}{2} x + \frac{\epsilon}{2} x = \epsilon x$$

In particular, $\left|\sum_{n \leq x} \mu(n) F(\frac{x}{n})\right| = o(x)$ and so $\psi(x) \sim x$. □

15. Lecture: Monday, October 16, 2000

Definition. For any positive integer n let $\Omega(n)$ denote the number of prime factors of n counted with multiplicity and let $\omega(n)$ denote the number of distinct prime factors of n.
Thus if $n = 2^3 \cdot 3^5 \cdot 13$, then $\Omega(n) = 2 + 5 + 1 = 8$ and $\omega(n) = 3$.

Definition. Let $k \in \mathbb{Z}^+$ and for each real number x let $\tau_k(x)$ be the number of positive integers n with $n \leq x$ and $\Omega(n) = k$.
Further, let $\pi_k(x)$ be the number of positive integers n with $n \leq x$ and $\omega(n) = \Omega(n) = k$.
In other words, π_k counts the n's up to x which are squarefree and have k prime factors.

Note that $\pi(x) = \pi_1(x) = \tau_1(x)$.

Theorem 21 (Landau,1900)**.** *Let k be a positive integer. Then*

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

Proof. We introduce the following functions

$$L_k(x) = \sum_{p_1 \cdots p_k \leq x}^{*} \frac{1}{p_1 \cdots p_k}$$

$$\Pi_k(x) = \sum_{p_1 \cdots p_k \leq x}^{*} 1$$

$$\Theta_k(x) = \sum_{p_1 \cdots p_k \leq x}^{*} \log(p_1 \cdots p_k)$$

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

For each positive integer n, let $c_n = (c_n{}^{(k)})$ denote the number of k-tuples $(p_1, \ldots, p_k)$ for which $p_1 \cdots p_k = n$.
Note $c_n = 0$ if n is not the product of k primes and is equal to $k!$ if n is squarefree and $\omega(n) = k$.
Thus we have

$$k!\pi_k(x) \leq \Pi_k(x) \leq k!\tau_k(x) \tag{1}$$

Note also that $\Pi_k(x) = \sum_{n \leq x} c_n$ and $\Theta_k(x) = \sum_{n \leq x} c_n \log n$.

For $k \geq 2$ note that the number of positive integers up to x with k primes factors and divisible by the square of a prime is $\tau_k(x) = \pi_k(x)$.

Thus

$$\tau_k(x) - \pi_k(x) \leq \sum_{\substack{p_1 \cdots p_k \leq x \\ p_i = p_j \text{ for some } i \neq j}}^{*} 1 \leq \binom{k}{2} \sum_{p_1 \cdots p_k \leq x} 1 = \binom{k}{2} \Pi_{k-1}(x) \tag{2}$$

We shall prove that

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

and then our result follows from (1) and (2).

From Lemma 1 with $a_n = 1$ and $f(x) = \log x$, we have

$$\Theta_k(x) = \sum_{n \leq x} c_n \log n = \Pi_k(x) \log x + \int_1^x \frac{\Pi_k(u)}{u} du$$

Observe that

$$\Pi_k(x) \leq k! \tau_k(x) \leq k! x$$

Thus $\Pi_k(u) = O(u)$ and so

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

Therefore, it suffices to prove that

$$\Theta_k(x) \sim kx(\log\log x)^{k-1} \text{ for } k \in \mathbb{Z}^+$$

We'll prove this by induction on k.

Note that $\Theta_1(x) = \theta(x) \sim x$ by the Prime Number Theorem.
Assume now that $\Theta_k(x) \sim kx(\log\log x)^{k-1}$ for k with $k \geq 1$. We'll prove it for $k+1$.

First note that for $k \geq 1$, $L_k(x) \sim (\log\log x)^k$, since

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

and by Theorem 12,

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

and

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

Further,

$$\left(\log\log(x^{\frac{1}{k}})\right)^k = \left(\log\left(\frac{\log x}{k}\right)\right)^k = (\log\log x - \log k)^k \sim (\log\log x)^k$$

It suffices to show that $\Theta_k(x) \sim k(\log\log x)^{k-1}$.

The result holds for $k = 1$ by the Prime Number Theorem. We now make the inductive hypothesis that

$$\Theta_k(x) \sim k(\log\log x)^{k-1} \text{ for } k \geq 1$$

and we'll deduce it for $\Theta_{k+1}(x)$.
Recall also that $L_k(x) \sim (\log\log x)^k$.
Therefore

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

$$k\Theta_{k+1}(x) = \sum_{p_1\cdots p_{k+1}\leq x}^{*} (\log(p_2\cdots p_{k+1}) + \log(p_1p_3\cdots p_{k+1}) + \cdots + \log(p_1\cdots p_k))$$

$$= (k+1)\sum_{p_2\cdots p_{k+1}\leq x}^{*} \log p_2\cdots p_{k+1}$$

$$= (k+1)\sum_{p_1\leq x} \Theta_k\left(\frac{x}{p_1}\right)$$

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

$$L_k(x) = \sum_{p_1\cdots p_k\leq x}^{*} \frac{1}{p_1\cdots p_k} = \sum_{p_1\leq x} \frac{1}{p_1} L_{k-1}\left(\frac{x}{p_1}\right)$$

Thus,

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

By inductive hypothesis,

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

Thus given $\epsilon > 0$, there exists $x_0 = x_0(\epsilon, k)$ such that for $y > x_0$,

$$\left|\Theta_k(y) - \frac{ky}{p_1}L_{k-1}(y)\right| \leq \epsilon y(\log\log y)^{k-1}$$

Further, there exists a positive number $c = c(\epsilon, k)$ such that for $y \leq x$,

$$\left|\Theta_k(y) - \frac{ky}{p_1}L_{k-1}(y)\right| \leq c$$

Therefore, for x sufficiently large,

$$|\Theta_{k+1}(x) - (k+1)L_k(x)| \leq 2\left(\sum_{\frac{x}{x_0}<p_1\leq x} c + \sum_{p_1\leq\frac{x}{x_0}} \epsilon\frac{x}{p_1}\left(\log\log\frac{x}{p_1}\right)^{k-1}\right)$$

$$\leq 2cx + 2\epsilon x(\log\log x)^{k-1}\sum_{p_1\leq\frac{x}{x_0}}\frac{1}{p_1} \leq 2cx + 4\epsilon x(\log\log x)^k$$

$$< 5\epsilon x(\log\log x)^k \text{ for } x \text{ suffiently large}$$

Thus,

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

and this completes the induction. The result follows. □

---

16. Lecture: Wednesday, October 18, 2000

Theorem 22.

$$\sum_{n\leq x}\omega(n) = x\log\log x + \beta_1 x + o(x)$$

and

$$\sum_{n\leq x}\Omega(n) = x\log\log x + \beta_2 x + o(x)$$

where β_1 is the constant in Theorem 12 and $\beta_2 = \beta_1 + \sum_p \frac{1}{p(p-1)}$.

Proof. Put $S_1 = S(x) = \sum_{n\leq x}\omega(n)$. Then

$$S_1 = \sum_{n\leq x}\sum_{p\mid n} 1 = \sum_{p\leq x}\left\lfloor\frac{x}{p}\right\rfloor$$

Thus by Theorem 12,

$$S_1 = x\sum_{p\leq x}\frac{1}{p} + O(\pi(x)) = x(\log\log x + \beta_1 + o(1)) + O(\pi(x))$$

By the Prime Number Theorem, or Theorem 6,

$$S_1 = x\log\log x + x\beta_1 + o(x)$$

Put $S_2 = S_2(x) = \sum_{n\leq x}\Omega(n)$. Then

$$S_2 - S_1 = \sum_{p^m\leq x, m\geq 2}\left\lfloor\frac{x}{p^m}\right\rfloor = \sum_{p^m\leq x, m\geq 2}\frac{x}{p^m} + O(x^{\frac{1}{2}}\log x)$$

(The $x^{\frac{1}{2}}$ arises since $m \geq 2$ so p is at most $\sqrt{x}$. The $\log x$ arises since m goes up to $\log x$.)

Continuing,

$$S_2 - S_1 = x\left(\sum_p \left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots\right) - \sum_{p^m \geq x} \frac{1}{p^m}\right) + O(x^{1/2}\log x)$$

Thus,

$$S_2 - S_1 = x\left(\sum_p \frac{1}{p(p-1)} + o(1)\right) + O(x^{1/2}\log x) = x\sum_p \frac{1}{p(p-1)} + o(x)$$

and the result follows. □

17. Lecture: Friday, October 20, 2000

Definition. Let A be a subset of $\mathbb{Z}^+$. For any $n \in \mathbb{Z}^+$ put $A(n) = \{1, 2, \ldots, n\} \cap A$.
Define the *upper density* $\overline{d}(A)$ of A by

$$\overline{d}(A) = \limsup_{n\to\infty} \frac{|A(n)|}{n}$$

$\overline{d}(A)$ is also known as the *asymptotic upper density* of A.

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

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

We say A has an *asymptotic density* $d(A)$ if $\underline{d}(A) = \overline{d}(A)$ in which case we put $d(A) = \overline{d}(A)$.

Examples:

(1) A set of primes, $\underline{d}(A) = \overline{d}(A) = 0$.
(2) $A = \{n \in \mathbb{Z}^+ : n \equiv 0 \pmod 5\}$ then $\underline{d}(A) = \overline{d}(A) = d(A) = \frac{1}{5}$.
(3) $A = \{n \in \mathbb{Z}^+ : n$ not of the form $k^2 + 1$ for $k \in \mathbb{Z}\}$, $\underline{d}(A) = \overline{d}(A) = d(A) = 1$.
(4) Take $A = \{a \in \mathbb{Z} : (2k)! < a < (2k+1)!$ for $k \in \mathbb{Z}\}$. Then $\underline{d}(A) = 0$ and $\overline{d}(A) = 1$.

Definition. Let $f(n)$ and $F(n)$ be functions from $\mathbb{Z}^+ \to \mathbb{R}$.
We say that $f(n)$ has *normal order* $F(n)$ if for each $\epsilon > 0$ the set

$$A(\epsilon) = \{n \in \mathbb{Z}^+ : (1-\epsilon)F(n) < f(n) < (1+\epsilon)F(n)\}$$

has the property that $\underline{\mathrm{d}}(A(\epsilon)) = 1$.
(Equivalently, if $B(\epsilon) = \mathbb{Z}^+ \backslash A(\epsilon)$ then $\underline{d}(B(\epsilon)) = 0$.)

We say that f has *average order* F if

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

Examples:

(1) Take
$$f(n) = \begin{cases} 1 & \text{if } n \neq k! \text{ for } k \in \mathbb{Z}^+ \\ n & \text{if } n = k! \end{cases}$$
Then f has normal order 1 but not average order 1.

(2) Put
$$f(n) = \begin{cases} 2 & \text{for } n \equiv 1 \pmod 2 \\ 0 & \text{for } n \equiv 0 \pmod 2 \end{cases}$$
Then f has average order 1 but does not have normal order 1.

(3) Put
$$f(n) = \begin{cases} \log n + (\log n)^{\frac{1}{2}} & \text{for } n \equiv 1 \pmod 2 \\ \log n - (\log n)^{\frac{1}{2}} & \text{for } n \equiv 0 \pmod 2 \end{cases}$$
Then f has both normal and average order 1.

We have already proven that $\omega(n)$ and $\Omega(n)$ have average order $\log\log n$. We'll now prove that they have normal order $\log\log n$.

18. Lecture: Monday, October 23, 2000

Theorem 23. *Let $\delta > 0$. The number of positive integers $n \le x$ with $|f(n) - \log\log n| < (\log\log n)^{\frac{1}{2}+\delta}$ is $o(x)$ where $f(n) = \omega(n)$ or $f(n) = \Omega(n)$.*

Proof. The first remark we make is that it is enough to prove that the number of positive integers n with $n \le x$ and

$$|f(n) - \log\log x| < (\log\log x)^{\frac{1}{2}+\delta}$$

is $o(x)$ since for $x^{\frac{1}{e}} \le n \le x$,

$$\log\log x \ge \log\log n \ge \log\left(\frac{\log x}{e}\right) = \log\log x - 1$$

Secondly, we may restrict our attention to $f(n) = \omega(n)$, since by Theorem 22,

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

Thus the number of $n \le x$ for which $\Omega(n) - \omega(n) > (\log\log n)^{1/2}$ is $o(x)$.

For each $n \le x$, we consider the ordered pairs (p, q) where p and q are distinct prime factors of n. There are $\omega(n)$ choices for p and then $\omega(n) - 1$ choices for q so

$$\omega(n)(\omega(n)-1) = \sum_{pq \mid n, p\ne q} 1 = \sum_{pq \mid n} 1 - \sum_{p^2 \mid n} 1$$

Thus

$$\sum_{n\le x}\omega(n)^2 - \sum_{n\le x}\omega(n) = \sum_{n\le x}\omega(n)(\omega(n)-1) = \sum_{n\le x}\left(\sum_{pq \mid n} 1 - \sum_{p^2 \mid n} 1\right) = \sum_{pq\le x}\left\lfloor\frac{x}{pq}\right\rfloor - \sum_{p^2\le x}\left\lfloor\frac{x}{p^2}\right\rfloor$$

Observe that

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

and

$$\sum_{pq\le x}\left\lfloor\frac{x}{pq}\right\rfloor \le \sum_{p^2\le x}\frac{x}{pq} + O(x)$$

Thus

$$\sum_{n\le x}\omega(n)^2 - \sum_{n\le x}\omega(n) = \sum_{n\le x}\omega(n)(\omega(n)-1) = \sum_{pq\le x}\frac{x}{pq} + O(x) \tag{1}$$

Next note that

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

Further,

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

and

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

Thus

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

By Theorem 22,

$$\sum_{n\leq x}\omega(n) = O(x\log\log x) \tag{3}$$

Thus by (1), (2), and (3),

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

Therefore,

$$\begin{aligned}\sum_{n\leq x}(\omega(n)^2 - \log\log x)^2 &= \sum_{n\leq x}\omega(n)^2 - 2\sum_{n\leq x}\omega(n)\log\log x + \sum_{n\leq x}(\log\log x)^2\\ &= ((x\log\log x)^2 + O(x\log\log x)) - 2\log\log x(\sum_{n\leq x}\omega(n)) + \lfloor x\rfloor\,(\log\log x)^2\\ = x(\log\log x)^2 + O(x\log\log x) - 2x(\log\log x)^2 + O(\log\log x) + x(\log\log x)^2 + O(\log\log x)^2\\ &= O(x\log\log x) \qquad (4)\end{aligned}$$

Let $\epsilon > 0$. If there are more than ϵx integers n with $1 \leq n \leq x$ for which

$$|\omega(n) - \log\log x| > (\log\log x)^{\frac{1}{2}+\delta}$$

then

$$\sum_{n\leq x}(\omega(n)^2 - \log\log x)^2 > \epsilon x(\log\log x)^{1+2\delta}$$

This cannot hold for x sufficiently large, by (4), and so the result follows. □

Recall, for $n \in \mathbb{Z}^+$, $d(n)$ denotes the number positive divisors of n. If

$$n = {p_1}^{a_1}\cdots{p_r}^{a_r}$$

where $a_1, \ldots, a_r$ are positive integers and $p_1, \ldots, p_r$ are distinct primes, then

$$\omega(n) = r,\ \Omega(n) = a_1 + \cdots + a_r,\ \text{and}\ d(n) = (a_1+1)\cdots(a_r+1)$$

Theorem 24. *Let $\epsilon > 0$. We have*

$$2^{(1-\epsilon)\log\log n} < d(n) < 2^{(1+\epsilon)\log\log n}$$

for a set of positive integers n with asymptotic density 1.

Proof. Since for any $a \in \mathbb{Z}$,

$$2 \leq (1+a) \leq 2^a$$

The result now follows from Theorem 23. □

Recall that the average order of $d(n)$ is $\log(n)$.
By Theorem 24, "normally" $d(n)$ satisfies

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

for any $\epsilon > 0$.

Definition. For any $n \in \mathbb{Z}^+$, let $\varphi(n)$ be the number of integers m with $\gcd(m,n) = 1$. $\varphi(n)$ is known as *Euler's φ-function.*

Theorem (Euler's Theorem). *Let a and b be positive integers with* $\gcd(a,n) = 1$. *Then*

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

Proof. Let $c_1, \ldots, c_{\varphi(n)}$ be a reduced residue system modulo n.
Then $ac_1, \ldots, ac_{\varphi(n)}$ is also a reduced residue system modulo n.

Thus

$$c_1 \cdots c_{\varphi(n)} \equiv (ac_1 \cdots ac_{\varphi(n)}) \pmod{n}$$

hence

$$c_1 \cdots c_{\varphi(n)} \equiv a^{\varphi(n)} c_1 \cdots c_{\varphi(n)} \pmod{n}$$

and so

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

□

(*Fermat's Theorem* follows from setting $n = p$.)

Theorem (Wilson's Theorem). *If p is a prime then* $(p-1)! \equiv -1 \pmod{p}$.

Proof. Consider $x^{p-1} - 1$ in $\mathbb{Z}_{p\mathbb{Z}}[x]$.
It factors by Fermat's Theorem as

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)) \text{ in } \mathbb{Z}_{p\mathbb{Z}}[x]$$

since $1, 2, \ldots, p-1$ are roots.
Considering the constant coefficient we find that

$$-1 \equiv (-1)(-2)\cdots(-(p-1)) \pmod{p}$$

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

If $p = 2$ the result holds since $-1 = 1$; otherwise p is odd, so $-1 \equiv (p-1)! \pmod{p}$ as required. □

19. Lecture: Wednesday, October 25, 2000

Wilson's Theorem was conjectured by Wilson (1741-1793). He communicated the conjecture to Waring (1734-1798) who published it in 1770. Shortly after, Lagrange gave the first proof. In fact, Leibniz had conjectured the result in 1682.

Here is another proof due to Stern from 1860. We have, for $|x| < 1$,

$$-\log(1-x) = \log\left(\frac{1}{1-x}\right) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots$$

and so

$$\exp\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots\right) = \frac{1}{1-x} = 1 + x + x^2 + \cdots$$

But

$$\exp\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots\right) = \exp(x)\exp(\tfrac{x^2}{2})\exp(\tfrac{x^3}{3})\cdots$$

$$= \left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)\left(1 + \frac{x^2}{2} + \frac{(\frac{x^2}{2})^2}{2!} + \cdots\right)\left(1 + \frac{x^3}{3} + \frac{(\frac{x^3}{3})^2}{2!} + \cdots\right)\cdots$$

$$= 1 + x + \left(\frac{1}{2} + \frac{1}{2!}\right)x^2 + \left(\frac{1}{3!} + \frac{1}{2} + \frac{1}{3}\right)x^3 + \cdots + \left(\frac{1}{p!} + \cdots + \frac{1}{p}\right)x^p + \cdots$$

In particular, the coefficient of x^p is of the form $\frac{1}{p!} + \frac{r}{s} + \frac{1}{p}$ where r and s are positive integers with $\gcd(r,s) = 1$ and $\gcd(s,p) = 1$.

But comparing coefficients in the power series, we see that

$$1 = \frac{1}{p!} + \frac{r}{s} + \frac{1}{p}$$

Therefore $1 - \frac{r}{s} = \frac{1}{p!} + \frac{1}{p}$ hence $\frac{s-r}{s} = \frac{1}{p!} + \frac{1}{p}$. Thus $s - r = \frac{s}{p!} + \frac{s}{p}$, so $(s-r)(p-1)! = \frac{s}{p} + \frac{s(p-1)!}{p} = \frac{s((p-1)!+1)}{p}$.

Since $(s-r)(p-1)!$ is an integer, we see that $p \mid s((p-1)!+1)$. But $\gcd(p,s) = 1$.

Therefore, $p \mid (p-1)! + 1$, as required.

Definition. Let p be a prime, and let a be an integer coprime with p. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ by the rule:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{if it has no solution} \end{cases}$$

If $\left(\frac{a}{p}\right) = 1$ we say that a is a quadratic residue mod p and otherwise a is a quadratic nonresidue mod p.

Theorem 25 (Euler's Criterion)**.** *Let p be an odd prime and let a be and integer coprime with p. Then*

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

Proof. The congruence $x^2 \equiv a \pmod{p}$ has at most 2 solutions modulo p. Suppose that it has a solution (so that $\left(\frac{a}{p}\right) = 1$ and that $b^2 \equiv a \pmod{p}$.

From $b^2 \equiv a \pmod{p}$, we get

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

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

And suppose that $x^2 \equiv a \pmod{p}$ has no solution. Split the integers into $\frac{p-1}{2}$ pairs (r, s) with $rs \equiv a \pmod{p}$. Thus

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

Note $(p-1)! \equiv -1 \pmod{p}$ by Wilson's Theorem, so $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$. □

20. Lecture: Monday, October 30, 2000

Extend the definition of the Legendre symbol to $\left(\frac{a}{p}\right)$ where p is a prime and $p \mid a$ by putting $\left(\frac{a}{p}\right) = 0$ in this case.

Theorem 26. *Let p be an odd prime and let a and b be integers. Then*

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

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

Proof. The first part plainly holds if $p \mid ab$. So we may assume that $p \nmid a$ and $p \nmid b$.
By Euler's Criterion,

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

Since $\left(\frac{ab}{p}\right)$ and $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ are in $\{-1, 1\}$ and p is and odd prime, we see that

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

Similarly, by Euler's Criterion,

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

and since p is an odd prime $\left(\frac{-1}{p}\right) = (-1)^{\frac{p(p-1)}{2}}$. □

21. Lecture: Wednesday, November 1, 2000

Theorem 27 (Gauss' Lemma)**.** *Let p be an odd prime and let a be an integer coprime with p. Let μ be the number of integers from $\{a, 2a, \ldots, (\frac{p-1}{2})a\}$ whose residues modulo p of least absolute value are negative. Then*

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

E.g. take $p = 5$ and $a = 2$. The set $\{2, 4\}$. The residues mod 5 of least absolute value are 2,-1. Thus $\mu = 1$ hence $\left(\frac{2}{5}\right) = (-1)^1 = -1$.

Proof. Replace the integers $a, \ldots, (\frac{p-1}{2})a$ by their residues of least absolute value.

Denote the positive ones by $r_1, \ldots, r_{\frac{p-1}{2}-\mu}$ and the negative ones by $-s_1, \ldots, -s_\mu$.

Plainly no two r_i's are equal and no two s_j's are equal.

Observe 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 $(m_1 + m_2)a \equiv 0 \pmod p$, hence $p \mid m_1 + m + 2$, which is not possible if $1 \le m_t \le \frac{p-1}{2}$ for $t = 1, 2$.
Therefore, no r_i is equal to an s_j. In particular, $r_1, \ldots, r_{\frac{p_1}{2}-\mu}, s_1, \ldots, s_\mu$ is a rearrangement of $1, \ldots, \frac{p-1}{2}$. Thus

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

and so $a^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod p$. The result now follows from Euler's Criterion. □

Corollary . If p is an odd prime, then

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

Proof. We apply Gauss' Lemma. We consider the number of integers from $\{1, 2, 4, \ldots, 2(\frac{p-1}{2})\}$ whose residues of least absolute value are negative.

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

□

If $p = 8k + 1$ then $\mu = 4k - \left\lfloor \frac{8k+1}{4} \right\rfloor = 4k - 2k \equiv 0 \pmod 2$.
If $p = 8k + 3$ then $\mu = 4k + 1 - 2k = 2k + 1 \equiv 1 \pmod 2$.
If $p = 8k + 5$ then $\mu = 4k + 2 - (2k + 1) = 2k + 1 \equiv 1 \pmod 2$.
If $p = 8k + 7$ then $\mu = 4k + 3 - (2k + 1) = 2k + 2 \equiv 0 \pmod 2$.

Therefore, 2 is a square modulo p if $p \equiv \pm 1 \pmod 8$ and 2 is a quadratic nonresidue if $p \equiv \pm 3 \pmod 8$.

---

22. Lecture: Friday, November 3, 2000

Theorem 28 (Law of Quadratic Reciprocity)**.** *If p and q are distinct odd primes, then*

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

Euler had stated the law. Legendre attempted to prove it. Gauss gave 8 proofs.

Proof. By Gauss' Lemma, $\left(\frac{q}{p}\right) = (-1)^\mu$ and $\left(\frac{q}{p}\right) = (-1)^\nu$, where μ is the number of integers from $\{q, 2q, \ldots, (\frac{p-1}{2})q\}$ whose residue mod p of least absolute value is negative, and ν is the number of integers from $\{p, 2p, \ldots, (\frac{q-1}{2})p\}$ whose residue mod q of least absolute value is negative.

It suffices to show that $\mu + \nu = (\frac{p-1}{2})(\frac{q-1}{2}) \pmod 2$.

Given x with $1 \le x \le \frac{p-1}{2}$ we determine y such that $-\frac{p}{2} < qx - py < \frac{p}{2}$.
Note that $-\frac{1}{2} - \frac{q}{p}x < -y < \frac{1}{2} - \frac{q}{p}x$ so y is uniquely determined and that $qx - py$ is the residue mod p of least absolute value of qx.

Note that y is nonnegative. If $y = 0$ there is no contribution to μ since $qx \geq 0$.
Further, if $x = \frac{p-1}{2}$, then

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

hence $y \leq \frac{q-1}{2}$ (since y is an integer).
Thus the number μ corresponds to the number of combinations of x and y from the sequences

$$(A) : 1, 2, \ldots, \frac{p-1}{2}$$
$$(B) : 1, 2, \ldots, \frac{q-1}{2}$$

respectively, such that $-\frac{p}{2} < qx - py < 0$, or equivalently that $0 < py - qx < \frac{p}{2}$.

Similarly, ν is the number of combinations of x and y from the sequences (A) and (B) respectively, for which $-\frac{q}{2} > py - qx < 0$.

For any other pair (x, y) with x from (A) and y from (B), either $py - qx < -\frac{q}{2}$ or $py - qx > \frac{p}{2}$.
Let ρ be the number of pairs (x, y) for which the first possibility holds, and λ the number of pairs for which the second possibility holds. Then

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

As x and y run through (A) and (B) respectively, $x' = \frac{p+1}{2} - x$ and $y' = \frac{q+1}{2} - y$ run through (A) and (B) respectively, but in reverse order.

And note $py - qx > \frac{p}{2}$ if and only if $py' - qx' = p(\frac{q+1}{2} - y) - q(\frac{p+1}{2} - x) = \frac{p-q}{2} - (py - qx) < -\frac{q}{2}$.
Further, $py - qx < -\frac{y}{2}$ if and only if $py' - qx' = \frac{p-q}{2} - (py - qx) > \frac{p}{2}$.

Then $\lambda = \rho$. So

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

□

Examples:

(1) What is $\left(\frac{13}{17}\right)$?
By the Law of Quadratic Reciprocity, $\left(\frac{13}{17}\right)\left(\frac{17}{13}\right) = (-1)^{(\frac{17-1}{2})(\frac{13-1}{2})} = 1$.
But $\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1$ so $\left(\frac{13}{17}\right) = 1$.

(2) What is $\left(\frac{713}{1009}\right)$?
1009 is prime and $713 = 23 \cdot 31$. So $\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$.
By the Law of Quadratic Reciprocity, $\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right)$ and $\left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right)$.
Now, $\left(\frac{20}{23}\right) = \left(\frac{4}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{5}{23}\right)$ and $\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1$.
Further $\left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right)$.

Applying the result on the quadratic character of 2 from our corollary to Gauss' Lemma, we have $\left(\frac{2}{17}\right) = 1$, so $\left(\frac{17}{31}\right) = 1 \cdot \left(\frac{7}{17}\right) = \left(\frac{3}{7}\right) = -1$.
Thus $\left(\frac{713}{1009}\right) = 1$.

(3) 5 is a quadratic residue for all primes p of the form $10k \pm 1$ and is a quadratic nonresidue for all primes of the form $10k \pm 3$ since by the Law of Quadratic Reciprocity, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, and 1 and -1 are quadratic residues mod 5 while 3 and -3 are not.

(4) The equation
$$x^4 - 17y^4 = 2w^2$$
has no solution in the integers x, y, w.
Assume we have a solution. We may suppose that x and y are coprime, hence that x and w are coprime.
If p is an odd prime which divides w then $\left(\frac{17}{p}\right) = 1$ since $x^4 \equiv 17y^4 \pmod{p}$.
By the Law of Quadratic Reciprocity, $\left(\frac{p}{17}\right)(-1)^{(\frac{17-1}{2})(\frac{p-1}{2})} = 1$ so p is a quadratic residue of 17. Further, $\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = 1$.
Thus, $w \equiv t^2 \pmod{17}$ for some t. Therefore, $x^4 \equiv 2t^4 \pmod{17}$ so there exists an integer r with $r^4 \equiv 2 \pmod{17}$, which is a contradiction, since no such r exists.

(5) Is the congruence $3x^2 - 7x - 42 \equiv 0 \pmod{391}$ solvable?
Note $391 = 17 \cdot 23$.
Multiply by 12: $36x^2 + 84x - 516 \equiv 0 \pmod{391}$ thus we have $(6x+7)^2 \equiv 565 \pmod{391}$.
This is equivalent to solving $x^2 \equiv 174 \pmod{391}$.
Note $x^2 \equiv 174 \pmod{17}$ is $x^2 \equiv 4 \pmod{17}$, which has a solution.
Also, $x^2 \equiv 174 \pmod{23}$ if and only if $x^2 \equiv 13 \pmod{23}$.
And $\left(\frac{13}{23}\right) = \left(\frac{23}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = -\left(\frac{5}{13}\right) = -\left(\frac{13}{5}\right) = -\left(\frac{3}{5}\right) = 1$. Hence by the Chinese Remainder Theorem, the original congruence has a solution.

---

23. Lecture: Monday, November 6, 2000

Review of congruences

Recall: $a, b \in \mathbb{Z}$ implies there exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. x, y are found using the Euclidean Algorithm.

Theorem 29 (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_t \in \mathbb{Z}^+$ with $\gcd(m_i, m_j)$ for $i \neq j$. Set $m = m_1 \cdots m_t$.*
Let $b_1, \ldots, b_t \in \mathbb{Z}^+$. Then the simultaneous congruences
$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_t \pmod{m_t} \end{aligned}$$

have a unique solution modulo m.

Proof. Let $n_i = \frac{M}{m_i}$ for $i = 1, \ldots, t$.
Then $\gcd(m_i, n_i) = 1$ so there exist $r_i, s_i \in \mathbb{Z}$ such that $r_i n_i + s_i m_i = 1$ for $i = 1, \ldots, t$.
Let $e_i = r_i n_i$ so that $e_i \equiv 1 \pmod{m_i}$.
Then take $x_0 = \sum_{i=1}^{t} b_i e_i$.
Notice that $x_0 \equiv b_i \pmod{m_i}$ for $i = 1, \ldots, t$.
Suppose also $x_1 \equiv b_i \pmod{M_i}$ for $i = 1, \ldots, t$.
Then $m_i \mid x_1 - x_0$ for $i = 1, \ldots, t$ and since $\gcd(m_i, m_j)$ for $i \neq j$ then $m = \prod_{i=1}^{t} m_i dv x_1 - x_0$.
Thus there is a unique solution modulo m.
For any positive integer n, $(\mathbb{Z}/n\mathbb{Z})^*$ is the set of invertible elements in $\mathbb{Z}/n\mathbb{Z}$. In particular, it is the set of congruence classes $r + n\mathbb{Z}$ for which there exists $s + n\mathbb{Z}$ with $(r + n\mathbb{Z})(s + n\mathbb{Z}) = 1 + n\mathbb{Z}$. □

Theorem 30. *Let $m_1, \ldots, m_t$ be positive integers with $\gcd(m_i, m_j) = 1$ for $i \neq j$ and put $m = m_1 \cdots m_t$.*
Then the ring $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ and the group $(\mathbb{Z}/m\mathbb{Z})^*$ is isomorphic to the group $(\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^*$.

Proof. Let $\psi : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ be defined by $\psi(n) = (n + m_1\mathbb{Z}, \ldots, n + m_t\mathbb{Z})$.
We check that ψ is a ring morphism.

ψ is surjective by the Chinese Remainder Theorem. Also by the Chinese Remainder Theorem, $\ker\psi = m\mathbb{Z}$. Thus by the First Isomorphism Theorem for Rings,

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

Let $\lambda : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^*$ be defined by $\lambda(n + m\mathbb{Z}) = (n + m_1\mathbb{Z}, \ldots, n + m_t\mathbb{Z})$.
We see that λ is a group morphism. It is bijective by the Chinese Remainder Theorem. □

Corollary 1. Let $m_1, \ldots, m_t$ be positive integers which are pairwise coprime. Put $m = m_1 \cdots m_t$. Then

$$\varphi(m) = \varphi(m_1) \cdots \varphi(m_t)$$

Proof. $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$ and

$$\varphi(m_1) \cdots \varphi(m_t) = |(\mathbb{Z}/m_1\mathbb{Z})^*| \cdots |(\mathbb{Z}/m_1\mathbb{Z})^*| = |(\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_1\mathbb{Z})^*|$$

and so the result follows from Theorem 30. □

Corollary 2. Let $m = {p_1}^{a_1} \cdots {p_t}^{a_t}$ where $p_1, \cdots p_t$ are distinct primes, $a_1, \ldots, a_t$ positive integers. Then

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

Proof. Take $m_i = {p_i}^{a_i}$ for $i = 1, \ldots, t$ in Corollary 1.
Since $\varphi({p_i}^{a_i}) = {p_i}^{a_i} - {p_i}^{a_i - 1} = p_i(1 - \frac{1}{p_i})$, then

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

□

Proposition 1. *Let p be a prime. If $d \mid p-1$ then $x^d \equiv 1 \pmod{p}$ has exactly d solutions modulo p.*

Proof. Suppose $p-1 = dk$ with $k \in \mathbb{Z}^+$. Then

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

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

Theorem 31. *$(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group.*

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

$$d = \sum_{c \mid d} \lambda(c)$$

Now by Möbius inversion, we then have

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

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. □

Definition. Let n be a positive integer and let a be an integer. a is said to be a *primitive root* modulo n if $a + n\mathbb{Z}$ generates $(\mathbb{Z}/n\mathbb{Z})^*$.

---

24. Lecture: Wednesday, November 8, 2000

Note: For any prime p $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic and so there exists a primitive root modulo p. In fact, there are $\varphi(p-1)$ primitive roots modulo p.

Artin conjectured that if a is a positive integer and a is not a perfect square, then a is a primitive root modulo p for infinitely many primes p. This is still open. It can be deduced from the generalized Riemann Hypothesis.

(Why do we require a not a perfect square? $p-1$ is even. We want a to have order $p-1$. Well, if $a = k^2$ then no power of a is congruent to k, for if $a^i \equiv k$ then $a^{2i} \equiv a$ so $a^{2i-1} \equiv 1$ so $p-1 \mid 2i-1$, but even cannot divide odd!)

Notice 2 is a primitive root mod 5 ($2 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 5, 2^4 \equiv 1$) but 2 is not a primitive root modulo 7 since $2^3 \equiv 1$.
In general, $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic so primitive roots do not exist modulo n.
(E.g. $(\mathbb{Z}/8\mathbb{Z})^* = \{[1],[3],[5],[7]\}$ and $1^2 \equiv 1, 3^2 \equiv 1, 5^2 \equiv 1, 7^2 \equiv 1$. Therefore this group is not cyclic!)

Proposition 2. *Let p be a prime. If $\ell \geq 1$ and $a \equiv b \pmod{p^\ell}$, then $a^p \equiv b^p \pmod{p^{\ell+1}}$.*

Proof. We may write $a = b + cp^\ell$ for some $c \in \mathbb{Z}$. Then

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

So $a^p \equiv b^p \pmod{p^{\ell+1}}$ since $2\ell \geq \ell + 1$. □

Proposition 3. *If $\ell \geq 2$ and p is an odd prime, then for any integer a,*

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

Proof. We prove the result by induction on ℓ.
The result is immediate for $\ell = 2$. Assume the result holds for some integer ℓ with $\ell \geq 2$ and we shall prove it for $\ell + 1$.

By Proposition 2, and our inductive hypothesis,

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

Note that $p^{2(\ell-1)+1}$ divides $(ap^{\ell-1})^k$ for $k = 3, \ldots, p$ since $\ell \geq 2$ implies that $2(\ell-1)+1 \leq 3(\ell-1) \leq k(\ell-1)$.
Further, $p^{2(\ell-1)+1}$ divides $\binom{p}{2}(ap^{\ell-1})^2$ also, since $\binom{p}{2}(ap^{\ell-1})^2 = \frac{p(p-1)}{2}(ap^{\ell-1})^2 = \frac{p-1}{2}(ap^\ell)^2$. Note $\frac{p-1}{2}$ is an integer since p is odd.

So $p^{2(\ell-1)+1}$ divides the sum

$$\binom{p}{2}(ap^{\ell-1})^2 + \binom{p}{3}(ap^{\ell-1})^3 + \cdots + \binom{p}{p}(ap^{\ell-1})^p \pmod{p^{\ell+1}}$$

Thus since $\ell \geq 2$ implies $2(\ell-1) + 1 \geq \ell + 1$ since p is odd, then

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

The result follows by induction. □

Proposition 4. *If p is an odd prime, ℓ a positive integer and a an integer coprime with p then $1 + ap$ has order $p^{\ell-1}$ in $(\mathbb{Z}/p^\ell\mathbb{Z})^*$.*

Proof. By Proposition 3,

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

Hence, since a is coprime with p,

$$(1 + ap)^{p^{\ell-2}} \not\equiv 1 \pmod{p^\ell}$$

But again by Proposition 3,

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

hence

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

Thus $1 + ap$ has order $p^{\ell-1}$ in $(\mathbb{Z}/p^\ell\mathbb{Z})^*$. □

25. Lecture: Friday, November 10, 2000

Theorem 32. *Let p be an odd prime and let ℓ be a positive integer. Then $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ is a cyclic group.*

Proof. By Theorem 31, there is a primitive root g modulo p.
If $g^{p-1} \equiv 1 \pmod{p^2}$, then

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

so

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

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

Therefore at least one of g^{p-1} and $(g+p)^{p-1}$ is not congruent to 1 modulo p^2. Without loss of generality, we may suppose that $g^{p-1} \not\equiv 1 \pmod{p^2}$.
We claim that in this case, g is a primitive root modulo p^ℓ.

Suppose that g has order m. By Euler's Theorem, $g^{\varphi(p^\ell)} \equiv 1 \pmod{p^2}$ so $m \mid p^\ell - p^{\ell-1} = (p-1)p^{\ell-1}$.
Write $m = dp^s$ where $d \mid p-1$ and $0 \le s \le \ell - 1$.
By Fermat's Theorem, $g^p \equiv g \pmod{p}$. Hence $g^{p^s} \equiv g \pmod{p}$ provided $s \neq 0$.
But $g^m \equiv 1 \pmod{p^\ell}$ so $g^m \equiv 1 \pmod{p}$, so $g^d \equiv 1 \pmod{p}$.

Since g is a primitive root, $p - 1 \mid d$. Thus $d = p - 1$, so $m = (p-1)p^\ell$.
Since $g^{p-1} \not\equiv 1 \pmod{p^2}$ and $g^{p-1} \equiv 1 \pmod{p}$ there exists an integer a coprime with p such that $g^{-1} \equiv 1 + ap \pmod{p^2}$.

And by proposition 4, $1+ap$ has order $p^{\ell-1}$ in $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ and so g has order $(p-1)p^\ell$ hence $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ is cyclic. □

Theorem 33. *Let ℓ be a positive integer.*

$(\mathbb{Z}/2^\ell\mathbb{Z})^*$ is cyclic for $\ell = 1, 2$.

For $\ell \ge 3$,

$$(\mathbb{Z}/2^\ell\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots$$

In particular,

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

Proof. $(\mathbb{Z}/2\mathbb{Z})^*$ and $(\mathbb{Z}/4\mathbb{Z})^*$ are plainly cyclic. Suppose $\ell \ge 3$. We claim that

$$5^{2^{\ell-3}} \equiv 1 + 2^{\ell-1} \pmod{2^\ell} \tag{1}$$

We'll prove it by induction. For $\ell = 3$ we have $5 = 1 + 2^2 \pmod{2^3}$ as required.

Suppose (1) holds for some ℓ for $\ell \geq 3$.

Note that $(1+2^{\ell-1})^2 = 1+2^\ell+2^{2(\ell-1)}$ and $2(\ell-1) \geq \ell+1$ for $\ell \geq 3$.

Now, $5^{2^{\ell-3}} = 1+2^{\ell-1}+k2^\ell$ for some $k \in \mathbb{Z}$. Hence

$$5^{2^{\ell-2}} = (1+2^{\ell-1}+k2^\ell)^2 = 1+2^{\ell-1}+k2^\ell+2^{\ell-1}+2^{2\ell-1}+k2^{2\ell-1}+k2^\ell+k2^{2\ell-1}$$
$$= 1+2^\ell+k2^{\ell+1}+2^{2\ell-2}+k2^{2\ell}+k^2 2^{2\ell}$$

so $5^{2^{\ell-2}} \equiv 1+2^\ell \pmod{2^{\ell+1}}$ since $2\ell-2 \geq \ell+1$ for $\ell \geq 3$.
The result follows by induction.

Thus by $5^{2^{\ell-3}} \not\equiv 1 \pmod{2^\ell}$ and $5^{2^{\ell-2}} \equiv 1 \pmod{2^\ell}$, hence 5 has order $2^{\ell-2}$ in $\mathbb{Z}/2^\ell\mathbb{Z}^*$.
We now show that the numbers

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

are distinct modulo 2, for $\ell \geq 3$.

Suppose that

$$(-1)^{a_1}5^{b_1} \equiv (-1)^{a_2}5^{b_2} \pmod{2^\ell}$$

with $0 \leq a_i \leq 1$ and $0 \leq b_i < 2^{\ell-2}$ for $i = 1, 2, \ldots$.
Then

$$(-1)^{a_1}5^{b_1} \equiv (-1)^{a_2}5^{b_2} \pmod 4$$

So $(-1)^{a_1} \equiv (-1)^{a_2} \pmod 4$ hence $a_1 = a_2$.
Therefore $5^{b_1} \equiv 5^{b_2} \pmod{2^\ell}$ and since 5 has order $2^{\ell-2}$, we see that $b_1 = b_2$.

Our result follows. □

Theorem 34. *The only positive integers having primitive roots are* $1, 2, 4, p^a$ *and* $2p^a$ *with* a *a positive integer and* p *an odd prime.*

Proof. Let $n = 2^{\ell_0}{p_1}^{\ell_1}\cdots{p_r}^{\ell_r}$ with $\ell_0, \ell_1 \ldots, \ell_r$, non-negative integers and $p_1, \ldots, p_r$ distinct odd primes. Then by Theorem 30, $(\mathbb{Z}/n\mathbb{Z})^*$ is isomorphic to $(\mathbb{Z}/2^{\ell_0}\mathbb{Z})^* \times (\mathbb{Z}/{p_1}^{\ell_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/{p_r}^{\ell_r}\mathbb{Z})^*$.

By Theorem 32, $(\mathbb{Z}/{p_i}^{\ell_i}\mathbb{Z})^*$ is cyclic for $i = 1, \ldots, r$.

By Theorem 33, $(\mathbb{Z}/2^{\ell_0}\mathbb{Z})^*$ is cyclic for $0 \leq \ell_0 \leq 2$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\ell_0-2}\mathbb{Z}$ for $\ell \geq 3$.
Therefore, the order of any element of $\mathbb{Z}/n\mathbb{Z}$ is a divisor of

$$\lambda(n) = \operatorname{lcm}(b, \varphi({p_1}^{\ell_1}), \ldots, \varphi({p_r}^{\ell_r}))$$

where

$$b = \begin{cases} \varphi(2^{\ell_0}) & \text{for } 0 \leq \ell_0 \leq 2 \\ \frac{\varphi(2^{\ell_0})}{2} & \ell_0 \geq 3 \end{cases}$$

Plainly, $\lambda(n) < \varphi(2^{\ell_0})\varphi({p_1}^{\ell_1})\cdots\varphi({p_r}^{\ell_r})$ except in the cases $1, 2, 4, p^a$ and $2p^a$. □

Definition. $\lambda(n)$ is known as the *universal exponent* of n.

Theorem 35. *Let n be a positive integer and define $\lambda(n)$ as before. Then for any integer a coprime with n,*

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

Proof. The proof follows from the proof of Theorem 34. □

Theorem 35 gives a strengthening of Euler's Theorem.

---

26. Lecture: Monday, November 13, 2000

Given a prime p one can ask for an upper bound for the smallest positive integer a which is a primitive root modulo p.

Hua proved

$$a < 2^{\omega(p-1)+1}\sqrt{p}$$

Theorem 36. *If p is a prime of the form $4q+1$ with q an odd prime then 2 is a primitive root modulo p.*

Proof. Let t be the order of 2 modulo p. By Fermat's Theorem, $t \mid p-1$ so $t \mid 4q$. Thus t is one of $1, 2, 4, q, 2q$ and $4q$.

Note that $p = 13$ or $p > 20$ so t is not 1,2,4.
Further, by Euler's Criterion,

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

But $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(4q)^2+8q}{8}} = (-1)^q = -1$.
Thus t is not q or $2q$ hence $t = 4q = p-1$ as required.

□

Let k and ℓ be positive integers with k and ℓ coprime. Dirichlet's Theorem asserts that $kn+\ell$ is prime for infinitely many integers n. For many primes (k, ℓ), we can prove Dirichlet's Theorem by elementary means.

Consider (4,3). Suppose that there are only finitely many primes, $p_1, \ldots, p_k$ say, of the form $4n+3$. Consider $4p_1 \cdots p_k + 3$.
This must be divisible by a prime of the form $4m+3$ (since a product of primes congruent to 1 modulo 4 can only yield numbers congruent to 1 modulo 4), and this prime $4n+3$ cannot be any of the $p_1, \ldots, p_k$.

Theorem 37. *Let n be a positive integer. There are infinitely many primes congruent to 1 modulo n.*

Proof. (Due to Birkhoff and Vandiver, 1904)

Let a be a positive integer with $a > 2$, and consider $\Phi_n(a)$, the nth cyclotomic polynomial evaluated at a.

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

where $\zeta_n = e^{\frac{2\pi i}{n}}$, $\Phi_n(x) \in \mathbb{Z}[x]$, and $x^n - 1 = \prod_{d \mid n} \Phi_n(x)$.
We claim that if p is a prime dividing $\Phi_n(a)$, then $p \mid n$ or $p \equiv 1 \pmod{n}$.

To see this, note that $p \mid a^n - 1^n$ hence $p \nmid a$. If $p \nmid a^d - 1$ for d a proper divisor of n, then the order of $a \pmod{p}$ is n. By Fermat's Theorem, $n \mid p - 1$, hence $p \equiv 1 \pmod{n}$.

Suppose next that $p \mid a^d - 1$ for some proper divisor d of n. Then since $p \mid \Phi_n(a)$, then $p \mid \frac{a^n-1}{a^d-1}$. We have

$$a^n = (1 + (a^d - 1))^{\frac{n}{d}} = 1 + \frac{n}{d}(a^d - 1) + \binom{n}{2}(a^d - 1)^2 + \binom{n}{3}(a^d - 1)^3 + \cdots$$

hence

$$\frac{a^n - 1}{a^d - 1} = \frac{n}{d} + \binom{n/d}{2}(a^d - 1) + \binom{n/d}{3}(a^d - 1)^2 + \cdots$$

Since $p \mid \frac{a^n-1}{a^d-1}$ and $p \mid a^d - 1$, we conclude that $p \mid \frac{n}{d}$ hence $p \mid n$ as required.

Assume that there only finitely many primes $p_1, \ldots, p_k$ which are congruent to 1 modulo n.

$$\Phi_n(x) = x^{\varphi(n)} + \cdots \pm 1$$

so $\Phi(np_1 \cdots p_k m)$ is not divisible by p_i for $i = 1, \ldots, k$ and is coprime with n.

Letting $m \to \infty$ we see that for m sufficiently large, $\Phi(np_1 \cdots p_k m) \geq 2$ and so has a prime divisor congruent to 1 modulo n which is not one of $\{p_1, \ldots, p_k\}$.

This is a contradiction. □

---

27. Lecture: Wednesday, November 15, 2000

Definition. Let G be a finite abelian group. A *character* of G is a homomorphism $\chi : G \to \mathbb{C}^*$.

The set of characters of a group form a group under $(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g)$.

This group is called the *dual group* of G and is denoted $\hat{G}$.

The identity of $\hat{G}$ is the character χ_0 where $\chi_0(g) = 1$ for all $g \in G$. χ_0 is known as the *principal character*.

Note that if $|G| = n$ then $g^n = e$ for all $g \in G$, hence $(\chi(g))^n = 1$ so $\chi(g)$ is an nth root of unity.

Theorem 38. *Let G be a finite abelian group. Then*

(i) $\left|\hat{G}\right| = |G|$

(ii) $\hat{G} \cong G$

(iii) *We have*

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

and

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

Proof. Recall that any finite abelian group is the direct product of cyclic groups.

Hence there exist $g_1, \ldots, g_r \in G$ and $h_1, \ldots, h_r \in \mathbb{N}$ with $h_1 \cdots h_r = n$ such that every element $g \in G$ has a unique representation in the form $g = {g_1}^{a_1} \cdots {g_r}^{a_r}$ with $0 \leq a_i \leq h_i$ for $i = 1, \ldots, r$ and ${g_i}^{h_i} = e$ for $i = 1, \ldots, r$.

Now any character is determined by its action on $g_1, \ldots, g_r$. But $(\chi(g_i))^{h_i} = 1$.
Therefore $\chi(g_i)$ is an h_ith root of unity. Hence there are at most $h_1 \cdots h_r$ characters.
But there are at least $h_1 \cdots h_r$ characters, since if w_i is a h_ith root of unity, we may define $\chi(g_i) = w_i$ for each i and extending multiplicatively to G.

(i) Hence $|G| = \left|\hat{G}\right|$.

(ii) Let χ_i be the character which maps g_i to $e^{\frac{2\pi i}{h_i}}$ and maps g_j to 1, for $j \neq i$.
Define $\phi : G \to \hat{G}$ by

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

Note ϕ is a homomorphism.

Clearly ϕ is injective since

$${\chi_1}^{a_1} \cdots {\chi_r}^{a_r}(g_j) = e^{\frac{2\pi j a_j}{h_j}}$$

Therefore, ϕ is surjective since G is finite and $|G| = \left|\hat{G}\right|$.

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

(iii) Let $S(g) = \sum_{\chi \in G} \chi(g)$.
If $g = e$ then $\chi(e) = 1$ for all $\chi \in \hat{G}$ so $S(e) = \left|\hat{G}\right| = |G|$.

So assume $g \neq e$. Then there exists a character $\chi_1 \in \hat{G}$ such that $\chi_1(g) \neq 1$. Now

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

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

Therefore $S(g) = 0$ since $\chi_1(g) \neq 1$, as required.

Let $T(\chi) = \sum_{g \in G} \chi(g)$.
If $\chi = \chi_0$ then $\chi_0(g) = 1$ for all $g \in G$; therefore $T(\chi) = |G|$.

If $\chi \neq \chi_0$ then there exists $g_1 \in G$ such that $\chi(g_1) \neq 1$. So

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

Therefore $T(\chi) = 0$ since $\chi(g_1) \neq 1$.

□

---

28. Lecture: Friday, November 17, 2000

Let k be a positive integer and denote $(\mathbb{Z}/k\mathbb{Z})^*$ by $G(k)$. Let χ be a character on $G(k)$. We associate to it a map from $\mathbb{Z}$ to $\mathbb{C}^*$. which we also denote by χ, by putting

$$\chi(a) = \chi([a])$$

where $[a]$ denote the congruence class of a for a coprime with k, and $\chi(a) = 0$ otherwise. χ is known as a *character mod k*.

Theorem 39. *Let χ be a character mod k.*

(a) *If $(n, k) = 1$ then $\chi(n)$ is a kth root of unity.*
(b) *The function χ is completely multiplicative, i.e. $\chi(mn) = \chi(m)\chi(n)$ for all $m, n \in \mathbb{Z}$.*
(c) *χ is periodic modulo k, i.e. $\chi(n + k) = \chi(n)$ for all $n \in \mathbb{Z}$.*
(d) *We have*

$$\sum_{n=1}^{k} \chi(n) = \begin{cases} \varphi(k) & \text{if } \chi \text{ is the principal character} \\ 0 & \text{otherwise} \end{cases}$$

and

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

(e) *Let $\overline{\chi}$ denote the conjugate character to χ.*
In particular, $\overline{\chi}(n) = \overline{\chi(n)}$ for all $n \in \mathbb{Z}$.
Let χ' be a character mod k. Then

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

and

$$\sum_{\chi a \text{ character mod } k} \chi(n)\overline{\chi}(m) = \begin{cases} \varphi(k) & \text{if } n \equiv m \pmod{k} \text{ and } (n, k) = 1 \\ 0 & \text{otherwise} \end{cases}$$

We'll now describe the group of characters mod k.
It is enough, by multiplicity, to discuss the characters mod p^a for p prime.
Assume first that p is an odd prime. Let g be a primitive root mod p^a.
If n is coprime with p there is a unique integer ν with $1 \le \nu \le \varphi(p^a)$ such that $n \equiv g^\nu \pmod{p^a}$.

To each integer b with $1 \le b \le \varphi(p^a)$ we define the character $\chi^b(n)$ by

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

We get in this way $\varphi(p^a)$ different characters mod p^a, and so this is the complete list.

Next suppose that $k = 2^a$. If $a = 1$ we just have the principal character. If $a = 2$ then we have the principal character and the character χ_4 where

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

If $a \ge 3$ then $(\mathbb{Z}/2^a\mathbb{Z})^*$ is not cyclic but for each odd integer there is a unique pair of integers (x, y) with $0 \le x \le 1, 0 \le y \le 2^{a-2}$ such that

$$n \equiv (-1)^x 5^y \pmod{2^a}$$

For each b with $1 \le b \le \varphi(2^a)$ we put

$$\chi^b(n) = \begin{cases} \exp(\pi i b x + \frac{\pi i b y}{2^{a-3}} & \text{for } n \equiv 1 \pmod 2 \\ 0 & \text{otherwise} \end{cases}$$

We have $\varphi(2^a)$ different characters mod 2^a, and so we have them all.

Let k be a positive integer, and let χ be a character mod k. We define, for $\mathrm{Re}(s) > 1$,

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

Theorem 40. *The function $L(s, \chi)$ can be analytically continued to $\mathrm{Re}(s) > 0$ except when χ is the principal character.*
If χ_0 is the principal character mod k then $L(s, \chi_0)$ can be analytically continued to $\mathrm{Re}(s) > 0$ except for the point $s = 1$ where $L(s, \chi_0)$ has a simple pole of residue $\frac{\varphi(k)}{k}$.

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

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

From Theorem 39 (d),

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

where $|R(x)| \le 2\varphi(k)$.
(This follows since for $\chi = \chi_0$,

$$C(x) = \left\lfloor \frac{x}{k} \right\rfloor \varphi(k) + T(x)$$

and for $\chi \neq \chi_0$,

$$C(x) = \left\lfloor \frac{x}{k} \right\rfloor 0 + T(x)$$

where in both cases $0 \leq T(x) \leq \varphi(k)$.)

By Abel's summation formula, with $A(x) = \sum_{n \leq x} \chi(n)$ and $f(n) = \frac{1}{n^s}$, we have

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

$$= E(\chi) \frac{\varphi(k)}{k} \frac{1}{x^{s-1}} + sE(\chi) \frac{\varphi(k)}{k} \left(\frac{-u^{-s+1}}{s-1} \Big|_1^x + \frac{R(x)}{x^s} + s \int_1^x \frac{R(u)}{u^{s+1}} du \right.$$

$$= E(\chi) \frac{\varphi(k)}{k} \left(x^{1-s} + \frac{s}{1-s} (x^{1-s} - 1) \right) + \frac{R(x)}{x^s} + s \int_1^x \frac{R(u)}{u^{s+1}} du$$

For $\mathrm{Re}(s) > E(\chi)$ we see on letting $x \to \infty$ that the term on the right hand side tends to

$$E(\chi) \frac{\varphi(k)}{k} \frac{s}{s-1} + s \int_1^\infty \frac{R(u)}{u^{s+1}} du$$

□

29. Lecture: Monday, November 20, 2000

Definition. Let $\{\lambda_n\}_{n=1}^{\infty}$ be a strictly increasing sequence of positive real numbers. A *Dirichlet series* attached to $\{\lambda_n\}_{n=1}^{\infty}$ is a series of the form

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

where $\{a_n\}_{n=1}^{\infty}$ is a sequence of complex numbers, and $z \in \mathbb{C}$.

Theorem 41. *If the Dirichlet series $\sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$ converges for $z = z_0$, then it converges uniformly for $\mathrm{Re}(z - z_0) \geq 0$ and $|arg(z - z_0)| < \alpha$ with $\alpha < \frac{\pi}{2}$.*

Proof. Without loss of generality, we may assume $z_0 = 0$. Then $\sum_{n=1}^{\infty} a_n$ converges.

Therefore, given $\epsilon > 0$, there exists $N = N(\epsilon)$ such that if $\ell, m > N$, then

$$\left| \sum_{n=\ell}^{m} a_n \right| < \epsilon$$

Denote $\sum_{n=\ell}^{m} a_n$ by $A_{\ell,m}$. Then

$$\sum_{n=\ell}^{m} a_n e^{-\lambda_n z} = \sum_{n=\ell}^{m} (A_{\ell,n} - A_{\ell,n-1}) e^{\lambda_n z}$$

$$= \sum_{n=\ell}^{m-1} A_{\ell,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z}) + A_{\ell,m} e^{-\lambda_m z}$$

Thus, for $\mathrm{Re}(z) > 0$,

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

But

$$e^{-\lambda_n z} - e^{-\lambda_{n+1} z} = z \int_{\lambda_n}^{\lambda_{n+1}} e^{-tz} dt$$

hence

$$\left| e^{-\lambda_n z} - e^{-\lambda_{n+1} z} \right| \leq |z| \int_{\lambda_n}^{\lambda_{n+1}} e^{-tx} dt$$

where $z = x + iy$. $x, y \in \mathbb{R}$. So

$$\left| e^{-\lambda_n z} - e^{-\lambda_{n+1} z} \right| \leq |z| \left(-\frac{e^{-tx}}{x} \Big|_{\lambda_n}^{\lambda_{n+1}} \right) = \frac{|z|}{x} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x})$$

Therefore,

$$\left| \sum_{n=\ell}^{m} a_n e^{-\lambda_n z} \right| \leq \epsilon \left(\frac{|z|}{x} (e^{-\lambda_\ell x} - e^{-\lambda_m x}) + 1 \right)$$

Hence for $|\arg(z)| < \alpha$, we have $\frac{|z|}{x} < k$, for some $k = k(\alpha)$. Further, $\left|e^{-\lambda_\ell x} - e^{-\lambda_m x}\right| \leq 2$.
Thus $\left|\sum_{n=\ell}^{m} a_n e^{-\lambda_n z}\right| < (2k+1)\epsilon$ and so the Dirichlet series converges for $\mathrm{Re}(z) \geq 0$ and $|\arg(z)| \leq \alpha$. □

Therefore, if the series converges for $z = z_0$, it determines an analytic function for $\mathrm{Re}(z - z_0) \geq 0$.

We'll show next that if the a_n's are positive real numbers, then the domain of convergence for the analytic function determined by the series is limited only by a singularity on the real axis.

---

30. Lecture: Wednesday, November 22, 2000

Theorem 42. *Let $f(z) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$ be a Dirichlet series with $a_n \in \mathbb{R}$ and $a_n \geq 0$, for $n = 1, 2, \ldots$. Suppose that the series converges for $\mathrm{Re}(z) > \sigma_0$ with $\sigma_0 \in \mathbb{R}$ and suppose that f can be analytically continued in a neighbourhood of σ_0.*
Then there exists an $\epsilon > 0$ such that $\sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$ converges for $\mathrm{Re}(z) > \sigma_0 - \epsilon$.

Proof. Assume, without loss of generality, that $\sigma_0 = 0$. Since f is holomorphic (analytic) in a neighbourhood of 0 and is holomorphic for $\mathrm{Re}(z) > 0$ by Theorem 41 (using uniform convergence), there is a positive real number ϵ such that f is analytic in $|z - 1| \leq 1 + \epsilon$.

We now consider the Taylor series expansion in $|z - 1| \leq 1 + \epsilon$.

Note that for $\mathrm{Re}(z) > 0$,

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

hence

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

The Taylor series expansion around 1 in $|z - 1| \leq 1 + \epsilon$ is

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

We now consider f at the point $z = -\epsilon$. We have

$$f(-\epsilon) = \sum_{m=0}^{\infty} \left(\sum_{n=1}^{\infty} a_n (-\lambda_n)^m e^{-\lambda_n}) \right) \frac{(-1-\epsilon)^m}{m!}$$

$$= \sum_{m=0}^{\infty} \left(\sum_{n=1}^{\infty} a_n (\lambda_n)^m e^{-\lambda_n}) \right) \frac{(1+\epsilon)^m}{m!}$$

and since $a_n \geq 0$ we may switch the orders of summation and so

$$f(-\epsilon) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n} \left(\sum_{m=1}^{\infty} \frac{(\lambda_n)^m (1+\epsilon)^m}{m!} \right)$$

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

Thus the series converges to f for $z = -\epsilon$ and so by Theorem 41 it converges to f for $\mathrm{Re}(z) > -\epsilon$. □

31. Lecture: Friday, November 24, 2000

Theorem 43. *if χ is a character mod k then $L(s,\chi)$ is nonzero for* $\mathrm{Re}(s) > 1$. *Further, if χ is not principal then $L(1,\chi)$ is nonzero.*

Proof. The first claim follows on noting that $L(s,\chi)$ converges absolutely for $\mathrm{Re}(s) > 1$. Further, χ is completely multiplicative and so $L(s,\chi)$ has a Euler product representation for $\mathrm{Re}(s) > 1$ given by

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Since the Euler product representation converges for $\mathrm{Re}(s) > 1$, then $L(s,\chi)$ is nonzero for $\mathrm{Re}(s) > 1$.

The second assertion splits into two cases, depending on whether χ is a real or a complex character. For $\mathrm{Re}(s) > 1$ we have, from the Euler product representation,

$$\log^*(L(s,\chi)) = \sum_p -\log\left(1 - \frac{\chi(p)}{p^s}\right)$$

$$= \sum_p \sum_{a=1}^{\infty} \frac{\chi(p^a)}{a p^{as}}$$

where log indicates the principal branch and $\log^*$ indicates a branch of the logarithm.

Let $k \geq 2$, and let ℓ be an integer coprime with k. Then

$$\sum_{\chi \in G(k)} \overline{\chi}(\ell) \log^* L(s,\chi) = \sum_p \sum_{a=1}^{\infty} \frac{1}{a p^{as}} \sum_{\chi \in G(k)} \overline{\chi}(\ell)\chi(p^a)$$

So by Theorem 39e,

$$\sum_{\chi in G(k)} \overline{\chi}(\ell) \log^* L(s,\chi) = \varphi(k) \sum_{a=1}^{\infty} \sum_{p^a \equiv \ell \pmod k} \frac{1}{a p^{as}} \tag{1}$$

If we take $\ell = 1$ in (1) and then exponentiate both sides of (1),

$$\prod_{\chi \in G(k)} L(s,\chi) = \exp\left(\varphi(k) \sum_{a=1}^{\infty} \sum_{p^a \equiv \ell \pmod k} \frac{1}{a p^{as}}\right)$$

and so for s real with $s > 1$,

$$\prod_{\chi \in G(k)} L(s,\chi) \geq 1 \tag{2}$$

Suppose first that $L(1,\chi)=0$ with χ a character which is not a real character. Then $\overline{\chi}$ is a character mod k with $\chi \neq \chi_0$.

But notice that $\overline{L(s,\chi)} = L(s,\overline{\chi})$ for s real with $s>1$. Thus

$$L(1,\overline{\chi}) = \overline{L(1,\chi)} = 0$$

$L(s,\chi_0)$ has a simple pole at $s=1$ and $L(s,\chi)$ does not have a pole at $s=1$ unless $\chi=\chi_0$ by Theorem 40.

Thus as $s \to 1$ from above on the real axis,

$$\prod_{\chi \in G(k)} L(s,\chi) = O((s-1)^{-1}(s-1)^2) = O(s-1)$$

But this contradicts (2).

Next, suppose that $L(1,\chi)=0$ with χ a real character.

Put $g(s) = \frac{\zeta(s)L(s,\chi)}{\zeta(2s)}$ for $\mathrm{Re}(s)>1$.

Consider the Euler product representation for $\mathrm{Re}(s)>1$,

$$g(s) = \prod_p \frac{(1-p^{-2s})}{(1-p^{-s})(1-\frac{\chi(p)}{p^s})} = \prod_p \frac{(1+p^{-s})}{(1-\frac{\chi(p)}{p^s})}$$

$$= \prod_p \left(1+\frac{1}{p^s}\right) \sum_{a=0}^{\infty} \frac{\chi(p^a)}{p^{as}} = \prod_p \left(1+\sum_{a=1}^{\infty} \frac{\chi(p^{a-1})+\chi(p^a)}{p^{as}}\right) = \prod_p \left(1+\sum_{a=1}^{\infty} \frac{b(p^a)}{p^{as}}\right)$$

Note that χ is a real character and so takes on values from $\{-1,0,1\}$.

Further, χ is multiplicative and so

$$b(p^a) = \chi(p^{a-1}) + \chi(p)\chi(p^{a-1}) \geq 0 \text{ for } a = 1,2,\ldots$$

Thus $g(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ where $a_1 = 1$ and $a_i \in \mathbb{R}$ with $a_i \geq 0$ for $i = 2,3,\ldots$.

We have $g(s) = \frac{\zeta(s)L(s,\chi)}{\zeta(2s)}$ for $\mathrm{Re}(s)>1$.

Since the zero of $L(1,\chi)$ eliminates the pole of $\zeta(s)$ at $s=1$, and since $\zeta(2s)$ is nonzero and analytic for $\mathrm{Re}(s) > \frac{1}{2}$, then $g(s)$ has an analytic continuation to $\mathrm{Re}(s) > \frac{1}{2}$.

We now apply Theorem 42 to conclude that the series defining g converges to g for $\mathrm{Re}(s) > \frac{1}{2}$.

Letting $s \to \frac{1}{2}$ from above on the real axis, we see, since $\zeta(2s)$ has a pole at $s=\frac{1}{2}$,

$$g(s) = O(s-\tfrac{1}{2}) = o(1)$$

But $g(s) \geq 1$ for $\mathrm{Re}(s) > \frac{1}{2}$ since

$$g(s) = 1 + \sum_{n=2}^{\infty} \frac{a_n}{n^s}$$

with $a_n \geq 0$ for $n = 2,3,\ldots$, which is a contradiction. Therefore $L(1,\chi) \neq 0$. $\square$

32. Lecture: Monday, November 27, 2000

Theorem 44. *If ℓ and k are coprime integers with $k \geq 2$ then the series $\sum_{p \equiv \ell \pmod k} \frac{1}{p}$ diverges.*

Proof. We appeal to (1) from Theorem 43:

$$\frac{1}{\varphi(k)} \sum_{\chi \in G(k)} \overline{\chi}(\ell) \log L(s,\chi) = \sum_{a=1}^{\infty} \sum_{p^a \equiv \ell \pmod k} \frac{1}{ap^{as}}$$

Now as s tends to 1 from the right on the nonzero real axis, $(s-1)^{E(\chi)} L(s,\chi)$ tends to a finite non-zero limit by Theorem 43.
Here $E(\chi) = 1$ if $\chi = \chi_0$, $E(\chi) = 0$ if $\chi \neq \chi_0$.

Thus $E(\chi)\log(s-1) + \log L(s,\chi)$ tends to a limit, hence $\log L(s,\chi) = -E(\chi)\log(s-1) + O(1)$ as $s \to 1$ from the right on the real axis, hence

$$\frac{1}{\varphi(k)} \sum_{\chi \in G(k)} \overline{\chi}(\ell) \log L(s,\chi) = -\frac{1}{\varphi(k)} \log(s-1) + O(1)$$

therefore

$$\sum_{a=1}^{\infty} \sum_{p^a \equiv \ell \pmod k} \frac{1}{ap^{as}} = -\frac{1}{\varphi(k)} \log(s-1) + O(1)$$

$$\sum_{p \equiv \ell \pmod k} \frac{1}{p^s} + \sum_{a=2}^{\infty} \sum_{p^a \equiv \ell \pmod k} \frac{1}{ap^{as}} = -\frac{1}{\varphi(k)} \log(s-1) + O(1)$$

But for $\mathrm{Re}(s) \geq 1$ and $s \in \mathbb{R}$,

$$\sum_{a=2}^{\infty} \sum_{p^a \equiv \ell \pmod k} \frac{1}{ap^{as}} \leq \frac{1}{2} \sum_{a=2}^{\infty} \sum_{p^a \equiv \ell \pmod k} \frac{1}{p^{as}}$$

$$\leq \sum_{a=2}^{\infty} \left(\frac{1}{n^{2s}} + \frac{1}{n^{3s}} + \cdots \right) \leq \frac{1}{2} \sum_{n=2}^{\infty} \frac{1}{n^{2s}} \left(\frac{1}{1 - \frac{1}{n^s}} \right) \leq \sum_{n=2}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Therefore

$$\sum_{p \equiv \ell \pmod k} \frac{1}{p^s} = -\frac{1}{\varphi(k)} \log(s-1) + O(1)$$

as $s \to 1$ from the right on the real axis, and the quantity $-\frac{1}{\varphi(k)} \log(s-1)$ blows up as $s \to 1$, so the result follows.

□

Let k and ℓ be coprime integers with $k \geq 2$.
Denote, for each $x \in \mathbb{R}$, the number of primes p with $p \leq x$ and $p \equiv \ell \pmod{k}$ by $\pi(x, k, \ell)$.
Then it is possible to prove that

$$\pi(x, k, \ell) \sim \frac{1}{\varphi(k)} \frac{x}{\log x} \sim \frac{\mathrm{Li}(x)}{\varphi(k)}$$

Let t be a real number and k a positive integer, and put $\tau(k, t) = \max\{|t|, k + 2\}$.
Let $c \in \mathbb{R}$ with $0 < c < 1$, and define $R_c(k)$ by

$$R_c(k) = \{\sigma + it : 1 - \frac{c}{\log \tau(k, t)} < \sigma\}$$

There exists a positive constant c_0 such that one can prove that if χ is a non-real character mod k, $k \geq 2$, then $L(s, \chi)$ is nonzero in $R_{c_0}(k)$.

For χ a real non-principal character we can't prove this, but we can show that such a c_0 exists if we change the requirement from "$L(s, \chi)$ is nonzero in $R_{c_0}(k)$" to "$L(s, \chi)$ is nonzero in $R_{c_0}(k)$ except perhaps for one point β on the real axis in $R_{c_0}(k)$".

Definition. If $L(s, \chi)$ vanishes at β then β is a simple zero of $L(s, \chi)$, and is known as a *Siegel zero*.

By the Extended Riemann Hypothesis, $L(s, \chi)$ is nonzero for $\mathrm{Re}(s) > \frac{1}{2}$ and so under this hypothesis, no Siegel zero exists.

Let k and ℓ be coprime integers with $k \geq 2$. Put $b = \beta(k)$ if there is a real nonprincipal character χ with β a zero of $L(s, \chi)$ in $R_{c_o}(k)$, and $b = 1$ otherwise. Then there exists $a > 0$ such that

$$\pi(x, k, \ell) = \frac{\mathrm{Li}(c)}{\varphi(k)} - \frac{\lambda(b)}{b} \frac{x^b}{\varphi(k)} + O(x \exp(-a\sqrt{\log x}))$$

where $\lambda(b) = 0$ if $b = 1$, and $\lambda(b) = \chi(\ell)$ if $b \neq 1$.

(We would like to know the term $\frac{\lambda(b)}{b} \frac{x^b}{\varphi(k)}$ doesn't exist (no Siegel zero exists) but we haven't been able to prove this.)

---

33. Lecture: Wednesday, November 29, 2000

The best "effective" estimate for the size of a Siegel zero $\beta(k)$ associated to $L(s, \chi)$ where χ is a real character mod k is due to Pintz. He proved

$$\beta(k) < 1 - \frac{c}{\sqrt{k}}$$

where c is an effectively computable positive number.

Siegel proved that for each $\epsilon > 0$, there exists a positive number $c(\epsilon)$ such that

$$\beta(k) < 1 - \frac{c(\epsilon)}{k^\epsilon}$$

Unfortunately, given ϵ, there is no general algorithm known for computing $c(\epsilon)$.

Using Siegel's estimate, one can prove that for each positive real number H if $k \leq (\log x)^H$. Then

$$\pi(x,k,\ell) = \frac{\mathrm{Li}(x)}{\varphi(k)} + O(\tfrac{x}{\exp a\sqrt{\log x}})$$

for some $a > 0$. The big-O term is not effective.

One can also prove for each $H > 0$,

$$\pi(x,k,\ell) = \frac{\mathrm{Li}(x)}{\varphi(k)} + O(\tfrac{x}{(\log x)^H})$$

(The big-O term is not effective.)

In 1770 Waring stated without proof that every positive integer can be expressed as the sum of 4 squares, of 9 cubes, of 19 biquadrates, and so on. For each positive integer k, let $g(k)$ denote the smallest positive integer such that every positive integer can be expressed as the sum of $g(k)$ kth powers.

It was not until 1909 that Hilbert proved that $g(k)$ exists for each positive integer k, Previously it had been shown that $g(k)$ exists for $k = 2, 3, 4, 5, 6, 7, 8$ and 10.

From work by Vinogradov it is known that

$$g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$$

provided that $k \geq 5$ and

$$3^k - 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor \leq 2^k - \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$$

If the condition isn't satisfied, there is another explicit formula for $g(k)$.

We know that $g(2) = 4$, $g(3) = 9$, $g(4) = 19$. We'll now prove that $g(2) = 4$.

Observe that $x^2 \pmod 8$ assumes only the congruences $0, 1, 4 \pmod 8$ as x runs over $\mathbb{Z}$. Thus ${x_1}^2 + {x_2}^2 + {x_3}^2 \not\equiv 7 \pmod 8$. Therefore $g(2) \geq 4$.

In 1770 Lagrange proved that $g(2) = 4$.

Theorem 45. *If p is an odd prime then there are integers x and y such that*

$$1 + x^2 + y^2 = mp \text{ with } 1 \leq m < p$$

Proof. Consider the set $S_1 = \{x^2 + p\mathbb{Z} : 0 \leq x \leq \frac{1}{2}(p-1)\}$ and the set $S_2 = \{-1 - y^2 + p\mathbb{Z} : 0 \leq y \leq \frac{1}{2}(p-1)\}$.

Note that $|S_1| = |S_2| = \frac{1}{2}(p+1)$. Therefore there is a congruence class in $S_1 \cap S_2$. In particular, for some x with $0 \leq x \leq \frac{1}{2}(p-1)$ and some y with $0 \leq y \leq \frac{1}{2}(p-1)$,

$$1 + x^2 + y^2 \equiv 0 \pmod p$$

Therefore, $1 + x^2 + y^2 = mp$ and

$$0 < m \leq \frac{1 + (\frac{1}{2}(p-1))^2 + (\frac{1}{2}(p-1))^2}{p} < p$$

□

For his proof, Lagrange appealed to the following identity:

$$\begin{aligned}&(x_1{}^2 + x_2{}^2 + x_3{}^2 + x_4{}^2)(y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2)\\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2\\ &+(x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned}$$

Therefore the product of two numbers which are representable as the sum of 4 squares is also representable as the sum of 4 squares.

Since $2 = 1^2 + 1^2 + 0^2 + 0^2$ it only remains to show that every odd prime is representable as the sum of 4 squares.

Theorem 46 (Lagrange's Theorem)**.** *Every positive integer can be expressed as the sum of 4 squares.*

Proof. Let p be an odd prime. It remains to show that p can be expressed as the sum of 4 squares.

It follows from Theorem 45 that there is a multiple of p, mp, such that

$$x_1{}^2 + x_2{}^2 + x_3{}^2 + x_4{}^2 = mp$$

with $1 \leq m \leq p$.

Let m_0 be the smallest positive multiple of p which can be written as the sum of 4 squares. It remains to show that $m_0 = 1$.

If m_0 is even, then since $x_1{}^2 + x_2{}^2 + x_3{}^2 + x_4{}^2 = m_0p$, we have that $x_1 + x_2 + x_3 + x_4$ is even.
We can have x_1, x_2, x_3, x_4 all even or all odd. Otherwise, 2 are even (say x_1, x_2), and 2 are odd (x_3, x_4). Therefore, in all cases,

$$x_1 + x_2, x_1 - x_2, x_3 + x_4, x_3 - x_4$$

are all even, and therefore

$$\frac{1}{2}m_0p = (x_1 + x_2)^2 + (x_1 - x_2)^2 + (x_3 + x_4)^2 + (x_3 - x_4)^2$$

which contradicts the minimality of m_0.

Thus m_0 is odd. Assume that $m_0 > 1$.
Note that not all of x_1, x_2, x_3, x_4 are divisible by m_0, for otherwise $m_0{}^2 \mid m_0p$ and $1 < m_0 < p$.
Thus we can find integers b_1, b_2, b_3, b_4 so that $y_i = x_i - b_im_0$ satisfies $|y_i| < \frac{m_0}{2}$ for $i = 1, 2, 3, 4$ and not all of the y_i's are 0.

Then

$$0 < y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2 < 4(\frac{1}{2}m_0)^2 = m_0{}^2$$

and $y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2 \equiv 0 \pmod{m_0}$.

Thus there exists a positive integer m_1 with $m_1 < m_0$ such that

$$y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2 = m_0 m_1$$

Applying this, together with the fact that $x_1{}^2 + x_2{}^2 + x_3{}^2 + x_4{}^2 = m_0 p$, to Lagrange's identity, we have

$$m_0{}^2 m_1 p = z_1{}^2 + z_2{}^2 + z_3{}^2 + z_4{}^2$$

where $z_1 = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4$, etc.

But $z_1 = \sum_{i=1}^{4} x_1(x_1 - b_i m_0)$, hence $z_1 \equiv 0 \pmod{m_0}$. Similarly z_2, z_3, z_4 are divisible by m_0.

Let $t_i = \frac{z_i}{m_0}$ for $i = 1, 2, 3, 4$.
Then $m_1 p = t_1{}^2 + t_2{}^2 + t_3{}^2 + t_4{}^2$ and $1 \leq m_1 \leq m_0$, a contradiction.

Thus $m_0 = 1$ for all primes p and the result follows. □

---

34. Lecture: Friday, December 1, 2000

Theorem 47.

$$g(4) \leq 53$$

Proof. We appeal to the identity

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4 + (a-b)^4 + (c+d)^4 + (c-d)^4 \\ &\quad + (a+c)^4 + (a-c)^4 + (b+d)^4 + (b-d)^4 \\ &\quad + (a+d)^4 + (a-d)^4 + (b+c)^4 + (b-c)^4 \end{aligned}$$

By Theorem 46, every integer of the form $6x^2$ can be expressed as the sum of 12 fourth powers (by the identity above).

Every positive integer can be written in the form $6k+r$ with k a nonnegative integer and $0 \leq r \leq 5$. Thus by Theorem 46 there is a representation for k as a sum of 4 squares, hence $6k$ can be represented as a sum of 48 fourth powers.

Finally, $r = \overbrace{1^4 + \cdots + 1^4}^{r \text{ times}}$, and the result follows.

□