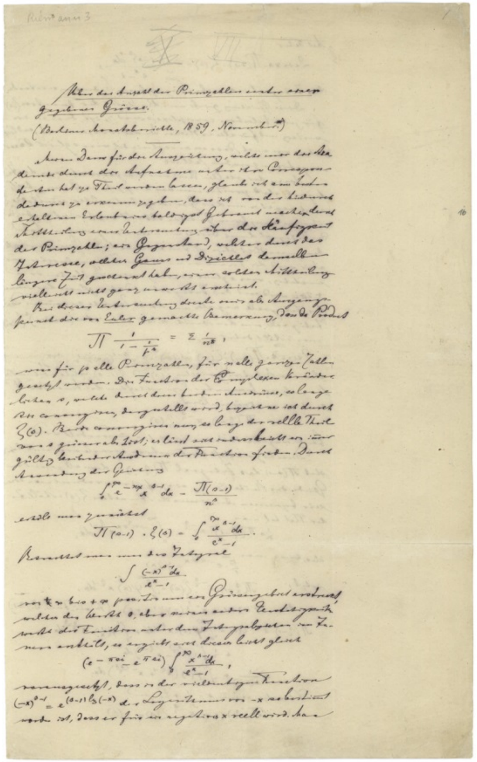
Riemann and Dirichlet: The distribution of primes



Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.

(Berliner Monatsberichte, 1859, November.)

Meinen Dank für die Auszeichnung, welche mir die Akademie durch die Aufnahme unter ihre Correspondenten hat zu Theil werden lassen, glaube ich am besten dadurch zu erkennen zu geben, dass ich von der hierdurch erhaltenen Erlaubniss baldigst Gebrauch mache durch Mittheilung einer Untersuchung über die Häufigkeit der Primzahlen; ein Gegenstand, welcher durch das Interesse, welches Gauss und Dirichlet demselben längere Zeit geschenkt haben, einer solchen Mittheilung vielleicht nicht ganz unwerth erscheint.

Bei dieser Untersuchung diente mir als Ausgangspunkt die von Euler gemachte Bemerkung, dass das Product

$$\Pi \frac{1}{1-\frac{1}{p^s}} = \Sigma \frac{1}{n^s},$$

wenn für p alle Primzahlen, für n alle ganzen Zahlen gesetzt werden. Die Function der complexen Veränderlichen s, welche durch diese beiden Ausdrücke, so lange sie convergiren, dargestellt wird, bezeichne ich durch $\zeta(s)$. Beide convergiren nur, so lange der reelle Theil von s grösser als 1 ist; es lässt sich indess leicht ein immer gültig bleibender Ausdruck der Function finden. Durch Anwendung der Gleichung

$$\int_0^\infty e^{-nx} x^{s-1}\,dx = \frac{\Pi(s-1)}{n^s}$$

erhält man zunächst

$$\Pi(s-1)\,\zeta(s) = \int_0^\infty \frac{x^{s-1}\,dx}{e^x-1}.$$

Betrachtet man nun das Integral

$$\int \frac{(-x)^{s-1}\,dx}{e^x-1}$$

von $+\infty$ bis $+\infty$ positiv um ein Grössengebiet erstreckt, welches den Werth 0, aber keinen andern Unstetigkeitswerth der Function unter dem Integralzeichen im Innern enthält, so ergiebt sich dieses leicht gleich

$$(e^{-\pi si} - e^{\pi si}) \int_0^\infty \frac{x^{s-1}\,dx}{e^x-1},$$

vorausgesetzt, dass in der vieldeutigen Function $(-x)^{s-1} = e^{(s-1)\log(-x)}$ der Logarithmus von $-x$ so bestimmt worden ist, dass er für ein negatives x reell wird. Man

Bernhard Riemann

- Bernhard Riemann (1826-1866) was a German mathematician who made important contributions to number theory, complex analysis and differential geometry.
- We do not have the time or space to describe all the discoveries he made in his short life but will highlight how he connected complex analysis and number theory.
- You will recall Gauss's conjecture about the distribution of primes, namely that if π(x) denotes the number of primes up to x, then π(x) ~ x/log x as x tends to infinity.
- Though Riemann did not prove this conjecture, he indicated how to do it by outlining a method of attack.

You may recall that Gauss made a more precise conjecture : as x tends to infinity,

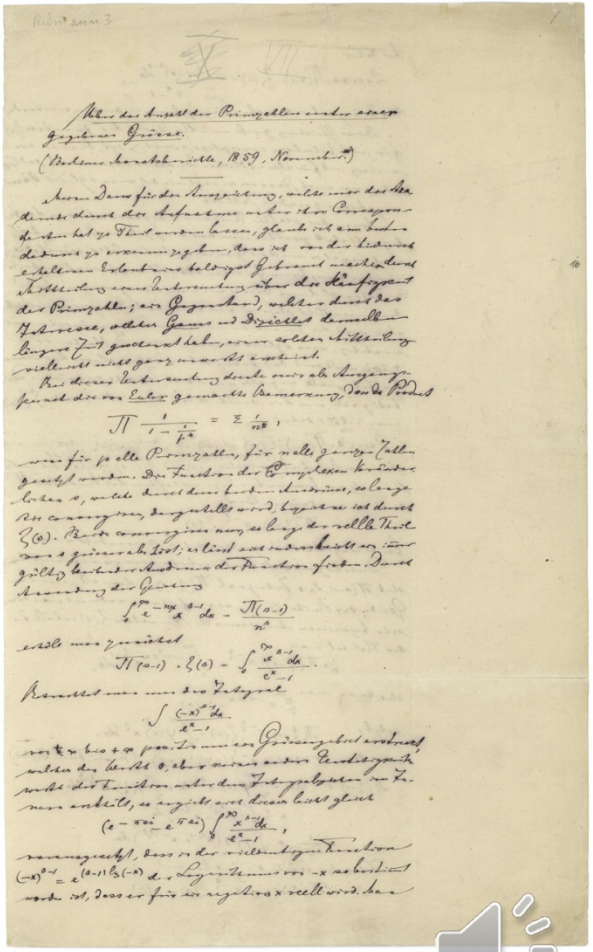
$$\pi(x) \sim \int_2^x \frac{dt}{\log t}.$$

Riemann showed how one can prove this.

The Riemann zeta function

$$\varsigma(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s} + \cdots,$$

- Riemann showed that this function which converges for Re(s)>1, can be extended to the entire complex plane such that ς(s) – 1/(s-1) is an entire function.
- The fact that ς(s) can also be expressed as an infinite product over primes now leads one to translate questions about prime numbers to properties of the zeta function.
- In particular, he stressed that studying the zeta function as a function of a complex variable will lead to a proof of Gauss's conjecture.
- He wrote this up in an 1859 paper and didn't have time to develop his idea because he died from tuberculosis at the age of 40.



Riemann 3

Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.

(Berliner Monatsberichte, 1859. November.)

Meinen Dank für die Auszeichnung, welche mir die Akademie durch die Aufnahme unter ihre Correspondenten hat zu Theil werden lassen, glaube ich am besten dadurch zu erkennen zu geben, dass ich von der hierdurch erhaltenen Erlaubniss baldigst Gebrauch mache durch Mittheilung einer Untersuchung über die Häufigkeit der Primzahlen; ein Gegenstand, welcher durch das Interesse, welches Gauss und Dirichlet demselben längere Zeit geschenkt haben, einer solchen Mittheilung vielleicht nicht ganz unwerth erscheint.

Bei dieser Untersuchung diente mir als Ausgangspunkt die von Euler gemachte Bemerkung, dass das Product

$$\prod \frac{1}{1-\frac{1}{p^s}} = \Sigma \frac{1}{n^s},$$

wenn für p alle Primzahlen, für n alle ganzen Zahlen gesetzt werden. Die Function der complexen Veränderlichen s, welche durch diese beiden Ausdrücke, so lange sie convergiren, dargestellt wird, bezeichne ich durch $\zeta(s)$. Beide convergiren nur, so lange der reelle Theil von s grösser als 1 ist; es lässt sich indess leicht ein immer gültig bleibender Ausdruck der Function finden. Durch Anwendung der Gleichung

$$\int_0^\infty e^{-nx} x^{s-1}\,dx = \frac{\Pi(s-1)}{n^s}$$

erhält man zunächst

$$\Pi(s-1)\cdot\zeta(s) = \int_0^\infty \frac{x^{s-1}\,dx}{e^x-1}.$$

Betrachtet man nun das Integral

$$\int \frac{(-x)^{s-1}\,dx}{e^x-1}$$

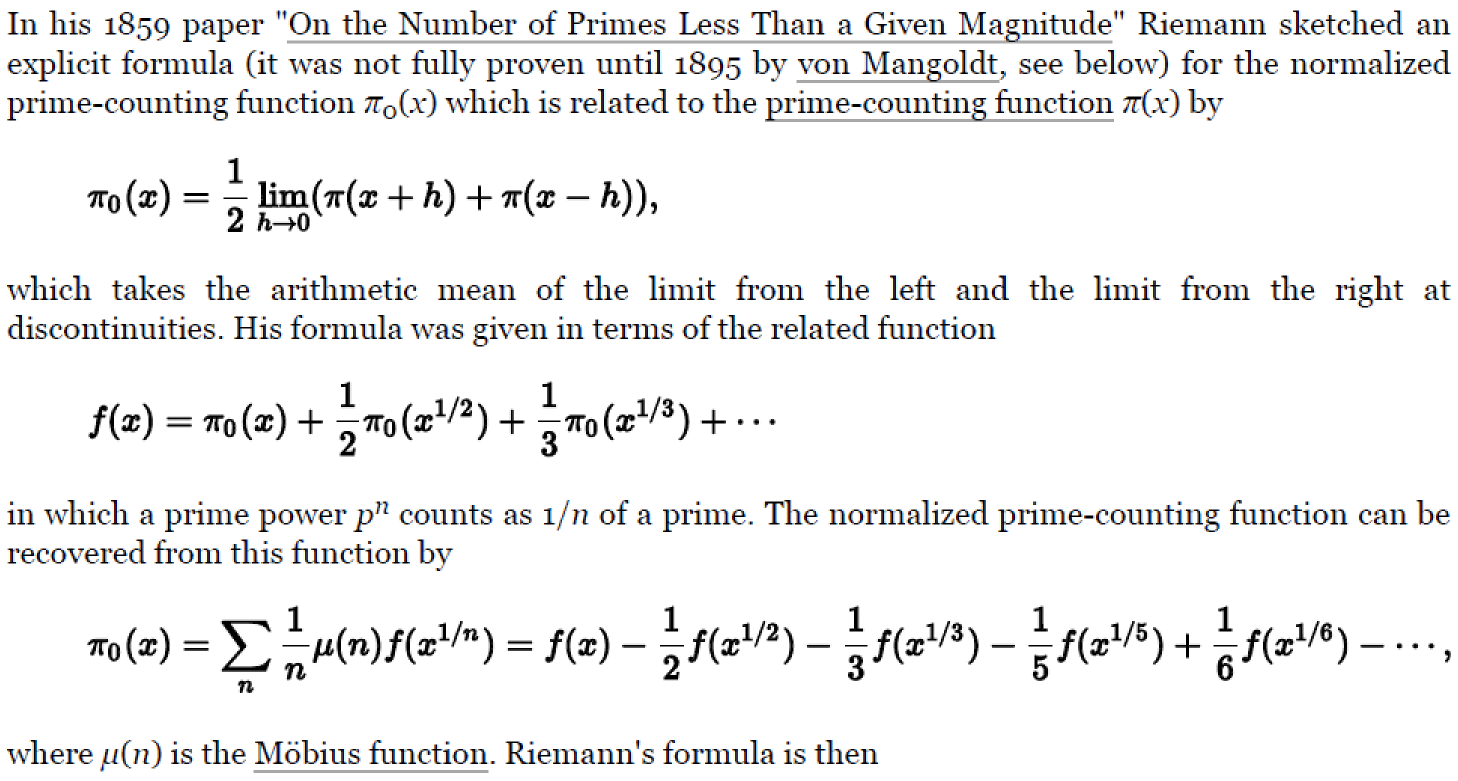
von $+\infty$ bis $+\infty$ positiv um ein Grössengebiet erstreckt, welches den Werth 0, aber keinen andern Unstetigkeitspunkt der Function unter dem Integralzeichen im Innern enthält, so ergiebt sich dieses leicht gleich

$$(e^{-\pi si} - e^{\pi si})\int_0^\infty \frac{x^{s-1}\,dx}{e^x-1},$$

vorausgesetzt, dass in der vieldeutigen Function $(-x)^{s-1} = e^{(s-1)\log(-x)}$ der Logarithmus von $-x$ so bestimmt worden ist, dass er für ein negatives x reell wird. Man

Riemann's explicit formula

- Recall the logarithmic integral which we already met in Gauss's conjecture: li(x)= $\int_2^x \frac{dt}{\log t}$.



In his 1859 paper "On the Number of Primes Less Than a Given Magnitude" Riemann sketched an explicit formula (it was not fully proven until 1895 by von Mangoldt, see below) for the normalized prime-counting function $\pi_0(x)$ which is related to the prime-counting function $\pi(x)$ by

$$\pi_0(x) = \frac{1}{2}\lim_{h\to 0}(\pi(x+h)+\pi(x-h)),$$

which takes the arithmetic mean of the limit from the left and the limit from the right at discontinuities. His formula was given in terms of the related function

$$f(x) = \pi_0(x) + \frac{1}{2}\pi_0(x^{1/2}) + \frac{1}{3}\pi_0(x^{1/3}) + \cdots$$

in which a prime power p^n counts as $1/n$ of a prime. The normalized prime-counting function can be recovered from this function by

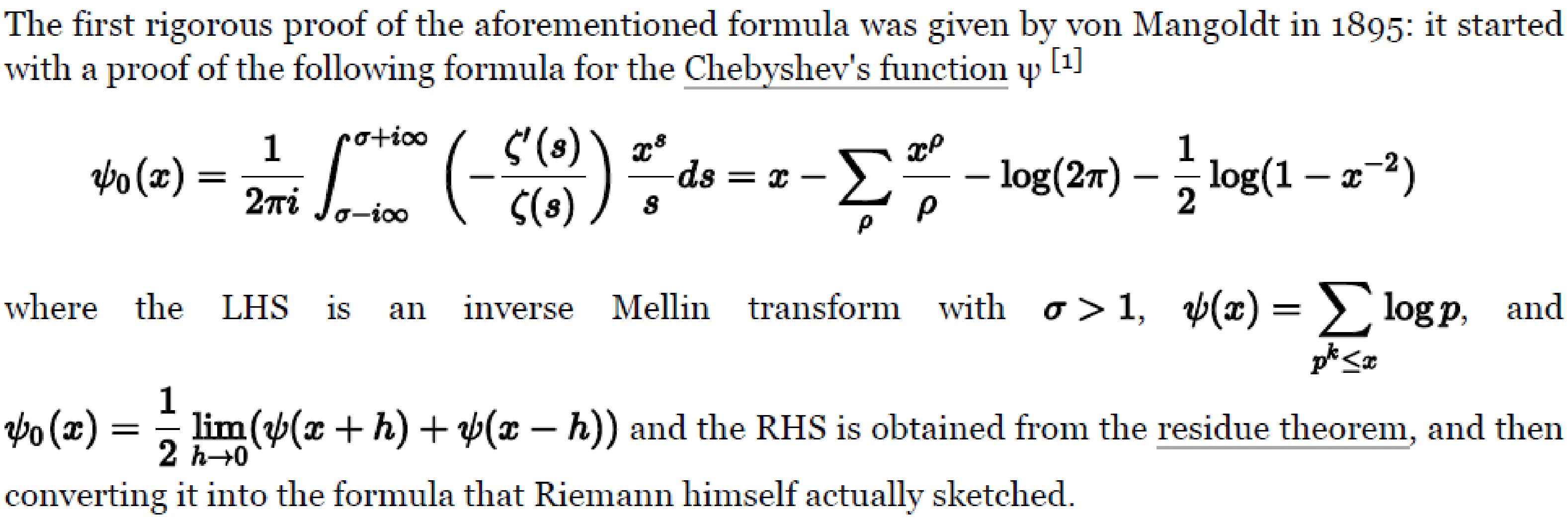
$$\pi_0(x) = \sum_n \frac{1}{n}\mu(n)f(x^{1/n}) = f(x) - \frac{1}{2}f(x^{1/2}) - \frac{1}{3}f(x^{1/3}) - \frac{1}{5}f(x^{1/5}) + \frac{1}{6}f(x^{1/6}) - \cdots,$$

where $\mu(n)$ is the Möbius function. Riemann's formula is then

$$f(x) = \operatorname{li}(x) - \sum_\rho \operatorname{li}(x^\rho) - \log(2) + \int_x^\infty \frac{dt}{t(t^2-1)\log(t)}$$

Von Mangoldt’s explicit formula

- Riemann’s explicit formula is quite messy since he was dealing with π(x).
- He never gave a rigorous proof of his formula. This was done later by von Mangoldt.
- It is better to deal with a slightly modified function ψ(x):



The first rigorous proof of the aforementioned formula was given by von Mangoldt in 1895: it started with a proof of the following formula for the Chebyshev's function ψ [1]

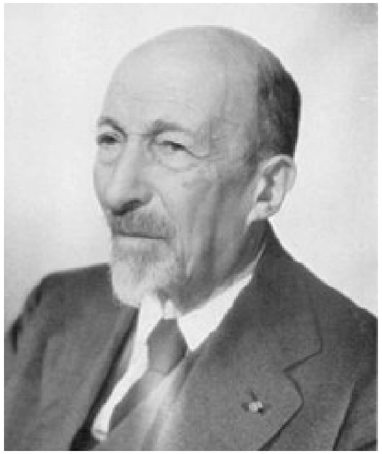
$$\psi_0(x) = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^s}{s}\,ds = x - \sum_{\rho}\frac{x^\rho}{\rho} - \log(2\pi) - \frac{1}{2}\log(1-x^{-2})$$

where the LHS is an inverse Mellin transform with $\sigma > 1$, $\psi(x) = \sum_{p^k \le x} \log p$, and $\psi_0(x) = \frac{1}{2}\lim_{h\to 0}(\psi(x+h)+\psi(x-h))$ and the RHS is obtained from the residue theorem, and then converting it into the formula that Riemann himself actually sketched.

What is remarkable about this formula is that the left hand side is essentially the sum of the logarithms of primes less than x, and the right hand side is a sum of over the zeros of the Riemann zeta function, showing how these two worlds are intimately connected.

The prime number theorem

- The prime number theorem was finally proved in 1896 by Jacques Hadamard and Charles de la Vallee Poussin (independently) using the program outlined by Riemann.
- Their work underscored the importance of complex analysis in number theory.

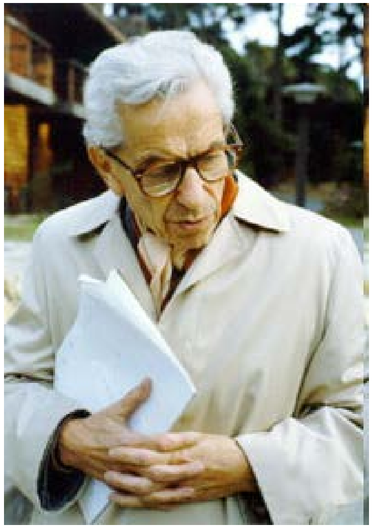


More precisely, the prime number theorem is the assertion that as x tends to infinity, π(x) is asymptotic to

$$\int_2^x \frac{dt}{\log t}$$

An essential ingredient in their proof is The assertion that ς(s)≠0 for Re(s)=1.

The Riemann hypothesis



- In his famous 1859 paper, Riemann made the (now famous) conjecture that all zeros of ς(s) in the region 0≤Re(s)≤1 lie on the line Re(s)=1/2.
- This is called the Riemann hypothesis and is still unsolved as of today.
- Hadamard and de la Vallee Poussin showed that there are no zeros on Re(s)=1 in their proof of the prime number theorem.
- In the 1930's, Norbert Wiener showed that π(x)~x/log x implies that ς(s)≠0 for Re(s)=1.
- Thus, the asymptotic for π(x) is equivalent to the non-vanishing of the zeta function on the line Re(s)=1.
- Since, the zeta function involves complex analysis, it was widely believed in the 1940's that the prime number theorem cannot be proved without using the zeta function.
- But this was refuted in 1949 when Atle Selberg and Paul Erdos showed that there is an "elementary proof" without using the zeta function.

Dirichlet and primes in arithmetic progressions

- An important development in prime number theory that preceded the work of Riemann lies in the work of Dirichlet whose work we now describe.
- Peter Gustav Lejeune Dirichlet (1805-1859) is credited with the creation of analytic number theory. Sadly, he died at the age of 54 of a heart attack.
- Dirichlet had Gauss and Riemann among his illustrious teachers at Gottingen, and after Gauss's death, succeeded him as Professor.
- In 1837, he showed that if m is any natural number and a is coprime to m, then there are infinitely many primes p≡a(mod m).
- This generalizes Euclid's famous theorem of the infinitude of primes.
- Dirichlet modified Euler's proof of the infinitude of primes by injecting group theory into number theory.

Primes ≡ 3 mod 4

- Let us look at a special case of Dirichlet's theorem, namely the case m=4.
- Here the two coprime residue classes are 1 and 3 (mod 4). Observe that any odd number is in one of these classes.
- Dirichlet's theorem says there are infinitely many primes in each of these residue classes.
- The case of 3 (mod 4) is easy and we can mimic Euclid. Suppose there are only finitely many such primes, $p_1, \dots, p_k$ (say).
- Consider $N=4p_1 \dots p_k -1$. This being an odd number we see that any prime divisor is either ≡1 or 3 (mod 4).
- If all the prime divisors of N are ≡1 (mod 4), then N would be ≡1 (mod 4) which it isn't. Therefore N has a prime ≡3 (mod 4) which is different from our earlier ones.
- This proof mimics Euclid's proof, but such a proof doesn't work for the residue class 1 (mod 4).

Primes ≡1 (mod 4)

- We can attempt a similar proof to show there are infinitely many primes $p \equiv 1 \pmod 4$. Suppose there are only finitely many $p_1, \ldots, p_k$ (say).
- Now consider $N= 4(p_1\ldots p_k)^2 +1$. This number being odd has prime divisors either congruent to 1 or 3 (mod 4).
- We claim it has no prime divisor congruent to 3 (mod 4).
- We prove this by contradiction. Suppose q is a prime ≡3 (mod 4) that divides N.
- Then reducing N (mod q) gives $x^2 \equiv -1 \pmod q$ where $x=2p_1\ldots p_k$.
- But by Fermat's little theorem, $x^{q-1}\equiv 1 \pmod q$ so raising both sides of our congruence to the power $(q-1)/2$ gives $1\equiv(-1)^{(q-1)/2}$.
- Now q is a prime of the form 4t+3 and so $(q-1)/2$ is of the form 2t+1 which is odd.so that $(-1)^{(q-1)/2} =-1$ which means 4 divides 2, a contradiction.
- Therefore all prime divisors of N are of the form 4t+1 and clearly N is coprime to $p_1, \ldots, p_k$ which is a contradiction.

Coprime residue classes mod q

- Even elementary attempts at proving Dirichlet's theorem require some knowledge of group theory.
- Here I want to recall one of the most basic facts due to Lagrange which I will use in the next slides to give a reasonably elementary proof that for any prime q, there are infinitely many primes $p\equiv 1$(mod q).
- Let us look at the non-zero residue classes (mod q). There are (q-1) such classes. Let g be such a class. We define the order of g to be the smallest natural number t such that $g^t \equiv 1$ (mod q).
- Such an element exists because by Fermat's little theorem, $g^{q-1} \equiv 1$ (mod q). We denote the order of g by o(g).
- Lagrange's theorem in this case is that o(g) divides q-1 for any non-zero residue class g.
- The proof makes use of the division algorithm. Since $o(g)\le q-1$, we can write $q-1 = o(g)k+b$ where $0\le b<o(g)$. But now by Fermat's little theorem, $1\equiv g^{q-1} \equiv g^{o(g)k}\, g^b$ (mod q). But $g^{o(g)} \equiv 1$ by definition, so we deduce $g^b\equiv 1$. If $b\neq 0$, we have a contradiction, so b must be zero and o(g) divides q-1.
- This is a special case of a very general theorem of Lagrange that says the order of an element of finite group divides the order of the group.

Dirichlet's proof and cyclotomic polynomials

- Dirichlet's proof in the general case developed a new branch of mathematics called character theory and Euler's proof was amenable to the implementation of character theory, whereas the ad hoc style proof of Euclid or the case $m=4$ doesn't generalize.
- However, there is one case that can be proved without character theory and that is the case if $m=q$ is prime and we are considering primes in the residue class 1 (mod q).
- The proof uses the q-th cyclotomic polynomial which we already met in the lecture on Gauss.
- Recall that this polynomial is $f(x)= (x^q-1)/(x-1)=x^{q-1} + \ldots + x + 1$.
- We suppose there are only finitely many primes $p_1, \ldots, p_k \equiv 1 (\text{mod } q)$ and let N be the product of these primes along with q.
- Consider f(N). If p is a prime dividing f(N), then p divides $N^q -1$ and clearly $p \neq q$.
- Now N is not congruent to 1 (mod p) for otherwise, $0 \equiv N^{q-1} + \ldots + N + 1 \equiv q$ (mod p) which means $p = q$. This contradicts $p \neq q$.
- Thus N has order q mod p. By Lagrange's theorem, q divides p-1.
- That is, $p \equiv 1 (\text{mod } q)$.Thus any prime divisor of f(N) has to be congruent to 1 (mod q).
- Now in this proof, we used the q-th cyclotomic polynomial for a prime q.
- One can adapt this proof to show infinitude of primes $\equiv 1$ (mod m) for any m.
- We will not do that here since it involves some detailed discussion of the general m-th cyclotomic polynomial, a topic we have not covered and perhaps you have not seen in an earlier course. Our treatment here should give you some idea of the depth and beauty of this theorem.