Dirichlet's Theorem

Daniel Harrer (ZetaX)

24. Februar 2011

Symbols and used theorems

$\mathbb{Z}$: the integers.
$\mathbb{N}$: the set $\{1, 2, 3, ...\}$ of positive integers.
$\mathbb{N}_0$: the set $\{0, 1, 2, ...\}$ of non-negative integers.
$\mathbb{P}$: the primes in $\mathbb{N}$.
$\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_p$: the (field of) residues $\mod p$, p prime.
A sums and products of 0 numbers are always set to 0 respectively 1.

Theorem 1. ***(Unique factorisation)***
For all $n \in \mathbb{N}$ there are (up to reordering) uniquely determined primes $q_1, q_2, ..., q_k$ such that $n = q_1 q_2 ... q_k$.

Theorem 2. ***(Binomial theorem)***
$(a+b)^n = \sum_{k=0}^{n} a^k b^{n-k} \binom{n}{k}$ *for all $a, b \in \mathbb{C}$.*

Preface

A lot of primes

A very fundamental result is

Theorem 3. *There are infinitely many primes (in $\mathbb{N}$).*

There are a lot of proofs for this theorem, but probably the oldest and most famous one is:

Proof. (Euklid) Assume that there are only finitely many primes, call them $p_1, p_2, ..., p_n$. Consider their product $P = p_1 \cdot p_2 \cdot ... \cdot p_n$. Since $P + 1 > 1$, there is (using theorem 1) at least one prime q dividing $P + 1$. But this q is different from all primes p_i because q and P are coprime, so q was not in the initial set, a contradiction. □

The proof above was known thousands of years ago. But in the $18th$ century Euler showed that there is a much stronger result:

Theorem 4. *The sum* $\sum_{p\in\mathbb{P}} \frac{1}{p}$ *diverges, in other words: grows to* ∞.

Proof. Every $k \in \mathbb{N}$ can be written as $k = t \cdot s^2$ with t not divisible by a square > 1. This gives the inequality

$$\sum_{k=1}^{n} \frac{1}{k} \leq \prod_{\substack{p\in\mathbb{P}\\ p\leq n}} \left(1 + \frac{1}{p}\right) \sum_{s=1}^{n} \frac{1}{s^2}.$$

Since $\frac{1}{s^2} \leq \frac{1}{s(s-1)} = \frac{1}{s-1} - \frac{1}{s}$ for $s \geq 2$ we get $\sum_{s=1}^{n} \frac{1}{s^2} \leq 1 + \sum_{s=2}^{n} \frac{1}{s-1} - \frac{1}{s} = 2 - \frac{1}{n} \leq 2$. Together with the easy to verify property $1 + x \leq e^x$ for all $x \in \mathbb{R}$ this yields

$$\sum_{k=1}^{n} \frac{1}{k} \leq \prod_{\substack{p\in\mathbb{P}\\ p\leq n}} \left(1 + \frac{1}{p}\right) \sum_{s=1}^{n} \frac{1}{s^2} \leq 2 \prod_{\substack{p\in\mathbb{P}\\ p\leq n}} \left(1 + \frac{1}{p}\right) \leq 2 \cdot \prod_{\substack{p\in\mathbb{P}\\ p\leq n}} e^{\frac{1}{p}} = 2 \cdot e^{\sum \frac{1}{p}}$$

where the last sum also runs over all primes $p \leq n$. To show that $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverges, it now suffices to show that $\sum_{k=1}^{\infty} \frac{1}{k}$ diverges. But the latter one is a well known property, shown by the following since for all $n \geq 2^m$ we have:

$$\sum_{k=1}^{n} \frac{1}{k} \geq \sum_{k=1}^{2^m-1} \frac{1}{k} = \sum_{s=0}^{m-1} \sum_{k=2^s}^{2^{s+1}-1} \frac{1}{k} \geq \sum_{s=0}^{m-1} \sum_{k=2^s}^{2^{s+1}-1} \frac{1}{2^{s+1}} = \sum_{s=0}^{m-1} \frac{1}{2} = \frac{m}{2},$$

giving the divergence because m can be chosen arbitrary large. □

Dirichlet's Theorem

It is a very natural question to ask if a given sequence contains infinitely many primes or not. One of the easiest cases seems to be an arithmetic sequence $a, a + m, a + 2m, a + 3m, ...$ In other words, it is asked for a lot of primes $p \equiv a \mod m$.
If $d > 1$ is a common divisor of a and m, then all terms of this sequence are divisible by d, thus there can be only a finite set of primes in the sequence; in fact, the only prime can be d itself. But for $\gcd(a, m) = 1$, Dirichlet was able to prove that there are a lot of primes by giving a much stronger result:

Theorem 5. *Let* $\gcd(a,m)=1$*, then there are infinitely many primes* $\equiv a \mod m$*. More exactly, the sum* $\sum_{\substack{p\in\mathbb{P}\\ p\equiv a \mod m}} \frac{1}{p}$ *diverges and the primes are "equally distributed" into the different residues a coprime to* m*.*

All known proofs for this(these) theorem(s) require a lot of real or complex analysis, especially concerning the so-called L-series $L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ with $\chi:\mathbb{N}\to\mathbb{C}$ some function (for those who know the term: χ is a "character" from $(\mathbb{Z}/n\mathbb{Z})^*$ to $\mathbb{C}$ here).
It's an interesting question whether there exist more elementary proofs for special cases, possibly based on the ideas of Euklid's proof of theorem 3 (note that Dirichlet's idea is more related to Euler's one).
Our goal is now to prove it for the cases $a=1$ and $a=-1$ and arbitrary m.

Special cases

Let's try some very special m, namely $m=4$ and $m=3$.

Theorem 6. *There are* ∞ *many primes* p *with:*

a) $p\equiv -1 \mod 4$*.*

b) $p\equiv -1 \mod 3$*.*

c) $p\not\equiv 1 \mod m$ *for any fixed* $m\in\mathbb{N}$ *in general.*

Proof. It's clear that c) implies a) and b) since there are only the residue classes 1 and $-1 \mod 3,4$, so we just need to prove this one.
Assume like before that there are only finitely many primes $p_1,p_2,...,p_n\not\equiv 1 \mod m$. Then let P be their product and consider the number $mP-1$: All its prime divisors $q_1,q_2,...,q_k$ are $\equiv 1 \mod m$ because they are coprime to P, thus different from the initial primes p_i. But $1=1\cdot 1\cdot ...\cdot 1\equiv q_1\cdot q_2\cdot ...\cdot q_k=mP-1\equiv -1 \mod m$, being impossible for $m\geq 3$. So we got our contradiction again. □

Another idea has to be used to attack $\equiv 1 \mod m$, which we will do first for $m=4$:

Theorem 7. *There are* ∞ *many primes* $\equiv 1 \mod 4$*.*

Before we can tackle this one, we need the following

Lemma 1. *Let* p *be a prime dividing* x^2+1 *for some* $x\in\mathbb{Z}$*. Then* $p=2$ *or* $p\equiv 1 \mod 4$*.*

Proof. Assuming that $p \equiv -1 \mod 4$, so that $\frac{p-1}{2}$ is odd, we want to bring $p|x^2+1$ to something absurd. We know that $x^2 \equiv -1 \mod p$, so we get using Fermat's little theorem:

$$1 \equiv x^{p-1} \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \mod p,$$

our so much desired contradiction. □

Now back to theorem 7:

Proof. Yes, it gets boring, but for the sake of proving the theorem assume that there are only finitly many primes $p_1, p_2, ..., p_n \equiv 1 \mod 4$ and let P be their product. Then consider any prime divisor q of $(2P)^2+1$: q is clearly odd, coprime to P, and $\equiv 1 \mod 4$ by the Lemma, done. □

Requirements

Before we can give a general proof like that of theorem 7, we need some more stuff.

Definition 1. *Let p be prime and $p \nmid a \in \mathbb{Z}$. Then the smallest $k \in \mathbb{N}$ with $a^k \equiv 1 \mod p$ is called the order of $a \mod p$ and is denoted by $\mathrm{ord}_p(a)$ (note that the order always exists since $a^{p-1} \equiv 1 \mod m$ by Fermat's little theorem).*
This definition can still be made if p is any integer coprime to a, but we will need only the case p prime.

A very powerful principle with striking simplicity is the next

Lemma 2. ***(Order lemma*** $\mod p$***)***
Take a, p as in the above definition and let k be given such that $a^k \equiv 1 \mod p$. Then $\mathrm{ord}_p(a)|k$. This holds also for any p, but will, as said before, not be required.

Proof. Take division with remainder to write $k = q \cdot \mathrm{ord}_p(a) + r$, $0 \leq r < \mathrm{ord}_p(a)$. By the definitions we get $a^r \equiv a^k \cdot a^{-q \cdot \mathrm{ord}_p(a)} \equiv 1 \cdot 1^{-q} \equiv 1 \mod p$. We can't have $r \neq 0$ since then $0 < r < \mathrm{ord}_p(a)$ and $a^r \equiv 1 \mod p$, contradicting that $\mathrm{ord}_p(a)$ is the minimal positive integer with $a^{\mathrm{ord}_p(a)} \equiv 1 \mod p$. So $r = 0$ and $k = q \cdot \mathrm{ord}_p(a)$, proving the lemma. □

A very useful type of polynomial, closely related to orders, is now given by

Definition 2. *Set $\zeta_n = e^{\frac{2 \cdot \pi i}{n}}$. Then the n-th cyclotomic polynomial $\Phi_n(x)$ is defined by*

$$\Phi_n(x) = \prod_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} (x - \zeta_n^k).$$

Theorem 8. *The cyclotomic polynomials $\Phi_n(x)$ fulfill the fundamental property*

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

Proof. Since both sides are monic polynomials (their leading coefficient is 1), it suffices to show that they have the same complex roots. The roots of $x^n - 1$ are $e^{\frac{2\cdot\pi\cdot k}{n}}$ for $k = 0, 1, 2, ..., n-1$, thus let $\zeta = e^{\frac{2\cdot\pi\cdot k}{n}}$ be a root of that polynomial.
Let $d = \gcd(k, n)$ and $n = d \cdot n'$, $k = d \cdot k'$. By that we have $\zeta = e^{\frac{2\cdot\pi\cdot k}{n}} = e^{\frac{2\cdot\pi\cdot dk'}{dn'}} = e^{\frac{2\cdot\pi\cdot k'}{n'}}$ and $\gcd(k', n') = 1$, thus ζ being a root of $\Phi_{n'}(x)$ by definition. This shows that any root of the left hand side (LHS from now) is one of the right hand side (RHS from now).
Now let ζ be a root of the RHS, let's say $\Phi_{n'}(\zeta) = 0$ for $n'|n$. By this $n = d \cdot n'$ for some integer d and because of that $\zeta^n = \left(\zeta^{n'}\right)^d = 1^d = 1$, so it is a root of the LHS. □

Theorem 9. *The coefficients of the $\Phi_n(x)$ are integers.*

Proof. We will use induction on n to show that $\Phi_n(x)$ is a polynomial with integers as coefficients. Clearly $\Phi_1(x) = x - 1$, so it is as nice as we want it to be. Thus assume the theorem to be proven for all $m < n$, so especially for the divisors $d \neq n$ of n. By that $\prod_{d|n, d\neq n} \Phi_d(x)$ is a monic polynomial with integer coefficients.
By theorem 8 we have $\Phi_n(x) = \dfrac{x^n - 1}{\prod_{d|n, d\neq n} \Phi_d(x)}$, and by making standard division of polynomials, we see that $\Phi_n(x)$ has indeed integers as coefficients. □

Primes $\equiv 1 \mod n$

Now the time has come to prove the infinity of primes $\equiv 1 \mod m$ for any m.
We will use cyclotomic polynomials for this, so let's start collecting their properties $\mod p$:

Lemma 3. *Let $n > 0$ and a be integers, p prime, and $g(x)$ a polynomial with integer coefficients. If $x^n - 1 \equiv (x - a)^2 \cdot g(x) \mod p$, then $p|n$ (polynomials $\mod p$ are archieved and handled by reducing all coefficients $\mod p$).*

Proof. Set $y = x - a$, then we have $(y + a)^n - 1 \equiv y^2 \cdot g(y + a) \mod p$. Expand the LHS by the binomial theorem to be $y^n + ... + n \cdot a^{n-1}y + (a^n - 1)$. From the factor y^2 on the RHS we get that the constant and linear coefficient are $0 \mod p$, thus $a^n \equiv 1 \mod p$ and $n \cdot a^{n-1} \equiv 0 \mod p$. So we get $n \cdot 1 \equiv n \cdot a^n \equiv (n \cdot a^{n-1}) \cdot a \equiv 0 \cdot a \equiv 0 \mod p$.
This means nothing else than $p|n$. □

Continuing with a way to construct primes we want:

Theorem 10. ***(Main theorem for cyclotomic polynomials** $\mod p$**)***
If p is a prime divisor of $\Phi_n(a)$ with $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, then $p|n$ or $p \equiv 1 \mod n$.

Proof. Let $o = \mathrm{ord}_p(a)$ (it exists because $p|\Phi_m(a) \Rightarrow p|a^m - 1 \Rightarrow p \nmid a^m \Rightarrow p \nmid a$). Assume also that $o \neq n$. By the order lemma we have $o|n$. Using that

$$x^n - 1 = \Phi_n(x) \cdot (x^o - 1) \cdot \prod_{\substack{d|n,\ d\nmid o \\ d\neq n}} \Phi_d(x)$$

(theorem 8) together with $\Phi_n(x) \equiv (x-a) \cdot g(x) \mod p$ and $x^o - 1 \equiv (x-a) \cdot h(x) \mod p$ (the last two because $x \equiv a \mod p$ is a root $\mod p$ of the LHSes), we are led to $x^n - 1 \equiv (x-a)^2 \cdot j(x) \mod p$ (with $j(x) = g(x) \cdot h(x) \cdot \prod_{\substack{d|n,\ d\nmid o \\ d \neq n}} \Phi_d(x)$). But this gives $p|n$ by lemma 3, proving this theorem. □

Theorem 11. *There are infinitly many primes* $\equiv 1 \mod n$.

Proof. For the fourth time now, we assume that there are only finitly many primes $p_1, p_2, ..., p_n \equiv 1 \mod n$. Then we take their product $P = p_1 \cdot p_2 \cdot ... \cdot p_n$ and choose q to be any prime divisor of $\Phi_n(k \cdot n \cdot P)$, where k is an integer just chosen big enough such that $\Phi_n(k \cdot n \cdot P) \neq \pm 1$ so that at least one prime divisor exists.
We have $q|(knP)^n - 1 \Rightarrow q \nmid (knP)^n \Rightarrow q \nmid n$ and $q \neq p_i$ (for all i). Because of $q \nmid n$ but $q|\Phi_n(k \cdot n \cdot P)$ when applying theorem 10, only the second case can happen there, giving that $q \equiv 1 \mod n$. Since q is different from all the p_i, this gives a contradiction. □

Fields, Orders and Polynomials

The approach of constructing a polynomial having, up to finitly many exceptions, only divisors $\equiv -1 \mod n$ fails for $n \geq 3$. Indeed it was proved that for given polynomial $f(x)$ the set of residues $a \mod n$ for which there are ∞ many primes $p \equiv a \mod n$ with $p|f(k)$ for some k build a group; especially, there will always be a lot of them $\equiv 1 \mod n$.
Our idea is now to construct a polynomial only (again up to some exceptions) archieving prime divisors $\equiv \pm 1 \mod n$.
This chapter is probably the most theoretic one: most stuff will not be needed again, and it is possible to show the important theorems only for the needed cases. But these proofs are neither shorter nor more intuitive, so we will handle the general case.

Lemma 4. *Let* $f(x) = a_k x^k + ... + a_0 + ... + a_{-k} x^{-k}$ *with* $a_k, a_{k-1}, ..., a_{-k+1}, a_{-k} \in \mathbb{Z}$ *be "symmetric", meaning that* $a_k = a_{-k}, ..., a_i = a_{-i}, ..., a_0 = a_0$ *or equivalently* $f(x) = f\left(\frac{1}{x}\right)$. *Then there exists a polynomial* $g(x)$ *(with integer coefficients) fulfilling* $g\left(x + \frac{1}{x}\right) = f(x)$.

Proof. This falls by induction:
It's clearly true for $k = 0$: we just take $g(x) = f(x) = a_0$.
Now let it be proved for alle $m < k$. We note that $\overline{g}(y) = a_k y^k$ fulfills

$$\overline{g}\left(x + \frac{1}{x}\right) = a_k \left(x + \frac{1}{x}\right)^k = a_k \sum_{i=0}^{k} \binom{k}{i} x^{k-i} \cdot x^{-i} = a_k x^k + a_{-k} x^{-k} + a_k \sum_{i=1}^{k-1} \binom{k}{i} x^{k-2i}.$$

Simple checking gives that the sum/difference (and the product, which we will not need) of symmetric terms is again symmetric. This leads to the symmetry (which also can be checked

directly) of

$$f(x) - \overline{g}\left(x + \frac{1}{x}\right) = \sum_{i=-(k-1)}^{k-1} a_i x^i - a_k \sum_{i=1}^{k-1} \binom{k}{i} x^{k-2i} = \sum_{i=-(k-1)}^{k-1} b_i x^i.$$

By induction hypothesis we have that $f(x) - \overline{g}\left(x + \frac{1}{x}\right) = \underline{g}\left(x + \frac{1}{x}\right)$ with a polynomial $\underline{g}(y)$. Thus we can take $g(y) = \overline{g}(y) + \underline{g}(y)$ as our polynomial. When we look back, we never left the integers by our operations since we never divided, just added, subtracted and multiplicated. □

The polynomial of our choice is more or less the following one:

Corollary 1. *For $n \in \mathbb{N}, n \geq 3$ there exists a polynomial $\pi_n(x)$ with integers as coefficients such that $x^{\frac{\varphi(n)}{2}} \cdot \pi_n\left(x + \frac{1}{x}\right) = \Phi_n(x)$. Here $\varphi(n)$ just denotes the degree of $\Phi_n(x)$.*

Proof. We remember that the roots of $\Phi_n(x)$ are ζ_n^k with $\gcd(k, n) = 1$, so we can pair up ζ_n^k and ζ_n^{-k}: If $\zeta_n^k = \zeta_n^{-k}$, then $\zeta_n^{2k} = 1$, thus $n|2k$; since n and k are coprime, we get $n|2$, contradicting $n \geq 3$. So we get that $\varphi(n)$ is indeed even. And we also get that

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq \frac{n}{2} \\ gcd(k,n)=1}} (x - \zeta_n^k)(x - \zeta_n^{-k}) = \prod_{\substack{1 \leq k \leq \frac{n}{2} \\ gcd(k,n)=1}} (x^2 - (\zeta_n^k + \zeta_n^{-k})x + 1),$$

yielding

$$r(x) := \frac{\Phi_n(x)}{x^{\frac{\phi(n)}{2}}} = \prod_{\substack{1 \leq k \leq \frac{n}{2} \\ gcd(k,n)=1}} (x - (\zeta_n^k + \zeta_n^{-k}) + x^{-1}),$$

giving $r(x) = r\left(\frac{1}{x}\right)$, so it is symmetric. Using the lemma, the result follows (we again never left the integers). □

As promised, we will prove the next theorems in a more general way. Thus we need fields and some related stuff.

Definition 3. *A field is a set K together with "addition" $+$ and "multiplication" $\cdot$ such that:*

- *there are 0_K and 1_K with $0_K + a = a = 1_K \cdot a$ for all $a \in K$.*
- *the known laws of associativity, commutativity and distrubitivity hold.*
- *for all $a \in K$ there is an $(-a) \in K$ with $a + (-a) = 0$.*
- *for all $a \in K \backslash \{0_K\}$ there is an $a^{-1} \in K$ with $a \cdot a^{-1} = 1_K$.*

To shorten things, for $n \in \mathbb{N}_0$ one often writes a^n for $\underbrace{a \cdot a \cdot ... \cdot a}_{n \text{ times}}$ and also often simplifies $a \cdot b$ to ab as one was always used to.

Thus fields are just things we can calculate in as we always did.
Examples are:

- the rationals $\mathbb{Q}$, the reals $\mathbb{R}$ or the complex numbers $\mathbb{C}$.
- the residues mod p for p prime; this field, from now denoted by $\mathbb{F}_p$, is more or less the only field we will need.

Some properties we will leave to the reader:

Properties 1. *For all $a \in K$:*

- $(-a) = (-1_K) \cdot a$.
- $0_K \cdot a = 0_K$.
- $(-1_K)^2 = 1_K$.
- $(-a)^2 = a^2$.
- $ab = 0 \implies a = 0$ *or* $b = 0$.

Definition 4. *Let $n \in \mathbb{Z}$. Then for any field K, n can be seen as some element n_K of K by $n_K := \underbrace{1_K + 1_K + ... + 1_K}_{n \text{ times}}$ if $n \geq 0$ and by $n_K := -(\underbrace{1_K + 1_K + ... + 1_K}_{(-n) \text{ times}})$ otherwise. An easy check gives $(-n)_K = -(n_K), (m+n)_K = m_k + n_K$ and $(m \cdot n)_K = m_k \cdot n_K$ for all $m, n \in \mathbb{Z}$ (one says that n_K is a ring homomorphism $\mathbb{Z} \to K$).*

From now on K will always be a field and we will often just write n instead of n_K for all integers when it is clear that we work in K.
Since integers can be seen as elements of K, especially the binomial coefficients can be seen so.

Theorem 12. ***(Binomial theorem)***
$(a+b)^n = \sum_{k=0}^{n} a^k b^{n-k} \binom{n}{k}$ *for all $a, b \in K$.*

Proof. This is proved exactly in the same way it is done for complex numbers inductively using $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. □

Corollary 2. *If p is a prime with $p_K = 0_K$, then $(a+b)^p = a^p + b^p$ for all $a, b \in K$.*

Proof. For $k = 1, 2, ..., p-1$ we have $p | \dfrac{p!}{k!(p-k)!} = \binom{p}{k}$ since the numerator is divisible by p, whereas the denominator is not. As a result $\binom{p}{k}_K = 0_K$ for those k. Now the binomial theorem finishes the proof by $(a+b)^p = \displaystyle\sum_{k=0}^{p} a^k b^{p-k} \binom{p}{k}_K = a^p + b^p$. □

Lemma 5. *If $x^2 = a$ has a solution $b \in K$, then all solutions are given by $x = \pm b$.*

Proof. Let b be a solution, then $b^2 = a$, thus $(-b)^2 = b^2 = a$, so $-b$ is also a solution.
Now let c be any solution, thus $c^2 - a = 0 \Leftrightarrow c^2 - b^2 = 0 \Leftrightarrow (c-b)(c+b) = 0$. If $c \neq b$, then $c - b \neq 0$, thus $(c-b)^{-1}$ exists, leading to
$b + c = (c-b)^{-1}(c-b)(c+b) = (c-b)^{-1} \cdot 0 = 0 \Rightarrow c = -b$, proving the lemma. □

We will now treat the lemmata we used and proved before in a more general way.

Definition 5. *Let $a \in K$, we call the smallest $k \in \mathbb{N}$ with $a^k = 1$ the order of a in K and write* $\mathrm{ord}_K(a)$ *for it. For those a for which there is no such k, we just write* $\mathrm{ord}_K(a) = \infty$.

Lemma 6. ***(order lemma)***
If $a \in K$ and $n \in \mathbb{N}$ such that $a^n = 1_K$, then $\mathrm{ord}_K(a) | n$.

Proof. The same as we did before when proving it $\mod p$:
Let $o = \mathrm{ord}_k(a)$ and take division with remainder to get $n = o \cdot q + r$ with $0 \leq r < o$. We get $a^r = a^{n - o \cdot q} = a^n \cdot (a^o)^{-q} = 1_K \cdot 1_K^{-q} = 1_K$, contradicting the minimality of o again if $r > 0$. Thus $r = 0$ and $o | n = qo$. □

Definition 6. *A polynomial over K, or sometimes also called a polynomial with coefficients in K, is a term of the type $a_k x^k + ... + a_1 x + a_0$ with $a_i \in K$ for all i. Polynomials can in general be added and multiplied exactly in the same way as we are used to in the complex numbers.*

Lemma 7. *Let $n \in \mathbb{N}$, $a \in K$, and $g(x)$ a polynomial with coefficients in K. If $x^n - 1 = (x-a)^2 g(x)$ as polynomials (so if $x^n - 1$ has a double root), then $n_K = 0_K$.*

Proof. We will just mimic the proof of lemma 3:
Set $y = x - a$, then $(y+a)^n - 1 = y^2 \cdot g(y+a)$. By expanding the LHS we get $y^n + ... + n_K \cdot a^{n-1} y + (a^n - 1)$, and the RHS gives $... + 0_K \cdot y + 0_K$, thus $n_K \cdot a^{n-1} = 0_K$ and $a^n = 1$, giving $n_K = n_K \cdot 1_K = n_K \cdot a^n = (n_K \cdot a^{n-1}) \cdot a = 0_K \cdot a = 0_K$. □

Since they have integer coefficients, we can treat the cyclotomic polynomials as polynomials over any field K. The same holds for all the other polynomials that will come and be viewed in some field.

Theorem 13. ***(main theorem on cyclotomic polynomials)***
Let $n \in \mathbb{N}$ again. If there is an $a \in K$ with $\Phi_n(a) = 0$, then $n_K = 0_K$ or $\mathrm{ord}_K(a) = n$.

Proof. Another one we can the proof copy for:
Assume that $o := \mathrm{ord}_K(a) \neq n$ (the order exists since $a^n = 1_K$). Then $o | n$ by the order lemma, so we get that

$$x^n - 1 = \Phi_n(x) \cdot (x^o - 1) \cdot \prod_{\substack{d|n,\ d \nmid o \\ d \neq n}} \Phi_d(x)$$

by theorem 8. Now by definition $\Phi_n(a) = 0_K$ and $a^o - 1 = 0_K$, thus $\Phi_n(x) = (x-a) \cdot g(x)$ and $x^o - 1 = (x-a) \cdot h(x)$ with $g(x), h(x)$ polynomials over K. But by this $x^n - 1 = (x-a)^2 \cdot j(x)$ with $j(x) = g(x) \cdot h(x) \cdot \prod_{\substack{d|n,\ d \nmid o \\ d \neq n}} \Phi_d(x)$.
Now using lemma 7 we get $n_K = 0_K$. □

If we have a field K, we can get another one containing K, e.g. by the following process:

Theorem 14. *If K is a field and $s \in K$ is such that $x^2 = s$ has no solution $x \in K$, then the set $L = K[\sqrt{s}]$ of numbers of type $a + b\sqrt{s}$ (with $a + b\sqrt{s} = c + d\sqrt{s}$ iff $a = c, b = d$) with the canonical and intuitive addition $(a + b\sqrt{s}) + (c + d\sqrt{s}) = (a + c) + (b + d)\sqrt{s}$ and multiplication $(a + b\sqrt{s}) \cdot (c + d\sqrt{s})[= ac + ad\sqrt{s} + b\sqrt{s}c + b\sqrt{s} \cdot d\sqrt{s}] = (ac + sbd) + (ad + bc)\sqrt{s}$ is again a field (with $\sqrt{s}^2 = s$). Additionally, K is a subset, $0_K = 0_L, 1_K = 1_L$ such that the new addition and multiplication are the old ones, too. One says K is a subfield of $K[\sqrt{s}]$ then. This especially implies that $n_K = 0$ iff $n_L = 0$, thus the property for an integer to be zero doesn't change.*

Proof. The easy checking of the properties of a field will be left to the reader:

- associativity, commutativity, distributivity are easy to check directly
- $0_L = 0 + 0\sqrt{s}$, $1_L = 1 + 0\sqrt{s}$
- $-(a + b\sqrt{s}) = (-a) + (-b)\sqrt{s}$, $(a + b\sqrt{s})^{-1} = (a(a - bs^2)^{-1}) + (-b(a - bs^2)^{-1})\sqrt{s}$ (here it has first to be shown that $a^2 - b^2 s = 0 \Leftrightarrow a = 0_K = b$).

K is a subfield by the numbers of type $a + 0\sqrt{s}$ (again just checking or simply intuition); the rest follows from this. □

Corollary 3. *If $2_K \neq 0_K$ (in fact, this restriction is not necessary), a quadratic equation $y^2 - py + q = 0$ has always exactly two solutions y_1, y_2 (counting roots with multiplicity, thus double roots are counted twice) in some field L "containing" K. Then also $y_1 + y_2 = a$ and $y_1 y_2 = b$ (Vieta's theorem).*

Proof. Exactly the same way one solves quadratic equations normally works (we need $2_K \neq 0_K$ to be able to divide by 2_K):

$$y^2 - ay + b = 0 \Leftrightarrow \left(y - \frac{a}{2_K}\right)^2 + b - \frac{a^2}{4_K} = 0 \Leftrightarrow \left(y - \frac{a}{2_K}\right)^2 = \frac{a^2}{4_K} - b.$$

Now if $x^2 = \frac{a^2}{4} - b$ has a solution $\sqrt{\frac{a^2}{4} - b} \in K$, we could proceed (here we use Lemma 5) with $y - \frac{a}{2_K} = \pm\sqrt{\frac{a^2}{4_K} - b} \Leftrightarrow y = \frac{a}{2_K} \pm \sqrt{\frac{a^2}{4_K} - b}$ and get our two solutions.
But also otherwise, we just consider $L = K\left[\sqrt{\frac{a^2}{4_K} - b}\right]$ and proceed then.
The other properties follow directly from expanding $(y - y_1)(y - y_2) = y^2 - (y_1 + y_2)y + (y_1 y_2)$, where y_1, y_2 are the solutions found before. □

Primes $\equiv -1 \mod n$

We are now able to construct the primes we want:

Theorem 15. *If $\pi_n(x) = 0$ has a root a in $\mathbb{F}_p$ (p prime), then $p|2n$ or $p \equiv \pm 1 \mod n$.*

Proof. We exclude $p = 2$ (we already have $p|2n$ then).
We are looking for an $b \neq 0$ with $b + \frac{1}{b} = a$ which happens iff $b^2 - ab + 1 = 0$. Let y_1 and y_2 be the solutions of $y^2 - ay + 1 = 0$ (either in $\mathbb{F}_p$ or in the field constructed in corollary 3); clearly $y = 0$ is not a solution, so we can always set $b = y_1$ to get $b + \frac{1}{b} = a$.
Now y_1^p is also a solution of the equation because using corollary 2 twice we get

$$0 = 0^p = (y_1^2 - ay_1 + 1)^p = \left(y_1^2\right)^p + (-ay_1 + 1)^p = \left(y_1^p\right)^2 - a^p y_1^p + 1^p = \left(y_1^p\right)^2 - ay_1^p + 1$$

(here we used that $a^p = a$, which is just Fermat's little theorem $a^p \equiv a \mod p$ since a is a standard residue $\mod p$). But $y^2 - ay + 1 = 0$ has just two solutions (corollary 3 again), thus $y_1^p = y_1$ or $y_1^p = y_2$. Before we start considering those two cases, we see (by definition of $\pi_n(x)$) that

$$\Phi_n(y_1) = y_1^{\frac{\varphi(n)}{2}} \pi_n\left(y_1 + \frac{1}{y_1}\right) = y_1^{\frac{\varphi(n)}{2}} \cdot 0 = 0.$$

Now using the main theorem on cyclotomic polynomials yields $p|n$ or $\operatorname{ord}(b) = n$. Assume that $\operatorname{ord}(b) = n$ from now on since otherwise ($p|n$) we are already done.

Case 1: $y_1^p = y_1$, thus $y_1^{p-1} = 1$, giving $n = \operatorname{ord}(y_1)|p - 1$ by the order lemma; but the latter means nothing else than $p \equiv 1 \mod n$.

Case 2: $y_1^p = y_2$. By Vieta's theorem (see corollary 3 once time) we have $y_1 y_2 = 1 \Rightarrow y_2 = \frac{1}{y_1}$. Using this gives $y_1^p = \frac{1}{y_1}$, implying $y_1^{p+1} = 1$. Again by the order lemma this gives $n|p + 1$, thus $p \equiv -1 \mod n$.

Now nothing more is to be shown. □

Corollary 4. *Let p be an odd (thus $p \neq 2$) prime divisor of $\pi_n(k)$ for some integer k. Then $p|n$ or $p \equiv \pm 1 \mod n$. (We will never use this corollary, but the theorem itself.)*

Our last problem is to "seperate" the divisors $\equiv 1 \mod n$ from those $\equiv -1 \mod n$. The polynomials $\pi_n(x)$ are not the best to do this, so we will construct a similar one.

Lemma 8. *There is a rational number t with $\pi_n(t) < 0$.*

Proof. By definition $\pi(\zeta_n + \zeta_n^{-1}) = \zeta_n^{\frac{\varphi(n)}{2}} \cdot \Phi_n(\zeta_n) = 0$, and $\zeta_n + \zeta_n^{-1} = \zeta_n + \overline{\zeta_n} = 2\mathfrak{Re}(\zeta_n) \in \mathbb{R}$. There are also no double roots of $\pi_n(x)$ in $\mathbb{C}$ because that would give double roots of $\Phi_n(x)$. Since $\pi_n(x)$ is a polynomial without double roots, it exactly changes its sign at it's roots. Since there is a real root (e.g. $2\mathfrak{Re}(\zeta_n)$), there is a change of sign and thus also a real number r with $\pi(r) < 0$. If we choose a rational t close enough to r (here we use that polynomials give continuous functions), we still have $\pi_n(t) < 0$. □

Definition 7. *We take fixed integers a_n, b_n such that $\pi_n\left(\frac{a_n}{b_n}\right) < 0$ (such a_n, b_n exist be the previous lemma) and take k to be the degree of $\pi_n(x)$.*
Then we define $\tau_n(x) := b_n^k \pi_n\left(x + \frac{a_n}{b_n}\right)$.
At last, we set $c_n = \tau_n(0) < 0$ and then $\Psi_n(x) := \dfrac{\tau(c_n x)}{-c_n}$.

Lemma 9. *The polynomials $\Psi_n(x)$ and $\tau_n(x)$ have integers as coefficients (especially c_n is an integer) and a positive leading coefficient.*

Proof. At first we prove that $\tau_n(x)$ has integers as coefficients:
Let $\pi_n(x) = r_k x^k + ... + r_1 x + r_0$ (all r_i are integers then) such that we have
$\tau_n(x) = b_n^k r_k \left(x + \frac{a_n}{b_n}\right)^k + ... + b_n^k r_1 \left(x + \frac{a_n}{b_n}\right) + b_n^k r_0$, so it suffices to show that the polynomials $b_n^k r_i \left(x + \frac{a_n}{b_n}\right)^i$ are integral for $i = 0, 1, ..., k$. But this follows directly from the binomial theorem:

$$b_n^k r_i \left(x + \frac{a_n}{b_n}\right)^i = b_n^k \sum_{m=0}^{i} r_k x^{i-m} a_n^m b_n^{-m} \binom{i}{m} = \sum_{m=0}^{i} b_n^{k-m} r_k x^{i-m} a_n^m \binom{i}{m},$$

where only integers occure (b_n^{k-m} is always an integer if $m \leq k$).
Let $\tau_n(x) = s_k x^k + ... + s_1 x + s_0$ with integers s_i now ($s_0 = \tau_n(0) = c_n$). Thus

$$\Psi_n(x) = \frac{\tau_n(c_n x)}{-c_n} = \frac{s_k c_n^k x^k}{-c_n} + ... + \frac{s_1 c_n x}{-c_n} + \frac{s_0}{-c_n},$$

has only integers as coefficients. Indeed $\frac{s_0}{-c_n} = -1 \in \mathbb{Z}$ and $\frac{s_i c_n^i}{-c_n} = -s_i c_n^{i-1} \in \mathbb{Z}$ for $i \geq 1$. The sign of the leading coefficient of $\Phi_n(x), \pi_n(x), \tau_n(x)$ and $\Psi_n(x)$ never changes (since $-c_n > 0$), thus it suffices to show that the one of $\Phi_n(x)$ is positive. But this is clear from the definition when we look back how they are defined. □

We just have to show that we didn't lose too much of the properties of $\pi_n(x)$.

Theorem 16. *Let p be a prime divisor of $\Psi_n(k)$ not dividing $2b_n c_n n$ (k some given integer). Then $p \equiv \pm 1 \mod n$.*

Proof. Lets work in the field $\mathbb{F}_p$ again. There we have $0 = \Psi_n(k) = \frac{\tau_n(c_n k)}{-c_n}$, thus $\tau_n(c_n k) = 0$, thus $b_n^k \pi_n\left(k + \frac{a_n}{b_n}\right) = 0$. But $b_n \neq 0$ in this field, so after multiplying with $\left(b_n^{-1}\right)^k$ this gives $\pi_n\left(k + \frac{a_n}{b_n}\right) = 0$. By theorem 15 we are finished. □

Now the goal is near. But we will need all the developed techniques.

Theorem 17. *There are infinitely many primes $p \equiv -1 \mod n$.*

Proof. We can assume n to be greater than 2 since otherwise it's trivial.
As expected, we assume that there are only finitely many such primes $p_1, ..., p_k \equiv -1 \mod n$ and call their product P. Lets take an integer k such that $\Psi_n(k \cdot 2b_n c_n nP) > 1$ (exists since the leading coefficient of $\Phi_n(x)$ is positive)and factor $\Psi_n(k \cdot 2b_n c_n nP) = q_1 q_2 ... q_m$ into not neccessary different primes q_i. We have $\Psi_n(k \cdot 2b_n c_n nP) \equiv \Psi_n(0) = \frac{\tau(0)}{-\tau(0)} = -1 \mod 2b_n c_n nP$ and especially $\Psi_n(k \cdot 2b_n c_n nP) \equiv -1 \mod n$. Thus $\Psi_n(k \cdot 2b_n c_n nP)$ is coprime to $2b_n c_n n$, thus by theorem 16 the q_i are $\equiv \pm 1 \mod n$. The same way we get that the q_i are different from the p_j, thus by assumption $q_i \equiv 1 \mod n$ for all i, giving that
$-1 \equiv \Psi_n(k \cdot 2b_n c_n nP) = q_1 q_2 ... q_m \equiv 1 \cdot 1 \cdot ... \cdot 1 = 1 \mod n$, contradicting $n > 2$. □