Fermat's Last Theorem for regular primes in Lean

Riccardo Brasca

Université Paris Cité
Institut de Mathématiques de Jussieu-Paris Rive Gauche

10th May, 2022

Introduction

The project has two main goals.

Introduction

The project has two main goals.

- Prove Fermat's Last Theorem for regular prime exponents in Lean.

Introduction

The project has two main goals.

- Prove Fermat's Last Theorem for regular prime exponents in Lean.
- Develop algebraic number theory in mathlib.

Introduction

The project has two main goals.

- Prove Fermat's Last Theorem for regular prime exponents in Lean.
- Develop algebraic number theory in mathlib.

https://github.com/leanprover-community/flt-regular.

Introduction

The project has two main goals.

- Prove Fermat's Last Theorem for regular prime exponents in Lean.
- Develop algebraic number theory in mathlib.

https://github.com/leanprover-community/flt-regular.
A lot of results are already in mathlib.

Joint work with the mathlib community.

Joint work with the mathlib community. Especially

- Alex Best
- Chris Birkbeck
- Eric Rodriguez

Joint work with the mathlib community. Especially

- Alex Best
- Chris Birkbeck
- Eric Rodriguez

If you want to contribute just write on Zulip, in the `flt-regular` stream.

Fermat's Last Theorem

Fermat's Last Theorem is the following statement.

Fermat's Last Theorem

Fermat's Last Theorem is the following statement.

Theorem

Let $n > 2$ be a natural number.

Fermat's Last Theorem

Fermat's Last Theorem is the following statement.

Theorem

Let $n > 2$ be a natural number. Then the equation

$$x^n + y^n = z^n$$

has no nontrivial solutions in $\mathbb{Z}$.

Fermat's Last Theorem

Fermat's Last Theorem is the following statement.

Theorem

Let $n > 2$ be a natural number. Then the equation

$$x^n + y^n = z^n$$

has no nontrivial solutions in $\mathbb{Z}$.

It has been conjectured by Fermat around 1637.

Fermat's Last Theorem

Fermat's Last Theorem is the following statement.

Theorem

Let $n > 2$ be a natural number. Then the equation

$$x^n + y^n = z^n$$

has no nontrivial solutions in $\mathbb{Z}$.

It has been conjectured by Fermat around 1637.
Finally proved by Wiles and Taylor in 1995.

The proof uses advanced 20th century mathematics.

The proof uses advanced 20th century mathematics. Results in several areas of mathematics.

The proof uses advanced 20th century mathematics. Results in several areas of mathematics.

- Number theory.

The proof uses advanced 20th century mathematics. Results in several areas of mathematics.

- Number theory.
- Algebraic geometry.

The proof uses advanced 20th century mathematics. Results in several areas of mathematics.

- Number theory.
- Algebraic geometry.
- Harmonic analysis...

The proof uses advanced 20th century mathematics. Results in several areas of mathematics.

- Number theory.
- Algebraic geometry.
- Harmonic analysis...

It's currently unreasonable to formalize it.

The proof uses advanced 20th century mathematics. Results in several areas of mathematics.

- Number theory.
- Algebraic geometry.
- Harmonic analysis...

It's currently unreasonable to formalize it.

We will concentrate on a special case.

Regular prime exponents

Proposition (Fermat)

Fermat's last theorem is true for $n = 4$.

Regular prime exponents

Proposition (Fermat)

Fermat's last theorem is true for $n = 4$.

Corollary

It is enough to prove FLT in the case the exponent is an odd prime p.

Regular prime exponents

Proposition (Fermat)

Fermat's last theorem is true for $n = 4$.

Corollary

It is enough to prove FLT in the case the exponent is an odd prime p.

The proposition is already in mathlib.

Regular prime exponents

Proposition (Fermat)

Fermat's last theorem is true for $n = 4$.

Corollary

It is enough to prove FLT in the case the exponent is an odd prime p.

The proposition is already in mathlib.

```
theorem not_fermat_4 {a b c : ℤ} (ha : a ≠ 0)
  (hb : b ≠ 0) : a ^ 4 + b ^ 4 ≠ c ^ 4
```

Regular prime exponents

Proposition (Fermat)

Fermat's last theorem is true for $n = 4$.

Corollary

It is enough to prove FLT in the case the exponent is an odd prime p.

The proposition is already in mathlib.

```
theorem not_fermat_4 {a b c : ℤ} (ha : a ≠ 0)
  (hb : b ≠ 0) : a ^ 4 + b ^ 4 ≠ c ^ 4
```

The proof is less than 300 lines of code.

Kummer's idea:

Kummer's idea: if $z^p = x^p + y^p$, then

$$z^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdots (x + \zeta_p^{p-1} y)$$

Kummer's idea: if $z^p = x^p + y^p$, then

$$z^p = (x+y)(x+\zeta_p y)(x+\zeta_p^2 y)\cdots(x+\zeta_p^{p-1} y)$$

in $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, where $\zeta_p = e^{\frac{2\pi i}{p}}$.

Kummer's idea: if $z^p = x^p + y^p$, then

$$z^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdots (x + \zeta_p^{p-1} y)$$

in $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, where $\zeta_p = e^{\frac{2\pi i}{p}}$.

This implies that

$$(z)^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdots (x + \zeta_p^{p-1} y)$$

as ideals.

The ideals on the right are coprime, so each of them must be a p-th power

The ideals on the right are coprime, so each of them must be a p-th power

$$(x + \zeta_p^k y) = I_k^p.$$

The ideals on the right are coprime, so each of them must be a p-th power

$$(x + \zeta_p^k y) = I_k^p.$$

In the class group of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ this implies

$$I_k^p = 1,$$

The ideals on the right are coprime, so each of them must be a p-th power

$$(x + \zeta_p^k y) = I_k^p.$$

In the class group of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ this implies

$$I_k^p = 1,$$

but in general $I_k \neq 1$.

The ideals on the right are coprime, so each of them must be a p-th power

$$(x + \zeta_p^k y) = I_k^p.$$

In the class group of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ this implies

$$I_k^p = 1,$$

but in general $I_k \neq 1$.

Definition

We say that an odd prime p is *regular* if p does not divide the order of the class group of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$.

Definition

We say that an odd prime p is *regular* if p does not divide the order of the class group of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$.

In this case, since $I_k^p = 1$, we have $I_k = 1$

Definition

We say that an odd prime p is *regular* if p does not divide the order of the class group of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$.

In this case, since $I_k^p = 1$, we have $I_k = 1$, so $I_k = (\alpha_k)$ is principal.

Definition

We say that an odd prime p is *regular* if p does not divide the order of the class group of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$.

In this case, since $I_k^p = 1$, we have $I_k = 1$, so $I_k = (\alpha_k)$ is principal.

Theorem (FLT for regular primes, case I)

Let p be a regular prime.

Definition

We say that an odd prime p is *regular* if p does not divide the order of the class group of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$.

In this case, since $I_k^p = 1$, we have $I_k = 1$, so $I_k = (\alpha_k)$ is principal.

Theorem (FLT for regular primes, case I)

Let p be a regular prime. The equation

$$x^p + y^p = z^p \text{ and } p \nmid xyz$$

has no nontrivial solutions in $\mathbb{Z}$.

Definition

We say that p is *strongly regular* if it is regular and the following holds.

Definition

We say that p is *strongly regular* if it is regular and the following holds. For all $u \in \mathbb{Z}[\zeta_p]^*$ with $u \equiv a \bmod p$ for some integer a, there is $v \in \mathbb{Z}[\zeta_p]^*$ such that $u = v^p$.

Definition

We say that p is *strongly regular* if it is regular and the following holds. For all $u \in \mathbb{Z}[\zeta_p]^*$ with $u \equiv a \bmod p$ for some integer a, there is $v \in \mathbb{Z}[\zeta_p]^*$ such that $u = v^p$.

Theorem (FLT for regular primes, case II)

Let p be a strongly regular prime.

Definition

We say that p is *strongly regular* if it is regular and the following holds. For all $u \in \mathbb{Z}[\zeta_p]^*$ with $u \equiv a \bmod p$ for some integer a, there is $v \in \mathbb{Z}[\zeta_p]^*$ such that $u = v^p$.

Theorem (FLT for regular primes, case II)

Let p be a strongly regular prime. The equation

$$x^p + y^p = z^p \text{ and } p \mid xyz$$

has no nontrivial solutions in $\mathbb{Z}$.

Lemma (Kummer's lemma)

A prime is regular if and only if it is strongly regular.

Lemma (Kummer's lemma)

A prime is regular if and only if it is strongly regular.

The proof needs several ingredients.

Lemma (Kummer's lemma)

A prime is regular if and only if it is strongly regular.

The proof needs several ingredients.

- Class field theory.

Lemma (Kummer's lemma)

A prime is regular if and only if it is strongly regular.

The proof needs several ingredients.

- Class field theory.
- Class number formula.

Lemma (Kummer's lemma)

A prime is regular if and only if it is strongly regular.

The proof needs several ingredients.

- Class field theory.
- Class number formula.

Corollary

An odd prime p is regular if and only if it does not divide the denominator of any of the Bernoulli numbers B_k for $k = 2, 4, 6, \ldots, p-3$.

Lemma (Kummer's lemma)

A prime is regular if and only if it is strongly regular.

The proof needs several ingredients.

- Class field theory.
- Class number formula.

Corollary

An odd prime p is regular if and only if it does not divide the denominator of any of the Bernoulli numbers B_k for $k = 2, 4, 6, \ldots, p - 3$.

This is very easy to check in practice.

Historically, Kummer's proof was the first that worked for many cases at once.

Historically, Kummer's proof was the first that worked for many cases at once.
The first irregular primes are:

Historically, Kummer's proof was the first that worked for many cases at once.
The first irregular primes are: $37, 59, 67, 101, 103, 131, \dots$

Historically, Kummer's proof was the first that worked for many cases at once.

The first irregular primes are: $37, 59, 67, 101, 103, 131, \ldots$

Conjecture

There are infinitely many regular primes.

Historically, Kummer's proof was the first that worked for many cases at once.
The first irregular primes are: $37, 59, 67, 101, 103, 131, \ldots$

Conjecture

There are infinitely many regular primes. More precisely the natural density of the set of regular primes among the primes is $e^{-1/2} \approx 0.61$.

Historically, Kummer's proof was the first that worked for many cases at once.
The first irregular primes are: $37, 59, 67, 101, 103, 131, \ldots$

Conjecture

There are infinitely many regular primes. More precisely the natural density of the set of regular primes among the primes is $e^{-1/2} \approx 0.61$.

Proposition

There are infinitely many irregular primes.

Dedekind domains

Thanks to the work of Baanen, Dahmen, Narayanan and Nuccio: fairly complete library about Dedekind domains already in mathlib.

Dedekind domains

Thanks to the work of Baanen, Dahmen, Narayanan and Nuccio: fairly complete library about Dedekind domains already in mathlib.

- Unique factorization of ideals.

Dedekind domains

Thanks to the work of Baanen, Dahmen, Narayanan and Nuccio: fairly complete library about Dedekind domains already in mathlib.

- Unique factorization of ideals.
- Ring of integers of a number field is a Dedekind domain.

Dedekind domains

Thanks to the work of Baanen, Dahmen, Narayanan and Nuccio: fairly complete library about Dedekind domains already in mathlib.

- Unique factorization of ideals.
- Ring of integers of a number field is a Dedekind domain.
- Finiteness of the class group.

Dedekind domains

Thanks to the work of Baanen, Dahmen, Narayanan and Nuccio: fairly complete library about Dedekind domains already in mathlib.

- Unique factorization of ideals.
- Ring of integers of a number field is a Dedekind domain.
- Finiteness of the class group.

Dedekind domains

Thanks to the work of Baanen, Dahmen, Narayanan and Nuccio: fairly complete library about Dedekind domains already in mathlib.

- Unique factorization of ideals.
- Ring of integers of a number field is a Dedekind domain.
- Finiteness of the class group.

Also in mathlib: cyclotomic polynomials

Dedekind domains

Thanks to the work of Baanen, Dahmen, Narayanan and Nuccio: fairly complete library about Dedekind domains already in mathlib.

- Unique factorization of ideals.
- Ring of integers of a number field is a Dedekind domain.
- Finiteness of the class group.

Also in mathlib: cyclotomic polynomials, but no theory of cyclotomic fields.

Cyclotomic extensions

Informal definition:

Cyclotomic extensions

Informal definition: a cyclotomic extension is an extension generated by roots of unity.

Cyclotomic extensions

Informal definition: a cyclotomic extension is an extension generated by roots of unity.
We want a definition as general as possible.

Cyclotomic extensions

Informal definition: a cyclotomic extension is an extension generated by roots of unity.

We want a definition as general as possible.

- Allows infinite extension like $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$.

Cyclotomic extensions

Informal definition: a cyclotomic extension is an extension generated by roots of unity.
We want a definition as general as possible.

- Allows infinite extension like $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$.
- Allows positive characteristic.

Cyclotomic extensions

Informal definition: a cyclotomic extension is an extension generated by roots of unity.
We want a definition as general as possible.

- Allows infinite extension like $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$.
- Allows positive characteristic.
- Allows rings extensions like $\mathbb{Z}[\zeta_p]/\mathbb{Z}$.

Cyclotomic extensions

Informal definition: a cyclotomic extension is an extension generated by roots of unity.
We want a definition as general as possible.

- Allows infinite extension like $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$.
- Allows positive characteristic.
- Allows rings extensions like $\mathbb{Z}[\zeta_p]/\mathbb{Z}$.

More importantly: we want a *characteristic predicate*:

Cyclotomic extensions

Informal definition: a cyclotomic extension is an extension generated by roots of unity.
We want a definition as general as possible.

- Allows infinite extension like $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$.
- Allows positive characteristic.
- Allows rings extensions like $\mathbb{Z}[\zeta_p]/\mathbb{Z}$.

More importantly: we want a *characteristic predicate*:

$$\mathbb{Q}(e^{\frac{2\pi i}{n}}) \subseteq \mathbb{C}$$

Cyclotomic extensions

Informal definition: a cyclotomic extension is an extension generated by roots of unity.
We want a definition as general as possible.

- Allows infinite extension like $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$.
- Allows positive characteristic.
- Allows rings extensions like $\mathbb{Z}[\zeta_p]/\mathbb{Z}$.

More importantly: we want a *characteristic predicate*:

$$\mathbb{Q}(e^{\frac{2\pi i}{n}}) \subseteq \mathbb{C} \text{ but also } \mathbb{Q}[x]/\Phi_n(x)$$

```
variables (S : set ℕ+) (A : Type) (B : Type)
  [comm_ring A] [comm_ring B] [algebra A B]
```

```
variables (S : set ℕ+) (A : Type) (B : Type)
  [comm_ring A] [comm_ring B] [algebra A B]
```

```
class is_cyclotomic_extension S A B : Prop :=
(exists_root {a : ℕ+} (ha : a ∈ S) :
    ∃ r : B, aeval r (cyclotomic a A) = 0)
(adjoin_roots : ∀ (x : B),
    x ∈ adjoin A { b : B | ∃ a : ℕ+, a ∈ S ∧ b ^ (a
    : ℕ) = 1 })
```

Cyclotomic fields

We want to be able to produce a cyclotomic extension of a field.

Cyclotomic fields

We want to be able to produce a cyclotomic extension of a field.

```
@[derive [field, algebra K]]
def cyclotomic_field (n : ℕ+) (K : Type) [field K] :
 Type := (cyclotomic n K).splitting_field
```

Cyclotomic fields

We want to be able to produce a cyclotomic extension of a field.

```
@[derive [field, algebra K]]
def cyclotomic_field (n : ℕ+) (K : Type) [field K] :
 Type := (cyclotomic n K).splitting_field
```

```
instance :
  is_cyclotomic_extension {n} K (cyclotomic_field n K)
```

Cyclotomic rings

We want to be able to produce a cyclotomic extension of a ring.

Cyclotomic rings

We want to be able to produce a cyclotomic extension of a ring.

```
variables (n : ℕ+) (A : Type) (K : Type)
  [comm_ring A] [field K] [is_domain A] [algebra A K]
  [is_fraction_ring A K]
```

Cyclotomic rings

We want to be able to produce a cyclotomic extension of a ring.

```
variables (n : ℕ+) (A : Type) (K : Type)
  [comm_ring A] [field K] [is_domain A] [algebra A K]
  [is_fraction_ring A K]
```

```
def cyclotomic_ring n A K : Type :=
adjoin A { b : (cyclotomic_field n K) |
  b ^ (n : ℕ) = 1 }
```

Cyclotomic rings

We want to be able to produce a cyclotomic extension of a ring.

```
variables (n : ℕ+) (A : Type) (K : Type)
  [comm_ring A] [field K] [is_domain A] [algebra A K]
  [is_fraction_ring A K]
```

```
def cyclotomic_ring n A K : Type :=
adjoin A { b : (cyclotomic_field n K) |
  b ^ (n : ℕ) = 1 }
```

One has to write `cyclotomic_ring n A K` even if `K` is mathematically irrelevant.

```
instance [ne_zero ((n : ℕ) : A)] :
  is_cyclotomic_extension {n} A
  (cyclotomic_ring n A K)
```

```
instance [ne_zero ((n : ℕ) : A)] :
  is_cyclotomic_extension {n} A
  (cyclotomic_ring n A K)
```

```
instance [ne_zero ((n : ℕ) : A)] :
  is_fraction_ring (cyclotomic_ring n A K)
  (cyclotomic_field n K)
```

Regular primes

```
instance (n : ℕ+) :
  fintype (class_group (cyclotomic_ring n ℤ ℚ)
  (cyclotomic_field n ℚ))
```

Regular primes

```
instance (n : ℕ+) :
  fintype (class_group (cyclotomic_ring n ℤ ℚ)
  (cyclotomic_field n ℚ))
```

This needs $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

Regular primes

```
instance (n : ℕ+) :
  fintype (class_group (cyclotomic_ring n ℤ ℚ)
  (cyclotomic_field n ℚ))
```

This needs $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

```
def is_regular_prime (p : ℕ) [hp : fact p.prime] :
    Prop :=
p.coprime
  (fintype.card (class_group (cyclotomic_ring ⟨p, hp
    .1.pos⟩ ℤ ℚ)
  (cyclotomic_field ⟨p, hp.1.pos⟩ ℚ)))
```

Ring of integers of cyclotomic extensions

Proposition

We have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$

Ring of integers of cyclotomic extensions

Proposition

We have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ *if* $n = p^k$ *is a prime power.*

Ring of integers of cyclotomic extensions

Proposition

We have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ if $n = p^k$ is a prime power.

We need two lemmas about number fields.

Ring of integers of cyclotomic extensions

Proposition

We have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ if $n = p^k$ is a prime power.

We need two lemmas about number fields. Let $x \in \overline{\mathbb{Z}}$.

Ring of integers of cyclotomic extensions

Proposition

We have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ if $n = p^k$ is a prime power.

We need two lemmas about number fields. Let $x \in \overline{\mathbb{Z}}$.

Lemma

The discriminant of $\mathbb{Q}(x)/\mathbb{Q}$ kills $\mathcal{O}_{\mathbb{Q}(x)}/\mathbb{Z}[x]$.

Ring of integers of cyclotomic extensions

Proposition

We have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ if $n = p^k$ is a prime power.

We need two lemmas about number fields. Let $x \in \overline{\mathbb{Z}}$.

Lemma

The discriminant of $\mathbb{Q}(x)/\mathbb{Q}$ kills $\mathcal{O}_{\mathbb{Q}(x)}/\mathbb{Z}[x]$.

Lemma

If the minimal polynomial of x is Eiseinstein at p, then the index of $\mathbb{Z}[x]$ inside $\mathcal{O}_{\mathbb{Q}(x)}$ is prime to p.

Proof of the proposition.

Let $\varepsilon_n = 1 - \zeta_n$.

Proof of the proposition.

Let $\varepsilon_n = 1 - \zeta_n$. Recall that $n = p^k$.

Proof of the proposition.

Let $\varepsilon_n = 1 - \zeta_n$. Recall that $n = p^k$.

- We have $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\varepsilon_n]$.

Proof of the proposition.

Let $\varepsilon_n = 1 - \zeta_n$. Recall that $n = p^k$.

- We have $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\varepsilon_n]$.
- The discriminant of $1, \varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{\varphi(n)-1}$ is

$$\pm p^{p^{k-1}((p-1)k-1)}.$$

Proof of the proposition.

Let $\varepsilon_n = 1 - \zeta_n$. Recall that $n = p^k$.

- We have $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\varepsilon_n]$.
- The discriminant of $1, \varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{\varphi(n)-1}$ is

$$\pm p^{p^{k-1}((p-1)k-1)}.$$

- The minimal polynomial of ε_n is Eiseinstein at p.

□

The discriminant

```
variables (A : Type) {B ι : Type}
  [comm_ring A] [comm_ring B] [algebra A B]
```

The discriminant

```
variables (A : Type) {B ι : Type}
  [comm_ring A] [comm_ring B] [algebra A B]
```

```
def trace_matrix (b : ι → B) : matrix ι ι A
| i j := trace_form A B (b i) (b j)
```

The discriminant

```
variables (A : Type) {B ι : Type}
  [comm_ring A] [comm_ring B] [algebra A B]
```

```
def trace_matrix (b : ι → B) : matrix ι ι A
| i j := trace_form A B (b i) (b j)
```

```
def discr [fintype ι] (b : ι → B) :=
by { classical, exact (trace_matrix A b).det }
```

```
variables (K : Type u) {L : Type v} [field K]
 [field L] [algebra K L] [finite K L]
 (pb : power_basis K L) [is_separable K L]
```

```
variables (K : Type u) {L : Type v} [field K]
 [field L] [algebra K L] [finite K L]
 (pb : power_basis K L) [is_separable K L]
```

```
lemma discr_power_basis_eq_norm :
  discr K pb.basis =
  (-1) ^ (n * (n - 1) / 2) * (norm K
  (aeval pb.gen (minpoly K pb.gen).derivative))
```

Here `n := finrank K L`.

```
lemma discr_eq_discr {K : Type} [number_field K]
  {b : basis ι ℚ K} {b' : basis ι' ℚ K}
  (h : ∀ i j, is_integral ℤ (b.to_matrix b' i j))
  (h' : ∀ i j, is_integral ℤ (b'.to_matrix b i j)) :
  discr ℚ b = discr ℚ b'
```

```
lemma discr_eq_discr {K : Type} [number_field K]
  {b : basis ι ℚ K} {b' : basis ι' ℚ K}
  (h : ∀ i j, is_integral ℤ (b.to_matrix b' i j))
  (h' : ∀ i j, is_integral ℤ (b'.to_matrix b i j)) :
  discr ℚ b = discr ℚ b'
```

No problems in formalizing the general results about the discriminant of number fields.

```
lemma discr_prime_pow {ζ : L} {k : ℕ} {p : ℕ+}
  [is_cyclotomic_extension {p ^ k} K L]
  [fact (p : ℕ).prime]
  [ne_zero ((p : ℕ) : K)]
  (hζ : is_primitive_root ζ ↑(p ^ k))
  (h : irreducible (cyclotomic (↑(p ^ k) : ℕ) K)) :
  discr K (hζ.power_basis K).basis =
  (-1) ^ (((p ^ k : ℕ).totient) / 2) *
  p ^ ((p : ℕ) ^ (k - 1) * ((p - 1) * k - 1))
```

```
lemma discr_prime_pow {ζ : L} {k : ℕ} {p : ℕ+}
  [is_cyclotomic_extension {p ^ k} K L]
  [fact (p : ℕ).prime]
  [ne_zero ((p : ℕ) : K)]
  (hζ : is_primitive_root ζ ↑(p ^ k))
  (h : irreducible (cyclotomic (↑(p ^ k) : ℕ) K)) :
  discr K (hζ.power_basis K).basis =
  (-1) ^ (((p ^ k : ℕ).totient) / 2) *
  p ^ ((p : ℕ) ^ (k - 1) * ((p - 1) * k - 1))
```

Remark

In $\mathbb{N}$ *we have* $1/2 = 0$ *and* $0 - 1 = 0$.

The ring of integers

```
variables {p : ℕ+} {k : ℕ} {K : Type} [field K]
  [char_zero K] {ζ : K} [hp : fact (p : ℕ).prime]
```

The ring of integers

```
variables {p : ℕ+} {k : ℕ} {K : Type} [field K]
 [char_zero K] {ζ : K} [hp : fact (p : ℕ).prime]
```

```
lemma is_integral_closure {ζ : K}
  [is_cyclotomic_extension {p ^ k} ℚ K]
  (hζ : is_primitive_root ζ ↑(p ^ k)) :
  is_integral_closure (adjoin ℤ ({ζ} : set K)) ℤ K
```

We are now ready for the final result.

We are now ready for the final result.

```
lemma cyclotomic_ring_is_integral_closure :
  is_integral_closure (cyclotomic_ring (p ^ k) ℤ ℚ)
  ℤ (cyclotomic_field (p ^ k) ℚ)
```

We are now ready for the final result.

```
lemma cyclotomic_ring_is_integral_closure :
  is_integral_closure (cyclotomic_ring (p ^ k) ℤ ℚ)
  ℤ (cyclotomic_field (p ^ k) ℚ)
```

We encounter here the `char_zero` diamond.

We are now ready for the final result.

```
lemma cyclotomic_ring_is_integral_closure :
  is_integral_closure (cyclotomic_ring (p ^ k) ℤ ℚ)
  ℤ (cyclotomic_field (p ^ k) ℚ)
```

We encounter here the char_zero diamond.

```
local attribute [-instance] cyclotomic_field.algebra
```

The ne_zero class

Let L/K be a n-th cyclotomic extension of fields.

The ne_zero class

Let L/K be a n-th cyclotomic extension of fields.

Lemma

If $n \neq 0$ in K, then L contains a primitive n-th root of unity.

The `ne_zero` class

Let L/K be a n-th cyclotomic extension of fields.

Lemma

If $n \neq 0$ in K, then L contains a primitive n-th root of unity.
This is false if $n = 0$ in K

The `ne_zero` class

Let L/K be a n-th cyclotomic extension of fields.

Lemma

If $n \neq 0$ in K, then L contains a primitive n-th root of unity.
This is false if $n = 0$ in K (since there are no primitive n-roots of unity in any extension of K).

The ne_zero class

Let L/K be a n-th cyclotomic extension of fields.

Lemma

If $n \neq 0$ in K, then L contains a primitive n-th root of unity. This is false if $n = 0$ in K (since there are no primitive n-roots of unity in any extension of K).

In practice the theory is rather different if $n = 0$ in K or not.

The ne_zero class

Let L/K be a n-th cyclotomic extension of fields.

Lemma

If $n \neq 0$ in K, then L contains a primitive n-th root of unity. This is false if $n = 0$ in K (since there are no primitive n-roots of unity in any extension of K).

In practice the theory is rather different if $n = 0$ in K or not.
We would like to assume this once and then forget about it.

The ne_zero class

Let L/K be a n-th cyclotomic extension of fields.

Lemma

If $n \neq 0$ in K, then L contains a primitive n-th root of unity. This is false if $n = 0$ in K (since there are no primitive n-roots of unity in any extension of K).

In practice the theory is rather different if $n = 0$ in K or not. We would like to assume this once and then forget about it.

```
class ne_zero {R : Type} [has_zero R] (n : R) : Prop
  := (out : n ≠ 0)
```

```
variables {n : ℕ+} {K : Type} {L : Type} (C : Type)
  [field K] [field L] [comm_ring C] [algebra K L]
  [algebra K C] [is_cyclotomic_extension {n} K L]
  {ζ : L} (hζ : is_primitive_root ζ n) [is_domain C]
  [ne_zero ((n : ℕ) : K)]
  (hirr : irreducible (cyclotomic n K))
```

```
variables {n : ℕ+} {K : Type} {L : Type} (C : Type)
  [field K] [field L] [comm_ring C] [algebra K L]
  [algebra K C] [is_cyclotomic_extension {n} K L]
  {ζ : L} (hζ : is_primitive_root ζ n) [is_domain C]
  [ne_zero ((n : ℕ) : K)]
  (hirr : irreducible (cyclotomic n K))
```

```
def embeddings_equiv_primitive_roots :
  (L →a[K] C) ≃ primitive_roots n C
```

In the proof we need

```
haveI hn : ne_zero ((n : ℕ) : C) :=
  ne_zero.of_no_zero_smul_divisors K C n,
```

In the proof we need

```
haveI hn : ne_zero ((n : ℕ) : C) :=
  ne_zero.of_no_zero_smul_divisors K C n,
```

Easy to prove

In the proof we need

```
haveI hn : ne_zero ((n : ℕ) : C) :=
  ne_zero.of_no_zero_smul_divisors K C n,
```

Easy to prove, but it is not automatically found.

In the proof we need

```
haveI hn : ne_zero ((n : ℕ) : C) :=
  ne_zero.of_no_zero_smul_divisors K C n,
```

Easy to prove, but it is not automatically found.
Lean wants `ne_zero ((n : ℕ) : C)`.

In the proof we need

```
haveI hn : ne_zero ((n : ℕ) : C) :=
  ne_zero.of_no_zero_smul_divisors K C n,
```

Easy to prove, but it is not automatically found.
Lean wants `ne_zero ((n : ℕ) : C)`. The problem with using `ne_zero ((n : ℕ) : K)` automatically is that Lean has no way of guessing `K`.

In the proof we need

```
haveI hn : ne_zero ((n : ℕ) : C) :=
  ne_zero.of_no_zero_smul_divisors K C n,
```

Easy to prove, but it is not automatically found.
Lean wants `ne_zero ((n : ℕ) : C)`. The problem with using `ne_zero ((n : ℕ) : K)` automatically is that Lean has no way of guessing `K`.
Moving between ℕ+ and ℕ also causes troubles.