FERMAT'S LAST THEOREM FOR REGULAR PRIMES

Contents

1. Introduction

We prove Fermat's Last Theorem for regular primes and give some of the necessary background. It uses [Sam70, Mar18, Was82].

2. Discriminants of number fields

lemma 2.1. *Let K be a number field, $\alpha \in K$ and let σ_i be the embeddings of K into $\mathbb{C}$. Then*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_i \sigma_i(\alpha) \qquad N_{K/\mathbb{Q}}(\alpha) = \prod_i \sigma_i(\alpha)$$

Definition 2.2. Let A, K be commutative rings with K and A-algebra. let $B = \{b_1, \ldots, b_n\}$ be a set of elements in K. The discriminant of B is defined as

$$\Delta(B) = \det \begin{pmatrix} \mathrm{Tr}_{K/A}(b_1 b_1) & \cdots & \mathrm{Tr}_{K/A}(b_1 b_n) \\ \vdots & & \vdots \\ \mathrm{Tr}_{K/A}(b_n b_1) & \cdots & \mathrm{Tr}_{K/A}(b_n b_n) \end{pmatrix}.$$

lemma 2.3. *Let K be a number field and let $B = \{b_1, \ldots, b_n\}$ be a set of elements in K. Then $\Delta(B) \neq 0$ if and only if the elements in B are linearly independent.*

lemma 2.4. *Let K be a number field and B, B' bases for $K/\mathbb{Q}$. If P denotes the change of basis matrix, then*

$$\Delta(B) = \det(P)^2 \Delta(B').$$

lemma 2.5. *Let K be a number field with basis $B = \{b_1, \ldots, b_n\}$ and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. Now let M be the matrix*

$$\begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_n) \\ \vdots & & \vdots \\ \sigma_n(b_1) & \cdots & \sigma_n(b_n) \end{pmatrix}.$$

Then

$$\Delta(B) = \det(M)^2.$$

Proof. By Proposition 2.1 we know that $\mathrm{Tr}_{K/\mathbb{Q}}(b_i b_j) = \sum_k \sigma_k(b_i)\sigma_k(b_j)$ which is the same as the (i,j) entry of $M^t M$. Therefore

$$\det(T_B) = \det(M^t M) = \det(M)^2.$$

□

lemma 2.6. *Let K be a number field and $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ for some $\alpha \in K$. Then*

$$\Delta(B) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

where σ_i are the embeddings of K into $\mathbb{C}$. Here $\Delta(B)$ denotes the discriminant.

Proof. First we recall a classical linear algebra result relating to the Vandermonde matrix, which states that

$$\det \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \vdots & & & \vdots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{i<j} (x_i - x_j).$$

Combining this with Proposition 2.5 gives the result. □

lemma 2.7. *Let f be a monic irreducible polynomial over a number field K and let α be one of its roots in $\mathbb{C}$. Then*

$$f'(\alpha) = \prod_{\beta \neq \alpha} (\alpha - \beta),$$

where the product is over the roots of f different from α.

Proof. We first write $f(x) = (x - \alpha)g(x)$ which we can do (over $\mathbb{C}$) as α is a root of f, where now $g(x) = \prod_{\beta \neq \alpha}(x - \beta)$. Differentiating we get

$$f'(x) = g(x) + (x - \alpha)g'(x).$$

If we now evaluate at α we get the result. □

lemma 2.8. *Let $K = \mathbb{Q}(\alpha)$ be a number field with $n = [K : \mathbb{Q}]$ and let $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Then*

$$\Delta(B) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(m'_\alpha(\alpha))$$

where m'_α is the derivative of $m_\alpha(x)$ (which we recall denotes the minimal polynomial of α).

Proof. By Proposition 2.6 we have $\Delta(B) = \prod_{i<j}(\alpha_i - \alpha_j)^2$ where $\alpha_k := \sigma_k(\alpha)$. Next, we note that the number of terms in this product is $1+2+\cdots+(n-1) = \frac{n(n-1)}{2}$. So if we write each term as $(\alpha_i - \alpha_j)^2 = -(\alpha_i - \alpha_j)(\alpha_j - \alpha_i)$ we get

$$\Delta(B) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Now, by lemma 2.7 and Proposition 2.1 we see that

$$N_{K/\mathbb{Q}}(m'_\alpha(\alpha)) = \prod_{i=1}^{n} m'_\alpha(\alpha_i) = \prod_{i=1}^{n} \prod_{i \neq j} (\alpha_i - \alpha_j),$$

which gives the result. □

lemma 2.9. *Let K be a number field and B, B' bases for $K/\mathbb{Q}$. If P denotes the change of basis matrix, then*

$$\Delta(B) = \det(P)^2 \Delta(B').$$

lemma 2.10. *If K is a number field and $\alpha \in \mathcal{O}_K$ then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha)$ are both in $\mathbb{Z}$.*

lemma 2.11. *Let K be a number field and $B = \{b_1, \ldots, b_n\}$ be elements in $\mathcal{O}_K$, then $\Delta(B) \in \mathbb{Z}$.*

lemma 2.12. *Let K be a number field and $B = \{b_1, \ldots, b_n\}$ be a basis for $K/\mathbb{Q}$ consisting of algebraic integers. If B is not an integral basis then there exists an algebraic integer of the form*

$$\alpha = \frac{x_1 b_1 + \cdots + x_n b_n}{p}$$

where p is a prime and $x_i \in \{0, \ldots, p-1\}$ with not all x_i zero. Moreover, if $x_i \neq 0$ and we let B' be the basis obtained by replacing b_i with α, then

$$\Delta(B') = \frac{x_i^2}{p^2} \Delta(B).$$

In particular $p^2 \mid \Delta(B)$.

Proof. If B is not an integral basis then we can find some element $\phi \in \mathcal{O}_K$ such that

$$\phi = y_1 b_1 + \ldots y_n b_n$$

with not all the y_i in $\mathbb{Z}$. So, let N be the least common multiple of the denominators of the y_i (meaning $N y_i \in \mathbb{Z}$ for all i). Now, let p be a prime factor of N. If we now consider $(N/p)\phi$ then all of the coefficients of b_i are in $\frac{1}{p}\mathbb{Z}$ (so they have denominator 1 or p.) and at least one of them has denominator p (since not all the y_i where in $\mathbb{Z}$). So by relabelling, wlog we can assume

$$\phi = y_1 b_1 + \ldots y_n b_n$$

with $y_i \in \frac{1}{p}\mathbb{Z}$

Now look at

$$\psi := \lfloor y_1 \rfloor b_1 + \cdots + \lfloor y_n \rfloor b_n$$

(here $\lfloor x \rfloor$ denotes the integer part of x). The both ψ and ϕ are algebraic integers (as the b_i are algebraic integers). Therefore, so is $\theta = \phi - \psi$. By construction, θ has coefficients of the for $\frac{x_i}{p} := y_i - \lfloor y_i \rfloor$ where $x_i \in \{0, \ldots, p-1\}$ and not all the x_i are zero (since, again, not all the y_i were in $\mathbb{Z}$). This gives the first part of the lemma.

Now, assume $x_i \neq 0$, then let us replace $b_i \in B$ with θ to get a new basis B' which again consists of algebraic integers. Next, we note that the change of basis matrix from B to B' is

$$\begin{pmatrix} 1 & 0 & \cdots & \frac{x_1}{p} & \cdots & 0 \\ 0 & 1 & \cdots & \frac{x_2}{p} & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{x_n}{p} & \cdots & 1 \end{pmatrix}$$

(here the column of x_j/p's is in the i-th column).

This matrix has determinant $\frac{x_i}{p}$. Therefore, by Proposition 2.9 we see that $\Delta(B') = \frac{x_i^2}{p^2}\Delta(B)$. But both $\Delta(B), \Delta(B')$ are in $\mathbb{Z}$ by Proposition 2.11, therefore $p^2 \mid \Delta(B)$ giving the result. □

lemma 2.13. *Let $K = \mathbb{Q}(\alpha)$ and α be an algebraic integer such that m_α satisfies Eisensteins Criterion for a prime p. Then none of the elements*

$$\phi = \frac{1}{p}(x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1})$$

is an algebraic integer, where $n = \deg(m_\alpha)$ and $x_i \in \{0, \ldots, p-1\}$.

Proof. Suppose for contradiction that $\phi \in \mathcal{O}_K$ and let x_d be the first non-zero coefficient, so

$$\phi = \frac{1}{p}(x_d\alpha^d + x_{d+1}\alpha^{d+1} + \cdots + x_{n-1}\alpha^{n-1}) \in \mathcal{O}_K.$$

Now, rewrite this as $\phi = \frac{1}{p}(x_d\alpha^d + \alpha^{d+1}\beta)$ for some $\beta \in \mathcal{O}_K$. Next, multiply through by α^{n-1-d}, then we have

$$\frac{x_d\alpha^{n-1}}{p} + \frac{\alpha^n\beta}{p} \in \mathcal{O}_K.$$

Now, since m_α satisfies Eisenstein at p, we see that $\alpha^n = pf(\alpha)$ for some $f \in \mathbb{Z}[x]$ and therefore the above gives us that

$$\frac{x_d\alpha^{n-1}}{p} + \beta f(\alpha) \in \mathcal{O}_K.$$

and thus

$$\frac{x_d\alpha^{n-1}}{p} \in \mathcal{O}_K.$$

Lets now calculate the norm of this:

$$N_{K/\mathbb{Q}}\left(\frac{x_d\alpha^{n-1}}{p}\right) = \frac{x_d^n N_{K/\mathbb{Q}}(\alpha)^{n-1}}{p^n}.$$

By Eisenstein the constant coefficient of m_α is divisible by p but not p^2, so since the constant coefficient of m_α is $N_{K/\mathbb{Q}}(\alpha)$ we see that $N_{K/\mathbb{Q}}(\alpha) = pa$ where $p \nmid a$. Therefore we have

$$N_{K/\mathbb{Q}}\left(\frac{x_d\alpha^{n-1}}{p}\right) = \frac{x_d^n p^{n-1} a^{n-1}}{p^n} = \frac{x_d^n a^{n-1}}{p}.$$

But this cant be in $\mathbb{Z}$ since p doesn't divide x_d or a, and this gives us a contradiction since Proposition 2.10 says that the norm of an algebraic integer must be an integer. So ϕ couldn't have been an algebraic integer. □

3. Cyclotomic fields

lemma 3.1. *For n any integer, Φ_n (the n-th cyclotomic polynomial) is an irreducible polynomial of degree $\varphi(n)$ (where φ is Euler's Totient function).*

Theorem 3.2. *Let ζ_p be a p-th root of unity for p an odd prime, let $\lambda_p = 1-\zeta_p$ and $K = \mathbb{Q}(\zeta_p)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_p] = \mathbb{Z}[\lambda_p]$ moreover*

$$\Delta(\{1, \zeta_p, \dots, \zeta_p^{p-2}\}) = \Delta(\{1, \lambda_p, \dots, \lambda_p^{p-2}\}) = (-1)^{\frac{(p-1)}{2}} p^{p-2}.$$

Proof. First note $[K : \mathbb{Q}] = p - 1$.

Since $\zeta_p = 1 - \lambda_p$ we at once get $\mathbb{Z}[\zeta_p] = \mathbb{Z}[\lambda_p]$ (just do double inclusion). Next, let $\alpha_i = \sigma_i(\zeta_p)$ denote the conjugates of ζ_p, which is the same as the image of ζ_p under one of the embeddings $\sigma_i : \mathbb{Q}(\zeta_p) \to \mathbb{C}$. Now by Proposition 2.6 we have

$$\begin{aligned}\Delta(\{1, \zeta_p, \dots, \zeta_p^{p-2}\}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 &= \prod_{i<j}((1-\alpha_i) - (1-\alpha_j))^2 \\ &= \Delta(\{1, \lambda_p, \dots, \lambda_p^{p-2}\})\end{aligned}$$

Now, by Proposition 2.8, we have

$$\Delta(\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{K/\mathbb{Q}}(\Phi_p'(\zeta_p))$$

Since p is odd $(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{(p-1)}{2}}$. Next, we see that

$$\Phi_p'(x) = \frac{px^{p-1}(x-1) - (x^p - 1)}{(x-1)^2}$$

therefore

$$\Phi_p'(\zeta_p) = -\frac{p\zeta_p^{p-1}}{\lambda_p}.$$

Lastly, note that $N_{K/\mathbb{Q}}(\zeta_p) = 1$, since this is the constant term in its minimal polynomial. Similarly, we see $N_{K/\mathbb{Q}}(\lambda_p) = p$. Putting this all together, we get

$$N_{K/\mathbb{Q}}(\Phi_p'(\zeta_p)) = \frac{N_{K/\mathbb{Q}}(p) N_{K\mathbb{Q}}(\zeta_p)^{p-1}}{N_{K/\mathbb{Q}}(-\lambda_p)} = (-1)^{p-1} p^{p-2} = p^{p-2}$$

So the last thing we need to prove is that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. From the calculation we just did, the only prime dividing the discriminant is p, therefore Lemma 2.12 tells us the only prime we need to check is p. But from Lemma 2.13 we know that dividing by p wont give us any new integral elements, so this must be an integral basis which give the result. □

lemma 3.3. *Let α be an algebraic integer all of whose conjugates have absolute value one. Then α is a root of unity.*

lemma 3.4. *Let p be a prime, $K = \mathbb{Q}(\zeta_p)$ $\alpha \in K$ such that there exists $n \in \mathbb{N}$ such that $\alpha^n = 1$, then $\alpha = \pm\zeta_p^k$ for some k.*

Proof. If n is different to p then K contains a $2pn$-th root of unity. Therefore $\mathbb{Q}(\zeta_{2pn}) \subset K$, but this cannot happen as $[K : \mathbb{Q}] = p-1$ and $[\mathbb{Q}(\zeta_{2pn}) : \mathbb{Q}] = \varphi(2np)$.

□

lemma 3.5. *Any unit u in $\mathbb{Z}[\zeta_p]$ can be written in the form $\beta\zeta_p^k$ with k an integer and $\beta \in \mathbb{R}$.*

lemma 3.6. *Let p be a prime and $n = p^k$. Then*

$$p = u(1-\zeta_n)^{\varphi(n)}$$

where $u \in \mathbb{Z}[\zeta_n]^\times$.

lemma 3.7. *Let R be a Dedekind domain, p a prime and $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ideals such that*

$$\mathfrak{a}\mathfrak{b} = \mathfrak{c}^p$$

and suppose $\mathfrak{a}, \mathfrak{b}$ are coprime. Then there exist ideals $\mathfrak{e}, \mathfrak{d}$ such that

$$\mathfrak{a} = \mathfrak{e}^p \qquad \mathfrak{b} = \mathfrak{d}^p \qquad \mathfrak{e}\mathfrak{d} = \mathfrak{c}$$

4. Fermats Last Theorem for regular primes

lemma 4.1. *Let $p \geq 5$ be an prime number, ζ_p a p-th root of unity and $x, y \in \mathbb{Z}$ coprime.*

For $i \neq j$ we can write

$$(\zeta_p^i - \zeta_p^j) = u(1 - \zeta_p)$$

with u a unit in $\mathbb{Z}[\zeta_p]$. From this it follows that the ideals

$$(x + y), (x + \zeta_p y), (x + \zeta_p^2 y), \ldots, (x + \zeta_p^{p-1} y)$$

are pairwise coprime.

Proof. Lemma 3.6 gives that u is a unit. So all that needs to be proved is that the ideals are coprime. Assume not, then for some $i \neq j$ we have some prime ideal $\mathfrak{p}$ dividing by $(x + y\zeta_p^i)$ and $(x + y\zeta_p^j)$. It must then also divide their sum and their difference, so we must have $\mathfrak{p}|(1 - \zeta_p)$ or $\mathfrak{p}|y$. Similarly, $\mathfrak{p}$ divides $\zeta_p^j(x + y\zeta_p^i) - \zeta_p^i(x + y\zeta_p^j)$ so $\mathfrak{p}$ divides x or $(1 - \zeta_p)$. We can't have $\mathfrak{p}$ dividing x, y since they are coprime, therefore $\mathfrak{p}|(1 - \zeta_p)$. We know that since $(1-\zeta_p)$ has norm p it must be a prime ideal, so $\mathfrak{p} = (1-\zeta_p)$. Now, note that $x + y \equiv x + y\zeta_+ p^i \equiv 0 \mod \mathfrak{p}$. But since $x, y \in \mathbb{Z}$ this means we would have $x + y \equiv 0 \pmod p$, which implies $z^p \equiv 0 \pmod p$ which contradicts our assumptions. □

lemma 4.2. *Let p be an prime number, ζ_p a p-th root of unity and $\alpha \in \mathbb{Z}[\zeta_p]$. Then α^p is congruent to an integer modulo p.*

Proof. Just use $(x + y)^p \equiv x^p + y^p \pmod p$ and that ζ_p is a p-th root of unity. □

lemma 4.3. *Let $p \geq 5$ be an prime number, ζ_p a p-th root of unity and $\alpha \in \mathbb{Z}[\zeta_p]$. If there is an integer n such that $\alpha/n \in \mathbb{Z}[\zeta_p]$, then n divides each a_i.*

Proof. Looking at $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$, if one of the a_i's is zero and $\alpha/n \in \mathbb{Z}[\zeta_p]$, then $\alpha/n = \sum_i a_i/n\zeta_p^i$. Now, as $\alpha/n \in \mathbb{Z}[\zeta_p]$, pick the basis of $\mathbb{Z}[\zeta_p]$ which does not contain ζ_p (which is possible as any subset of $\{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$ with $p - 1$ elements forms a basis of $\mathbb{Z}[\zeta_p]$.]). Then $\alpha = \sum_i b_i\zeta_p^i$ where $b_i \in \mathbb{Z}$. Therefore comparing coefficients, we get the result. □

lemma 4.4. *Let $p \geq 5$ be an prime number, ζ_p a p-th root of unity and $\alpha \in \mathbb{Z}[\zeta_p]$. Suppose that $x + y\zeta_p^i = u\alpha^p$ with $u \in \mathbb{Z}[\zeta_p]^\times$ and $\alpha \in \mathbb{Z}[\zeta_p]$. Then there is an integer k such that*

$$x + y\zeta_p^i - \zeta_p^{2k}x - \zeta_p^{2k-i}y \equiv 0 \pmod p.$$

Proof. Using lemma 3.5 we have $(x + y\zeta_p^i) = \beta\zeta_p^k\alpha^p$ which is equivalent to $\beta\zeta_p^k a \pmod p$ with a and integer 4.2). Now, if we consider the complex conjugate we have $\overline{(x + y\zeta_p^i)} \equiv \beta\zeta_p^{-k}a \pmod p$. Looking at $(x + y\zeta_p^i) - \zeta_p^{2k}\overline{(x + y\zeta_p^i)}$ then gives the result. □

lemma 4.5. *Let $p \geq 5$ be an prime number, ζ_p a p-th root of unity and $K = \mathbb{Q}(\zeta_p)$. Assume that we have $x, y, z \in \mathbb{Z}$ with $\gcd(xyz, p) = 1$ and such that*

$$x^p + y^p = z^p.$$

Then without loss of generality, we may assume x, y, z are pairwise coprime and

$$x \not\equiv y \mod p.$$

Proof. The first part is easy.

Reducing modulo p, using Fermat's little theorem, you get that if $x \equiv y \equiv -z \pmod p$ then $3z \equiv 0 \pmod p$. But since $p > 3$ this means $p|z$ but this contradicts $\gcd(xyz, p) = 1$. Now, if $x \equiv y \pmod p$ then $x \not\equiv -z \pmod p$ we can relabel y, z so that wlog $x \not\equiv y$ (this uses that p is odd). □

Definition 4.6. A prime number p is called regular if it does not divide the class number of $\mathbb{Q}(\zeta_p)$.

Theorem 4.7. *Let p be an odd regular prime. Then*

$$x^p + y^p = z^p$$

has no solutions with $x, y, z \in \mathbb{Z}$ and $\gcd(xyz, p) = 1$.

Proof. First thing is to note that if $x^p + y^p = z^p$ then

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

as ideals. Then since by 4.1 we know the ideals are coprime, then by lemma 3.7 we have that each $(x + y\zeta_p^i) = \mathfrak{a}^p$, for $\mathfrak{a}$ some ideal. Note that, $[\mathfrak{a}^p] = 1$ in the class group. Now, since p does not divide the size of the class group we have that $[\mathfrak{a}] = 1$ in the class group, so its principal. So we have $x + y\zeta_p^i = u_i\alpha_i^p$ with u_i a unit. So by 4.4 we have some k such that $x + y\zeta_p - \zeta_p^{2k}x - \zeta_p^{2k-1} \equiv 0 \pmod p$. If $1, \zeta_p, \zeta_p^{2k}, \zeta_p^{2k-1}$ are distinct, then 4.3 (which uses that $p > 3$) says that p divides x, y, contrary to our assumption. So they cannot be distinct, but checking each case leads to a contradiction, therefore there cannot be any such solutions. □

Theorem 4.8. *Let p be a regular prime and let $u \in \mathbb{Z}[\zeta_p]^\times$. If $u^p \equiv a \mod p$ for some $a \in \mathbb{Z}$, then there exists $v \in \mathbb{Z}[\zeta_p]^\times$ such that $u = v^p$.*

Theorem 4.9. *Let p be an odd regular prime. Then*

$$x^p + y^p = z^p$$

has no solutions with $x, y, z \in \mathbb{Z}$ and $p|xyz$.

Theorem 4.10. *Let p be an odd regular prime. Then*

$$x^p + y^p = z^p$$

has no solutions with $x, y, z \in \mathbb{Z}$ and $xyz \neq 0$.

References

[Mar18] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, 2018. Second edition of [MR0457396], With a foreword by Barry Mazur.

[Sam70] Pierre Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[Was82] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.