Pierre de Fermat

1608–1665

Paulo Ribenboim

# 13 Lectures on Fermat's Last Theorem



Springer-Verlag
New York Heidelberg Berlin

number is independent of the system of units: $R = 2^{(p-3)/2}|\det(L)|$, where

$$L = \begin{pmatrix} \log|\varepsilon_1^{(1)}| & \cdots & \log|\varepsilon_1^{(r)}| \\ \vdots & & \vdots \\ \log|\varepsilon_r^{(1)}| & \cdots & \log|\varepsilon_r^{(r)}| \end{pmatrix}.$$

$R$ is called the *regulator* of the cyclotomic field $K$.

The explicit determination of a fundamental system of units turns out to be, in general, extremely difficult. I will indicate later its connection with the class number.

Among the units, I have already mentioned the roots of unity (they are $1, -1, \zeta, -\zeta, \ldots, \zeta^{p-1}, -\zeta^{p-1}$) and the elements $(1-\zeta^j)/(1-\zeta^k)$, where $1 \le j \ne k \le p-1$.

Certain units are real numbers, for example the *Kummer units* (*Kreiseinheiten*):

$$\delta_k = \sqrt{\frac{1-\zeta^k}{1-\zeta} \cdot \frac{1-\zeta^{-k}}{1-\zeta^{-1}}} \quad \text{(positive square root)}$$

for $k = 2, \ldots, (p-1)/2$. (It is necessary to prove that

$$\frac{1-\zeta^k}{1-\zeta} \cdot \frac{1-\zeta^{-k}}{1-\zeta^{-1}}$$

is a square in $K$; this follows from (2G) below).

Let $U^+$ be the totality of real units of $K$. It is a subgroup of the group $U$ of all units of $K$. Let $V$ denote the subgroup of $U^+$, generated by the $(p-3)/2$ Kummer units. It is important to compare these three groups $V \subset U^+ \subset U$. First, Kummer proved:

**(2G)** *Every unit of $K$ is the product of a root of unity and a real positive unit.*

The Kummer units are multiplicatively independent: if

$$\prod_{k=2}^{(p-1)/2} \delta_k^{e_k} = 1, \text{ then } e_2 = \cdots = e_{(p-1)/2} = 0.$$

To say that they form a fundamental system of units amounts saying that $V = U^+$. Thus the index of $V$ in $U^+$ measures how far $V$ is from $U^+$ and it will be connected with the class number.

Later I will mention the deepest of Kummer's results about units, which is valid under a special hypothesis about the class number.

## 3. Kummer's Main Theorem

In 1847, Kummer announced his main theorem in a letter to Dirichlet, who then communicated it to the Academy of Sciences of Berlin.

In this proof, published in 1850, Kummer claims that Fermat's equation, for "regular" prime exponents, has only the trivial solution in the cyclotomic



field $\mathbb{Q}(\zeta)$. Yet, his proof contains an "unaccountable lapse" (in Weil's expression; see Kummer's *Collected Papers*, vol. I, Notes by A. Weil, page 955). This concerns the unjustified assumption that a solution $\alpha, \beta, \gamma$ in the cyclotomic field may be chosen such that $\alpha, \beta, \gamma$ have no nontrivial common divisor. However, Kummer's argument did establish without any gaps, that there are no (nontrivial) solutions in ordinary integers when the exponent is a regular prime. Later, in 1897, Hilbert succeeded in adapting Kummer's proof, so as to exclude solutions from the cyclotomic field.

At the beginning, Kummer proved the theorem under two hypothesis about the exponent $p$:

**Hypothesis 1.** The $p$th power of a nonprincipal ideal is never a principal ideal.
**Hypothesis 2.** If $\alpha$ is a cyclotomic unit and there exists an ordinary integer $m$ such that $\alpha \equiv m \pmod{Ap}$, then there exists a unit $\beta$ such that $\alpha = \beta^p$.

In his second communication to the Academy, Kummer writes:

> My proof of Fermat's theorem, which Mr. Lejeune Dirichlet has communicated to the Royal Academy of Sciences, is based on two hypotheses. At that time, I could not in general decide which primes satisfied these hypothesis. For this purpose I was lacking the expression for the number of nonequivalent classes of complex ideal numbers, about which, already for a long time, Mr. Dirichlet has promised an article. After waiting for its publication, I have undertaken, with the help of some oral suggestions from Dirichlet, to derive the required expressions, and I have succeeded not only to discover them, but also to base, on these expressions, both hypotheses in my proof of Fermat's theorem.

Later, I will indicate how Kummer succeeded in characterizing the exponents $p$ for which these hypotheses hold. As a matter of fact, he actually proved that if the first hypothesis is satisfied then the second one follows automatically.

A role is played in the proof by the semi-primary integers. An element $\alpha \in A$ is said to be *semi-primary* if $\alpha \not\equiv 0 \pmod{A\lambda}$ but there exists an ordinary integer $m$ such that $\alpha \equiv m \pmod{A\lambda^2}$. The following lemma will be useful (it is easy to prove):

**Lemma 3.1.**
1. *If $\alpha \equiv m + n\lambda \pmod{A\lambda^2}$, with $m$, $n$ ordinary integers, $m \not\equiv 0 \pmod{p}$ and if $l$ is an integer such that $lm \equiv n \pmod{p}$, then $\zeta^l\alpha$ is semi-primary.*
2. *If $\alpha, \beta \in A$ are semi-primary, there exists an integer $m$ such that $\alpha \equiv m\beta \pmod{A\lambda^2}$.*

In the next lemma, I indicate what can be proved without making any hypothesis concerning the exponent.

**Lemma 3.2.** *Let $p > 2$ be a prime. Assume that $\alpha, \beta, \gamma \in A$ and let*

$$I = \gcd(A(\alpha + \zeta^k\beta) \mid k = 0, 1, \ldots, p-1).$$

1. *If* $\alpha^p + \beta^p + \gamma^p = 0$ *and if* $\lambda \nmid \gamma$, *then for every* $k = 0, 1, \ldots, p-1$ *there exists an ideal* $J_k$ *of* $A$ *such that*

$$A(\alpha + \zeta^k \beta) = J_k^p I. \tag{3.1}$$

*The ideals* $J_0, J_1, \ldots, J_{p-1}$ *are pairwise relatively prime and not multiples of* $A\lambda$.

2. *If* $\alpha^p + \beta^p = \varepsilon \delta^p \lambda^{mp}$, *where* $\varepsilon$ *is a unit of* $A$, $\delta \in A$ *and* $\lambda$ *does not divide* $\alpha, \beta, \delta$, *then* $m \geq 2$.

3. *If* $\alpha^p + \beta^p + \gamma^p = 0$ *and if* $\gamma = \delta \lambda^m$, *with* $m \geq 1$, $\delta \in A$, $\lambda$ *not dividing* $\alpha, \beta, \delta$, *then there exists* $j_0$, $0 \leq j_0 \leq p-1$, *such that for every* $k = 0, 1, \ldots, p-1$ *there exists an ideal* $J_k$ *of* $A$, *such that*

$$\begin{aligned} A(\alpha + \zeta^{j_0}\beta) &= (A\lambda)^{p(m-1)+1} I' J_{j_0}^p, \\ A(\alpha + \zeta^k \beta) &= (A\lambda) I' J_k^p \quad (\text{when } k \neq j_0), \end{aligned} \tag{3.2}$$

*where* $I' = \gcd(A\alpha, A\beta)$. *The ideals* $J_0, J_1, \ldots, J_{p-1}$ *are pairwise relatively prime and not multiples of* $A\lambda$.

PROOF.

(1) To begin

$$-\gamma^p = \alpha^p + \beta^p = \prod_{k=0}^{p-1} (\alpha + \zeta^k \beta). \tag{3.3}$$

First I note that if $1 \leq j < k \leq p-1$, then $\gcd(A(\alpha + \zeta^j\beta), A(\alpha + \zeta^k\beta)) = I$. This is quite easy. Indeed, if $P$ is any prime ideal, $e \geq 1$, and $P^e$ divides both ideals $A(\alpha + \zeta^j\beta)$, $A(\alpha + \zeta^k\beta)$, then

$$\begin{aligned} \alpha + \zeta^j \beta &\in P^e \\ \alpha + \zeta^k \beta &\in P^e. \end{aligned}$$

Then, taking the difference yields

$$(\zeta^j - \zeta^k)\beta = \zeta^j(1 - \zeta^{k-j})\beta \in P^e.$$

But $1 - \zeta^{k-j} \sim 1 - \zeta = \lambda$, so $\lambda\beta \in P^e$ and $P^e \mid A\lambda\beta$.

Similarly $(\zeta^k - \zeta^j)\alpha = \zeta^j(\zeta^{k-j} - 1)\alpha \in P^e$ and $P^e \mid A\lambda\alpha$. But $P \nmid A\lambda$, otherwise $P \mid A\lambda$, so $P = A\lambda$ (both being prime ideals) and from (3.3) $A\lambda \mid A\gamma$ against the hypothesis. It follows that $P^e$ divides $A\alpha$, $A\beta$ and therefore $P^e \mid A(\alpha + \zeta^i\beta)$ for every $i = 0, 1, \ldots, p-1$. This is enough to prove the assertion.

Let

$$J_k' = \frac{A(\alpha + \zeta^k \beta)}{I} \quad \text{for } k = 0, 1, \ldots, \quad p-1, \tag{3.4}$$

so $J_0', J_1', \ldots, J_{p-1}'$ are pairwise relatively prime ideals, not multiples of $A\lambda$ and

$$\left(\frac{A\gamma}{I}\right)^p = \prod_{k=0}^{p-1} J_k'.$$



Then each $J_k'$ is the $p$th power of an ideal $J_k' = J_k^p$, in virtue of the unique factorization theorem for ideals.

(2) Multiplying $\alpha$, $\beta$ by any $p$th roots of 1 still gives algebraic integers satisfying the same equation $\alpha^p + \beta^p = \varepsilon\delta^p\lambda^{mp}$. Thus, by Lemma 3.1, it may be assumed that $\alpha$, $\beta$ are semi-primary integers.

Assume that $m = 1$. Since $\alpha$, $\beta$ are semi-primary, there exist $a, b \in \mathbb{Z}$ such that

$$\alpha \equiv a \pmod{A\lambda^2} \quad \text{and} \quad \beta \equiv b \pmod{A\lambda^2}.$$

Since $Ap = A\lambda^{p-1}$,

$$\alpha^p \equiv a^p \pmod{A\lambda^{p+1}} \quad \text{and} \quad \beta^p \equiv b^p \pmod{A\lambda^{p+1}}.$$

Since $m = 1$, $a^p + b^p = \alpha^p + \beta^p + \rho\lambda^{p+1} = \varepsilon\lambda^p(\delta^p + \varepsilon^{-1}\rho\lambda)$, where $p \in A$, $\lambda \nmid \delta$.

If $p^e$ is the exact power of $p$ dividing $a^p + b^p$ (with $e \geq 0$), then the exact power of $A\lambda$ dividing $A(a^p + b^p)$ is a multiple of $p-1$, because $Ap = A\lambda^{p-1}$. Since $\lambda \nmid \delta$, $A\lambda \nmid A(\delta^p + \varepsilon^{-1}\rho\lambda)$, so the exact power of $A\lambda$ dividing the ideal $A(\varepsilon\lambda^p(\delta^p + \varepsilon^{-1}\rho\lambda))$ is $A\lambda^p$—a contradiction. This proves that $m \geq 2$.

(3) From

$$\varepsilon\delta^p\lambda^{mp} = \alpha^p + \beta^p = \prod_{k=0}^{p-1} (\alpha + \zeta^k\beta) \tag{3.5}$$

it follows that there exists $j$, $0 \leq j \leq p-1$ such that $A\lambda \mid A(\alpha + \zeta^j\beta)$.

But then $A\lambda \mid A(\alpha + \zeta^k\beta)$ for every index $k$. Indeed, if $k \neq j$, then $\alpha + \zeta^k\beta = (\alpha + \zeta^j\beta) + \zeta^j(\zeta^{k-j} - 1)\beta$ and $\zeta^{k-j} - 1 \sim \lambda$. So

$$\frac{\alpha + \beta}{\lambda}, \frac{\alpha + \zeta\beta}{\lambda}, \ldots, \frac{\alpha + \zeta^{p-1}\beta}{\lambda} \in A.$$

These elements are pairwise incongruent modulo $A\lambda$. Otherwise,

$$\alpha + \zeta^j\beta \equiv \alpha + \zeta^k\beta \pmod{A\lambda^2}$$

with $j \neq k$. So $\lambda^2 \mid (\zeta^j - \zeta^k)\beta \sim \lambda\beta$ and $\lambda \mid \beta$, against the hypothesis.

Since the number of congruence classes modulo $\lambda$ is $p$, there exists an unique index $j_0$, such that $(\alpha + \zeta^{j_0}\beta)/\lambda^p \equiv 0 \pmod{A\lambda}$, that is, $\lambda^2 \mid \alpha + \zeta^{j_0}\beta$ and $\lambda^2 \nmid \alpha + \zeta^k\beta$ for $k \neq j_0$. So from (3.5)

$$(A\lambda)^{mp-(p-1)} = A\lambda^{p(m-1)+1} \quad \text{divides } A(\alpha + \zeta^{j_0}\beta)$$

and $p(m-1) + 1 > 1$ since $m \geq 2$ (by part (2)).

If $I' = \gcd(A\alpha, A\beta)$, then $I' \mid A(\alpha + \zeta^k\beta)$ for every $k$ and $A\lambda \nmid I'$. Hence

$$\begin{aligned} A(\alpha + \zeta^{j_0}\beta) &= (A\lambda)^{p(m-1)+1} I' J_{j_0}', \\ A(\alpha + \zeta^k \beta) &= (A\lambda) I' J_k' \quad (\text{for } k \neq j_0), \end{aligned} \tag{3.6}$$

where $J_0', J_1', \ldots, J_{p-1}'$ are ideals, not multiples of $A\lambda$.

These ideals are pairwise relatively prime: if $P$ is a prime ideal dividing $J_j'$, $J_k'$ $(k \neq j)$, then $(A\lambda)I'P$ divides $A(\alpha + \zeta^j\beta)$, $A(\alpha + \zeta^k\beta)$, hence also $A(\beta - \zeta^{j-k}\beta) = (A\lambda)A\beta$, so $I'P \mid A\beta$. Similarly $I'P \mid A\alpha$, hence $I'P$ divides $I' = \gcd(A\alpha, A\beta)$, which is impossible.

Multiplying the relations (3.6) yields

$$(A\delta)^p(A\lambda)^{mp} = \prod_{k=0}^{p-1} A(\alpha + \zeta^k\beta) = (A\lambda)^{mp} I'^p J'_0 \cdots J'_{p-1}$$

so

$$(A\delta)^p = I'^p J'_0 \cdots J'_{p-1}.$$

By the unique factorization of ideals, for each $k$ there exists an ideal $J_k$ such that $J'_k = J_k^p$ and clearly $A\lambda \nmid J_k$ moreover these ideals are pairwise relatively prime.

In view of (3.6) this concludes the proof. □

A prime $p$ is said to be *regular* if $p$ does not divide the class number $h = h(p)$ of the cyclotomic field $K$.

**Lemma 3.3.** *The prime $p$ is regular if and only if the* pth *power of a non-principal ideal of $A$ is never a principal ideal.*

PROOF. By definition $p$ is regular when $p$ does not divide the order $h$ of the class group $\mathscr{C}\ell(K)$. This means that the $p$-Sylow subgroup of $\mathscr{C}\ell(K)$ is trivial. In other words, there is no element $[J]$ in $\mathscr{C}\ell(K)$ having order $p$: if $[J]^p = [A]$, then $[J] = [A]$. Or equivalently, if $J^p$ is a principal ideal, then $J$ is already a principal ideal. □

I have indicated already that Kummer succeeded in proving that first hypothesis implies the second. This is the contents of his difficult and important *lemma on units*:

**Lemma 3.4.** *If $p$ is a regular prime, if $\alpha$ is a unit of $A$ such that there exists $m \in \mathbb{Z}$ satisfying the congruence $\alpha \equiv m \pmod{Ap}$, then $\alpha = \beta^p$, where $\beta$ is a unit of $A$.*

In order to prove this lemma, Kummer introduced $\lambda$-adic methods. I shall give a full proof of this lemma in my forthcoming other book on Fermat's theorem.

And now, finally, here is Kummer's main theorem:

**(3A)** *If $p$ is a regular prime, there exist no (nonzero) cyclotomic integers $\alpha, \beta, \gamma$ such that $\alpha^p + \beta^p + \gamma^p = 0$.*

PROOF. By Gauss's theorem for the exponent 3, the assertion is true for $p = 3$. I shall assume the theorem false (hence $p > 3$) and will consider the traditional two cases.

*First Case.* $\alpha, \beta, \gamma$ are not multiples of $\lambda = 1 - \zeta$.

I may assume $p \geq 7$. Indeed, if $p = 5$, then $\alpha, \beta, \gamma$ are congruent modulo $A\lambda$ to the integers $\pm 1$, or $\pm 2$, because $A/A\lambda = \mathbb{F}_5$ (the field with 5 elements).



Then $\alpha^5, \beta^5, \gamma^5$ are congruent to $\pm 1$, or $\pm 32$, modulo $A\lambda^5$ (note that $A5 = A\lambda^4$). In any case, $\alpha^5 + \beta^5 + \gamma^5 \not\equiv 0 \pmod{A\lambda^5}$, so the theorem would be true for the exponent 5.

Thus, let $p \geq 7$.

Multiplying $\alpha, \beta$ by any root of 1 still gives algebraic integers satisfying the same relation. So, by Lemma 3.1, it is possible to assume, without loss of generality, that $\alpha, \beta$ are semi-primary integers in $K$.

By Lemma 3.2

$$A(\alpha + \zeta^k\beta) = J_k^p I \qquad (k = 0,1,\ldots,p-1),$$

where the ideals $J_0, J_1, \ldots, J_{p-1}$ are pairwise relatively prime and not multiples of $A\lambda$, and $I = \gcd(A(\alpha+\beta), A(\alpha+\zeta\beta), \ldots, A(\alpha+\zeta^{p-1}\beta))$.

Since $\alpha + \zeta^{p-1}\beta \not\equiv 0 \pmod{A\lambda}$, because $A\lambda$ does not divide $A\gamma$, there exists a root of unity $\zeta'$ such that $\zeta'(\alpha + \zeta^{p-1}\beta)$ is a semi-primary integer. Let

$$\alpha' = \frac{\alpha}{\zeta'(\alpha + \zeta^{p-1}\beta)}, \qquad \beta' = \frac{\beta}{\zeta'(\alpha + \zeta^{p-1}\beta)}.$$

Hence $\alpha' + \zeta^{p-1}\beta' = \zeta'^{-1}$ and $A(\alpha' + \zeta^k\beta') = (J_k/J_{p-1})^p$ for $k = 0, 1, \ldots, p-2$.

The fractional ideals $(J_k/J_{p-1})^p$ are principal, and $p$ is a regular prime. By Lemma 3.3, $J_k/J_{p-1}$ is also a principal ideal, say $J_k/J_{p-1} = A(\mu_k/n_k)$ (for $k = 0,1,\ldots,p-2$), where $\mu_k \in A$, $n_k \in \mathbb{Z}$ and $\mu_k$, $n_k$ have no common factor (not a unit) in $A$. We note also that $A\lambda$ does not divide $A\mu_k$, $An_k$.

Taking into account (2G), then

$$\alpha' + \zeta^k\beta' = \varepsilon_k\zeta^{c_k}\left(\frac{\mu_k}{n_k}\right) \qquad (0 \leq k \leq p-2), \tag{3.7}$$

where $\varepsilon_k$ is a real unit of $K$, $0 \leq c_k \leq p-1$. Since $A/A\lambda = \mathbb{F}_p$, $\mu_k \equiv m_k \pmod{A\lambda}$, where $m_k \in \mathbb{Z}$. Hence $\mu_k^p \equiv m_k^p \pmod{A\lambda^p}$ because $Ap = A\lambda^{p-1}$. Therefore

$$n_k(\alpha' + \zeta^k\beta') \equiv \varepsilon_k\zeta^{c_k}m_k^p \pmod{A\lambda^p}$$

(for $k = 0,1,\ldots,p-2$). Considering the complex-conjugates, we have

$$n_k(\overline{\alpha'} + \zeta^{-k}\overline{\beta'}) \equiv \varepsilon_k\zeta^{-c_k}m_k^p \pmod{A\lambda^p}$$

(because $\overline{\lambda} = 1 - \zeta^{-1}$ is associate to $\lambda$). Hence $\varepsilon_k m_k^p \equiv \zeta^{-c_k}n_k(\alpha' + \zeta^k\beta') \equiv \zeta^{c_k}n_k(\overline{\alpha'} + \zeta^{-k}\overline{\beta'}) \pmod{A\lambda^p}$ and since $A\lambda$ does not divide $An_k$,

$$\alpha' + \zeta^k\beta' \equiv \zeta^{2c_k}(\overline{\alpha'} + \zeta^{-k}\overline{\beta'}) \pmod{A\lambda^p}. \tag{3.8}$$

We now evaluate the exponents $c_k$. Since $\alpha$, $\beta$, $\zeta'(\alpha + \zeta^{p-1}\beta)$ are semi-primary integers, it follows from Lemma 3.1 that there exist rational integers $a, b$ such that

$$\alpha \equiv a\zeta'(a + \zeta^{p-1}\beta) \pmod{A\lambda^2},$$
$$\beta \equiv b\zeta'(a + \zeta^{p-1}\beta) \pmod{A\lambda^2}.$$

Since $A\lambda \nmid A(\alpha + \zeta^{p-1}\beta)$,

$$\alpha' + \zeta^k\beta' \equiv a + \zeta^k b \pmod{A\lambda^2}.$$

Similarly

$$\overline{\alpha}' + \zeta^{-k}\overline{\beta}' \equiv a + \zeta^{-k}b \pmod{A\lambda^2}.$$

But $\zeta^j = (1-\lambda)^j \equiv 1 - j\lambda \pmod{A\lambda^2}$ for every $j \in \mathbb{Z}$. Hence

$$a + b - kb\lambda \equiv (1 - 2c_k\lambda)(a + b + kb\lambda) \pmod{A\lambda^2}$$

so

$$2c_k(a+b)\lambda \equiv 2kb\lambda \pmod{A\lambda^2}$$

hence

$$c_k(a+b) \equiv kb \pmod{A\lambda}.$$

Since $a, b, c_k, k \in \mathbb{Z}$,

$$c_k(a+b) \equiv kb \pmod{p}.$$

From $\alpha + \zeta^{p-1}\beta \equiv (a + \zeta^{p-1}b)\zeta'(\alpha + \zeta^{p-1}\beta) \pmod{A\lambda^2}$ it follows that

$$1 \equiv (a + \zeta^{p-1}b)\zeta' \pmod{A\lambda^2}.$$

But $\zeta \equiv 1 \pmod{A\lambda}$, hence $\zeta^{p-1} \equiv \zeta' \equiv 1 \pmod{A\lambda}$, so

$$a + b \equiv 1 \pmod{A\lambda},$$

hence $a + b \equiv 1 \pmod{p}$, so $c_k \equiv kb \pmod{p}$ for $k = 0, 1, \ldots, p-2$.

In particular

$$c_0 \equiv 0 \pmod{p}, \qquad c_1 \equiv b \pmod{p}, \qquad c_2 \equiv 2b \pmod{p}, \qquad c_3 \equiv 3b \pmod{p}.$$

Thus we may rewrite (3.8) as follows (for $k = 0,1,2,3$):

$$\begin{aligned} \alpha' + \beta' - \overline{\alpha}' - \overline{\beta}' &= \rho_0\lambda^p, \\ \alpha' + \zeta\beta' - \zeta^{2b}\overline{\alpha}' - \zeta^{2b-1}\overline{\beta}' &= \rho_1\lambda^p, \\ \alpha' + \zeta^2\beta' - \zeta^{4b}\overline{\alpha}' - \zeta^{4b-2}\overline{\beta}' &= \rho_2\lambda^p, \\ \alpha' + \zeta^3\beta' - \zeta^{6b}\overline{\alpha}' - \zeta^{6b-3}\overline{\beta}' &= \rho_3\lambda^p, \end{aligned} \tag{3.9}$$

where $\rho_0, \rho_1, \rho_2, \rho_3 \in A$.

Consider the matrix of coefficients

$$M = \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & \zeta & -\zeta^{2b} & -\zeta^{2b-1} \\ 1 & \zeta^2 & -\zeta^{4b} & -\zeta^{4b-2} \\ 1 & \zeta^3 & -\zeta^{6b} & -\zeta^{6b-3} \end{pmatrix}.$$

By Cramer's rule

$$\alpha' = \frac{\det(M_1)}{\det(M)}, \qquad \beta' = \frac{\det(M_2)}{\det(M)}, \qquad \overline{\alpha}' = \frac{\det(M_3)}{\det(M)}, \qquad \overline{\beta}' = \frac{\det(M_4)}{\det(M)},$$

where $M_i$ is the matrix obtained from $M$ by replacing the $i$th column by the right-hand side of the relations (3.9). Thus $\det(M_i) \in A\lambda^p$ and since $A\lambda$ does not divide $A\alpha', A\beta', A\overline{\alpha}', A\overline{\beta}'$, then necessarily $A\lambda^p$ divides $\det(M)$, that is

$$(1-\zeta)(1-\zeta^{2b})(1-\zeta^{2b-1})(\zeta-\zeta^{2b})(\zeta-\zeta^{2b-1})(\zeta^{2b}-\zeta^{2b-1}) \equiv 0 \pmod{A\lambda^p}. \tag{3.10}$$



We discuss several possibilities.

1. $b \equiv 0 \pmod{p}$: then $\beta \equiv 0 \pmod{A\lambda}$, against the hypothesis.
2. $b \equiv 1 \pmod{p}$: then $\beta \equiv \alpha + \beta \pmod{A\lambda}$, hence $\alpha \equiv 0 \pmod{A\lambda}$, against the hypothesis.
3. $n \not\equiv 0, 1 \pmod{p}$ and $2b \not\equiv 1 \pmod{p}$: then all the factors in (3.10) are associated with $\lambda$, thus $\lambda^p$ divides $\lambda^6$, so $p \le 6$, against the hypothesis.
4. $b \not\equiv 0, 1 \pmod{p}$ and $2b \equiv 1 \pmod{p}$: then $2\beta \equiv \alpha + \beta \pmod{A\lambda}$ so $\alpha \equiv \beta \pmod{A\lambda}$.

In view of the symmetry of the relation $\alpha^p + \beta^p + \gamma^p = 0$, we must also have $\alpha \equiv \gamma \pmod{A\lambda}$. But $\alpha^p \equiv \alpha$, $\beta^p \equiv \beta$, $\gamma^p \equiv \gamma \pmod{A\lambda}$, because $A/A\lambda = \mathbb{F}_p$. It follows that $\alpha + \beta + \gamma \equiv 3\alpha \equiv 0 \pmod{A\lambda}$ so $\alpha \equiv 0 \pmod{A\lambda}$ contradicting the hypothesis. So, we have again reached a contradiction, concluding the proof for the first case.

*Second Case.* $\lambda$ divides $\alpha$, $\beta$, or $\gamma$.

We assume without loss of generality that $\lambda$ divides $\gamma$.

We may write $\gamma = \delta\lambda^m$, where $\delta \in A$, $\lambda$ does not divide $\delta$, and

$$\alpha^p + \beta^p = -\delta^p\lambda^{mp}.$$

So there is a relation of the form

$$\alpha^p + \beta^p = \varepsilon\delta^p\lambda^{mp}, \tag{3.11}$$

where $\varepsilon$ is a unit, $\lambda$ does not divide $\delta$ and $m$ is minimal. By Lemma 3.2, $m \ge 2$. It follows that $\lambda$ does not divide $\alpha$ otherwise $\lambda$ also divides $\beta$ and from (3.11), after dividing by $\lambda^p$, we would obtain a similar relation with exponent $(m-1)p$ for $\lambda$, against the minimality of $m$. Similarly $\lambda$ does not divide $\beta$.

Our purpose will be to derive a relation analogous to (3.11) with smaller exponent of $\lambda$. By Lemma 3.2, after changing $\beta$ into $\zeta^{j_0}\beta$ (without loss of generality), we may write

$$\begin{aligned} A(\alpha+\beta) &= (A\lambda)^{p(m-1)+1}I'J_0^p, \\ A(\alpha+\zeta^k\beta) &= (A\lambda)I'J_k^p \quad (\text{for } 1 \le k \le p-1), \end{aligned} \tag{3.12}$$

where $I' = \gcd(A\alpha, A\beta)$, and the ideals $J_0, J_1, \ldots, J_{p-1}$ are pairwise relatively prime and not multiples of $A\lambda$. Then

$$A\left(\frac{\alpha+\zeta^k\beta}{\alpha+\beta}\right) = (A\lambda)^{-p(m-1)}\left(\frac{J_k}{J_0}\right)^p \qquad (1 \le k \le p-1). \tag{3.13}$$

This shows that the fractional ideals $(J_k/J_0)^p$ are principal and since $p$ is regular, $J_k/J_0$ is also principal. Thus there exist elements $\mu_k \in A$, $n_k \in \mathbb{Z}$ such that $J_k/J_0 = A(\mu_k/n_k)$. Since $A\lambda$ does not divide $J_k$ $(0 \le k \le p-1)$, we may assume that $\lambda$ does not divide the elements $\mu_k$, $n_k$. So there exist units $\varepsilon_k$ of $A$ such that

$$(\alpha+\zeta^k\beta)\lambda^{p(m-1)} = \varepsilon_k(\alpha+\beta)\left(\frac{\mu_k}{n_k}\right)^p \qquad (1 \le k \le p-1).$$

In particular, if $k = 1, 2$, then

$$(\alpha + \zeta\beta)\lambda^{p(m-1)} = \varepsilon_1(\alpha + \beta)\left(\frac{\mu_1}{n_1}\right)^p,$$

$$(\alpha + \zeta^2\beta)\lambda^{p(m-1)} = \varepsilon_2(\alpha + \beta)\left(\frac{\mu_2}{n_2}\right)^p.$$

Multiplying the first relation by $1 + \zeta$ and then subtracting the second relation gives

$$\zeta(\alpha + \beta)\lambda^{p(m-1)} = (\alpha + \beta)\left[\left(\frac{\mu_1}{n_1}\right)^p \varepsilon_1(1 + \zeta) - \left(\frac{\mu_2}{n_2}\right)^p \varepsilon_2\right].$$

Hence

$$(\mu_1 n_2)^p - \frac{(\mu_2 n_1)^p \varepsilon_2}{\varepsilon_1(1 + \zeta)} = \frac{\zeta}{\varepsilon_1(1 + \zeta)} \lambda^{p(m-1)}(n_1 n_2)^p.$$

But $1 + \zeta$ is a unit of $A$ and the above relation has the form:

$$(\alpha')^p + \varepsilon'(\beta')^p = \varepsilon''(\delta')^p \lambda^{(m-1)p}, \tag{3.14}$$

where $\alpha' = \mu_1 n_2$, $\beta' = \mu_2 n_1$, $\delta' = n_1 n_2$, $\lambda \nmid \delta'$, and $\varepsilon'$, $\varepsilon''$ are units. This is not yet like relation (3.11), but we shall transform it into a relation of that type.

Since $p(m-1) \geq p$, $\lambda^p$ divides $(\alpha')^p + \varepsilon'(\beta')^p$. But $A\beta' = A\mu_2 n_1$ is relatively prime to $A\lambda$, i.e., $A\beta' + A\lambda = A$, so there exists an element $\kappa \in A$ such that $\kappa\beta' \equiv 1 \pmod{A\lambda}$. Then $\kappa^p \beta'^p \equiv 1 \pmod{A\lambda^p}$ and $(\kappa\alpha')^p + \varepsilon' \equiv 0 \pmod{A\lambda^p}$. So there exists $\rho \in A$ such that $\varepsilon' \equiv \rho^p \pmod{A\lambda^p}$. But $A/A\lambda = \mathbb{F}_p$ so there exists $r \in \mathbb{Z}$ such that $\rho \equiv r \pmod{A\lambda}$. Then $\varepsilon' \equiv \rho^p \equiv r^p \pmod{A\lambda^p}$. By Kummer's Lemma 3.4 on units, $\varepsilon'$ is the $p$th power of a unit $\varepsilon_1'$ in $A$: $\varepsilon' = (\varepsilon_1')^p$ and we may rewrite (3.14) as follows:

$$(\alpha')^p + (\varepsilon_1'\beta')^p = \varepsilon''(\delta')^p \lambda^{(m-1)p}. \tag{3.15}$$

This is now a relation like (3.11), with $m - 1$ instead of $m$. This contradicts the choice of a minimal $m$, and the proof is concluded. □

In particular, if $p$ is a regular prime, there exist no nonzero integers $x, y, z \in \mathbb{Z}$ such that $x^p + y^p + z^p = 0$.

In order to understand the force of Kummer's theorem, it will be necessary to find out which primes are regular. Is there any neat characterization of regularity? This, and other questions, will be considered in the next lecture.

# Bibliography

1846 Dirichlet, G. L.
Zur Theorie der Complexen Einheiten. Bericht Acad. d. Wiss., Berlin, 1846, 103–107. Also in *Werke*, Vol. I, G. Reimer Verlag, Berlin, 1889, 640–643. (Reprinted by Chelsea Publ. Co., New York, 1969).



1847 Kummer, E. E.*
Zur Theorie der complexen Zahlen. *J. reine u. angew. Math.*, **35**, 1847, 319–326.

1847 Kummer, E. E.
Beweis des Fermatschen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen $\lambda$. *Monatsber. Akad. d. Wiss., Berlin*, 1847, 132–139, 140–141, 305–319.

1847 Kummer, E. E.
Über die Zerlegung der aus Wurzeln der Einheit Gebildeten complexen Zahlen in ihren Primfactoren. *J. reine u. angew Math.*, **35**, 1847, 327–367.

1847 Dirichlet, G. L.
Bemerkungen zu Kummer's Beweis des Fermat schen Satzes, die Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl von Primzahlen $\lambda$ betreffend. *Monatsber. Akad. d. Wiss.*, 1847, 139–141. Also in *Werke*, vol. II, G. Reimer Verlag, Berlin, 1889, 254–255. Reprinted by Chelsea Publ. Co., New York, 1969.

1850 Kummer, E. E.
Allgemeiner Beweis des Fermat'schen Satzes dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten $\lambda$, welche ungerade Primzahlen sind und in die Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoulli'schen Zahlen als Factoren nicht Vorkommen. *J. reine u. angew. Math.*, **40**, 1850, 130–138.

1897 Hilbert, D.
Die Theorie der algebraischen Zahlkörper. *Jahresber. d. Deutschen Math. Verein.* **4**, 1897, 175–546. Also in *Gesammelte Abhandlungen*, vol. I. Springer-Verlag, Berlin, 1932. Reprinted by Chelsea Publ. Co., New York, 1965.

* See also *Collected Papers*, vol. I, edited by A. Weil, Springer-Verlag, Berlin, 1975.