Fermat's Last Theorem: an Introduction

Rodney Coleman, Laurent Zwald

Fermat's Last Theorem: an Introduction

Rodney Coleman, Laurent Zwald

June 7, 2021

Abstract

The aim of this note is to present the famous last theorem of Pierre Fermat with some elementary results. Our object is not to give a complete proof of this result, but rather to give the proof of certain special cases. These in themselves require considerable work and should give an idea of why the general result took so long to prove.

Fermat's Last Theorem considers the existence of non-trivial solutions in the integers of the equation

$$X^n + Y^n = Z^n.$$

For $n = 2$ there are solutions, in fact an infinite number, but for $n > 2$ there are no solutions.

The case $n = 2$: $X^2 + Y^2 = Z^2$.

We consider solutions $(x, y, z) \in \mathbf{Z}^3$, where x, y, z are coprime, because any solution is a multiple of a solution with all three elements coprime. This implies that x, y, z are pairwise coprime: if p divides two of the elements, then p divides the third, which is not possible, because the three elements are coprime. As $\gcd(x, y) = 1$, x or y must be odd; without loss of generality, suppose that x is odd. This implies that y is even. (If y is odd, then $x^2 + y^2 \equiv 2 \pmod 4$, which is impossible, because 2 is not a square modulo 4.) Now

$$x^2 + y^2 = z^2 \Longrightarrow (z + x)(z - x) = y^2 \Longrightarrow \frac{z + x}{y} \cdot \frac{z - x}{y} = 1 \Longrightarrow \frac{z + x}{y} = \frac{y}{z - x}.$$

There exist integers m and n such that $\gcd(m, n) = 1$ and $\frac{z+x}{y} = \frac{m}{n}$. Then $\frac{y}{z-x} = \frac{n}{m}$ and we have

$$\frac{z}{y} + \frac{x}{y} = \frac{m}{n} \qquad \text{and} \qquad \frac{z}{y} - \frac{x}{y} = \frac{n}{m},$$

from which we obtain

$$\frac{z}{y} = \frac{1}{2}\left(\frac{m}{n} + \frac{n}{m}\right) = \frac{m^2 + n^2}{2mn} \qquad \text{and} \qquad \frac{x}{y} = \frac{1}{2}\left(\frac{m}{n} - \frac{n}{m}\right) = \frac{m^2 - n^2}{2mn}.$$

As $\gcd(m, n) = 1$, m and n cannot both be even. If they are both odd, then $m^2 - n^2 \equiv 0 \pmod 4$, which implies that $4 | m^2 - n^2$ and $2mn \equiv 2 \pmod 4$, implying that $2mn$ is not a multiple of 4. However, $2mnx = y(m^2 - n^2)$, which is not possible, because 8 divides the right-hand side of the expression, which is not the case for the left-hand side. Hence m and n are not both odd. It follows that m and n have different parities and so $m^2 + n^2$ and $m^2 - n^2$ are odd.

We claim that $\gcd(m^2 \pm n^2, 2mn) = 1$. As $m^2 \pm n^2$ is odd, 2 does not divide $m^2 \pm n^2$. If p is an odd prime and p divides both $m^2 \pm n^2$ and $2mn$, then p divides m or n. Without loss of

generality let us suppose that p divides m. Then p divides m^2 which implies that p divides n^2 and so n, which is not possible, because m and n are coprime. This proves our claim. It follows that $\frac{m^2+n^2}{2mn}$ and $\frac{m^2-n^2}{2mn}$ are both fully reduced. Thus up to sign we can write

$$x = m^2 - n^2 \qquad y = 2mn \qquad z = m^2 + n^2.$$

We have thus found the form of possible solutions. Now let us suppose that m, n are integers of different parities and coprime. Setting

$$x = m^2 - n^2 \qquad y = 2mn \qquad z = m^2 + n^2,$$

we obtain

$$x^2 + y^2 = (m^2 - n^2)^2 + 4m^2n^2 = (m^2 + n^2)^2 = z^2,$$

so (x, y, z) is a solution. In addition x, y and z are coprime: Let p be prime dividing the three elements. As x is odd, $p \neq 2$, so p must be odd. If p divides y, then p divides m or n, but not both, because m and n are coprime. Without loss of generality, suppose that p divides m. If p divides x, then p divides $m^2 - n^2$, which implies that p divides n^2 and hence p divides n, a contradiction, so p does not divide x. We deduce that x, y and z are coprime. To sum up, we have

Theorem 1 *The solutions (x, y, z) of the equation $X^2 + Y^2 = Z^2$, with x, y and z coprime, have the form*

$$x = m^2 - n^2 \qquad y = 2mn \qquad z = m^2 + n^2,$$

or

$$y = m^2 - n^2 \qquad x = 2mn \qquad z = m^2 + n^2,$$

where m, n are coprime and of different parities.

Examples $(3, 4, 5)$, with $m = 2, n = 1$; $(5, 12, 13)$, with $m = 3, n = 2$. More generally, any pair of nonzero adjacent integers $\{2b, 2b + 1\}$ or $\{2b - 1, 2b\}$ "generate" a solution.

The case $n = 4$: $X^4 + Y^4 = Z^4$.

We aim to show that in this case there are no nontrivial solutions. Suppose that (x, y, z) is a nontrivial solution of the equation. We may suppose that x, y and z are coprime, from which we deduce that x, y and z are pairwise coprime. Then $x^4 + y^4 = (z^2)^2$, so the equation

$$X^4 + Y^4 = Z^2$$

has a solution. It is sufficient to show that this equation has no nontrivial solution. Suppose that (x, y, z) is a nontrivial solution of this equation, with x, y and z coprime. We may suppose that z is positive and minimal. As in the the case $n = 2$, we may assume that x and z are odd and y even. Reasoning as above we may find m and n coprime and of differnt parities such that

$$x^2 = m^2 - n^2 \qquad y^2 = 2mn \qquad z = m^2 + n^2,$$

from which we deduce

$$x^2 + n^2 = m^2.$$

If x and n are both odd, then $x^2 + n^2 \equiv 2 \pmod 4$, which is impossible, because m^2 cannot be congruent to 2 modulo 4. Thus x and n cannot both be odd. As x is odd, n must be even.

In addition, x, m and n are coprime: It is sufficient to show that x and m are coprime. If p is a prime dividing x and m, then p divides $m^2 - n^2$ and m, which implies that p divides n^2 and hence n, which is not possible, because m and n are coprime. Hence x and m are coprime.

We now may use the argument of the case $n = 2$ to deduce the existence of coprime integers a and b, with different parities, such that

$$x = a^2 - b^2 \qquad n = 2ab \qquad m = a^2 + b^2,$$

from which we obtain

$$y^2 = 4ab(a^2 + b^2).$$

The numbers a, b and $a^2 + b^2$ are pairwise coprime. As $\mathbf{Z}$ is a UFD, we may write $a = \alpha^2$, $b = \beta^2$ and $a^2 + b^2 = \gamma^2$, with $\alpha, \beta, \gamma \in \mathbf{N}^*$. Then

$$\gamma^2 = a^2 + b^2 = \alpha^4 + \beta^4,$$

and

$$0 < \gamma \leq \gamma^2 = a^2 + b^2 = m < m^2 + n^2 = z$$

Thus (α, β, γ) is a solution of the equation $X^4 + Y^4 = Z^2$, with $\gamma < z$, contradicting the minimality of z. Thus we have proved the following result:

Theorem 2 *The equation $X^4 + Y^4 = Z^4$ has no nontrivial solution.*

Corollary 1 *If n is a multiple of 4, then the equation $X^n + Y^n = Z^n$ has no nontrivial solution.*

The case $n = 3$: $X^3 + Y^3 = Z^3$.

Our aim here is to show, as in the previous case, that there is no nontrivial solution, i.e., (x, y, z) with $xyz \neq 0$. We need a preliminary result. We recall that, if $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$, then the ring $\mathbf{Z}[\omega]$, referred to as the ring of Eisenstein integers, is Euclidean. It is not difficult to see that $\mathbf{Z}[\sqrt{-3}] \subset \mathbf{Z}[\omega]$.

FERMATlem1 **Lemma 1** *If $x \in \mathbf{Z}[\omega]$, the ring of Eisenstein integers, then there exists $\epsilon \in \mathbf{Z}[\omega]^\times$ such that $x\epsilon \in \mathbf{Z}[\sqrt{-3}]$*

PROOF Let $x \in \mathbf{Z}[\omega]$. There exist $a, b \in \mathbf{Z}$ such that $x = a + b\omega = \frac{(2a-b)+ib\sqrt{3}}{2}$. We set $u = 2a - b$. We notice that u and b have the same parity, hence $u + b$ is even. We recall that the units in $\mathbf{Z}[\omega]$ are $\pm 1, \pm\omega, \pm\omega^2$. If u and b are both even, then there is nothing to prove, so let us suppose that this not the case.

Case 1: $u \equiv 1 \pmod 4$, $b \equiv -1 \pmod 4$:

$$\frac{u + ib\sqrt{3}}{2}(\omega^2) = \frac{u + ib\sqrt{3}}{2} \cdot \frac{-1 - i\sqrt{3}}{2} = \frac{1}{4}\left((-u + 3b) - i\sqrt{3}(u + b)\right) \in \mathbf{Z}[\sqrt{-3}].$$

Case 2: $u \equiv -1 \pmod 4$, $b \equiv 1 \pmod 4$:

$$\frac{u + ib\sqrt{3}}{2}(-\omega^2) = \frac{1}{4}\left((3b - u) + i\sqrt{3}(u + b)\right) \in \mathbf{Z}[\sqrt{-3}].$$

Case 3: $u \equiv -1 \pmod 4$, $b \equiv -1 \pmod 4$:

$$\frac{u + ib\sqrt{3}}{2}(\omega) = \frac{u + ib\sqrt{3}}{2} \cdot \frac{-1 + i\sqrt{3}}{2} = \frac{1}{4}\left((-u - 3b) + i\sqrt{3}(u - b)\right) \in \mathbf{Z}[\sqrt{-3}].$$

Case 4: $u \equiv 1 \pmod 4$, $b \equiv 1 \pmod 4$:

$$\frac{u+ib\sqrt{3}}{2}(-\omega) = -\frac{u+ib\sqrt{3}}{2} \cdot \frac{1-i\sqrt{3}}{2} = \frac{1}{4}\Big((u+3b)+i\sqrt{3}(b-u)\Big) \in \mathbf{Z}[\sqrt{-3}].$$

This ends the proof. □

We turn now to the proof of the main result. There is a nontrivial solution of the equation, if and only if there is a nontrivial soltion of the equation $X^3+Y^3+Z^3=0$. Let (x,y,z) be such a solution:

$$x^3+y^3+z^3=0,$$

with $xyz \neq 0$. We may assume that x, y and z are coprime and then deduce that they are pairwise coprime. There is one and only one element even. Clearly, one element must be even. Two of the elements cannot be even, because this would imply that the third is even. Without loss of generality we suppose that y is even and x and z odd. We also suppose that $|y|$ is minimal. We set $a = \frac{x+z}{2}$ and $b = \frac{x-z}{2}$, which implies that $x = a+b$ and $z = a-b$, so we obtain

$$(a+b)^3+y^3+(a-b)^3 = 0 \Longrightarrow 2a(a^2+3b^2) = -y^3.$$

As x and z are coprime, so are a and b. Also, a and b have different parities, because x is odd, hence a^2+3b^2 is odd. Since y is even, 8 divides $2a$ and so a is even and b odd. If p is a prime divisor of $2a$ and a^2+3b^2, then p is odd and so divides a and hence $3b^2$. Because a and b are coprime, p does not divide b and it follows that p divides 3. Hence $p=1$ or $p=3$ and it follows that $\gcd(2a, a^2+3b^2) = 1$ or $\gcd(2a, a^2+3b^2) = 3$. From hereon we will work in $\mathbf{Z}[\omega]$, the ring of Eisenstein integers. Since $\mathbf{Z}[\omega]$ is a Euclidean domain, it is a UFD; in addition its norm is defined as follows: for $z = u+v\omega$, we have $N(z) = z\bar{z} = u^2-uv+v^2$. The units are $\pm 1, \pm\omega, \pm\omega^2$, which are all sixth roots of unity.

Case 1: $\gcd(2a, a^2+3b^2) = 1$.

Considering the factorization into primes of $2a$, a^2+3b^2 and $-y^3$, we deduce that there are integers r and s such that $2a = r^3$ and $a^2+3b^2 = s^3$, with r even and s odd. Since $\mathbf{Z}[\sqrt{-3}] \subset \mathbf{Z}[\omega]$,

$$(a+ib\sqrt{3})(a-ib\sqrt{3}) = a^2+3b^2 = s^3$$

is a factorization in the UFD $\mathbf{Z}[\omega]$. Our first task is to show that $a+ib\sqrt{3})$ is a cube in $\mathbf{Z}[\omega]$. We claim that $a+ib\sqrt{3}$ and $a-ib\sqrt{3}$ are coprime in $\mathbf{Z}[\omega]$. If q is a prime element in $\mathbf{Z}[\omega]$ dividing both terms, then q divides their sum and their difference, namely $2a$ and $2bi\sqrt{3}$. Taking norms we obtain $N(q)|4a^2$ and $N(q)|12b^2$ in $\mathbf{Z}$. However, $N(q)$ divides $N(a+ib\sqrt{3}) = a^2+3b^2$, and so is odd. Hence $N(q)|a^2$ and $N(q)|a^2+3b^2$. As a and a^2+3b^2 are coprime, we have $N(q)=1$, which is not possible, because q is not a unit. Hence our claim is correct. We deduce that there is $t \in \mathbf{Z}[\omega]$ such that $t^3 = a+ib\sqrt{3}$.

From Lemma 1 there exists $\epsilon \in \mathbf{Z}[\omega]^\times$ such that $t\epsilon \in \mathbf{Z}[i\sqrt{3}]$. As ϵ is a sixth root of unity, we have $\epsilon^{-3} = \pm 1$. Then $a+ib\sqrt{3} = \epsilon^{-3}(\epsilon t)^3 = (\pm\epsilon t)^3$ and so there exist $u, v \in \mathbf{Z}$ such that $a+ib\sqrt{3} = (u+iv\sqrt{3})^3$. Developping $(u+iv\sqrt{3})^3$, we obtain

$$a = u(u+3v)(u-3v) \qquad \text{and} \qquad b = 3v(u-v)(u+v).$$

Our next task is to show that $2u$, $u+3v$ and $u-3v$ are pairwise coprime. As b is odd, u and v have different parities; v must be odd and therefore u even. If p is a prime dividing $2u$ and

$3v$, then p must be odd and divides u. This means that p divides a and b, which are coprime. It follows that $2u$ and $3v$ are coprime. If p is a prime dividing $2u$ and $u+3v$, then p must be odd, because $u+3v$ is odd. It follows that p divides u, which implies that p divides $3v$, so $2u$ and $3v$ are not coprime, a contradiction. Hence $2u$ and $u+3v$ are coprime. In the same way, $2u$ and $u-3v$ are coprime. If p is a prime dividing $u+3v$ and $u-3v$, then p divides the sum $2u$ and the difference $6v$. As $u+3v$ is odd, p must be odd. Given that $6v = 2 \cdot 3v$, p divides $3v$, so $2u$ and $3v$ are not coprime, a contradiction. It follows that $u+3v$ and $u-3v$ are coprime. We have shown that $2u$, $u+3v$ and $u-3v$ are pairwise coprime.

Given that $2a = r^3$, we have

$$r^3 = 2u(u+3v)(u-3v) \Longrightarrow 2u = l^3, u+3v = m^3, u-3v = n^3,$$

with $l, m, n \in \mathbf{Z}$. Summing and setting $k = -l$ we obtain

$$m^3 + k^3 + n^3 = 0,$$

where k is even, m, n odd and k, m, n pairwise coprime. In addition,

$$|y^3| = |2a(a^2+3b^2)| = |l^3(u^2-9v^2)(a^2+3b^2)| > |(3l)^3| = |(3k)^3|.$$

Thus $|y| > |3k| > |k|$ and we have a contradiction to the minimality of $|y|$.

Case 2: $\gcd(2a, a^2+3b^2) = 3$.

Since 3 divides $2a$ and does not divide 2, necessarily 3 divides a and so we may write $a = 3c$. Then we obtain

$$2a(a^2+3b^2) = 6c(9c^2+3b^2) = 18c(3c^2+b^2) = -y^3,$$

We claim that $18c$ and $3c^2+b^2$ are coprime. If not, then there is a prime p dividing both terms, which must be odd, because $3c^2+b^2$ is odd. Thus p divides $9c$. If $p = 3$, then p divides a and b, which is impossible, because a and b are coprime. Thus $p \neq 3$, which implies that p divides c and it follows that p divides a and b, which is not possible. This establishes the claim.

Taking into account the factorization in $\mathbf{Z}$, we see that there are integers r and s such that $r^3 = 18c$ and $s^3 = 3c^2+b^2$, with r even and s odd. As in Case 1, we factorize b^2+3c^2 in $\mathbf{Z}[\omega]$:

$$(b+ic\sqrt{3})(b-ic\sqrt{3}) = b^2+3c^2 = s^3$$

and show that the two factors are coprime and hence cubes, from which we deduce that there are integers u and v such that $b+ic\sqrt{3} = (u+iv\sqrt{3})^3$. Developping this expression we obtain

$$b = u(u+3v)(u-3v) \qquad \text{and} \qquad c = 3v(u-v)(u+v),$$

with u odd and v even, because b is odd and c even. In addition, u and v are coprime. (If p is a prime dividing u and v, then p divides b and c, which implies that p divides $18c$ and $3c^2+b^2$, which we know to be coprime.)

Since $18c = r^3$, we have

$$r^3 = 54v(u-v)(u+v) \Longrightarrow r'^3 = 2v(u-v)(u+v),$$

where $r = 3r'$. It is not difficult to see that the three terms $2v$, $u - v$ and $u + v$ are pairwise coprime, hence there exist integers l, m, n such that $2v = l^3$, $u - v = m^3$ and $u + v = n^3$. Setting $k = -l$ we obtain $m^3 + k^3 + n^3 = 0$, with k even. Finally,

$$|y^3| = |18c(3c^2 + b^2)| = |27(2v)(u^2 - v^2)(3c^2 + b^2)| > |(3l)^3| > |k^3|,$$

thus $|y| > |k|$, contradicting the minimality of $|y|$.

To sum up we have proved the following result:

Theorem 3 *The equation $X^3 + Y^3 = Z^3$ has no nontrivial solution.*

Corollary 2 *If n is a multiple of 3, then the equation $X^n + Y^n = Z^n$ has no nontrivial solution.*

Sophie Germain's Theorem

The theorem of Sophie Germain was a great step forward in the treatment of Fermat's last theorem. Although it does not give a complete solution of the problem it shows that for certain odd prime numbers p, if there is a nontrivial solution of the equation $X^p + Y^p + Z^p = 0$, then it must have a certain form. Thus, if we want to show that there are no solutions, we can concentrate on certain possibilities.

A prime p is a Sophie Germain prime if p is odd and $q = 2p + 1$ is prime. For example 3, 5, 11 and 23 are Sophie Germain primes, but 7, 13, 17 and 19 are not.

Theorem 4 *If p is a Sophie Gerain prime, then there is no nontrivial solution (x, y, z) in the integers of the equation*

$$X^p + Y^p + Z^p = 0,$$

such that $p \nmid xyz$. In other words, if a nontrivial solution (x, y, z) exists, then p must divide one of the elements x, y, z.

PROOF Suppose that (x, y, z) is a nontrivial solution such that $p \nmid xyz$. We may suppose that the elements x, y, z are coprime and hence pairwise coprime. As p is odd, we have

$$z^p + y^p = (z + y)(z^{p-1} - z^{p-2}y + z^{p-3}y^2 - \cdots + y^{p-1}),$$

which we can write

$$(y + z)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = -x^p = (-x)^p.$$

Claim 1 $y + z$ and $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ are coprime and hence there are integers α and a such that

$$y + z = a^p \qquad \text{and} \qquad \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p.$$

PROOF Suppose that r is a prime dividing both $y+z$ and $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$. Then $r^2|x^p \Longrightarrow r|x$. As $y \equiv -z \pmod r$, we have

$$\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1} \pmod r.$$

By hypothesis, the first term is congruent to 0 modulo r, so r divides py^{p-1}, and so r divides p or y^{p-1}. In the first case, we obtain $r = p$, so p divides x. However, the hypothesis $p \not| xyz$ implies that $p \not| x$, so we are left with the second alternative, which implies that r divides y, which implies that $r|z$, which is impossible, because $\gcd(y, z) = 1$. It follows that $y + z$ and $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ are coprime.

For the second part of the claim, we notice that the RHS of the expression

$$(y + z)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = (-x)^p.$$

is a product of pth powers of primes, each of which figures in one and only one of the factors $y + z$ and $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ on the LHS. □

Remark In an analogous manner, we may show that there are integers b, β, c and γ such that

$$z + x = b^p \qquad \text{and} \qquad \sum_{k=0}^{p-1}(-x)^{p-1-k}z^k = \beta^p$$

and

$$x + y = c^p \qquad \text{and} \qquad \sum_{k=0}^{p-1}(-y)^{p-1-k}x^k = \gamma^p$$

Since the elements x, y, z are pairwise coprime, only one of them can be divisible by q. We aim to show that there is in fact one such element.

Claim 2 If m is an integer and q does not divide m, then $m^p \equiv \pm 1 \pmod q$.

PROOF From Fermat's little theorem

$$(m^p)^2 = m^{2p} = m^{q-1} \equiv 1 \pmod q$$

and it follows that $m^p \equiv \pm 1 \pmod q$. □

Now we show that one of the elements x, y, z is divisible by q. If this not the case, then $x^p + y^p + z^p = 0$. However, from Claim 2 this sum is congruent to 3, 1, -1 or -3 modulo q, which is not possible, because $q \geq 7$, Hence q divides x, y or z. Without loss of generality, let us suppose that q divides x, which implies that q does not divide y or z, because of the pairwise coprimality. Then

$$b^p + c^p - a^p = (x + z) + (x + y) - (y + z) = 2x \equiv 0 \pmod q.$$

As $q \not| y$, from Claim 2 we have $y \equiv \pm 1 \pmod q$. Also, $q \not| z$, so $z \equiv \pm 1 \pmod q$. We deduce that $a^p = y + z$ is congruent to 2, 0 or -2 modulo q. However, with the first and last alternatives we have a contradiction, because $q \not| a^p$ implies that $a^p \equiv \pm 1 \pmod q$. It follows that $y + z \equiv 0 \pmod q$.

We now may conclude the proof. Using the fact that $-z \equiv y \pmod q$, we obtain

$$\alpha^p = \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \equiv py^{p-1} \pmod q.$$

Since $y \equiv \pm 1 \pmod q$ and $p-1$ is even, we see that $\alpha^p \equiv p \pmod q$. However, from Claim 2, we have α^p congruent to 1, 0 or -1, a contradiction. Therefore (x, y, z) is not a solution. This ends the proof. □

The case $n = 5$: $X^5 + Y^5 = Z^5$

As for the case $n = 3$, we will show that there is no nontrivial solution, i.e., a solution (x, y, z), with $xyz \neq 0$. To do so will use Sophie Germain's theorem. Let $\omega = e^{\frac{2\pi i}{5}}$ and $K = \mathbf{Q}(\omega)$. We recall that O_K, the subring of integers of K, is $\mathbf{Z}[\omega]$. We need a preliminary result, which will provide us with a sufficient condition for a unit in $\mathbf{Z}[\omega]$ to be a fifth power. We extend the notation $x \equiv y \pmod z$ to $\mathbf{Z}[\omega]$, i.e., for $x, y, z \in \mathbf{Z}[\omega], x \equiv y \pmod z$ if and only if $z|x - y$.

FERMATlem2 **Lemma 2** *Let ϵ be a unit in $\mathbf{Z}[\omega]$. If there exists $a \in \mathbf{Z}$ such that $\epsilon \equiv a \pmod 5$ in $\mathbf{Z}[\omega]$, then there exists a unit η in $\mathbf{Z}[\omega]$ such that $\epsilon = \eta^5$.*

PROOF Let $\epsilon \in \mathbf{Z}[\omega]^\times$. We know that $\epsilon = \pm\omega^n u^k$, where $n \in \{1, \ldots, 5\}$, $k \in \mathbf{Z}$ and $u = \frac{1+\sqrt{5}}{2}$. Then the conjugate $\bar\epsilon = \pm\bar\omega^n u^k$. By hypothesis there there exists $d \in \mathbf{Z}[\omega]$ such that $\epsilon = a + 5d$, which implies that $\bar\epsilon = a + 5\bar d$. As $d \in \mathbf{Z}[\omega]$, so does $\bar d$ and thus $\bar\epsilon \equiv a \pmod 5$. We have

$$\epsilon\bar\epsilon = (a + 5d)(a + 5\bar d) = a^2 + 5(ad + a\bar d + 5d\bar d) \equiv a^2 \pmod 5,$$

which implies that $u^{2k} \equiv a^2 \pmod 5$. We claim that k is a multiple of 5, i.e., $k = 5h$, with $h \in \mathbf{Z}$.

Now

$$\left(\frac{1+\sqrt{5}}{2}\right)^{2k} \equiv a^2 \pmod 5 \Longrightarrow (1+\sqrt{5})^{2k} \equiv c \pmod 5, \quad c \in \mathbf{Z}$$

and

$$(1+\sqrt{5})^{2k} = 1 + 2k\sqrt{5} + \binom{2k}{2}5 + \cdots + 5^k = 1 + 2k\sqrt{5} + 5b,$$

where $b \in \mathbf{Z}[\sqrt{5}]5$. However, $\mathbf{Z}[\sqrt{5}] \subset \mathbf{Z}[\frac{-1+\sqrt{5}}{2}] \subset \mathbf{Z}[\omega]$, because $\mathbf{Q}(\omega + \omega^{-1}) = \mathbf{Q}(\sqrt{5})$ implies that the ring of integers of $\mathbf{Q}(\sqrt{5})$ is contained in the ring of integers of K, i.e., $\mathbf{Z}[\frac{-1+\sqrt{5}}{2}] \subset \mathbf{Z}[\omega]$. Hence $1 + 2k\sqrt{5} \equiv c \pmod 5$.

We may write $b = b_1 + b_2$, where b_1 is the sum of the elements in b which are integers and b_2 the sum of the others. Setting $c' = 1 + b_1 \in \mathbf{Z}$, we obtain $1 + 2k\sqrt{5} \equiv c' \pmod 5$.

We now consider

$$(1-\sqrt{5})^{2k} = 1 - 2k\sqrt{5} + \binom{2k}{2}5 - \cdots + 5^k = 1 - 2k\sqrt{5} + 5b',$$

where $b' \in \mathbf{Z}[\sqrt{5}]5 \subset \mathbf{Z}[\omega]$. We write $b' = b'_1 + b'_2$, where b'_1 is the sum of the elements in b' which are integers and b'_2 the sum of the others. Then $b'_1 = b_1$ and so we obtain $1 - 2k\sqrt{5} \equiv c' \pmod 5$.

From the expressions $1 + 2k\sqrt{5} \equiv c' \pmod 5$ and $1 - 2k\sqrt{5} \equiv c' \pmod 5$, we obtain $4k\sqrt{5} \equiv 0 \pmod 5$, which implies that $4k\sqrt{5} = 5q$, with $q \in \mathbf{Z}[\omega]$. As q is real, q belongs to the maximal real subfield of $\mathbf{Q}(\omega)$, namely $\mathbf{Q}(\sqrt{5})$. Taking norms in $\mathbf{Q}(\sqrt{5})$, we obtain

$$16k^2 5 = 25N(q) \Longrightarrow 16k^2 = 5N(q) \Longrightarrow 5|k,$$

as claimed. Hence we may write $k = 5h$, with $h \in \mathbf{Z}$, and then $\epsilon = \pm\omega^n u^{5h}$.

Our next step is to show that $n = 5$. We notice that $u = 1 + v$, where $v = \frac{-1+\sqrt{5}}{2}$. Then

$$u^5 = (1+v)^5 = 1 + 5v + \binom{5}{2}v^2 + \cdots + \binom{5}{4}v^4 + v^5.$$

Since $v \in \mathbf{Z}[\omega]$, we have $u^5 \equiv 1 + v^5 \pmod 5$. Moreover,

$$\begin{aligned} v^5 = \frac{1}{32}(-1+\sqrt{5})^5 = -\frac{1}{32}(1-\sqrt{5})^5 &= -\frac{1}{32}\left(1 + 5(-\sqrt{5}) + \binom{5}{2}(-\sqrt{5})^2 - \cdots + (-\sqrt{5})^5\right) \\ &= -\frac{1}{32}(176 - 80\sqrt{5}) = -\frac{11 - 5\sqrt{5}}{2} \\ &= -3 + 5\frac{-1+\sqrt{5}}{2} = -3 + 5v, \end{aligned}$$

hence $v^5 \equiv -3 \pmod 5$, from which we deduce that $u^5 \equiv -2 \pmod 5$.

Now

$$\epsilon = \pm\omega^n u^k = \pm\omega^n u^{5h} \equiv \pm\omega^n(-2)^h \pmod 5,$$

thus $\omega^n(-2)^h \equiv \pm a \pmod 5$. Taking conjugates we find $\bar{\omega}^n(-2)^h \equiv \pm a$ and so

$$(-2)^h \cos\left(\frac{2n\pi}{5}\right) \equiv \pm 2a \pmod 5.$$

If $n \neq 5$, then $\cos(\frac{2n\pi}{5}) = \frac{-1\pm\sqrt{5}}{4}$. Setting $s = (-2)^h$, in the first case we obtain

$$s\left(\frac{-1+\sqrt{5}}{4}\right) \equiv \pm a \pmod 5 \Longrightarrow s + s\sqrt{5} \equiv \pm 8a \pmod 5,$$

which implies that 5 divides $(s \mp 8a) + s\sqrt{5}$, i.e., there exists $w \in \mathbf{Z}[\omega]$ such that $5w = (s \mp 8a) + s\sqrt{5}$. Given that 5 and $(s \mp 8a) + s\sqrt{5}$ are real, w must be real. We claim that $w \in \mathbf{Z}[\frac{-1+\sqrt{5}}{2}]$, the number ring of the number field $\mathbf{Q}(\sqrt{5})$: We have

$$w = a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\omega^4,$$

with $a_i \in \mathbf{Z}$. Then

$$\begin{aligned} \bar{\alpha} &= a_0 + a_1\bar{\omega} + a_2\bar{\omega}^2 + a_3\bar{\omega}^3 + a_4\bar{\omega}^4 \\ &= a_0 + a_1\omega^4 + a_2\omega^3 + a_3\omega^2 + a_4\omega. \end{aligned}$$

As $w = \bar{w}$, we have $a_1 = a_4$ and $a_2 = a_3$, hence

$$\begin{aligned} w &= a_0 + a_1(\omega + \bar{\omega}) + a_2(\omega^2 + \bar{\omega}^2) \\ &= a_0 + a_1(\frac{-1+\sqrt{5}}{2}) + a_2(\frac{-1-\sqrt{5}}{2}) \in \mathbf{Z}[\frac{-1+\sqrt{5}}{2}], \end{aligned}$$

as claimed.

We now take norms in $\mathbf{Q}(\sqrt{5})$. We find that $25N(w) = (s \mp 8a)^2 - 5s^2$. As w is an algebraic integer, $N(w)$ is an integer and so 25 divides $(s \mp 8a)^2 - 5s^2$ in $\mathbf{Z}$. Thus 5 divides $(s \mp 8a)^2$ and hence $s \mp 8a$. From this we deduce that we may write $(s \mp 8a)^2 - 5s^2 = 25v^2 - 5s^2$ and, dividing by 5, we obtain that s^2 is a multiple of 5, which is not possible, because s is a power of 2. We are left with the conclusion that $n = 5$, as claimed. To conclude, we have $\epsilon = \pm\omega^5 u^{5h} = (\pm u^h)^5$. □

We now consider the equation

$$X^5 + Y^5 = Z^5. \tag{1}$$ FERMATeqn1

(In the following we will use the notation AN to refer to results in the book Algebraic Number Theory ... by RC and LZ.) Suppose that there is a nontrivial solution (x, y, z), i.e.,

$$x^5 + y^5 = z^5. \tag{2}$$ FERMATeqn2

In the light of Sopnie Germain's theorem, one of the three number x, y and z is divisible by 5; for example $z = 5z'$, with $z' \in \mathbf{Z}$. We may assume that x, y and z are coprime, and hence pairwise coprime. We set $\lambda = 1 - \omega$. Then $N_{K/\mathbf{Q}}(\lambda) = 5$ (see the proof of Proposition 11.10 in AN) and λ divides $N_{K/\mathbf{Q}}(\lambda)$ (see Proposition 10.2 in AN). Thus there exists λ' such that $\lambda\lambda' = 5$, so we can write

$$x^5 + y^5 = (5z')^5 = \lambda^5(\lambda' z')^5.$$

We notice that $\lambda' \in \mathbf{Z}[\omega]^\times$, because $N(\lambda) = 5$ implies that $N(\lambda') = 1$. (To simplify the notation, from hereon we will write N for $N_{K/\mathbf{Q}}$.)

We now consider the equation

$$X^5 + Y^5 = \epsilon\lambda^{5k} Z^5, \tag{3}$$ FERMATeqn3

where $\epsilon \in \mathbf{Z}[\omega]^\times$ and $k \in \mathbf{N}^*$. If this equation has no nontrivial solution (x, y, z) with the elements pairwise coprime, then the equation (1) also has no such solution with z a multiple of 5, Let us suppose that (x, y, z) is a solution of the equation (3), with k minimal.

We claim that

$$x^5 + y^5 = (x + y)(x + \omega y)(x + \omega^2 y)(x + \omega^3 y)(x + \omega^4 y) = \epsilon\lambda^{5k} z^5. \tag{4}$$ FERMATeqn1a

The roots of the polynomial $X^5 + y^5$ are $-y, -\omega y, \ldots, -\omega^4 y$, so

$$X^5 + y^5 = (X + y)(X + \omega y)(X + \omega^2 y)(X + \omega^3 y)(X + \omega^4 y) = \epsilon\lambda^{5k} z^5.$$

Setting $X = x$, we obtain the required expression.

The rest of the proof is long, so we will divide it into parts. In the first part we will examine the expression (4). In particular, we will show that λ divides each of the factors $x + \omega^i y$ and that λ^2 divides just one of them.

Part 1:

Our first step is to show that λ divides each of the components of the decomposition. Since $N(\lambda)$ is prime, λ is irreducible. We have shown elsewhere that $\mathbf{Z}[\omega]$ is Euclidean, hence a PID and so a UFD, and it follows that λ is a prime element in $\mathbf{Z}[\omega]$. This being the case, λ divides $x + \omega^i y$,

for some $i \in \{0, 1, \ldots, 4\}$. Moreover, if $j > i$, then $(x + \omega^j y) - (x + \omega^i y) = \omega^i y(1 - \omega^{j-i})$ and λ divides $1-\omega^{j-i}$, so λ divides $x+\omega^j y$. A similar argument shows that λ divides $x+\omega^j y$, for $j < i$.

We claim that the numbers $\frac{x+\omega^i y}{\lambda}$ are pairwise coprime. Suppose that d is a prime divisor of $\frac{x+\omega^i y}{\lambda}$ and $\frac{x+\omega^j y}{\lambda}$, where $i < j$. Then d divides $x + \omega^i y$ and $x + \omega^j y$. It follows that d divides $y(\omega^j - \omega^i)$, their difference. Since d is prime, d divides y or d divides $\omega^j - \omega^i$. In the first case, d divides x and y, which is impossible, because x and y are coprime. Therefore d divides $\omega^j - \omega^i = \omega^i(\omega^{j-i} - 1)$. Now

$$\omega^{j-i} - 1 = (\omega - 1)(\omega^{i-j-1} + \omega^{i-j-2} + \cdots + 1).$$

The index $i - j - 1$ may take the values $0, 1, 2, 3$, so we have

$$1, \omega + 1, \omega^2 + \omega + 1 \text{ and } \omega^3 + \omega^2 + \omega + 1$$

for possible values of $\omega^{i-j-1}+\omega^{i-j-2}+\cdots+1$. 1 is clearly a unit and, as $(\omega+1)(\omega^4+\omega^2+1) = 1$, $\omega+1$ is also a unit. In addition, $\omega^2+\omega+1 = -\omega^3-\omega^4 = -\omega^3(1+\omega)$ and $\omega^3+\omega^2+\omega+1 = -\omega^4$, which are both units. Therefore, in all four cases, $\omega^{j-i} - 1$ is the product of λ and a unit ϵ. This means that there exists $u \in \mathbf{Z}[\omega]$ such that $du = \epsilon\lambda$. If λ divides u, then we have a contradiction to the unique factorization in $\mathbf{Z}[\omega]$; it follows that λ divides d and there exists a unit η such that $d = \eta\lambda$.

If d is a prime and d^2 divides $x + \omega^i y$ and $x + \omega^j y$, then d^2 divides $\omega^{j-i} - 1$ and so d divides $\omega^{i-j-1} + \omega^{i-j-2} + \cdots + 1$, which is impossible, because $\omega^{i-j-1} + \omega^{i-j-2} + \cdots + 1$ is a unit. Therefore we may write $x+\omega^i y = da$ and $x+\omega^j y = db$, where d does not divide both a and b. If a and b are not coprime, then the exists a prime element δ dividing both a and b. Then $d\delta$ divides $\omega^{j-i} - 1$. If δ divides $\omega - 1$, then we have a contradiction to the unique factorization of $\omega - 1$ and so δ divides $\omega^{i-j-1}+\omega^{i-j-2}+\cdots+1$, which is impossible, because this expression is a unit. It follows that a and b are coprime and we deduce that $\frac{x+\omega^i y}{\lambda}$ and $\frac{x+\omega^j y}{\lambda}$ are coprime., because $d = \eta\lambda$, with η a unit. We have shown that that the numbers $\frac{x+\omega^i y}{\lambda}$ are pairwise coprime, as claimed.

We have found that λ divides all the factors $x + \omega^i y$. Our next step is to show that there is just one factor divisible by λ^2. If λ^2 divides $x+\omega^i y$ and $x+\omega^j y$, with $i \neq j$, then λ divides both $\frac{x+\omega^i y}{\lambda}$and $\frac{x+\omega^j y}{\lambda}$, which implies that these expressions are not coprime, a contradiction. Thus there can be at most one $x + \omega^i y$ divisible by λ^2, so we only need to show that such an element exists. First we observe that the set $\{1, \lambda, \lambda^2, \lambda^3\}$ is an integral basis of $\mathbf{Z}[\omega]$. To see this we notice that

$$\omega = 1 - \lambda,\ \omega^2 = 1 - 2\lambda + \lambda^2 \text{ and } \omega^3 = 1 - 3\lambda + 3\lambda^2 - \lambda^3.$$

Thus all elements of $\mathbf{Z}[\omega]$ can be expressed as linear combinations of 1, λ, λ^2 and λ^3 and there is no difficulty in showing that 1, λ, λ^2 and λ^3 are independant. Therefore we may write

$$x = a_0 + a_1\lambda + a_2\lambda^2 + a_3\lambda^3 \quad \text{and} \quad y = b_0 + b_1\lambda + b_2\lambda^2 + b_3\lambda^3,$$

with $a_i, b_j \in \mathbf{Z}$, for $0 \leq i, j \leq 3$. Thus $x \equiv a_0 + a_1\lambda \pmod{\lambda^2}$ and $y \equiv b_0 + b_1\lambda \pmod{\lambda^2}$. In addition, $\omega^i \equiv 1 - i\lambda \pmod{\lambda^2}$, for $i = 0, \ldots, 3$. From this we deduce

$$\begin{aligned} x + \omega^i y &\equiv a_0 + a_1\lambda + (1 - i\lambda)(b_0 + b_1\lambda) \pmod{\lambda^2} \\ &\equiv a_0 + b_0 + (a_1 + b_1 - ib_0)\lambda \pmod{\lambda^2}. \end{aligned}$$

We have shown above that λ divides $x+\omega^i y$, for $i=0,\ldots,3$, so λ divides a_0+b_0. In fact, λ^2 divides a_0+b_0, as we will now see. Taking norms we find that $N(\lambda)$ divides $(a_0+b_0)^2$, i.e., 5 divides $(a_0+b_0)^2$, which implies that 5 divides a_0+b_0, because 5 is a prime number. However,

$$N(\lambda)=(1-\omega)((1-\omega^2)(1-\omega^3)((1-\omega^4),$$

because the Galois group $Gal(\mathbf{Q}(\omega)/\mathbf{Q})$ is composed of the homomorphisms $\sigma_1,\ldots,\sigma_4$, where $\sigma_i(\omega)=\omega^i$. It follows that $(1-\omega)(1-\omega^4)$ divides a_0+b_0. However,

$$(1-\omega)(1-\omega^4)=-\omega^4(1-\omega)^2 \Longrightarrow -\omega^4(1-\omega)^2|(a_0+b_0) \Longrightarrow \lambda^2|(a_0+b_0).$$

We deduce that

$$\frac{x+\omega^i y}{\lambda}\equiv a_1+b_1-ib_0 \ (\bmod \lambda). \tag{5}$$

We claim that 5 does not divide b_0 in $\mathbf{Z}$. If this is the case, then λ divides both x and y, because λ divides $N(\lambda)=5$. As x and y are coprime in $\mathbf{Z}$, they are also coprime in $\mathbf{Z}[\omega]$, so λ cannot divide both x and y. It follows that 5 does not divide b_0 in $\mathbf{Z}$. We now consider the congruence

$$a_1-b_1-ib_0\equiv 0 \ (\bmod 5) \quad \text{or} \quad a_1-b_1\equiv ib_0 \ (\bmod 5).$$

As 5 does not divide b_0, the element b_0 is invertible modulo 5, i.e., there exists $c\not\equiv 0 \ (\bmod 5)$ such that $b_0c\equiv 1 \ (\bmod 5)$. If we take $i\equiv c(a_1-b_1) \ (\bmod 5)$, then i is a solution of the congruence. As $a_1-b_1-ib_0\equiv 0 \ (\bmod 5)$, we have $a_1-b_1-ib_0\equiv 0 \ (\bmod \lambda)$, because λ divides 5. From equation (5), we deduce that

$$\frac{x+\omega^i y}{\lambda}\equiv 0 \ \ (\bmod \lambda),$$

which implies that λ^2 divides $x+\omega^i y$.

Part 2:

We know that λ^2 divides one of the expressions $x+\omega^i y$. Without loss of generality, let us suppose that this is $x+y$. Since λ divides $x+\omega^i y$, for $i\in\{1,\ldots,4\}$, from the equation (4) we deduce that $x^5+y^5\neq\epsilon\lambda^{5k}z^5$, if $k=1$. Therefore we may suppose that $k\geq 2$. We also notice that $\frac{x+y}{\lambda^{5k-4}}$ belongs to $\mathbf{Z}[\omega]$: We have

$$(x+y)\frac{x+\omega y}{\lambda}\cdots\frac{x+\omega^4 y}{\lambda}=\epsilon\lambda^{5k-4}z^5$$

As λ is prime and does not divide $\frac{x+\omega y}{\lambda},\cdots,\frac{x+\omega^4 y}{\lambda}$, necessarily λ^{5k-4} divides $x+y$, and it follows that $\frac{x+y}{\lambda^{5k-4}}$ belongs to $\mathbf{Z}[\omega]$. In addition, $\frac{x+y}{\lambda^{5k-4}}$ is coprime to $\frac{x+\omega^i y}{\lambda}$, for $i=1,\ldots,4$. (This follows from the fact that $\frac{x+y}{\lambda}$ is coprime to $\frac{x+\omega^i y}{\lambda}$, for $i=1,\ldots,4$.) Therefore we may write

$$\frac{x+y}{\lambda^{5k-4}}\frac{x+\omega y}{\lambda}\cdots\frac{x+\omega^4 y}{\lambda}=\epsilon z^5,$$

where the factors on the LHS are pairwise coprime. Let $z=p_1^{n_1}\cdots p_s^{n_s}$ be a prime factorization of z. Then any factor on the LHS is a product of associates of the p_i. As the factors are pairwise coprime, no two factors can be productets of associates of the same prime p_i. It follows that a factor can be written as a product of 5th powers of primes p_i multiplied by a unit, hence we have

$$\frac{x+y}{\lambda^{5k-4}}=e_0\alpha^5 \Longrightarrow x+y=\lambda^{5k-4}e_0\alpha^5$$

and, for $i = 1, \ldots, 4$,

$$\frac{x + \omega^i y}{\lambda} = e_i \beta_i^5 \Longrightarrow x + \omega^i y = e_i \lambda \beta_i^5,$$

where the e_i are units. Clearly, $\alpha, \beta_1, \ldots, \beta_4$ are pairwise coprime.

Part 3:

To simplify the notation we replace β_1 by β and β_2 by γ. From the equations

$$x + \omega y = e_1 \lambda \beta^5 \quad \text{and} \quad x + \omega^2 y = e_2 \lambda \gamma^5,$$

we obtain

$$x = -e_1 \omega \beta^5 + e_2 \gamma^5 \quad \text{and} \quad y = e_1 \omega^4 \beta^5 - e_2 \omega^4 \gamma^5.$$

Substituting the expressions for x and y in the expression for $x + y$, we obtain

$$(-\omega + \omega^4) e_1 \beta^5 + (1 - \omega^4) e_2 \gamma^5 = \epsilon_1 \lambda^{5k-4} \alpha^5.$$

Moreover,

$$-\omega + \omega^4 = -\omega + \omega^{-1} = \omega^{-1}(-\omega^2 + 1) = \omega^{-1}(1 - \omega)(1 + \omega)$$

and

$$1 - \omega^4 = (1 - \omega)(1 + \omega + \omega^2 + \omega^3) = (1 - \omega)(-\omega^4) = (1 - \omega)(-\omega^{-1}),$$

from which we obtain

$$(1 + \omega) e_1 \beta^5 - e_2 \gamma^5 = \epsilon_1 \lambda^{5(k-1)} \omega \alpha^5 \Longrightarrow \beta^5 - u\gamma^5 = u \epsilon_1 \omega \lambda^{5(k-1)} \alpha^5,$$

where $u = (1 + \omega)^{-1} e_1^{-1}$. Setting $v = u\epsilon_1 \omega$, we obtain

$$\beta^5 - u\gamma^5 = v \lambda^{5(k-1)} \alpha^5, \tag{6}$$

FERMATeqn5

where u and v are units in $\mathbf{Z}[\omega]$.

Part 4:

We now show that u is a 5th power, which will enable us to conclude the proof. If $\theta = a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 \in \mathbf{Z}[\omega]$, then by the multinomial theorem we obtain

$$\theta^5 = \sum_{i_0 + \ldots + i_3 = 5} \frac{5!}{i_0! \cdots i_3!} a_0^{i_0} (a_1\omega)^{i_1} (a_2\omega^2)^{i_2} (a_3\omega^3)^{i_3},$$

and so θ^5 is congruent to an integer modulo 5; in particular, λ^5 is congruent to an integer modulo 5. Using equation (6), we may write

FERMATeqn5

$$A - uB \equiv 0 \pmod 5,$$

where A and B are integers. If $B \equiv 0 \pmod 5$, then $A \equiv 0 \pmod 5$. In this case, 5 divides β and γ, which is not possible, because β and γ are coprime. Therefore $B \not\equiv 0 \pmod 5$ and we deduce that there is an integer C such that $BC \equiv 1 \pmod 5$. Then

$$AC - uBC \equiv 0 \pmod 5 \Longrightarrow u \equiv AC \pmod 5.$$

We now use Lemma 2 to conclude that there exists $\eta \in \mathbf{Z}[\omega]$ such that $u = \eta^5$. We may now rewrite the equation (6) in the form

$$\beta^5 + (-\eta\gamma)^5 = v\lambda^{5(k-1)}\alpha^5,$$

a contradiction to the minimality of k.

Thus we have the following result:

Theorem 5 *The equation $X^5 + Y^5 = Z^5$ has no nontrivial solution.*

Corollary 3 *If n is a multiple of 5, then the equation $X^n + Y^n = Z^n$ has no nontrivial solution.*

Remark If the equation $X^s + Y^s = Z^s$ has no nontrivial solution in the integers and n is a multiple of s, then $X^n + Y^n = Z^n$ has no nontrivial solution in the integers. Therefore, if we can show that $X^p + Y^p = Z^p$ has no nontrivial solution in the integers for any odd prime p, then $X^n + Y^n = Z^n$ has no nontrivial solution in the integers, for any number $n > 2$, because in this case either 4 or an odd prime divides n. Having proved the result for $s = 4, 3, 5$, to establish the general result we only need to consider primes greater than 5, by no means an easy task.