Fermat's Last Theorem in the XIXth century

Arkadiusz Męcel

am234204@students.mimuw.edu.pl

http://students.mimuw.edu.pl/˜am234204/

Faculty of Mathematics, Informatics and Mechanics
University of Warsaw

Fermat's Hypothesis...

test

- $2 + 2 = 5$

Theorem. *The Diophantine equation:*

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

where x, y, z, n are nonzero integers, has no nonzero solutions for $n > 2$.

***

I have discovered a truly marvellous proof of this,
which this margin is too narrow to contain.

Pierre de Fermat – around 400 years before...

Fermat's Hypothesis...

Theorem. *The Diophantine equation:*

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

where x, y, z, n *are nonzero integers, has no nonzero solutions for* $n > 2$*.*

***

I have discovered a truly marvellous proof of this,
which this margin is too narrow to contain.

Pierre de Fermat – around 400 years before...

***

Proof [Wiles, 1995]. *Every semistable elliptic curve over* $\mathbb{Q}$ *is modular.*

The spring of the year 1847

The spring of the year 1847

Lamé's idea [The meeting of the Paris Academy, 1847]. *We have to decompose* $x^n + y^n$ *completely into n* ***linear factors*** *– if* $\zeta^n = 1, \zeta \neq 1$, *n – odd then:*

$$x^n + y^n = (x+y)(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{n-1}y\right) = z^n. \qquad (\star)$$

The spring of the year 1847

Lamé's idea [The meeting of the Paris Academy, 1847]. *We have to decompose* $x^n + y^n$ *completely into n* ***linear factors*** *– if* $\zeta^n = 1, \zeta \neq 1$, *n – odd then:*

$$x^n + y^n = (x+y)(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{n-1}y\right) = z^n. \qquad (\star)$$

Two possible cases:

1. x, y *are such that* $x+y, x+\zeta y, x+\zeta^2 y, \ldots, x+\zeta^{n-1}y$ *are relatively prime.*
2. *They are not such, but there is a common factor m, that when divided by it, they are.*

The spring of the year 1847

Lamé's idea [The meeting of the Paris Academy, 1847]. *We have to decompose* $x^n + y^n$ *completely into n* ***linear factors*** *– if* $\zeta^n = 1, \zeta \neq 1$, *n – odd then:*

$$x^n + y^n = (x+y)(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{n-1}y\right) = z^n. \qquad (\star)$$

Two possible cases:

1. x, y *are such that* $x+y, x+\zeta y, x+\zeta^2 y, \ldots, x+\zeta^{n-1}y$ *are relatively prime.*
2. *They are not such, but there is a common factor m, that when divided by it, they are.*

Lamé's collorary. *From* $(\star)$, *each of these relatively prime factors must itself be an n – th power, thus we can derive an impossible infinite descent.*

The spring of the year 1847

Remark (Liouville)**.** *The collorary is uncertain. We do not know whether the numbers of form:*

$$a_1 + a_2\zeta + a_3\zeta^2 + \ldots + a_{n-1}\zeta^{n-1}, a_i \in \mathbb{Z}$$

posess the property of unique factorization into irreducible elements.

The spring of the year 1847

Remark (Liouville)**.** *The collorary is uncertain. We do not know whether the numbers of form:*

$$a_1 + a_2\zeta + a_3\zeta^2 + \ldots + a_{n-1}\zeta^{n-1}, a_i \in \mathbb{Z}$$

posess the property of unique factorization into irreducible elements.

***

Theorem (Kummer, 1844)**.** *If* $\zeta \neq 1, \zeta^{23} = 1$ *then* $1 - \zeta + \zeta^{21} \in \mathbb{Z}[\zeta_{23}]$ *is an irreducible element, which is not prime.*

The spring of the year 1847

Remark (Liouville)**.** *The collorary is uncertain. We do not know whether the numbers of form:*

$$a_1 + a_2\zeta + a_3\zeta^2 + \ldots + a_{n-1}\zeta^{n-1}, a_i \in \mathbb{Z}$$

posess the property of unique factorization into irreducible elements.

***

Theorem (Kummer, 1844)**.** *If* $\zeta \neq 1$, $\zeta^{23} = 1$ *then* $1 - \zeta + \zeta^{21} \in \mathbb{Z}[\zeta_{23}]$ *is an irreducible element, which is not prime.*

Theorem (Masley, 1976)**.** *There are only 29 values of* $n \in \mathbb{N}_+$ *such, that* $\mathbb{Z}[\zeta]$ *is a UFD. The smallest* n*, for which unique factorization fails, is 23.*

Saving unique factorization

Example (Irreducible, but not prime)**.** $\mathbb{Z}[\sqrt{-5}]$ *is not UFD since:*

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Saving unique factorization

Example (Irreducible, but not prime). $\mathbb{Z}[\sqrt{-5}]$ *is not UFD since:*

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Kummer's idea. *Extend the set of prime factors to have:*

$$\begin{aligned} 6 &= \quad 2 \quad \cdot \quad 3 &= 1+\sqrt{-5} \cdot 1-\sqrt{-5} \\ &= (P_1 \cdot P_2) \cdot (P_3 \cdot P_4) &= (P_1 \cdot P_3) \cdot (P_2 \cdot P_4), \end{aligned}$$

where P_1, P_2, P_3, P_4 *are* ***ideal prime factors****.*

Saving unique factorization

Example (Irreducible, but not prime). $\mathbb{Z}[\sqrt{-5}]$ *is not UFD since:*

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Kummer's idea. *Extend the set of prime factors to have:*

$$\begin{aligned} 6 &= 2 \cdot 3 = 1+\sqrt{-5} \cdot 1-\sqrt{-5} \\ &= (P_1 \cdot P_2) \cdot (P_3 \cdot P_4) = (P_1 \cdot P_3) \cdot (P_2 \cdot P_4), \end{aligned}$$

where P_1, P_2, P_3, P_4 are ***ideal prime factors****.*

HOW TO CONSTRUCT THESE 'IDEAL FACTORS'?

Ideal factors

Kummer's ideal factors [1846]. *We expect that:*

$$P|0,$$

$$P|x, P|y \Rightarrow P|x \pm y,$$

$$P|x \Rightarrow P|xy, \text{ for all } y \in \mathbb{Z}[\sqrt{-5}].$$

Ideal factors

Kummer's ideal factors [1846]. *We expect that:*

$$P|0,$$

$$P|x, P|y \Rightarrow P|x \pm y,$$

$$P|x \Rightarrow P|xy, \text{ for all } y \in \mathbb{Z}[\sqrt{-5}].$$

The additional property of prime ideal factor should be:

$$P|xy \Rightarrow P|x \text{ or } P|y.$$

Ideal factors

Kummer's ideal factors [1846]. *We expect that:*

$$P|0,$$

$$P|x, P|y \Rightarrow P|x \pm y,$$

$$P|x \Rightarrow P|xy, \text{ for all } y \in \mathbb{Z}[\sqrt{-5}].$$

The additional property of prime ideal factor should be:

$$P|xy \Rightarrow P|x \text{ or } P|y.$$

Theorem (Kummer, 1846)**.** *If two cyclotomic integers $g(\zeta)$ and $h(\zeta)$ are divisible by exactly the same prime ideal divisors with exactly the same multiplicities, then they differ only by a unit multiple.*

Ideal factors

Dedekind's ideals [1871]. *A subset P of the considered ring R, that satisfies:*

$$0 \in P,$$

$$x \in P, y \in P \Rightarrow x \pm y \in P,$$

$$x \in P \Rightarrow xy \in P, \text{ for all } y \in R.$$

The additional property of prime ideal is:

$$xy \in P \Rightarrow x \in P \text{ or } y \in P.$$

Ideal factors

Dedekind's ideals [1871]. *A subset P of the considered ring R, that satisfies:*

$$0 \in P,$$

$$x \in P, y \in P \Rightarrow x \pm y \in P,$$

$$x \in P \Rightarrow xy \in P, \text{ for all } y \in R.$$

The additional property of prime ideal is:

$$xy \in P \Rightarrow x \in P \text{ or } y \in P.$$

Remark. *Dedekind proved the generalization of Kummer's theorem on unique factorization for a wider class of rings, later called Dedekind domains. Noether proved that it is the only class of rings with that property.*

Ideal factors

Kummer's idea. *Extend the set of prime factors to have:*

$$\begin{aligned} 6 &= 2 \cdot 3 = 1+\sqrt{-5} \cdot 1-\sqrt{-5} \\ &= (P_1 \cdot P_2) \cdot (P_3 \cdot P_4) = (P_1 \cdot P_3) \cdot (P_2 \cdot P_4). \end{aligned}$$

Ideal factors

Kummer's idea. *Extend the set of prime factors to have:*

$$\begin{array}{rccccccc} 6 & = & 2 & \cdot & 3 & = & 1+\sqrt{-5} & \cdot & 1-\sqrt{-5} \\ & = & (P_1 \cdot P_2) & \cdot & (P_3 \cdot P_4) & = & (P_1 \cdot P_3) & \cdot & (P_2 \cdot P_4). \end{array}$$

Dedekind's idea. *Exchange numbers for ideals. Then:*

$$\begin{array}{rccccccc} (6) & = & (2) & \cdot & (3) & = & (1+\sqrt{-5}) & \cdot & (1-\sqrt{-5}) \\ & = & (P_1 \cdot P_2) & \cdot & (P_3 \cdot P_4) & = & (P_1 \cdot P_3) & \cdot & (P_2 \cdot P_4). \end{array}$$

where:

$$\begin{array}{ll} P_1 = (2, 1+\sqrt{-5}), & P_2 = (2, 1-\sqrt{-5}), \\ P_3 = (3, 1+\sqrt{-5}), & P_4 = (3, 1-\sqrt{-5}). \end{array}$$

This is not enough...

Lamé's idea [The meeting of the Paris Academy, 1847]. *We have to decompose $x^n + y^n$ completely into n* ***linear factors*** *– if $\zeta^n = 1, \zeta \neq 1$, n – odd then:*

$$x^n + y^n = (x + y)(x + \zeta y)\left(x + \zeta^2 y\right) \cdots \left(x + \zeta^{n-1} y\right) = z^n.$$

Even if we exchange numbers for ideals:

$$(x + y)(x + \zeta y)\left(x + \zeta^2 y\right) \cdots \left(x + \zeta^{n-1} y\right) = (z)^n,$$

and even if they are relatively prime, all we get from the unique factorization is:

$$\left(x + \zeta^k y\right) = J_k^n,$$

for some J_k - ideals of $\mathbb{Z}[\zeta_n]$.

Equivalent ideals

Definition (Ideal class)**.** *Let R by any integral domain. We say that two nontrivial ideals A, B of R are in the same ideal class (which we denote as* $A \sim B$*) if and only if there exist principal ideals I, J such that* $AI = BJ$*.*

Equivalent ideals

Definition (Ideal class)**.** *Let R by any integral domain. We say that two nontrivial ideals A, B of R are in the same ideal class (which we denote as* $A \sim B$*) if and only if there exist principal ideals I, J such that* $AI = BJ$*.*

Ideal classes can be multiplied:

1. *The multiplication [A][B] = [AB] is well defined and commutative.*
2. *The principal ideals form the ideal class, which serves as an identity element for this multiplication.*

Equivalent ideals

Definition (Ideal class)**.** *Let R by any integral domain. We say that two nontrivial ideals A, B of R are in the same ideal class (which we denote as* $A \sim B$*) if and only if there exist principal ideals I, J such that* $AI = BJ$*.*

Ideal classes can be multiplied:

1. *The multiplication [A][B] = [AB] is well defined and commutative.*
2. *The principal ideals form the ideal class, which serves as an identity element for this multiplication.*

Remark. *In every Dedekind domain R, if A is a nontrivial ideal, then there exists an ideal B such that AB is principal.*

Equivalent ideals

Definition (Ideal class)**.** *Let R by any integral domain. We say that two nontrivial ideals A, B of R are in the same ideal class (which we denote as* $A \sim B$*) if and only if there exist principal ideals I, J such that* $AI = BJ$*.*

Ideal classes can be multiplied:

1. *The multiplication [A][B] = [AB] is well defined and commutative.*
2. *The principal ideals form the ideal class, which serves as an identity element for this multiplication.*

Remark. *In every Dedekind domain R, if A is a nontrivial ideal, then there exists an ideal B such that AB is principal.*

Collorary. *For every Dedekind domain R, the set of its ideal classes forms an abelian group called:* ***ideal class group****. If it is finite (not truth in general), its order is called* ***class number****.*

Half-factorial domains

Observation. *The order of the ideal class group tells us how much 'non – UFD' can a particular Dedekind domain be.*

Half-factorial domains

Observation. *The order of the ideal class group tells us how much 'non – UFD' can a particular Dedekind domain be.*

Unique factorization domain. *Let R be a Dedekind domain. We say that R is an UFD if and only if* $a_1 a_2 \ldots a_n = b_1 b_2 \ldots b_m$*,* a_i, b_j *- irreducibles, implies that:*

1. *n = m,*
2. *There exists* $\sigma \in S_n$ *such that* $a_i, b_{\sigma(i)}$ *are associates.*

Half-factorial domains

Observation. *The order of the ideal class group tells us how much 'non – UFD' can a particular Dedekind domain be.*

Unique factorization domain. *Let R be a Dedekind domain. We say that R is an UFD if and only if* $a_1 a_2 \ldots a_n = b_1 b_2 \ldots b_m$, a_i, b_j *- irreducibles, implies that:*

1. *n = m,*
2. *There exists* $\sigma \in S_n$ *such that* $a_i, b_{\sigma(i)}$ *are associates.*

Half-factorial domain. *A Dedekind domain R that satisfies only (1).*

Half-factorial domains

Observation. *The order of the ideal class group tells us how much 'non – UFD' can a particular Dedekind domain be.*

Unique factorization domain. *Let R be a Dedekind domain. We say that R is an UFD if and only if* $a_1a_2\dots a_n = b_1b_2\dots b_m$, a_i, b_j *- irreducibles, implies that:*

1. *n = m,*
2. *There exists* $\sigma \in S_n$ *such that* $a_i, b_{\sigma(i)}$ *are associates.*

Half-factorial domain. *A Dedekind domain R that satisfies only (1).*

Theorem (Carlitz, 1960)**.** *Let R be a Dedekind domain. Then R has class number less or equal to 2 if and only if R is HFD.*

The class number of cyclotomic integers

Theorem (Masley, 1976). *Let m be an integer greater than 2, $m \neq 2$ mod 4. Then all the values of m, for which the cyclotomic integers $\mathbb{Z}[\zeta_m]$ have class number h_m with $2 \leq h_m \leq 10$ are listed in the table:*

h_m	2	3	4	5	6	7	8	9	10
m	39	23	120	51	*none*	63	29	31	55
	56	52		80			68	57	
		72						96	

Furthermore, all the other values of m with $\phi(m) = [\mathbb{Q}[\zeta_m] : \mathbb{Q}] \leq 24$ give the twenty-nine values of m for which $h_m = 1$:

$$3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25,$$
$$27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.$$

FLT for regular primes

FLT for regular primes

Definition (Regular prime)**.** *An odd prime p is called* ***regular*** *if p does not divide the class number of $\mathbb{Z}[\zeta_p]$.*

Announcement (Kummer, 1847)**.** *FLT holds for regular primes.*

FLT for regular primes

Definition (Regular prime). *An odd prime p is called **regular** if p does not divide the class number of* $\mathbb{Z}[\zeta_p]$.

Announcement (Kummer, 1847). *FLT holds for regular primes.*

The key idea. *If we restrict ourselves to the 'first case' of FLT, we can prove that* $x + \zeta^k y$ *are relatively prime for* $0 \leq k \leq p-1$. *Thus, in terms of ideals we have:*

$$(x+y)(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{p-1}y\right) = (z)^p.$$

FLT for regular primes

Definition (Regular prime)**.** *An odd prime p is called* ***regular*** *if p does not divide the class number of* $\mathbb{Z}[\zeta_p]$.

Announcement (Kummer, 1847)**.** *FLT holds for regular primes.*

The key idea. *If we restrict ourselves to the 'first case' of FLT, we can prove that* $x + \zeta^k y$ *are relatively prime for* $0 \leq k \leq p - 1$. *Thus, in terms of ideals we have:*

$$(x + y)(x + \zeta y)\left(x + \zeta^2 y\right) \cdots \left(x + \zeta^{p-1} y\right) = (z)^p.$$

From the unique factorization we can deduce that: $\left(x + \zeta^k y\right) = J_k^p$.

FLT for regular primes

Definition (Regular prime). *An odd prime p is called **regular** if p does not divide the class number of* $\mathbb{Z}[\zeta_p]$.

Announcement (Kummer, 1847). *FLT holds for regular primes.*

The key idea. *If we restrict ourselves to the 'first case' of FLT, we can prove that* $x + \zeta^k y$ *are relatively prime for* $0 \leq k \leq p-1$. *Thus, in terms of ideals we have:*

$$(x+y)\,(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{p-1}y\right) = (z)^p.$$

From the unique factorization we can deduce that: $\left(x+\zeta^k y\right) \;=\; J_k^p.$

In the class group: $\left[\left(x+\zeta^k y\right)\right] = [J_k]^p.$

The order of $[J_k]$ *divides* $|Cl(\mathbb{Z}[\zeta_p])|$. *But it **cannot**, since p is regular! Thus* J_k *are principal.*

FLT for regular primes

Definition (Regular prime)**.** *An odd prime p is called **regular** if p does not divide the class number of* $\mathbb{Z}[\zeta_p]$.

Announcement (Kummer, 1847)**.** *FLT holds for regular primes.*

The key idea. *If we restrict ourselves to the 'first case' of FLT, we can prove that* $x + \zeta^k y$ *are relatively prime for* $0 \leq k \leq p-1$. *Thus, in terms of ideals we have:*

$$(x+y)(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{p-1}y\right) = (z)^p.$$

For some $\alpha_k \in \mathbb{Z}[\zeta_p]$ *and invertible* $u_k \in \mathbb{Z}[\zeta_p]^*$ *we have:*

$$x + \zeta^k y = u_k \alpha_k^p.$$

FLT for regular primes

Definition (Regular prime)**.** *An odd prime p is called* ***regular*** *if p does not divide the class number of* $\mathbb{Z}[\zeta_p]$.

Announcement (Kummer, 1847)**.** *FLT holds for regular primes.*

The key idea. *If we restrict ourselves to the 'first case' of FLT, we can prove that* $x + \zeta^k y$ *are relatively prime for* $0 \leq k \leq p-1$. *Thus, in terms of ideals we have:*

$$(x+y)\,(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{p-1} y\right) = (z)^p.$$

For some $\alpha_k \in \mathbb{Z}[\zeta_p]$ *and invertible* $u_k \in \mathbb{Z}[\zeta_p]^*$ *we have:*

$$x + \zeta^k y = u_k \alpha_k^p.$$

....

Regular vs. Irregular

Theorem (Kummer, 1847)**.** *Prime p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers* B_k *for* $k = 2, 4, \ldots, p - 3$.

Regular vs. Irregular

Theorem (Kummer, 1847)**.** *Prime p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers* B_k *for* $k = 2, 4, \ldots, p-3$.

Bernoulli numbers. *A sequence* B_n *of signed rational numbers that can be defined by the identity:*

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n x^n}{n!}.$$

Regular vs. Irregular

Theorem (Kummer, 1847)**.** *Prime p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers* B_k *for* $k = 2, 4, \ldots, p-3$.

Bernoulli numbers. *A sequence* B_n *of signed rational numbers that can be defined by the identity:*

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n x^n}{n!}.$$

They can be also defined recursively by setting $B_0 = 1$*, and then using:*

$$\binom{k+1}{1} B_k + \binom{k+1}{2} B_{k-1} + \ldots + \binom{k+1}{k} B_1 + B_0 = 0.$$

Regular vs. Irregular

Theorem (Kummer, 1847)**.** *Prime p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers* B_k *for* $k = 2, 4, \ldots, p-3$.

Hypothesis. *There are only finitely many irregular primes. Up to year 1871 Kummer had found only 8 of them:*

$$37, 59, 67, 101, 103, 131, 149, 157.$$

Regular vs. Irregular

Theorem (Kummer, 1847)**.** *Prime p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers* B_k *for* $k = 2, 4, \ldots, p-3.$

Theorem (Jensen, 1915)**.** *There are infinitely many irregular primes.*

Regular vs. Irregular

Theorem (Kummer, 1847)**.** *Prime p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers* B_k *for* $k = 2, 4, \ldots, p - 3.$

Theorem (Jensen, 1915)**.** *There are infinitely many irregular primes.*

Open question. *Are there infinitely many regular primes? Are they exactly* $e^{-\frac{1}{2}}$ *of all primes?*

Regular vs. Irregular

Theorem (Kummer, 1847)**.** *Prime p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers* B_k *for* $k = 2, 4, \ldots, p-3$.

Theorem (Jensen, 1915)**.** *There are infinitely many irregular primes.*

Open question. *Are there infinitely many regular primes? Are they exactly* $e^{-\frac{1}{2}}$ *of all primes?*

Definition (Irregularity index)**.** *A prime p has* ***irregularity index*** *s if p divides exactly s numerators of Bernoulli numbers* B_k *for* $k = 2, 4, \ldots p-3$.

Regular vs. Irregular

Theorem (Kummer, 1847). *Prime p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers* B_k *for* $k = 2, 4, \ldots, p-3$.

Theorem (Jensen, 1915). *There are infinitely many irregular primes.*

Open question. *Are there infinitely many regular primes? Are they exactly* $e^{-\frac{1}{2}}$ *of all primes?*

Definition (Irregularity index). *A prime p has* ***irregularity index*** *s if p divides exactly s numerators of Bernoulli numbers* B_k *for* $k = 2, 4, \ldots p-3$.

Conjecture (Johnson, Wooldridge, 1975). *As* $p \longrightarrow \infty$*, the probability that p has index of irregularity r goes to:*

$$\left(\frac{1}{2}\right)^r \frac{e^{-\frac{1}{2}}}{r!}.$$

Euler regular primes

Definition (E - regular number, 1940)**.** *A prime p is E – regular if it divides one of Euler numbers E_{2n} with $0 < 2n < p - 1$.*

Euler regular primes

Definition (E - regular number, 1940)**.** *A prime p is E – regular if it divides one of Euler numbers* E_{2n} *with* $0 < 2n < p - 1$*.*

Definition (Euler numbers)**.** *A sequence* E_n *of signed integral numbers that can be defined by the identity:*

$$\frac{1}{\cosh(x)} = \sum_{n=0}^{\infty} (-1)^n \cdot \frac{E_n x^{2n}}{2n!}, \quad |x| < \frac{\pi}{2}.$$

Euler regular primes

Definition (E - regular number, 1940)**.** *A prime p is E – regular if it divides one of Euler numbers* E_{2n} *with* $0 < 2n < p - 1$*.*

Definition (Euler numbers)**.** *A sequence* E_n *of signed integral numbers that can be defined by the identity:*

$$\frac{1}{\cosh(x)} = \sum_{n=0}^{\infty} (-1)^n \cdot \frac{E_n x^{2n}}{2n!}, \quad |x| < \frac{\pi}{2}.$$

Theorem (Vandiver, 1940)**.** *The first case of FLT holds for E – regular primes.*

Theorem (Carlitz, 1954)**.** *There are infinitely many E – irregular primes.*

Conjecture. *The E - irregular primes of index r satisfy a Poisson distribution.*

Fermat's Hypothesis...

Theorem. *The Diophantine equation:*

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

where x, y, z, n are nonzero integers, has no nonzero solutions for $n > 2$.

***

I have discovered a truly marvellous proof of this,
which this margin is too narrow to contain.

Pierre de Fermat – around 350 years before...

***

Proof [Wiles, 1995]. *Every semistable elliptic curve over $\mathbb{Q}$ is modular.*

THE END

Thank you for your attention!

Arkadiusz Męcel

University of Warsaw
am234204@students.mimuw.edu.pl

http://students.mimuw.edu.pl/~am234204/