FERMAT NUMBERS AND CYCLOTOMY

Nikolai VAVILOV

Department of Mathematics and Computer Science
St. Petersburg State University

06 April 2023
History of Mathematics Seminar

The **original** conjecture concerning Fermat numbers was stated, as a *challenge*, by Fermat in 1640.

Fermat conjecture. Prove that all **Fermat numbers**

$$F_n = 2^{2^n} + 1, \qquad \text{where } n \in \mathbb{N}_0,$$

are prime.

Fermat himself never stated it as a *fact*. Mersenne did.

Fermat was only able to verify that

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65537$$

are prime.

No other Fermat prime was discovered since then.

Most certainly, no further Fermat primes exist.

By being completely wrong, Fermat conjecture does not become any less great! Its role in the development of number theory and algebra is **enormous**!

• The disproof of this conjecture, namely the factorisation of F_5,

$$F_5 = 4294967297 = 641 \cdot 6700417 = (5 \cdot 2^7 + 1) \cdot (52347 \cdot 2^7 + 1),$$

constituted the contents of the *first* paper of Euler in number theory — altogether Euler published about a *hundred* papers in number theory!

• The possibility to construct a regular 17-gon, also intimately related to Fermat primes, constituted the contents of the *first* mathematical paper by Gauß, after which he finally decided to become a mathematician.

• Fermat numbers and their kin are a natural testing ground for our computing power.

As of today, we know 360 prime divisors of the [composite] Fermat numbers.

Of those, 16 were discovered during the > 300 years of the pre-computer time, roughly one divisor every 19 years.

At the same time during the < 70 years of computer era, 344 new prime divisors were discovered, roughly 5 divisors per year *on average* — but in fact quite irregularly, none were discovered in 1989, say.

• Also, Fermat numbers are intimately related to **cyclotomy**.

This is an yet another interesting CASE STUDY:

• History of mathematics in mathematical texts is in an APPALLING STATE, in its present form it is not history of mathematics, but HERO WORSHIP.

• The historians, especially those who do not master Latin, German, French, and whatever other language used in the XVII–XIX centuries, cannot do history of mathematics, whereas mathematicians themselves are not interested.

• Computers have dramatically increased our ability to solve classical XVII–XVIII century problems in their original forms.

I've spoken on that twice 2 years ago:

"Who solved Waring problem?"

"Who solved Goldbach problem?"

Fermat **never** stated that all F_n are prime as a fact.

Why did he *wish* them to be prime?

• He wanted a **formula** that would produce *arbitrarily large primes*, not just an inductive procedure.

• He was interested in establishing the converse of **little Fermat theorem**.

• He expected generalisations in the direction of **generalised Fermat numbers**

$$F_n(a,b) = a^{2^n} + b^{2^n},$$

which would then have tons of applications.

2 Fermat numbers in the correspondence of Euler and Goldbach

In 1729 Goldbach communicated to Euler Fermat's conjecture.

This made Euler greedily study every page written by Fermat.

- New proof of Euclid's theorem on infinity of primes
- **Pepin criterium**
- **Euler—Lucas criterium**

• Only seven complete factorisations are known, F_5 and F_6 were factored by hand — by Euler in 1732 and by Clausen in 1854:

$$F_6 = 18446744073709551617 = 274177 \cdot 67280421310721 = \\ (1071 \cdot 2^8 + 1) \cdot (262814145745 \cdot 2^8 + 1).$$

The second factor was *the* largest prime known at the time.

• All other complete factorisations known today, those of F_7, F_8, F_9, F_{10} and F_{11} are obtained with the use of computers after 1970.

4 Man-made Fermat divisors

The first prime divisors of Fermat numbers F_n, $n \geq 7$, were found by Ivan Pervushin in 1877 and 1878.

The last one found by hand — by Maurice Kraichik in 1925.

In my paper I give a complete list.

5 Computer-made Fermat divisors

see the full text of the paper

John Cosgrave, "The Irish Time", 16 August 1999:

". . . F_5 to F_{23} are composite, but F_{24} (5,050,446 decimal digits), requiring a 47 by 47 feet surface to write it, allowing four digits per inch, is unresolved. A team led by Dr Richard Crandall has been attempting to establish its status as prime or composite for some time.

While F_{24} is large, it is insignificant compared to F_{382447} found by me on July 24th in St Patrick's College, Drumcondra, Dublin, to be evenly divisible by 3×2 to-the-power-of $382449 + 1$ (115130 digits). This almost unimaginably large number — F_{382447} (over 10 to-the-power-of 115136 digits) — would require a board measuring more than 10 to-the-power-of 57550 by 10 to-the-power-of 57550 light years to write out at four digits per inch."

7 Proth numbers and generalised Fermat numbers

see the full text of the paper

The field $\mathbb{K}$ of **constructible numbers** is the smallest **quadratically closed** subfield of $\mathbb{C}$.

In other words, $\mathbb{K}$ contains 0,1 and is closed with respect to the extraction of square roots:

For any $x \in \mathbb{K}$ there exists an $y \in \mathbb{K}$ such that $y^2 = x$.

Wantzel theorem. The elements of $\mathbb{K}$ and only these elements can be constructed by the straightedge and compass.

This theorem proven in 1837 solves three classical problems:

- **cyclotomy** — which regular polygons can be so constructed,
- **doubling the cube**,
- **trisecting the angle**.

Gauß has not solved cyclotomy in the difficult direction.

Gauß—Wantzel theorem. Circle can be divided into n equal parts by straightedge and compass $\iff$ n has the form

$$n = 2^m p_1 \dots p_s, \quad \text{where } p_i \text{ are pair-wise distinct Fermat primes.}$$

• In "Disquisitiones" Gauß has proven that the condition is *sufficient*, but **not** the difficult part that it is necessary!

Quite opposite to what Klein claims: "und die Unmöglichkeit für alle andern Zahlen bewiss".

This was first noted by Kazarinoff in 1968.

• In 1796–1801 Gauß has **not** given an explicit geometric *construction* of the 17-gon either, he has calculated $\cos(2\pi/17)$.

In other words, he has proven that such construction is *possible*.

• According to Archibald's survey article 1920, in 1802 J.F. Pfaff wrote a letter to Gauss in which he quotes the construction of a regular 17-gon from a letter he received from C.F. Pfleiderer.

• The first actual geometric *construction* of the regular 17-gon was published by von Pauker in 1817.

• However, the work of von Pauker was unknown in Germany, many geometers refer to the von Staudt construction of 1842.

• In 1822 von Pauker has calculated $\cos(2\pi/257)$. In 1834 Fischer has calculated all other roots of the equation $x^{257} = 1$.

von Pauker M. G., Geometrische Verzeichnung des regelmäßigen Siebzehn-Ecks und Zweyhundersiebenundfünfzig-Ecks in den Kreis. — Jahresverhandlungen der Kurländischen Gesellschaft für Literatur und Kunst **2** (1822), 160–219.

• In 1832 Richelot gave the first geometric *construction* of the regular 257-gon.

Further such constructions were published by Pascal in 1887 and by Schwendenwein in 1893.

• In 1894 Hermes calculated the primitive root and gave the first geometric *construction* of the regular 65537-gon.

10 Gauss—Pierpoint theorem

see the full text of the paper

11 Conclusions

Here are my principles. If you don't like them, I have others.

• The history of Mathematics is written by victors, and is *totally* falsified.

• One should check everything against the original sources, since everything that can be falsified is falsified. Everything that cannot be falsified was falsified as well.

• It is ridiculous to believe that at a given time there are 3–4–5 heroes and everybody else does not matter. Actually, there is the general level of our understanding at a certain time, and the difference between the 10th and the 11th best is negligible.

• The actual historical development was much more tortuous, than we see it today, and what seems a miracle was a necessary outcome of a step by step development.

THANK YOU!