Why is 1093 an interesting prime?

Abstract. This all started with a question that Abel posed in Crelle's journal in 1828, under the heading "Aufgaben und Lehrsätze". The question was answered by Jacobi and appeared in the same issue of the journal. Astonishingly, a special case of Abel's question, not addressed by Jacobi, turned out to be intimately related to Fermat's Last Theorem. Furthermore, the question was also closely related to the Fermat and Mersenne primes, as well as the Bernoulli numbers (and thereby to the Riemann zeta function).

Reminder

$a \equiv b \pmod{m}$ means $m \mid (a - b)$. In particular, $a \equiv 0 \pmod{m}$ simply means that $m \mid a$.

Example

$7 \equiv -45 \pmod{13}$ since $13 \mid (7 - (-45)) = 52$.

Interpretation of $a \equiv b \pmod{m}$, using the Euclidean algorithm:

$$a = q_1 m + r_1, \quad 0 \leq r_1 < m$$
$$b = q_2 m + r_2, \quad 0 \leq r_2 < m$$

Then $a \equiv b \pmod{m}$ if and only if $r_1 = r_2$.

$a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

If m prime then (multiplicative) inverses exist, i.e. if $m \nmid a$, then there exists $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$. So we may write

$$\bar{a} = \frac{1}{a}, \text{ or } \bar{a} = a^{-1}.$$

Fermat's "Little" Theorem

Let p be a prime and let $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod{p}, \quad \text{i.e.} \quad p \mid (a^{p-1} - 1).$$

Example

$p = 7$, $a = 2$. Then $2^6 \equiv 1 \pmod{7}$, i.e. $7 \mid (2^6 - 1) = 63$.

Observe

$a^{p-1} \equiv 1 \pmod{p^2} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$,
since $p^2 \mid (a^{p-1} - 1) \Rightarrow p \mid (a^{p-1} - 1)$

21.
Aufgaben und Lehrsätze,
erstere aufzulösen, letztere zu beweisen. (1828)

(Von Herrn *N. H. Abel* zu Christiania in Norwegen.)

28. Aufgabe. Kann $\alpha^{\mu-1}-1$, wenn μ eine Primzahl und α eine ganze Zahl und kleiner als μ und gröfser als 1 ist, durch μ^2 theilbar sein?

Abel's question: Can $\alpha^{\mu-1}-1$ be divisible by μ^2, when μ is a prime and $1<\alpha<\mu$? In other words, can $\alpha^{\mu-1}\equiv 1 \pmod{\mu^2}$ for some prime μ?

26.
Beantwortung der Aufgabe S. 212. dieses Bandes: (Band 3)
„Kann $\alpha^{\mu-1}-1$, wenn μ eine Primzahl und α eine ganze Zahl und kleiner als μ und gröfser als 1 ist, durch $\mu\mu$ theilbar sein."

(Von Herrn Prof. *C. G. J. Jacobi.*)

Veranlafst durch vorstehende interessante Aufgabe, ersuchte ich einen meiner Freunde hieselbst, Hrn. Busch, die Congruenz

$$x^{\mu-1} = 1$$

in Bezug auf den Modul $\mu\mu$ für die Primzahlen bis 37 nach allen ihren Wurzeln aufzulösen. Das Resultat dieser Arbeit enthält die unten stehende Tabelle. Es ist darin den Wurzeln die Form $\alpha + \mu\alpha'$ gegeben, wo α und α' positive Zahlen sind, die kleiner sind als μ; zu dem α, das in der ersten Verticalreihe steht, giebt sie für $\mu = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$, welche Zahlen sich in der obersten Horizontalreihe befinden, das entsprechende α', damit $\alpha + \mu\alpha'$ eine Wurzel sei. So z. B. sind die Wurzeln von $x^{36} = 1$ (Mod. 37^2)

$$1,\ 2 + 2.37,\ 3 + 17.37,\ 4 + 8.37,\ 5 + 24.37, \text{ etc. etc.}$$

Ist $a' = 0$, so ist eine in der Aufgabe verlangte Zahl gefunden. Die Tabelle giebt $a' = 0$, für

μ	α
11	3.9.
29	14.
37	18.

Die einfachste Lösung giebt $3^5 = 243 = 2.11^2 + 1$; also auch $3^{10} = 1$, wenn man die Vielfachen von 121 fortläßt.

$$3^{10} \equiv 1 \pmod{11^2}$$
$$14^{28} \equiv 1 \pmod{29^2}$$
$$18^{36} \equiv 1 \pmod{37^2}$$
$$(9^{10} \equiv 1 \pmod{11^2})$$

(Only examples for primes ≤ 37)

Recall Abel's question: Can $\alpha^{\mu-1} \equiv 1 \pmod{\mu^2}$ occur? It turns out that $\alpha = 2$ is **the** most interesting case. So the following question therefore arises:

Are there primes $p \geq 3$ such that

$$2^{p-1} \equiv 1 \pmod{p^2}, \quad \text{i.e.} \quad p^2 \mid (2^{p-1} - 1)?$$

Theorem (Wieferich, 1909).

If the first case of Fermat's Last Theorem (FLT1) fails for the prime p, then $2^{p-1} \equiv 1 \pmod{p^2}$. (Consequently, if $2^{p-1} \not\equiv 1 \pmod{p^2}$ then (FLT1) is true.)

Fermat's Last Theorem (FLT) (proved by Andrew Wiles in 1994).

Let $n \geq 3$. Then the equation

$$(*) \qquad x^n + y^n = z^n$$

has no solution in integers $0 < x < y < z$.

Remark

Enough to prove this for primes n. Can also assume that x, y, z are pairwise relatively prime.

First case of (FLT) (Notation (FLT1))

In $(*)$ we assume $n \nmid xyz$, i.e. n is not a divisor of x, nor y, nor z, where $n \geq 3$ is a prime.

The smallest prime $p \geq 3$ such that $2^{p-1} \equiv 1 \pmod{p^2}$ is $p = 1093$. This was discovered by Meissner in 1913. A further search by D. H. Lehmer has shown that for $p < 6 \times 10^9$ only the primes p equal to 1093 and 3511 satisfy $2^{p-1} \equiv 1 \pmod{p^2}$

So by Wieferich's theorem, (FLT1) is true for all primes $p < 6 \times 10^9$ except possibly for $p = 1093$ and $p = 3511$. (Mirimanoff showed that (FLT1) is also true for $p = 1093$ and $p = 3511$. In doing this he invoked Abel's original question, not restricting to $\alpha = 2$.)

Two natural questions that arise from this are:

(i) Are there infinitely many primes p such that $2^{p-1} \not\equiv 1 \pmod{p^2}$?

(ii) Are there infinitely many primes p such that $2^{p-1} \equiv 1 \pmod{p^2}$?

A digression: What motivated Abel to ask his question?
Let's speculate!

II. ABEL TIL HOLMBOE

Kjøbenhavn [4 August 1823[1]]

Aar $\sqrt[3]{6.064.321.219}$ | Tag Decimal-brøken med.

Foruden at jeg læser arbeider jeg ogsaa selv. Saaledes har jeg søgt at bevise Umuligheden af Ligningen $a^n = b^n + c^n$ i hele Tal naar n er større end 2; men jeg har jeg været hældet[5]. Jeg har ikke kommet videre end til indlagte Theoremer,* som ere snorrige nok.

Theorem I.

Ligningen

$$a^n = b^n + c^n$$

hvor n er et Primtal er umuelig naar een eller flere af Størrelserne:

$$a,\ b,\ c,\quad a+b,\quad a+c,\quad b-c,\quad \sqrt[n]{a},\quad \sqrt[n]{b},\quad \sqrt[n]{c}$$

ere Primtal.

Abel's claim

If a, b, c are nonzero pairwise relatively prime integers such that $0 < c < b < a$ and $a^n = b^n + c^n$, where $n > 2$ is a prime, then none of a, b, c are prime powers.

No direct proof of this statement has ever been discovered. However, it is correct if $n \nmid abc$, but the proof of this is not easy and requires analytical methods. (We are talking pre-Andrew Wiles here!). So maybe Abel thought he had a proof of his claim by assuming the answer to his question: "Can $\alpha^{\mu-1} \equiv 1 \pmod{\mu^2}$", was no?

If $2 \leq a < p$, where p is a prime, we define

$$q_p(a) = \frac{a^{p-1} - 1}{p}$$

Remark

$q_p(a)$ is an integer by Fermat's Little Theorem, and we call $q_p(a)$ a *Fermat quotient* (with base a and exponent p). We have that $q_p(a) \equiv 0 \pmod{p}$, i.e. $p \mid q_p(a)$, if and only if $a^{p-1} \equiv 1 \pmod{p^2}$.

Sylvester showed in 1861 the following congruence:

$$q_p(2) \equiv 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2} \pmod{p}$$

(He showed a similar congruence for $q_p(a)$.)

In 1910, Mirimanoff showed: If $p = 2^r \pm 1$ is a prime, then

$$q_p(2) \equiv \mp\frac{1}{r} \pmod{p}, \text{ and so, in particular, } q_p(2) \not\equiv 0 \pmod{p}.$$

Combining previous results, we get:
(FLT1) holds for prime exponents p of the form $p = 2^r \pm 1$.

Two cases

(i) For $2^r + 1$ to be a prime, r has to be of the form 2^n for some $n \geq 0$. The numbers $F_n = 2^{2^n} + 1$ are called *Fermat numbers*, and F_n is called a *Fermat prime* if F_n is prime.

(Fermat (1607-1665)).

(ii) For $2^r - 1$ to be a prime, r has to be a prime p. The numbers $M_p = 2^p - 1$, p prime, are called *Mersenne numbers*, and M_p is called a *Mersenne prime* if M_p is prime.

(Mersenne (1588-1648)).

Proposition

(i) If $2^r + 1$ is a prime, then $r = 2^n$ for some n.

(ii) If $2^r - 1$ is a prime, then r has to be prime.

Proof: (i) Sufficient to show that r has no odd factor. Assume to the contrary that $r = l \cdot k$, where $k > 1$ is odd. We have the identity

$$x^k + 1 = (x+1)(x^{k-1} - x^{k-2} + x^{k-3} - x^{k-4} + \cdots - x + 1)$$

Set $x = 2^l$. Then

$$2^r + 1 = (2^l)^k + 1 = (2^l + 1)(2^{l(k-1)} - 2^{l(k-2)} + \cdots - 2^l + 1)$$

Which shows that $2^r + 1$ is not a prime, contradicting our assumption.

Proposition

(i) If $2^r + 1$ is a prime, then $r = 2^n$ for some n.

(ii) If $2^r - 1$ is a prime, then r has to be prime.

Proof: (ii) Assume to the contrary that $r = s \cdot t$, where $s, t \geq 2$. We have the identity

$$x^t - 1 = (x - 1)(x^{t-1} + x^{t-2} + \cdots + x + 1)$$

Set $x = 2^s$. Then

$$2^r - 1 = (2^s)^t - 1 = (2^s - 1)(2^{s(t-1)} + \cdots + 2^s + 1),$$

so $2^r - 1$ is not a prime, contradicting our assumption.

Eisenstein (1844) conjectured: There are infinitely many Fermat numbers that are prime. Even today only five Fermat primes are known:

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

(Fermat believed that all Fermat numbers are prime!)

One can show that

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

if and only if F_n is a prime.

As for Mersenne numbers, Euler (1707-1783) gave the first test for finding factors of these:
If $p > 3$ is a prime such that $p \equiv 3 \pmod 4$, then $2p + 1$ divides M_p if and only if $2p + 1$ is again a prime. In this way, Euler concluded that 23 divides M_{11},..., 503 divides M_{251}, etc.

Primes p such that $2p + 1$ is again a prime are called *Sophie Germain primes*. She proved (around 1820):
If p and $2p + 1$ are primes, then (FLT1) is true for the exponent p.

Lucas in 1878 derived a very effective primality test for Mersenne numbers by utilizing the Fibonacci numbers (and the closely related Lucas numbers) $\{F_n\}$, given by $F_0 = 0$, $F_1 = 1$ and the recurrence relation $F_n = F_{n-1} + F_{n-2}$. Lucas showed:

(i) If $p \equiv 1 \pmod 4$, then $M_p = 2^p - 1$ is a prime if and only if M_p divides R_p, where $\{R_n\}$ is given by $R_2 = -4$, $R_{n+1} = R_n^2 - 2$. (So the sequence $-4, 14, 194, \dots$).

(ii) If $p \equiv 3 \pmod 4$ and $p > 3$, then $M_p = 2^p - 1$ is prime if and only if M_p divides $\bar{R}_p$, where $\{\bar{R}_n\}$ is given by $\bar{R}_2 = -3$, $\bar{R}_{n+1} = \bar{R}^2 - 2$. (So the sequence $-3, 7, 47, \dots$)

Schinzel (1963) conjectures the following:
There exist infinitely many square-free Mersenne numbers.
(To date no Fermat or Mersenne number with a square factor has ever been found.)

Rotkiewicz (1965) showed the following:
If Schinzel's conjecture is true, there exists infinitely many primes p such that

$$2^{p-1} \not\equiv 1 \pmod{p^2}.$$

So by the earlier mentioned theorem by Wieferich (1907), (FLT1) would be true for infinitely many prime exponents p.

Fermat quotients: $$q_p(a) = \frac{a^{p-1} - 1}{p}$$

Wilson quotients: $$W(p) = \frac{(p-1)! + 1}{p}$$

Wilson's Theorem (1782)

Let p be a prime. Then $(p-1)! \equiv -1 \pmod{p}$ i.e. $p \mid ((p-1)! + 1)$.

If $W(p) \equiv 0 \pmod{p}$, i.e. $(p-1)! + 1 \equiv 0 \pmod{p^2}$, then p is called a *Wilson prime*.

Remark

The only known Wilson primes are $p = 5, 13, 563$.

Lerch proved in 1905 the following: $$\sum_{j=1}^{p-1} q_p(j) \equiv W(p) \pmod{p}$$

Furthermore, Lerch showed that: $W(p) \equiv B_{2(p-1)} - B_{p-1} \pmod{p}$

Definition

B_n denotes the n'th Bernoulli number, these being generated by the function

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

In particular, $B_0 = 1$, $B_1 = \frac{1}{2}$. Also, $B_n = 0$ for all n odd, $n \geq 3$.

Euler discovered that the Bernoulli numbers were connected to the Riemann zeta function ζ:

$$B_{2n} = (-1)^{n-1}\frac{2(2n)!}{(2\pi)^{2n}}\zeta(2n), \text{ for } n \geq 1.$$

$$\text{Here } \zeta(s) = \sum_{k=1}^{\infty}\frac{1}{k^s}, \quad \mathrm{Re}(s) > 1.$$

Recall $\sum_{j=1}^{p-1} q_p(j) \equiv W(p) \pmod{p}$

In 1909, Friedman and Tamarkine, in a letter to Hensel, proved:

$$\sum_{j=1}^{p-1} j^n q_p(j) \equiv -\frac{B_n}{n} \equiv \zeta(1-n) \pmod{p}$$

(Here $p \nmid n$).

There are similar formulas to the ones we have exhibited relating the Fermat quotients (as well as the Wilson quotients) to the Legendre symbol as well as to the class number of quadratic fields $\mathbb{Q}(\sqrt{a})$. (Here a is a square-free integer.)

The proofs of these formulas use deep results by Kummer and Dirichlet in class field theory.

Summary

We have seen that there is a rather surprising connection between such dissimilar topics as Fermat's Last Theorem, the factorization of Mersenne numbers, the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ as well as sums of Fermat and Wilson quotients and the Bernoulli numbers, respectively the Riemann zeta function.

Open problems

Are there infinitely many Fermat primes, Mersenne primes, Wilson primes or primes p such that $2^{p-1} \equiv 1 \pmod{p^2}$?

So in a sense we link up to (the special case of) Abel's original question!

Reference

P. Ribenboin, “1093”, The Mathematical Intelligencer Vol. 5, No 2 (1983), pp. 28-34.