TOKYO J. MATH.
VOL. 11, NO. 2, 1988

An Observation on the First Case of Fermat's Last Theorem

Norio ADACHI

Waseda University

Let p be an odd prime number. We consider Fermat's equation

$$x^p+y^p+z^p=0 \tag{1}$$

under the condition

$$xyz\not\equiv 0 \quad (\mathrm{mod}\ p)\ . \tag{2}$$

We abbreviate as $\mathrm{FLT}_1(p)$ the statement that the equation (1) has no solutions in integers under the condition (2). It is well-known that if p does not divide the (relative) class number of the cyclotomic field $L=\boldsymbol{Q}(\zeta)$, where ζ is a primitive p-th root of unity, then $\mathrm{FLT}_1(p)$ is true.

In the present paper, we study what we can say about $\mathrm{FLT}_1(p)$, supposing the relative class number of an imaginary subfield of L is not divisible by p. We prove the following:

THEOREM. *Suppose that $FLT_1(p)$ is not true, and let x, y, z be non-zero integers satisfying* (1) *and* (2). *Put $t=x/y$ and let*

$$H=\left\{t,\ \frac{1}{t},\ -\frac{1}{1+t},\ -(1+t),\ -\frac{t}{1+t},\ -\left(1+\frac{1}{t}\right)\right\}\ .$$

Let M be an arbitrarily fixed imaginary proper subfield of the cyclotomic field L. Put

$$\Phi(T)=N_{L/M}(T+\zeta)-N_{L/M}(T+\zeta^{-1})\ ,$$

where $N_{L/M}$ denotes the relative norm map from L to M. If p does not divide the relative class number h_M^- of the field M, then any number in the set H satisfies the congruence

$$\Phi(T)\equiv 0 \quad (\mathrm{mod}\ p)\ . \tag{3}$$

As an example, we consider the case M is a quadratic field $\boldsymbol{Q}(\sqrt{-p})$

Received September 9, 1987

with $p\equiv -1 \pmod 4$. Then it is well-known that p does not divide the class number of the quadratic field; in fact, it is easily seen that the class number is less than p (cf. for example, Lemma 2 in [2]). In § 2, we will give the table of the solutions of (3) for any prime number $p\leqq 199$, by which we will know that $\mathrm{FLT}_1(p)$ is true for these prime numbers.

We note that p divides the relative class number h_M^- of the imaginary field M with $m=[L:M]$, if and only if p divides the Bernoulli number B_{mj+1} for some $j=1, 3, 5, \cdots, (p-4)/m$: This was first proved by Carlitz, later by Metsänkylä and also by the author; cf. Theorem A in [1].

§ 1. Proof.

Suppose that the assumptions in the theorem are all satisfied. We may assume that x, y, z are pairwise relatively prime. Then it is well-known (and easily shown) that $x+\zeta^j y$'s are pairwise relatively prime for $j=1, 2, \cdots, p-1$. Therefore $N_{L/M}(x+\zeta y)=A^p$ for some ideal A of M.

The p-Sylow subgroup C_0 of the ideal class group of the maximal real subfield M_0 of M naturally injects into the p-Sylow subgroup C of the ideal class group of M, since $[M:M_0]=2$ is prime to p. As the relative class number h_M^- is not divisible by p, the injection of C_0 to C is, in fact, surjective. Therefore the ideal A can be written $(\rho)S$ with $\rho\in M$ and S an ideal of M_0, so

$$N_{L/M}(x+\zeta y)=(\rho^p)S^p .$$

Since the left-hand side is prime to p, we may assume that ρ and S are prime to p. The above implies that S^p is principal in M. Since the natural map of C_0 to C is injective, S^p is principal in M_0 from the first beginning: $S^p=(\alpha)$ with $\alpha\in M_0$. Thus we obtain

$$N_{L/M}(x+\zeta y)=\varepsilon\alpha\rho^p ,$$

where ε is a unit of M. By Kummer's lemma ε can be written $\zeta^s\varepsilon_0$ with ε_0 a real unit. Then $\zeta^{2s}=\varepsilon/\bar{\varepsilon}\in M$. Here, and in what follows, $\bar{\alpha}$ denotes the complex conjugate of α. But M contains none of the p-th roots of unity other than 1, since $M\subsetneqq L$. Therefore s is divisible by p: $\varepsilon=\varepsilon_0\in M_0$. We have

$$\bar{\rho}^p\equiv\rho^p \pmod p$$

for any $\rho\in M$. Therefore we obtain

$$N_{L/M}(x+\zeta y)\equiv N_{L/M}(x+\zeta^{-1}y) \pmod p .$$

This implies

$$\Phi(t) \equiv 0 \pmod{p} .$$

On the other hand, we obtain $x+y+z \equiv 0 \pmod{p}$ by (1). Therefore the elements of H are congruent modulo p to those of the set

$$\left\{\frac{x}{y}, \frac{y}{x}, \frac{x}{z}, \frac{z}{x}, \frac{y}{z}, \frac{z}{y}\right\} .$$

By the symmetry of the equation (1), the fact that $T=t$ satisfies the congruence (3) implies that the elements of H other than t also satisfy the congruence (3). This completes the proof of the theorem.

§ 2. Some special cases.

In some special cases, the set H degenerates: If $t \equiv 1$, or -2, or $-1/2 \pmod{p}$, then $H=\{1, -2, -1/2\}$. If $t^2+t+1 \equiv 0 \pmod{p}$, then $p \equiv 1 \pmod{6}$ and H has only 2 distinct elements. In all other cases, H has 6 distinct elements. However, Pollaczek proved that the second case never happens ([3]), that is, $t^2+t+1 \not\equiv 0 \pmod{p}$.

We note that the congruence (3) is never trivial, because it is not satisfied by $T \equiv -1 \pmod{p}$. We note also that (3) is always satisfied by $T \equiv 0, 1 \pmod{p}$. These are immediate consequences of the fact $N_{L/M}\zeta=1$. Therefore, if $\mathrm{FLT}_1(p)$ fails, and if h_M^- is not divisible by p, the number of the solutions of (3) must be $\geqq 4$. If we admit using Pollaczek's result, then either -2 modulo p satisfies (3) or the number of the solutions of (3) must be $\geqq 8$.

If $m=[L:M]=3$, then the degree of Φ is 2; so 0 and 1 are all of the solutions of (3). Thus we obtain the following:

COROLLARY. *Suppose $p \equiv 1 \pmod{3}$. If $FLT_1(p)$ fails, then p divides B_{3j+1} for some $j=1, 3, \cdots, (p-4)/3$.*

This corollary is weaker than classical results derived from "Kummer's congruences". Our proof, however, is different from their proofs.

Finally, we list the solutions of $\Phi(T) \equiv 0 \pmod{p}$ when $p \equiv -1 \pmod{4}$ and $M=\boldsymbol{Q}(\sqrt{-p})$. Incidentally, $\Phi(T)/\sqrt{-p}$ is a monic polynomial with integral coefficients of degree $(p-3)/2$.

In the table below, the prime numbers for each of which there is a solution t of the congruence (3) such that the set H is contained in the set of solutions of (3) are 19, 43, 67, 139 and 163. But these are of the type $t^2+t+1\equiv 0 \pmod p$, which is excluded by Pollaczek's result.

p	the solutions modulo p					
7	0	1				
11	0	1				
19	0	1	17	11		
23	0	1	7	19		
31	0	1				
43	0	1	6	36		
47	0	1	17	35	36	43
59	0	1	22	51		
67	0	1	29	37		
71	0	1				
79	0	1				
83	0	1				
103	0	1				
107	0	1				
127	0	1				
131	0	1	10	118		
139	0	1	42	96		
151	0	1	66	135		
163	0	1	58	104		
167	0	1				
179	0	1	65	168		
191	0	1	56	58		
199	0	1				

The result in the present paper seems to have relation to Kummer's congruences. It is, however, still unknown to the author.

References

[1] N. Adachi, Generalization of Kummer's criterion for divisibility of class numbers, J. Number Theory, **5** (1973), 253–265.

[2] N. Adachi, The Diophantine equation $x^2 \pm ly^2 = z^l$ connected with Fermat's Last Theorem, Tokyo J. Math., **11** (1988), 85–94.

[3] F. POLLACZEK, Über den grossen Fermat'schen Satz, Sitzungsber. Akad. Wiss. Wien II a, **126** (1917), 45–59.

Present Address:
DEPARTMENT OF MATHEMATICS, SCHOOL OF SCIENCE AND ENGINEERING, WASEDA UNIVERSITY
OKUBO, SHINJUKU-KU, TOKYO 160, JAPAN