100. *An Average Type Result on the Number of Primes Satisfying Generalized Wieferich Condition*

By Leo MURATA
Department of Mathematics, Faculty of Science,
Tokyo Metropolitan University

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1981)

1. Statement of results. In 1909 Wieferich ([1]) proved that if an odd prime p satisfies the condition

$$2^{p-1}-1\not\equiv 0 \pmod{p^2},$$

then the case I of Fermat's Last Theorem is true for this prime p, i.e. under the condition $(xyz, p)=1$, there exists no integral solution for the Diophantine equation $x^p+y^p=z^p$. Moreover, it is now known (see for example [2]) that we can deduce the same conclusion, if an odd prime p satisfies

$$a^{p-1}-1\not\equiv 0 \pmod{p^2}$$

for some prime value a, $2\leqslant a\leqslant 43$.

Now we shall call

$$(*)\qquad a^{p-1}-1\equiv 0 \pmod{p^2}$$

the generalized Wieferich condition for a (a may be any natural number). We define for real $x>0$,

$$F_a(x)=\{p\,;\, p \text{ is an odd prime} \leqslant x,\, p \text{ satisfies } (*)\}.$$

We have an average type result as to the cardinal $\sharp F_a(x)$ of $F_a(x)$, which states as follows:

Theorem 1. *Let δ be an arbitrary fixed real number satisfying $1/2<\delta<1$. We have, if $x\geqslant 286$,*

$$\sharp F_a(x)=\log\log x+\theta((\log\log x)^\delta)+\left(C-\frac{1}{2}\right)+\frac{1}{2}\theta((\log x)^{-2})$$

for all a such that $2\leqslant a\leqslant x^4$ with at most

$$2x^4(\log\log x)^{1-2\delta}$$

exceptions of a, where $C=\gamma+\sum_{p:\text{ prime}}\{\log(1-1/p)+1/p\}$ and γ is Euler's constant. ($f(x)$ being positive valued function of x, $\theta(f(x))$ denotes a function of x whose absolute value $\leqslant f(x)$.)

Similarly we have:

Theorem 2. *Let D be an arbitrary fixed real number >0 and $y\geqslant x^6$. We defined for a natural number a and real $x>0$,*

$$F_a^{(3)}(x)=\{p\,;\, p \text{ is an odd prime} \leqslant x,\ a^{p-1}-1\equiv 0 \pmod{p^3}\}.$$

Then we have

$$\left|\sharp F_a^{(3)}(x)-\sum_{\substack{3\leqslant p\leqslant x\\ p:\text{ prime}}}\frac{1}{p^2}\right|<D$$

for all a such that $2 \leqslant a \leqslant y$ *with at most* $D^{-2}(\sum_{\substack{3 \leqslant p \leqslant x \\ p:\text{ prime}}} (p^2-1)/p^4)(x^6+y)$ *exceptions of* a.

We can deduce from Theorem 2:

Corollary. *We put for real* $M>0$,

$$A_M=\{a\,;\, a^{p-1}-1 \not\equiv 0 \pmod{p^3} \text{ for any odd prime } p \leqslant M\}.$$

Then the natural density of A_M *is larger than* 0.7 *for any* M.

We can prove these theorems by means of an analytic method of Warlimont ([3]).

2. Sketch of the proof of Theorem 1. Let χ_p be a primitive character mod p^2, i.e. taking a primitive $p(p-1)$-th root of unity as value for a primitive root mod p^2. (We assume p to be odd prime.) Put

$$W(a,p)=\frac{1}{p}\sum_{i=0}^{p-1}\chi_p^{i(p-1)}(a).$$

Then it is easy to prove that

$$W(a,p)=\begin{cases}1 & \text{if } p \text{ satisfies } (*),\\ 0 & \text{if not.}\end{cases}$$

Thus

$$\#F_a(x)=\sum_{3\leqslant p\leqslant x}W(a,p)=\sum_{3\leqslant p\leqslant x}\frac{1}{p}+\sum_{3\leqslant p\leqslant x}\frac{1}{p}\sum_{i=1}^{p-1}\chi_p^{i(p-1)}(a).$$

We abbreviate the second term to $E_a(x)$ and put

$$M=M(x,\delta)=\{a\,;\,2\leqslant a\leqslant x^4,\ |E_a(x)|>(\log\log x)^{\delta}\},$$

$$\eta_a(x)=\begin{cases}0 & \text{if } E_a(x)=0,\\ \exp(-i\arg(E_a(x))) & \text{if not.}\end{cases}$$

Then we have

$$\begin{aligned}(\#M)(\log\log x)^{\delta} &\leqslant \sum_{a\in M}\eta_a(x)E_a(x)\\ &\leqslant \sum_{3\leqslant p\leqslant x}\sum_{i=1}^{p-1}\frac{1}{p}\left|\sum_{a\in M}\eta_a(x)\chi_p^{i(p-1)}(a)\right|,\end{aligned}$$

and Schwarz's inequality gives that

$$(\#M)(\log\log x)^{\delta}\leqslant S^{1/2}T^{1/2},$$

where

$$S=\sum_{3\leqslant p\leqslant x}\frac{p-1}{p^2}$$

$$T=\sum_{3\leqslant p\leqslant x}\sum_{i=1}^{p-1}\left|\sum_{a\in M}\eta_a(x)\chi_p^{i(p-1)}(a)\right|^2.$$

Since

$$(**)\qquad \sum_{p\leqslant x}\frac{1}{p}=\log\log x+C+\frac{1}{2}\theta((\log x)^{-2}),\qquad \text{if } x\geqslant 286,$$

([4]), it is proved that $S<\log\log x$. And we can prove by the aid of "large sieve inequality" that $T\leqslant 2x^4(\#M)$. Therefore

$$\#M<2x^4(\log\log x)^{1-2\delta}.$$

Thus we have proved that the formula

$$\sharp F_a(x)=\sum_{3\leqslant p\leqslant x}\frac{1}{p}+\theta\,((\log\log x)^3),$$

holds for all a such that $2\leqslant a\leqslant x^4$ with at most $\sharp M$ exceptions of a. We can accomplish our proof here by (**) again. Q.E.D.

Theorem 2 can be proved similarly.

3. A conjecture. The statement of our result and its proof are based on an adoptation of the method of Warlimont ([3]) on Artin's conjecture. Putting

$$N_a(x)=\{p:\text{prime}\,;\,p\leqslant x,\ [(Z/pZ)^*:\langle a \bmod p\rangle]=1\},$$

Artin's well-known conjecture says:

$$({}^{\ *}_{**})\qquad \sharp N_a(x)\sim C_a\pi(x)\qquad \text{as } x\to\infty,$$

where C_a is a constant depending on a, and this was proved by Hooley ([5]) under the assumption of the generalized Riemann hypothesis. Warlimont ([3]) proved on the other hand (without any assumption about Riemann hypothesis) an average type result saying:

$$({}^{**}_{**})\qquad \sharp N_a(x)=C\pi(x)+O(x\,(\log x)^{-2})$$

with an absolute constant C, for "almost all" $a\leqslant x^2$.

Obviously, we can write

$$F_a(x)=\{p:\text{prime}\,;\,3\leqslant p\leqslant x,\ [(Z/p^2Z)^*:\langle a \bmod p^2\rangle]\equiv 0 \pmod p\},$$

and our result is an analogue to $({}^{**}_{**})$. It seems difficult to obtain an analogue to $({}^{\ *}_{**})$, even if we assumed the generalized Riemann hypothesis. But it is tempting to enounce the following asymptotic formula as a conjecture:

$$\sharp F_a(x)\sim D_a\cdot\log\log x,$$

where D_a is a constant depending on a. (We have $F_2(31\,059\,000)=\{1093,\ 3511\}$, $\sharp F_2(31\,059\,000)=2$ and $\log\log(31\,059\,000)\fallingdotseq 2.85$. This is just one example, but could one surmise $\sharp F_2(x)\sim\log\log x$ with $D_2=1$? Concerning some numerical examples for $a\geqslant 3$, see [6].)

References

[1] A. Wieferich: Zum letzten Fermatschen Theorem. J. reine angew. Math., **136**, 293–302 (1909).

[2] D. H. Lehmer and E. Lehmer: On the first case of Fermat's last theorem. Bull. Amer. Math. Soc., **47**, 139–142 (1941).

[3] R. Warlimont: On Artin's conjecture. J. London Math. Soc., (2), **5**, 91–94 (1972).

[4] J. B. Rosser and L. Schoenfeld: Approximate formulas for some functions of prime numbers. Illinois J. Math., **6**, 64–94 (1962).

[5] C. Hooley: On Artin's conjecture. J. reine angew. Math., **225**, 209–220 (1967).

[6] H. Riese: Note on the congruence $a^{p-1}\equiv 1 \pmod{p^2}$. Math. Comp., **18**, 149–150 (1964).