ACTA ARITHMETICA
LVIII.2 (1991)

The distribution of primes satisfying the condition $a^{p-1} \equiv 1 \pmod{p^2}$

by

LEO MURATA (Nancy)

1. Introduction. For any fixed natural number $a \geqslant 2$, it is well known that a rational prime p with $(a, p) = 1$ satisfies the relation $a^{p-1} \equiv 1 \pmod{p}$ (Fermat's little theorem). But only little is known about the distribution of primes p which satisfy

$$a^{p-1} \equiv 1 \pmod{p^2}. \tag{1}$$

To investigate these primes is an interesting problem not only from the view point of distribution of primes but also in relation to Fermat's last theorem. We know that (see, for example [4]):

THEOREM A. *Let p be an odd prime number. If (1) fails to hold for at least one prime value of $a \leqslant 89$, then Fermat's last theorem Case* I *is true for this prime p, that is*

$$x^p + y^p = z^p, \quad (xyz, p) = 1,$$

has no non-trivial integral solution.

Let a, b denote distinct natural integers. We set

$$L_a(x) = \{p;\ p \text{ is an odd prime} \leqslant x,\ a^{p-1} \equiv 1 \pmod{p^2}\},$$

$$L_{a,b}(x) = L_a(x) \cap L_b(x).$$

Some numerical results (see, e.g., [1]) show that these sets are very thin:

$$L_2(3 \times 10^9) = \{1093, 3511\}, \quad L_3(2^{30}) = \{11, 1006003\},$$

$$L_{12}(2^{28}) = \{2693, 123653\}, \quad \text{etc.}$$

Moreover, numerical evidence (see [1]) seems to show that there is no big difference according to whether a is prime or not. To some extent, this justifies the approach of considering the average and normal behaviour of $|L_a(x)|$. We already proved in [3] the following theorem which means, roughly speaking, that $|L_a(x)|$ can be *normally* approximated by $\log\log x$.

For an arbitrary positive valued function $f(x)$, we denote by $\theta(f(x))$ a function of x with absolute value $\leqslant f(x)$.

THEOREM 1. *Let δ be an arbitrary fixed real number satisfying $1/2 < \delta < 1$, $y = y(x)$ be any function of x with $y(x) \geqslant x^4$. We have*

$$|L_a(x)| = \log\log x + \theta((\log\log x)^{\delta}) + O(1)$$

for all a such that $2 \leqslant a \leqslant y$ with at most $2y(\log\log x)^{1-2\delta}$ exceptions for a.

The above-cited Theorem A states that Fermat's last theorem Case I is true outside the intersection of several $L_a(x)$'s, so it is reasonable to consider the behaviour of $|L_{a,b}(x)|$. Since we are motivated by Theorem A, we now have to limit a and b to be prime numbers. We obtain the following average type result:

THEOREM 2. *Let $y(x)$ be any function of x with the property that*

$$x^{3/2}\sqrt{\log x} = o(y(x)).$$

Set

$$\mathfrak{A}(x) = \{(a, b);\ 2 \leqslant a < b \leqslant y(x),\ a \text{ and } b \text{ are primes}\},$$

$$\mathfrak{F}_0(x) = \{(a, b) \in \mathfrak{A}(x);\ |L_{a,b}(x)| = 0\}.$$

Then we have

$$\lim_{x\to\infty} \frac{|\mathfrak{F}_0(x)|}{|\mathfrak{A}(x)|} = \frac{8}{\pi^2}.$$

For given a, the probability that p satisfies $a^{p-1} \equiv 1 \pmod{p^2}$ is roughly $(p-1)/p^2$. It is hence expected that

$$|L_a(x)| \sim \sum_{3\leqslant p\leqslant x} (p-1)/p^2 = \log\log x + O(1),$$

and this is well-matched with our Theorem 1. Similarly, given two distinct primes a and b, the probability that p satisfies $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p^2}$ is roughly p^{-2}. So, for given a, b, it is expected that

$$|L_{a,b}(x)| \sim \sum_{3\leqslant p\leqslant x} p^{-2} \doteqdot 0.199\ldots = 1 - 0.800\ldots \tag{2}$$

Since $8/\pi^2 \doteqdot 0.81057$, there is a little difference with (2). We can interpret this as follows: $8/\pi^2$ of the elements of $\mathfrak{A}(x)$ satisfy the condition $|L_{a,b}(x)| = 0$, a certain density D_1 elements of $\mathfrak{A}(x)$ satisfy $|L_{a,b}(x)| = 1$, a certain density D_2 elements of $\mathfrak{A}(x)$ satisfy $|L_{a,b}(x)| = 2$, etc., and the average of all these quantities is equal to $\sum_{p:\text{odd prime}} p^{-2}$. Actually, we can prove the following result.

THEOREM 3. *Under the notations of Theorem 2, we define for any $i \in \mathbf{N}$,*

$$\mathfrak{F}_i(x) = \{(a, b) \in \mathfrak{A}(x);\ |L_{a,b}(x)| = i\}.$$

(i) *The natural density $D_i = \lim_{x\to\infty} |\mathfrak{F}_i(x)|/|\mathfrak{A}(x)|$ exists for any i, and is given by*

$$D_i = \frac{8}{\pi^2} \sum_n^{(i)} \left(\prod_{p|n} \frac{1}{p^2-1} \right),$$

where, $\omega(n)$ being the number of distinct prime factors of n, $\sum_n^{(i)}$ denotes that the summation is restricted to all odd square-free n with $\omega(n) = i$.

(ii) *D_i satisfies the relations:*

$$\sum_{i=0}^{\infty} D_i = 1, \tag{*}$$

$$\sum_{i=0}^{\infty} iD_i = \sum_{p:\text{odd prime}} p^{-2}. \tag{**}$$

Let $\phi(x)$ be a function with $\lim_{x\to\infty} \phi(x) = \infty$. Then the formula (*) says that

$$|L_{a,b}(x)| \leqslant \phi(x) \quad \text{for all } (a, b) \in \mathfrak{A}(x) \text{ with at most } o(\pi(y(x))^2) \text{ exceptions,} \tag{3}$$

and the formula (**) says that

$$\frac{1}{|\mathfrak{A}(x)|} \sum_{(a,b)\in\mathfrak{A}(x)} |L_{a,b}(x)| \to \sum_{p:\text{odd prime}} p^{-2} \doteqdot 0.199\ldots, \quad \text{as } x \to \infty. \tag{4}$$

Therefore our Theorems 2 and 3 are also well-matched with the probabilistic observation (2).

It is worth noting that the power series formed with the sequence $\{D_i\}_{i=0}^{\infty}$ has the following Euler product:

$$\sum_{i=0}^{\infty} D_i u^i = \prod_{p\geqslant 3} \left(1 + \frac{u-1}{p^2}\right) = \frac{8}{\pi^2} \prod_{p\geqslant 3} \left(1 + \frac{u}{p^2-1}\right). \tag{5}$$

Our assertion (3) follows immediately from (4). At the same time we can obtain a quantitative estimate:

$$|\{(a, b) \in \mathfrak{A}(x);\ |L_{a,b}(x)| > \phi(x)\}| = O(|\mathfrak{A}(x)|\phi(x)^{-1}).$$

Nevertheless, this estimate may be improved noticeably by making use of analytic properties of the function defined in (5)—at least when $\phi(x)$ tends to infinity suitably slowly.

The quality of the information contained in Theorems 2 and 3 is better for the smaller choice of $y(x)$; it hence looks interesting to extend the range of the validity of $y(x)$ in these results. But this might be very difficult, since it is closely connected with the problem of the distribution, for given prime p, of those residue classes $f_i \pmod{p^2}$ which satisfy $f_i^{p-1} \equiv 1 \pmod{p^2}$.

We give the proofs of Theorems 2 and 3 in the next section.

At the end of this section we want to add two theorems which are related to the same subject. The proofs proceed along the same lines, and we omit them here.

THEOREM 4. *Let $y(x)$ be any function of x with the property that $x^2 = o(y(x))$. We put*

$$M_a(x) = \{p \leqslant x;\ a^{p-1} \equiv 1 \pmod{p^3}\},$$

$$\tilde{\mathfrak{F}}_i(x) = \{a \leqslant y(x);\ a \text{ is a prime}, |M_a(x)| = i\}, \quad i = 0, 1, \ldots$$

Then we have

$$\lim_{x\to\infty} \frac{|\tilde{\mathfrak{F}}_i(x)|}{\pi(y(x))} = D_i,$$

where D_i is the number defined in Theorem 3.

THEOREM 5. *Let $y(x)$ be any function of x with the property that*

$$x^{4/3}(\log x)^{2/3} = o(y(x)).$$

We put

$$\mathfrak{B}(x) = \{(a, b, c);\ 2 \leqslant a < b < c \leqslant y(x),\ a, b, c \text{ are primes}\},$$

$$\mathfrak{G}_i(x) = \{(a, b, c) \in \mathfrak{B}(x);\ |L_a(x) \cap L_b(x) \cap L_c(x)| = i\}, \quad i = 0, 1, \ldots$$

(i) *The natural density $E_i = \lim_{x\to\infty} |\mathfrak{G}_i(x)|/|\mathfrak{B}(x)|$ exists for any i, and is given by*

$$E_i = \frac{8}{7}\zeta(3)^{-1} \sum\nolimits_n^{(i)} \Big(\prod_{p|n} 1/(p^3-1)\Big),$$

where $\sum_n^{(i)}$ denotes that the summation is restricted to all odd square-free n with $\omega(n) = i$.

(ii) *E_i satisfies the relations:*

$$(*) \qquad \sum_{i=0}^{\infty} E_i = 1,$$

$$(**) \qquad \sum_{i=0}^{\infty} iE_i = \sum_{p:\,\text{odd prime}} p^{-3}.$$

The above theorems show that it can happen rather frequently that $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p^2}$ or $a^{p-1} \equiv 1 \pmod{p^3}$. Indeed, we found several such examples in [1]: $L_{17,19}(100) = \{3\}$, $M_{19}(100) = \{7\}$, $L_{53,67,71}(100) = \{47\}$, etc.

The author expresses here his hearty gratitude to Gérald Tenenbaum for carefully reading the original manuscript and for some important comments which enabled the author to improve his original statements, especially in Theorem 3.

2. Proofs of Theorems 2 and 3. The letters p, a and b always indicate a prime number, $\pi(x)$ denotes the number of primes not exceeding x, $\pi(x;\ k, l)$ the number of primes $\leqslant x$ which are congruent to l modulo k, $\varphi(n)$ Euler's totient function, $\boldsymbol{Z}$ the ring of integers, and $\mathrm{Li}(x) = \int_2^x (\log t)^{-1}\,dt$.

Now we give the proof of Theorem 2. We define

$$W(a, p) = \begin{cases} 1 & \text{if } a \text{ and } p \text{ satisfy the relation (1),} \\ 0 & \text{if not,} \end{cases}$$

$$z = \log\log x,$$

and start from the formula

$$(6) \qquad |L_{a,b}(x)| = \sum_{3\leqslant p\leqslant x} W(a, p)W(b, p) = \Big(\sum_{3\leqslant p\leqslant z} + \sum_{z<p\leqslant x}\Big) W(a, p)W(b, p)$$
$$= T_{a,b}^{(1)} + T_{a,b}^{(2)}, \quad \text{say.}$$

First we consider the second term. Let p be a fixed odd prime number; we can easily verify the following facts:

(7) among the $p(p-1)$ invertible residue classes modulo p^2, there exist just $p-1$ residue classes $f_i \pmod{p^2}$, $i = 1, 2, \ldots, p-1$, which satisfy $f_i^{p-1} \equiv 1 \pmod{p^2}$,

(8) a prime number a satisfies the relation $a^{p-1} \equiv 1 \pmod{p^2}$, if, and only if, $a \equiv f_i \pmod{p^2}$ for some $i = 1, 2, \ldots, p-1$.

Therefore, for a fixed prime p and for a real number $y = y(x)$, we have

$$(9) \qquad \sum_{a\leqslant y} W(a, p) = \sum_{i=1}^{p-1} \pi(y;\ p^2, f_i).$$

Now we consider the sum $\sum_{2\leqslant a\leqslant y}\sum_{2\leqslant b\leqslant y} T_{a,b}^{(2)}$. The formulas (6) and (9) yield

$$\sum_{2\leqslant a\leqslant y}\sum_{2\leqslant b\leqslant y} T_{a,b}^{(2)} = \sum_{z<p\leqslant x}\Big(\sum_{i=1}^{p-1} \pi(y;\ p^2, f_i)\Big)^2$$
$$= \Big(\sum_{z<p\leqslant \sqrt[3]{y}} + \sum_{\sqrt[3]{y}<p\leqslant x}\Big)\Big(\sum_{i=1}^{p-1} \pi(y;\ p^2, f_i)\Big)^2 = U_1 + U_2, \text{ say.}$$

The Brun–Titchmarsh theorem (cf. for example [2, Theorem 3.8]) says that

$$\pi(y;\ k, l) < \frac{3y}{\varphi(k)\log(y/k)}, \quad 1 \leqslant k < y,\ (k, l) = 1,$$

and we can estimate U_1 as follows:

$$(10) \qquad U_1 \ll y^2(\log y)^{-2} \sum_{z<p\leqslant \sqrt[3]{y}} p^{-2} = \pi(y)^2 O((z\log z)^{-1}).$$

If $\sqrt[3]{y} < p \leqslant x$, we use the trivial bound:

$$\pi(y;\ p^2, f_i) \leqslant \sum_{\substack{n\leqslant y \\ n\equiv f_i \pmod{p^2}}} 1 \leqslant [y/p^2] + 1 \leqslant y/p^2 + 1;$$

then we have

$$U_2 \leqslant \sum_{\sqrt[3]{y}<p\leqslant x} (p-1)^2(1+2yp^{-2}+y^2p^{-4}) \tag{11}$$
$$\ll x^2\pi(x)+y\pi(x)+y^{5/3}(\log y)^{-1}.$$

From the assumption on $y(x)$, we get

$$x^2\pi(x) = o(\pi(y)^2), \quad y\pi(x) = o(\pi(y)^2),$$

and consequently, (10) and (11) yield that $\sum_{2\leqslant a\leqslant y}\sum_{2\leqslant b\leqslant y} T_{a,b}^{(2)} = o(\pi(y)^2)$. This shows that

(12) the density of the set $\{(a, b)\in\mathfrak{A}(x);\ |L_{a,b}(x)|-|L_{a,b}(z)|\geqslant 1\}$ tends to zero as x tends to infinity.

Therefore, in order to calculate the limiting density of $\mathfrak{F}_0(x)$, it is sufficient to consider the distribution of the values of $T_{a,b}^{(1)}$.

We put $P = \{p;\ 3\leqslant p\leqslant z\}$ and $Q = \prod_{p\in P} p^2$. The prime number theorem tells us that $Q \ll (\log x)^{2+\varepsilon}$, for any positive real ε. For any integer k satisfying $(k, Q) = 1$, by virtue of the Siegel–Walfisz theorem, we have

$$\pi(y;\ Q,\ k) = \frac{1}{\varphi(Q)}\mathrm{Li}(y)+O\big(y\exp(-C\sqrt{\log y})\big), \tag{13}$$

with some positive constant C. From the Chinese remainder theorem we have

$$(\boldsymbol{Z}/Q\boldsymbol{Z})^* = \bigotimes_{p\in P}(\boldsymbol{Z}/p^2\boldsymbol{Z})^*, \tag{14}$$

that is, among the $\varphi(Q)$ residue classes $\{k \pmod Q;\ (k, Q) = 1\}$, all combinations of all invertible residue classes modulo p^2, $p\in P$, appear exactly once respectively.

We define

$$\mathfrak{A}'(x) = \{(a, b);\ 2\leqslant a\leqslant y(x),\ 2\leqslant b\leqslant y(x)\},$$
$$\mathfrak{F}_0'(x) = \{(a, b)\in\mathfrak{A}'(x);\ L_{a,b}(z) = \emptyset\},$$

and calculate $|\mathfrak{F}_0'(x)|$. We split the set $\mathfrak{F}_0'(x)$ into classes according to the set $L_a(z)$:

$$\mathfrak{F}_0'(x) = \bigcup_{S\subseteq P}\{(a, b)\in\mathfrak{A}'(x);\ L_a(z) = S,\ L_{a,b}(z) = \emptyset\}, \tag{15}$$

where this expression is a disjoint union. The condition "$L_a(z) = S$ and $L_{a,b}(z) = \emptyset$" is equivalent to the condition "$L_a(z) = S$ and $L_b(z)\subseteq P-S$". From (7) and (14), we know that "$L_a(z) = S$" occurs if, and only if, a is contained in certain $\prod_{p\in S}(p-1)\prod_{p\in P-S}(p-1)^2$ residue classes modulo Q. Similarly, "$L_b(z)\subseteq P-S$" occurs if, and only if, b is contained in certain

$\prod_{p\in S}(p-1)^2\prod_{p\in P-S}p(p-1)$ residue classes modulo Q. Combining with (13), we have

$$\begin{aligned}
&|\{(a, b)\in\mathfrak{A}'(x);\ L_a(z) = S \text{ and } L_{a,b}(z) = \emptyset\}| \\
&= |\{a\leqslant y(x);\ L_a(z) = S\}|\times|\{b\leqslant y(x);\ L_b(z)\subseteq P-S\}| \\
&= \left\{\frac{\left(\prod_{p\in S}(p-1)\right)\left(\prod_{p\in P-S}(p-1)^2\right)}{\varphi(Q)}\mathrm{Li}(y)+O\big(y(\log x)^{2+\varepsilon}\exp(-C\sqrt{\log y})\big)\right\} \\
&\times\left\{\frac{\left(\prod_{p\in S}(p-1)^2\right)\left(\prod_{p\in P-S}p(p-1)\right)}{\varphi(Q)}\mathrm{Li}(y)+O\big(y(\log x)^{2+\varepsilon}\exp(-C\sqrt{\log y})\big)\right\}.
\end{aligned}$$

Since

$$\frac{\prod_{p\in S}(p-1)\prod_{p\in P-S}(p-1)^2}{\varphi(Q)} = \left(\prod_{p\in P-S}\left(1-\frac{1}{p}\right)\right)\left(\prod_{p\in S}\frac{1}{p}\right) \quad \text{and}$$
$$\frac{\prod_{p\in S}(p-1)^2\prod_{p\in P-S}p(p-1)}{\varphi(Q)} = \prod_{p\in S}\left(1-\frac{1}{p}\right),$$

we obtain

$$\begin{aligned}
&|\{(a, b)\in\mathfrak{A}'(x);\ L_a(z) = S \text{ and } L_{a,b}(z) = \emptyset\}| \\
&= \left(\prod_{p\in P}\left(1-\frac{1}{p}\right)\right)\left(\prod_{p\in S}\frac{1}{p}\right)\mathrm{Li}(y)^2+O\big(\mathrm{Li}(y)\,y(\log x)^{2+\varepsilon}\exp(-C\sqrt{\log y})\big).
\end{aligned}$$

Now, we sum up this formula for all $S\subseteq P$. The number of such S is $2^{|P|} = O(\log x)$, thus we have

$$\begin{aligned}
|\mathfrak{F}_0'(x)| &= \prod_{p\in P}\left(1-\frac{1}{p}\right)\sum_{S\subseteq P}\left(\prod_{p\in S}\frac{1}{p}\right)\pi(y)^2+O\big(\mathrm{Li}(y)\,y(\log x)^{3+\varepsilon}\exp(-C\sqrt{\log y})\big) \\
&= \prod_{p\in P}\left(1-\frac{1}{p^2}\right)\pi(y)^2+o(\pi(y)^2),
\end{aligned}$$

and

$$\prod_{3\leqslant p\leqslant z}\left(1-\frac{1}{p^2}\right) = \frac{8}{\pi^2}(1+O(z^{-1})).$$

For any a, b and x, we have $L_{a,b}(x) = L_{b,a}(x)$, and $|\{(a, b)\in\mathfrak{A}'(x);\ a = b\}| = \pi(y)$. Therefore we get

$$|\{(a, b)\in\mathfrak{A}(x);\ L_{a,b}(z) = \emptyset\}| = \frac{1}{2}\frac{8}{\pi^2}\pi(y)^2 + o(\pi(y)^2),$$

and

$$|\mathfrak{A}(x)| = \tfrac{1}{2}(|\mathfrak{A}'(x)| - \pi(y)) = \tfrac{1}{2}\pi(y)^2 + O(\pi(y)).$$

Taking account of (12), we obtain the desired result. ∎

We can prove Theorem 3 by the same method, and it is sufficient to sketch some crucial points. We start again from (6). The first half of the proof of Theorem 2 gives again that the $T^{(2)}_{a,b}$-part makes no contribution to the limiting density of any $|\mathfrak{F}_i(x)|$. We have a partition

$$\{(a, b);\ 2 \leqslant a, b \leqslant y(x), |L_{a,b}(z)| = i\} = \bigcup_{\substack{J\subseteq P\\ |J|=i}} \bigcup_{\substack{S\subseteq P\\ S\supseteq J}} \{(a, b)\in\mathfrak{A}'(x);\ L_a(z) = S, L_{a,b}(z) = J\},$$

where this expression is a disjoint union. Then, by the same way, we obtain

$$|\{(a, b)\in\mathfrak{A}'(x);\ L_a(z) = S, L_{a,b}(z) = J\}| = \left(\prod_{p\in J}\frac{1}{p^2}\right)\left(\prod_{p\in S-J}\frac{p-1}{p^2}\right)\left(\prod_{p\in P-S}\left(1-\frac{1}{p}\right)\right)\mathrm{Li}(y)^2 + O\left(\mathrm{Li}(y)\,y(\log x)^{2+\varepsilon}\exp\left(-C\sqrt{\log y}\right)\right).$$

Firstly, we sum up this formula for all $S \supseteq J$, secondly for all $J \subseteq P$ with $|J| = i$; then

$$2|\mathfrak{F}_i(x)| = \prod_{p\in P}\left(1-\frac{1}{p^2}\right)\sum_{\substack{J\subseteq P\\ |J|=i}}\left(\prod_{p\in J}\frac{1}{p^2-1}\right)\mathrm{Li}(y)^2 + O\left(\mathrm{Li}(y)\,y(\log x)^{4+\varepsilon}\exp\left(-C\sqrt{\log y}\right)\right),$$

and this gives the density of $\mathfrak{F}_i(x)$.

Now it is easy to verify the relations (*) and (**).

We define the function $f(u)$ by (5). The series converges absolutely when $|u| \leqslant D$ with any positive constant D. It is clear that $f(1) = 1$, which proves (*) and that $f'(1) = \sum_{p>2} p^{-2}$, which proves (**). ∎

References

[1] J. Brillhart, J. Tonscia and P. Weinberger, *On the Fermat quotient*, in: *Computers in Number Theory* (Atkin–Birch, ed.), 1971, 213–222.

[2] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, 1974.

[3] L. Murata, *An average type result on the number of primes satisfying generalized Wieferich condition*, Proc. Japan Acad. 57 (1981), 430–432.

[4] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, 1979.

Present address:
DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ DE NANCY I
B. P. 239, 54506 Vandoeuvre-lés-Nancy Cedex
France

Permanent address:
DEPARTMENT OF MATHEMATICS
MEIJI-GAKUIN UNIVERSITY
1518 Kamikurata, Totsuka, Yokohama
244 Japan

Received on 22.11.1988
and in revised form on 28.2.1990 (1887)