Astérisque

LEO MURATA

On the magnitude of the least primitive root

Astérisque, tome 198-199-200 (1991), p. 253-257

<http://www.numdam.org/item?id=AST_1991__198-199-200__253_0>

© Société mathématique de France, 1991, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

ON THE MAGNITUDE OF THE LEAST PRIMITIVE ROOT

by

Leo MURATA

1. Let p be an odd prime number. We define

$g(p)$ = the least positive integer which is a primitive root mod p,
$G(p)$ = the least prime which is a primitive root mod p.

In most cases, $g(p)$ are very small. For example, among the 19862 odd primes ≤ 223051, $g(p) = 2$ happens for 7429 primes (37.4 %), $g(p) = 3$ happens for 4518 primes (22.8 %), and $g(p) \leq 6$ holds for about 80 % of these primes. And we can support this fact by a probabilistic argument. In fact, for a given prime p, there are $p-1$ invertible residue classes, among which $\varphi(p-1)$ residue classes are primitive modulo p, where φ denotes Euler's totient function. Therefore, on the assumption of good distribution of the primitive residue classes mod p, we can surmise that,

(1) for almost all prime $p, g(p)$ is not very far from $\dfrac{p-1}{\varphi(p-1)} + 1$.

The function $(p-1)/\varphi(p-1)$ fluctuates irregularly, but we can prove the asymptotic formula :

$$\pi(x)^{-1} \sum_{\substack{p \leq x \\ p:\text{prime}}} \frac{p-1}{\varphi(p-1)} = C + O\left(\frac{\log\log x}{\log x}\right), C = \prod_{p:\text{prime}} \left(1 + \frac{1}{(p-1)^2}\right) \doteq 2.827.$$

So, we can guess that

(2) for almost all prime p, $\dfrac{p-1}{\varphi(p-1)}$ is not very far from the constant C ,

and, combining (1) and (2), we can expect that,

(3) for almost all p, $g(p)$ is not very far from the constant $C+1$.

So, it seems very natural to conjecture that, for any monotone increasing positive function $\psi(x)$ tending to $+\infty$, we have an estimate

$$|\{p \leq x \ ; \ g(p) > \psi(p)\}| \ = \ o(\pi(x)). \tag{4}$$

In this direction, we have already a lot of results :

- BURGESS [1] : $g(p) \ll p^{(1/4)+\varepsilon}$, for any $\varepsilon > 0$,
- WANG [12] : under the assumption of the Generalized Riemann Hypothesis (G.R.H.),

$$g(p) \ll (\log p)^2 \omega(p-1)^6 \ ,$$

where $\omega(n)$ denotes the number of distinct prime divisors of n.

- If we take $\psi(x) = C$, the constant function, then we can prove, from MATTHEWS' result about ARTIN's conjecture [10] that, under G.R.H. ,

$$|\{p \leq x \ ; \ g(p) > C\}| \ = \ A_c \pi(x) + o(\pi(x)) \ ,$$

where A_c is a positive constant depending on C, with $0 < A_c \leq 1$.

The last result shows that our conjecture (4) does not hold for the constant function. So, we are interested in the problem, when $\psi(x)$ is a function tends to $+\infty$ rather slowly, is our conjecture (4) true or not ?

Our first result shows that our conjecture is true, under the assumption of G.R.H..

THEOREM 1. ([11]). *We assume G.R.H.. Let $\psi(x)$ be a monotone increasing positive function with the properties*

$$\lim_{x\to\infty} \psi(x) = +\infty, \psi(x) \ll (\log x)^A \text{ for some } A > 0, \psi(x) \ll \psi(x(\log x)^{-1}).$$

Then we have

$$|\{p \leq x \ ; \ G(p) > \psi(p)\}| \ \ll \ \pi(x)(\log \psi(x))^{-1}.$$

This is a result about $G(p)$, but the trivial inequality $g(p) \leq G(p)$ implies that the same estimate still holds for $g(p)$, which verifies (4).

To clarify the contents of our theorem, we take, for example, $\psi(x) = \log\log x$. Then we have $g(p) \leq G(p) \leq \log\log p$, except for $O\left(\frac{\pi(x)}{\log\log\log x}\right)$ primes, whose density is zero.

2. Here we consider the average value of $g(p)$.

It is already proved in 1967 by BURGESS-ELLIOTT [2] that

$$\pi(x)^{-1}\sum_{p\leq x} g(p) \ll (\log x)^2(\log\log x)^4.$$

We can improve this estimate, under G.R.H. , as follows :

THEOREM 2. ([8]). *We assume G.R.H.. Then we have, for any* $\varepsilon > 0$,

$$\pi(x)^{-1}\sum_{p\leq x} g(p) \leq \pi(x)^{-1}\sum_{p\leq x} G(p) \ll (\log x)(\log\log x)^{1+\varepsilon}.$$

Making use of the same argument, we have the following corollary. Let $n_2(p)$ be the least quadratic non-residue mod p, MONTGOMERY proved in 1971 that, under G.R.H., $n_2(p) = \Omega((\log p)(\log\log p))$.

(Remark. Very recently, GRAHAM and RINGROSE proved unconditionally that $n_2(p) = \Omega((\log p)(\log\log\log p))$ cf.[9]). Since $g(p) \geq n_2(p)$, under G.R.H. we have

$$g(p) = \Omega((\log p)(\log\log p)) . \tag{5}$$

Now, we can prove that the primes which satisfy the inequality (5) are rather exceptional :

COROLLARY. *We assume G.R.H.. Let B be an arbitrary positive constant, then we have, for any* $\varepsilon > 0$,

$$|\{p \leq x \ ; \ g(p) \geq B(\log p)(\log\log p)\}| \ll \pi(x)(\log x)^{(-1/2+\varepsilon)},$$

where the constant implied by the $\ll$-symbol depends only on B and ε.

3. We want to think about our problem from a little different point of view. We define

$n_k(p)$ = the least positive integer which is not a k-th power residue mod p,

$r_k(p)$ = the least prime which is a k-th power residue mod p,

then, $n_k(p)$ and $r_k(p)$ have the similar property as $g(p)$ and $G(p)$, respectively. In fact, among $p-1$ invertible residue classes mod p, there are $(1-k^{-1})(p-1)$ classes which are not k-th power residue mod p, and, on the assumption of good distribution of these classes, we can expect that $n_k(p)$ is not very far from the constant $k(k-1)^{-1}+1$, etc. Concerning $n_k(p)$ and $r_k(p)$, more than twenty years ago, ELLIOTT obtained the following asymptotic relations (cf.[3], [4] , see also [5], [6], [7]) :

- If $\delta < 4\ \exp(1-k^{-1})$, then

$$\pi(x)^{-1}\sum_{p\leq x} n_k(p)^\delta \ = \ C_{k,\delta}+o(1), \quad \text{as } x\to+\infty,$$

where $C_{k,\delta}$ is a constant depending only on k and δ.

- If $\delta < 4$, then

$$\pi(x)^{-1}\sum_{p\leq x} r_2(p)^\delta \ = \ D_\delta + O\left(\exp\left(-D\frac{\log\log x}{\log\log\log x}\right)\right)\ ,\ D>0\ ,$$

where D_δ is a constant depending on δ.

- If $k\geq 3$, then there exists a constant $\delta(k)<1$, and for any $\delta<\delta(k)$,

$$\pi(x)^{-1}\sum_{p\leq x} r_k(p)^\delta \ = \ D_{k,\delta}+o(1)\ ,\ \text{as } x\to+\infty. \tag{6}$$

where $D_{k,\delta}$ is a constant depending only on k and δ.

Therefore it seems very natural to seek the same asymptotic formula for the averages of $g(p)^\delta$ and $G(p)^\delta$. And actually, we have

THEOREM 3. ([8]). *We assume G.R.H.. If $\delta<\frac{1}{2}$, then we can prove the asymptotic relation :*

$$\begin{cases} \pi(x)^{-1}\sum_{p\leq x} g(p)^\delta = E_\delta+o(1)\ , \\ \pi(x)^{-1}\sum_{p\leq x} G(p)^\delta = E'_\delta+o(1)\ , \end{cases} \tag{7}$$

where E_δ and E'_δ are constants depending only on δ.

So, in some sense, by Theorem 3 we arrived at the same stage with (6) under the assumption of G.R.H..

The asymptotic relations (7) are likely to be true for $\delta = 1$, but it seems very difficult to prove it, if we assume G.R.H. only.

REFERENCES

[1] BURGESS D.A., The least quadratic non-residue, *Ann.of Math.* (2), **55** (1962), 65-71.

[2] BURGESS D.A.-ELLIOTT P.D.T.A., The average of the least primitive root, *Mathematika*, **15** (1968), 39-50.

[3] ELLIOTT P.D.T.A., A problem of Erdős concerning power residue sums, *Acta Arithmetica*, **13** (1967), 131-149.

[4] ELLIOTT P.D.T.A., Some notes on k-th power residues, *Acta Arithmetica*, **14** (1968), 153-162.

[5] ELLIOTT P.D.T.A., The distribution of primitive roots, *Canadian J. of Math.*, **21** (1969), 822-841.

[6] ELLIOTT P.D.T.A., The distribution of power residues and certain related results, *Acta Arithmetica*, **17** (1970), 141-159.

[7] ELLIOTT P.D.T.A., On the mean value of $f(p)$, *Proc. of London Math. Soc.* (3), **21** (1970), 28-96.

[8] ELLIOTT P.D.T.A.-MURATA L., a paper on "The average of the least primitive root modulo p", in preparation.

[9] GRAHAM S.W. - RINGROSE C.J., *Lower bounds for least quadratic non-residues,* preprint.

[10] MATTHEWS K.R., A generalization of Artin's conjecture for primitive roots, *Acta Arithmetica*, **29** (1976), 113-146.

[11] MURATA L., On the magnitude of the least prime primitive root, to appear, *J. of Number Theory*, **36** (1990).

[12] WANG Y. , On the least primitive root of a prime, *Sci. Sinica*, **10** (1961), 1-14.

Present address :
LEO MURATA
Department of Mathematics
Meiji-gakuin University
1518 Kami-kurata, Totsuka,
Yokohama 244, Japan.