ARTIN'S CONJECTURE ON THE AVERAGE

MORRIS GOLDFELD

1. *Introduction.* It was conjectured by Artin [1] that each non-zero integer a unequal to $+1$, -1 or a perfect square is a primitive root for infinitely many primes p. More precisely, denoting by $N_a(x)$ the number of primes $p \leqslant x$ for which a is a primitive root, he conjectured that

$$N_a(x) \sim c(a)\,\mathrm{Li}(x) \qquad (x \to \infty),$$

where $c(a)$ is a positive constant. This conjecture has recently been proved by C. Hooley [2] under the assumption that the Riemann hypothesis holds for fields of the type $Q(\sqrt[k]{a}, \sqrt[k]{1})$.

It is the object of this paper to prove (without using the Riemann hypothesis) that $N_a(x)$ is approximated by $c\,\mathrm{Li}\,(x)$ for most integers $a \leqslant A$, for suitable choices of the parameters x, A and the constant c. We shall prove the following theorem:

THEOREM. *Let $1 < A \leqslant x$. Then for each $D \geqslant 1$,*

$$N_a(x) = c\,\mathrm{Li}\,(x) + O(x/\log^D x), \qquad c = \Pi\,(1 - 1/p(p-1))$$

for all integers $a \leqslant A$ with at most

$$c_1\,A^{9/10}(5\log x + 1)^{g+D+2}, \qquad g = \log x/\log A,$$

exceptions, where c_1 and the constant implied by the O-notation are positive and depend at most on D.

The exponent 9/10 which occurs in the theorem is not the best possible. Actually, it can be replaced by $7/8 + \lambda(g)$ where $\lambda(g) = 0$ if g is an integer and otherwise $0 < \lambda(g) < 1/(8g)$.

Finally, I should like to take this opportunity to thank Prof. P. X. Gallagher for his helpful and most encouraging advice in the preparation of this paper.

2. *Notation and formulation of method.* In what follows p is a prime number, a is a positive integer other than 1 or a perfect square, and for $p \nmid a$, $e_a(p)$ is the least positive integer d such that

$$a^d \equiv 1 \bmod p.$$

We set $f_a(p) = (p-1)/e_a(p)$. Then a is a primitive root mod p if and only if $f_a(p) = 1$; following Hooley [2], we have

$$N_a(x) = \sum_{k \leqslant x} \mu(k)\,P_a(x,k), \text{ with } P_a(x,k) = \sum_{\substack{p \leqslant x \\ k \mid f_a(p) \\ p \nmid a}} 1. \tag{1}$$

Now, $p \nmid a$ and $k \mid f_a(p)$, if, and only if,

$$p \equiv 1 \bmod k \quad \text{and} \quad a^{(p-1)/k} \equiv 1 \bmod p. \tag{2}$$

Consequently, the primes p counted in the sum

$$M_a(x) = \sum_{k > x^{3/4}} P_a(x,k)$$

must divide
$$\prod_{m \leqslant x^{1/4}} (a^m - 1).$$
Therefore
$$2^{M_a(x)} \leqslant \prod_{m \leqslant x^{1/4}} a^m,$$
and so
$$M_a(x) \leqslant \frac{\log a}{\log 2} x^{\frac{1}{2}}.$$
Let $D \geqslant 1$ be given. Assuming, for some a, that†
$$\sum_{k \leqslant x^{3/4}} \left| P_a(x, k) - \frac{\operatorname{Li}(x)}{k\phi(k)} \right| \ll x/\log^D x, \tag{3}$$
it follows by (1) and (3) that
$$N_a(x) - \sum_{k \leqslant x^{3/4}} \left(\frac{\mu(k)}{k\phi(k)}\right) \operatorname{Li}(x) \ll x/\log^D x + M_a(x)$$
$$\ll x/\log^D x.$$
Since
$$\sum_{k \leqslant x^{3/4}} \frac{\mu(k)}{k\phi(k)} = c + O(x^{-3/4}), \qquad c = \prod_p \left(1 - \frac{1}{p(p-1)}\right),$$
we get
$$N_a(x) - c \operatorname{Li}(x) \ll x/\log^D x.$$

3. *Proof of theorem.* From the results of the previous section, it only remains to prove the following:

LEMMA 1. *Let $1 < A \leqslant x$. Then* (3) *holds for all but $c_1 A^{9/10}(5 \log x + 1)^{g+D+1}$ exceptional values of $a \leqslant A$, where $g = \log x/\log A$.*

Proof. Let $\chi_{p,k}$ be any fixed character mod p of order k. Then for $p \equiv 1 \bmod k$, we have
$$\frac{1}{k} \sum_{\nu=0}^{k-1} \chi_{p,k}^{\nu}(a) = 1 \text{ or } 0$$
according as $a^{(p-1)/k} \equiv 1 \bmod p$ or not. Consequently, by (1) and (2),‡
$$P_a(x, k) = \frac{1}{k} \sum_{\substack{p \leqslant x \\ p \equiv 1\,(k)}} \sum_{\nu=0}^{k-1} \chi_{p,k}^{\nu}(a)$$
$$= \frac{1}{k} \left(\Pi(x;\ k, 1) + O(\log a) + S_a(x, k)\right), \tag{4}$$
where
$$S_a(x, k) = \sum_{\substack{p \leqslant x \\ p \equiv 1\,(k)}} \sum_{\nu=1}^{k-1} \chi_{p,k}^{\nu}(a).$$

† Throughout this paper, by $A \ll B$ or alternatively $A = O(B)$, we shall mean $|A| \leqslant c_0 B$ for some positive constant c_0 depending only on D and the context in which the symbols $\ll$, O, are being used.

‡ $\Pi(x;\ k, 1)$ denotes the number of primes $p \leqslant x$ which are congruent to 1 mod k.

We have

$$\sum_{k \leqslant x^{3/4}} \frac{1}{k} \left| \Pi(x;\, k, 1) - \frac{\mathrm{Li}\,(x)}{\phi(k)} \right| = \sum_{k \leqslant \log^D x} + \sum_{\log^D x < k \leqslant x^{3/4}} .$$

In the first sum use the Siegel–Walfisz [3] estimate

$$\Pi(x;\, k, 1) - \frac{\mathrm{Li}\,(x)}{\phi(k)} \ll x/\log^{D+1} x,$$

and in the second sum the trivial estimate

$$\Pi(x;\, k, 1) - \frac{\mathrm{Li}\,(x)}{\phi(k)} \ll x/k.$$

We get

$$\sum_{k \leqslant x^{3/4}} \frac{1}{k} \left| \Pi(x;\, k, 1) - \frac{\mathrm{Li}\,(x)}{\phi(k)} \right| \ll x/\log^D x.$$

It therefore follows by this and equation (4) that

$$\sum_{k \leqslant x^{3/4}} \left| P_a(x, k) - \frac{\mathrm{Li}\,(x)}{k\phi(k)} \right| \ll x/\log^D x + S_a(x), \tag{5}$$

where we have set

$$S_a(x) = \sum_{k \leqslant x^{3/4}} \frac{1}{k} \left| S_a(x, k) \right|.$$

For the next steps we use a technique introduced by Heilbronn [4]. Note that $\chi_{p_1}^{\nu_1} \overline{\chi_{p_2}^{\nu_2}}$ can be principal only if $p_1 = p_2$. Otherwise it is a primitive character mod $p_1 p_2$ of order dividing k. Hence we may write

$$\sum_{a \leqslant A} |S_a(x, k)| \leqslant A(xk)^{\frac{1}{2}} + A^{\frac{1}{2}} \left(\sum_{\substack{p_1, p_2 \leqslant x \\ p_1, p_2 \equiv 1\ (k) \\ p_1 \neq p_2}} \; \sum_{\chi \bmod p_1 p_2}{}' S(\chi) \right)^{\frac{1}{2}}, \tag{6}$$

where we have put

$$S(\chi) = \sum_{a \leqslant A} \chi(a),$$

and where $\sum'$ indicates that we are summing over primitive characters of order dividing k.

Let T denote the double sum on the right side of equation (6). By Hölder's inequality, for each integer $r \geqslant 1$,

$$\begin{aligned} T^{\frac{1}{2}} &\leqslant \left(\sum_{\substack{p_1, p_2 \leqslant x \\ p_1, p_2 \equiv 1\ (k)}} \; \sum_{\chi \bmod p_1 p_2}{}' 1 \right)^{\frac{1}{2}(1 - 1/2r)} \left(\sum_{\substack{p_1, p_2 \leqslant x \\ p_1, p_2 \equiv 1\ (k)}} \; \sum_{\chi \bmod p_1 p_2}{}' |S(\chi)|^{2r} \right)^{1/4r} \\ &\leqslant x^{1 - 1/2r} \left(\sum_{\substack{p_1, p_2 \leqslant x \\ p_1, p_2 \equiv 1\ (k)}} \; \sum_{\chi \bmod p_1 p_2}{}' |S(\chi)|^{2r} \right)^{1/4r}, \end{aligned} \tag{7}$$

and we write

$$S(\chi)^r = \sum_{a=1}^{A^r} \tau_r'(a) \chi(a)$$

and where $\tau_r'(a)$ denotes the number of ways a can be written as a product of r integers, each of which is less than A.

To estimate the right side of (7), we use the following "large sieve" inequality [5], valid for arbitrary complex constants a_n.

If

$$Z = \sum_{n=1}^{N} |a_n|^2,$$

then

$$\sum_{q \leq Q} \sum_{\chi \bmod q} \left| \sum_{n=1}^{N} a_n \chi(n) \right|^2 \ll (Q^2 + N) Z.$$

We apply this inequality with $a_n = \tau_r'(a)$, $Q = x^2$ and $N = A^r$. Since $\tau_r'(a) \leqslant \tau_r(a)$, where $\tau_r(a)$ denotes the number of ways a can be written as a product of r integers, we have (*cf.* [6])

$$Z \leqslant \sum_{a=1}^{A^r} \tau_r(a)^2 \ll A^r(\log A^r + 1)^{r^2-1}.$$

Substituting in (7), we arrive at

$$T^{\frac{1}{2}} \ll x^{1-\frac{1}{2}r}\big((x^4 + A^r)\, A^r(\log A^r + 1)^{r^2}\big)^{1/4r}. \tag{8}$$

We now let

$$r = Q(4g), \qquad g = \log x/\log A, \tag{9}$$

where $Q(y)$ denotes the least integer greater than or equal to y. The combination of equations (6), (8) and (9) proves the lemma.

References

1. S. Lang and J. Tate, *The Collected Papers of Emil Artin* (Addison–Wesley, 1965), Preface.
2. C. Hooley, " On Artin's Conjecture ", *Journal für Math.*, 225 (1967), 209–220.
3. K. Prachar, *Primzahlverteilung* (Springer, 1957).
4. H. Heilbronn, " On the averages of some arithmetical functions of two variables ", *Mathematika*, 5 (1958), 1–7.
5. P. X. Gallagher, " The large sieve ", *Mathematika*, 14 (1967), 14–20.
6. I. M. Vinogradov, *The method of trigonometric sums in the theory of numbers* (Interscience, 1961), 41–43.

Columbia University,
New York 27, N.Y.

(*Received on the 27th of March*, 1968.)