Canad. Math. Bull. Vol. **30** (1), 1987

SOME REMARKS ON ARTIN'S CONJECTURE

BY
M. RAM MURTY AND S. SRINIVASAN

ABSTRACT. It is a classical conjecture of E. Artin that any integer $a > 1$ which is not a perfect square generates the co-prime residue classes (mod p) for infinitely many primes p. Let E be the set of $a > 1$, a not a perfect square, for which Artin's conjecture is false. Set $E(x) = \text{card}(e \in E: e \leq x)$. We prove that $E(x) = 0(\log^6 x)$ and that the number of prime numbers in E is at most 6.

A conjecture of E. Artin [1] asserts that any natural number $a > 1$, which is not a perfect square, is a primitive root (mod p) for infinitely many primes p. We shall abbreviate this conjecture of Artin as AC. Artin's conjecture was proved to be correct by Hooley [5] provided one assumes the generalized Riemann hypothesis for certain Dedekind zeta functions. The first unconditional result was obtained by Gupta and Ram Murty in [2], where it was shown that there is a finite set S, consisting of thirteen elements, such that for some $a \in S$, AC is true for a. Subsequently, S was replaced by another finite set of seven elements in [3]. In this paper, we consider the exceptional set for Artin's conjecture. More precisely, let

$$E = \{a: a > 1, a \neq n^2, n \in \mathbb{Z}, \text{AC is false for } a\}$$

and put $E(x) = \text{card}(a: a \in E, a \leq x)$.

THEOREM 1.

$$E(x) = 0(\log^6 x)$$

This theorem will follow from the following:

PROPOSITION 2. *The number of multiplicatively independent elements in E is at most* 6.

Our method has its genesis in [2]. We consider the quantity $(p - 1)$ for p a rational prime p. By using a lower bound sieve technique, we ensure that all the odd prime factors of $(p - 1)$ are large. Indeed, the lower bound Selberg sieve, coupled with the Bombieri-Vinogradov theorem on primes in arithmetic progressions ensures many primes p such that all the odd prime factors of $p - 1$ are $>p^{1/6-\epsilon}$. Rosser's sieve as

Received by the editors October 15, 1985, and, in revised form, December 11, 1985.
AMS Subject Classification (1980): 10H35, 10H32.
Key words and phrases: Artin's conjecture, primitive roots.

modified by Iwaniec [6] yields a corresponding result with the odd prime factors of $p - 1$ greater than $p^{1/4-\epsilon}$. An improvement in the exponent 1/2 appearing in the Bombieri-Vinogradov theorem yields a commensurate improvement in our main theorem. To make this precise, let $\pi(x, q)$ denote the number of primes $p \leq x$, $p \equiv 1 (\bmod q)$. Consider the hypothesis:

$$H_\theta\colon \sum_{q<x^\theta} \left|\pi(x, q) - \frac{\operatorname{li} x}{\varphi(q)}\right| = 0\left(\frac{x}{\log^A x}\right)$$

for any $A > 0$.

This is a conjecture of Halberstam and Richert [4] asserting that H_θ is true for every $\theta < 1$.

THEOREM 3. *If H_θ is true for some $\theta > 2/3$, then $E(x) = 0(\log x)$ and E consists of at most the powers of a single number.*

It is natural to investigate which additional hypothesis is necessary for Artin's conjecture. The following theorem provides the answer.

THEOREM 4. *Let $f_a(p)$ be the order of $a (\bmod p)$.*

(i) Suppose that

$$\sum_{p<x} \frac{1}{f_a(p)} = 0(x^\theta)$$

for some $\theta < 1/2$. Then AC is true for a on the assumption of H_ρ where $\rho = 1 - \epsilon$.
(ii) If

$$\sum_{p<x} \frac{1}{f_a(p)} = 0(x^{1/4})$$

then AC is true for a (independent of any additional hypothesis).

REMARK. It is probably true that

$$\sum_{p<x} \frac{1}{f_a(p)} = 0(x^\epsilon)$$

for every $\epsilon > 0$.

COROLLARY. *Either AC is true for a or*

$$\limsup_{n\to\infty} \frac{P(a^n - 1)}{n^{4/3}} > 0,$$

where $P(m)$ denotes the greatest prime factor of m.

The essential ingredients in the proofs of these theorems are the following lemmas.

LEMMA 1. *Let Γ be a subgroup of $\mathbb{Q}^\times$ of rank r. Then, if Γ_p denotes the image of $\Gamma (\bmod p)$, the number of primes p such that*

$$|\Gamma_p| < y$$

is

$$0(y^{1+1/r})$$

PROOF. The proof of this lemma is similar to lemma 2 of [2] and is therefore suppressed.

LEMMA 2. *Let a be a non-square and b a natural number which is not a square or a power of a. Then,*

(i) the number of primes $p \leq x$ *such that* $p - 1 = 2q_1q_2q_3$, $q_i > x^{\frac{1}{4}+\epsilon}$, *and* $f_a(p), f_b(p)$ *even is* $\gg x/\log^2 x$.

(ii) If the hypothesis H_θ *is true with* $\theta = 2/3 + \epsilon$, *then the number of primes* $p \leq x$ *such that* $p - 1 = 2q_1q_2$, *with* $q_i > x^{1/3+\epsilon}$, *and* $f_a(p), f_b(p)$ *even is* $\gg x/\log^2 x$. $H_{1-\epsilon}$ *would yield* $q_i > x^{1/2-\epsilon}$.

PROOF. (i) is essentially Lemma 1 of [2]. The condition that $f_a(p)$ and $f_b(p)$ be even forces an extra congruence condition (mod $4ab$) on p, by quadratic reciprocity. The lower bound sieve then yields the result, as described in [2] and [3]. (ii) is deduced similarly.

We begin with the proof of Theorem 3.

PROOF OF THEOREM 3. Let a, b be as in Lemma 2. Suppose that $f_a(p) = f_b(p)$ and let $\Gamma = \langle a, b\rangle$. In view of lemma 2(ii) and the assumption of H_θ, with $\theta = 2/3 + \epsilon$, we infer that for $\delta x/\log^2 x$ primes $p \leq x$, $\delta > 0$, satisfying

$$p - 1 = 2q_1q_2, \qquad q_i > x^{1/3+\epsilon},$$

the image of $\Gamma(\text{mod } p)$ is $< x^{2/3-\epsilon}$ if it is not the complete set of co-prime residue classes. By lemma 1, the number of such primes is $0(x^{1-\epsilon})$. We may therefore suppose that for the primes described above, $f_a(p) \neq f_b(p)$. Suppose that $f_a(p) = 2q_1$, $f_b(p) = 2q_2$ (without loss of generality). Then, by lemma 1, for $r = 1$, we deduce that

$$q_i > x^{1/2}/\log^A x$$

for $A \geq 2$. As $p - 1$ is composite, we can suppose one of the primes is less than $x^{1/2}$. Again without loss, suppose it is $q_1 \leq x^{1/2}$. This means that

$$p - 1 = 2q_1q_2$$

with $x^{1/2}/\log^A x < q_1 \leq x^{1/2}$. By any sieve method, the number of such primes for fixed q_1 is

$$0\left(\frac{x}{q_1 \log^2 (x/q_1)}\right)$$

Thus, the total number of such primes, summing over the range for q_1 is

$$\ll \frac{x \log \log x}{\log^3 x},$$

by a simple computation.

As this is $0(x/\log^2 x)$, we may therefore suppose that at least one of $f_a(p)$ or $f_b(p) = p - 1$. That is, one of a or b is a primitive root(mod p). Let us therefore suppose that E has a single prime number a. If the above argument is repeated with a and b any natural number which is not a power of a or a perfect square, then we deduce that b must be a primitive root(mod p) for infinitely many primes p. Therefore, the exceptional set E can consist of at most, the powers of a single a. This proves that $E(x) = 0(\log x)$ and completes the proof of Theorem 3.

We can now prove Theorem 1. But first, we begin with a proof of Proposition 2.

PROOF OF PROPOSITION 2. Let $a_1, a_2, \ldots, a_7$ be any seven multiplicatively independent numbers. Suppose that

$$f_{a_i}(p) \neq p - 1, \; 1 \leq i \leq 7$$

for the primes produced by lemma 2. (Here, as before, we can suppose that $2 \mid f_{a_i}(p)$, $1 \leq i \leq 7$.). By applying lemma 1, with $r = 1$, we can also suppose, without loss, that

$$f_{a_i}(p) > x^{1/2}/\log^A x$$

for $A \geq 2$. Since $q_i < x^{1/2-\epsilon}$ for the primes produced by lemma 2, we therefore have

$$f_{a_i}(p) = 2q_1q_2, \; 1 \leq i \leq 7.$$

That is, each order is composed of two odd primes. Amongst these seven orders, three of the orders must be the same. Hence, there are three distinct a_1, a_2, a_3 such that

$$\Gamma = \langle a_1, a_2, a_3 \rangle$$

is of order (mod p) less than $x^{3/4-\epsilon}$. Again, by lemma 1, with $r = 3$, the number of such primes is $0(x^{1-\epsilon})$.

Therefore, by eliminating these exceptional primes, we find that at least one of the seven numbers is a primitive root (mod p) for infinitely many prime numbers p. This proves the proposition.

PROOF OF THEOREM 1. Now let $a_1, \ldots, a_6$ be the (possible) exceptional numbers of the proposition. If a is a natural number, which is not a perfect square, and not composed by only these six numbers $a_1, \ldots, a_6$, then the argument of the proof of the proposition applied to the seven numbers $a_1, \ldots, a_6, a$ yields that a is a primitive root (mod p) for infinitely many primes p. Hence E consists of only numbers composed of the possible six exceptional numbers. Therefore, $E(x) = 0(\log^6 x)$. This completes the proof of the theorem.

PROOF OF THEOREM 4. We begin by observing that

$$\sum_{p<x} \frac{1}{f_a(p)} = 0(x^{1/2}).$$

https://doi.org/10.4153/CMB-1987-012-5 Published online by Cambridge University Press

Indeed

$$\sum_{p<x} \frac{1}{f_a(p)} = \sum_{f_a(p)<y} + \sum_{f_a(p)>y}$$
$$= 0(Y) + 0(x/Y)$$

where the second estimate is trivial and the first estimate is from lemma 1 and partial summation. Setting $Y = x^{1/2}$ gives the result. If we have

(*) $$\sum_{p<x} \frac{1}{f_a(p)} = 0(x^\theta),\ \theta < 1/2,$$

then the hypothesis H_ρ, $\rho = 1 - \epsilon$ implies the existence of $\delta x/\log^2 x$ primes $p \le x$, $\delta > 0$, such that

$$p - 1 = 2q_1q_2,\ q_i > x^{1/2-\epsilon}.$$

Then, if $f_a(p) = 2q_1$ or $2q_2$, then

$$f_a(p) < x^{1/2-\epsilon}$$

From (*), the number of such primes is $0(x^{1/2+\theta+\epsilon})$. We now choose $\theta + \epsilon < 1/2$ to get the desired result. The result stated with $0(x^{1/4})$ can be deduced on a similar way from the unconditional result given by lemma 2.

PROOF OF THE COROLLARY. Suppose that for some α,

$$\limsup_{n\to\infty} \frac{P(a^n - 1)}{n^\alpha} = 0.$$

Then, for any $\epsilon > 0$, and all n sufficiently large (depending on ϵ), we have

$$P(a^n - 1) < \epsilon n^\alpha.$$

But then

$$p \le P(a^{f_a(p)} - 1) < \epsilon f_a(p)^\alpha$$

so that, $f_a(p) \gg p^{1/\alpha}$ for all p sufficiently large. If AC is false for a, then for the primes given by lemma 2, we would have

$$f_a(p) < p^{3/4-\epsilon},$$

so that this would contradict the above for the value $\alpha = 4/3$.

ACKNOWLEDGEMENT. The first author would like to thank the kind hospitality of the Tata Institute for Fundamental Research, Bombay, during January 1985 when this joint work was done.

REFERENCES

1. E. Artin, *The collected papers of Emil Artin* (S. Lang and J. Tate, Eds.), Reading, Mass., Addison-Wesley 1965; Math. Rev. 31, #1159.

2. R. Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Inv. Math. **78**(1984) 127–130.

3. R. Gupta, V. Kumar Murty, and M. Ram Murty, *The Euclidean algorithm for S-integers*, (to appear).

4. H. Halberstam and M. Richert, *Sieve Methods*, Academic Press.
5. C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225**(1967) 209–220.
6. H. Iwaniec, *Rosser's sieve*, Acta Arith. **36**(1980) 171–202.

DEPARTMENT OF MATHEMATICS
MCGILL UNIVERSITY,
MONTREAL, CANADA

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD
BOMBAY, INDIA