Invent. math. 78, 127–130 (1984)

Inventiones mathematicae

A remark on Artin's conjecture

Rajiv Gupta* and M. Ram Murty**

[1] The Institute for Advanced Study, School of Mathematics, Princeton, N.J. 08540, USA
[2] Department of Mathematics, Mc Gill University, Montreal, Quebec, Canada

A famous conjecture of E. Artin [1] states that for any integer $a \neq \pm 1$ or a perfect square, there are infinitely many primes p for which a is a primitive root $(\bmod p)$. This conjecture was shown to be true if one assumes the generalized Riemann hypothesis by Hooley [5]. The purpose of this note is to exhibit a finite set S such that for some $a \in S$, a is a primitive root $(\bmod p)$ for an infinity of primes p.

To this end, let q, r and s denote three distinct primes. Define the following set:

$$S = \{qs^2,\ q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3,\ qrs\}.$$

Theorem. *For some $a \in S$, there is a $\delta > 0$ such that for at least $\delta x/\log^2 x$ primes $p \leqq x$, a is a primitive root* $(\bmod p)$.

Our theorem is proved in the following way. First we show that there are at least $cx/\log^2 x$ primes $p \leqq x$ such that all odd prime divisors of $(p-1)$ exceed $x^{\frac{1}{4}+\varepsilon}$. For such primes, we prove that $\mathbb{F}_p^* = \langle q, r, s\rangle$ with at most $o(x/\log^2 x)$ exceptional primes $p \leqq x$. Hence, for at least $cx/\log^2 x$ primes $p \leqq x$, $\mathbb{F}_p^*$ has a generator of the form $q^u r^v s^w$ for some u, v, w. The final step is to show that we can find u, v, w bounded by three. In fact, we can take a generator as in the set S above.

Lemma 1. *Fix a prime q, and $0 < \varepsilon < \frac{1}{4}$. If $\alpha = \frac{1}{4} - \varepsilon$, there is a constant $c > 0$ such that* $\operatorname{card}\left(p \leqq x\colon \left(\frac{q}{p}\right) = -1,\ t \mid (p-1),\ t \text{ prime} \Rightarrow t = 2 \text{ or } t > x^{\alpha}\right) \geqq \dfrac{cx}{\log^2 x}$.

Remark. Results of this nature are proved by using the lower bound sieve method and are very classical. Indeed, the lower bound Selberg sieve, coupled with the Bombieri-Vinogradov theorem on primes in arithmetic progressions yields the result with an exponent of $\alpha = \frac{1}{6} - \varepsilon$ instead of $\frac{1}{4} - \varepsilon$. A beautiful exposition of this can be found in Bombieri [2, p. 71–75]. The result with an exponent $\alpha = \frac{1}{4} - \varepsilon$ can be obtained from Theorem 1 of Iwaniec [7] by utilising the Bombieri-Vinogradov theorem. A weighted form of the latter theorem was proved for an extended range

* Research partially supported by an NSF grant.
** Research partially supported by NSERC grant # U0237.

of progressions beyond $x^{\frac{1}{2}}$, by Fouvry and Iwaniec [3]. Utilising this finer result in [6] yields Lemma 1 with an exponent $\alpha > \frac{1}{4}$. An $\alpha > 0$ in Lemma 1 suffices to yield a finite set in Theorem 1. The size of the set decreases with any increasing value of α allowed by Lemma 1. We therefore assume Lemma 1 with $\alpha = \frac{1}{4} + \varepsilon$ to obtain an "optimal" set S.

Now consider

$$\Gamma = \{q^a r^b s^c : a, b, c \in \mathbb{Z}\}.$$

Let Γ_p be the reduction of $\Gamma \pmod p$, for any prime $p > \max(q, r, s)$.

Lemma 2. *The number of primes p satisfying*

$$|\Gamma_p| < y$$

is $O(y^{\frac{4}{3}})$.

Proof. We consider all triples (a, b, c) such that $|a| + |b| + |c| \leqq Y$. The number of such triples is easily seen to be $\frac{4}{3} Y^3 + O(Y^2)$. Choosing $Y = y^{\frac{1}{3}}$, we find that if p is a prime satisfying $|\Gamma_p| < y$, then for at least two *distinct* such triples (a, b, c) and (α, β, γ) we have

$$q^\alpha r^\beta s^\gamma \equiv q^a r^b s^c \pmod p.$$

Hence, p divides the numerator of $(q^{\alpha - a} r^{\beta - b} s^{\gamma - c} - 1)$. The number of primes dividing the numerator is $\ll |\alpha - a| + |\beta - b| + |\gamma - c| \leqq 2Y$. If p is a prime such that $|\Gamma_p| < y$, then p divides the numerator of $(q^u r^v s^w - 1)$ for some (u, v, w) satisfying $|u| + |v| + |w| \leqq 2Y$. The number of such triples is

$$\tfrac{4}{3}(2Y)^3 + O(Y^2)$$

and each such triple gives rise to at most $O(Y)$ prime factors of the numerator. The total number of primes is therefore $O(Y^4) = O(y^{\frac{4}{3}})$, as desired.

Lemma 3. *There is a* $\delta > 0$ *such that for at least* $\delta x/\log^2 x$ *primes* $p \leqq x$, *we have* $\mathbb{F}_p^* = \langle q, r, s\rangle$.

Proof. Let p be a prime $\leqq x$ such that p does not split in $\mathbb{Q}(\sqrt{q})$ and so that any odd prime divisor of $p - 1$ is $> x^{\frac{1}{4}+\varepsilon}$. By Lemma 1, the number of such primes $p < x$ is $\delta x/\log^2 x$. For these primes, we count how often $\mathbb{F}_p^* \neq \langle q, r, s\rangle$. Let t be a prime dividing the index of $\langle q, r, s\rangle$ in $\mathbb{F}_p^*$. Then $t = 2$ or $t > x^{\frac{1}{4}+\varepsilon}$. If $t = 2$, then $2 \mid (\mathbb{F}_p^* : \langle q\rangle)$, but then q must be a quadratic residue mod p, contrary to our choice of p. Therefore, if $t \mid (\mathbb{F}_p^* : \langle q, r, s\rangle)$ then $t > x^{\frac{1}{4}+\varepsilon}$. Hence,

$$|\langle q, r, s\rangle| < x^{\frac{3}{4}-\varepsilon}.$$

By Lemma 2, we find the number of such primes is $O(x^{1-\varepsilon})$. This estimate counts the exceptional primes and we have the desired result.

Now suppose we are given a 3-tuple of non-negative integers $u = (u_1, u_2, u_3)$. We shall write $(q, r, s)^u$ for $q^{u_1} r^{u_2} s^{u_3}$.

Lemma 4. *Suppose we have a set* $\tilde{S}$ *of thirteen* 3-*tuples satisfying*:

(i) $u \not\equiv (0,0,0) \pmod 2$ *for any* $u \in \tilde{S}$,

(ii) *for each* $u \in \tilde{S}$, *there is at most one* $u' \in \tilde{S}$, $u' \neq u$ *with* $u \equiv u' \pmod 2$,

(iii) *for each two dimensional subspace* V *of* $(\mathbb{Z}/2\mathbb{Z})^3$, *any three elements of* $S_V = \{u \in \tilde{S} : u \not\equiv v \pmod 2$ *for any* $v \in V\}$ *are linearly independent.*

If $\mathbb{F}_p^* = \langle q, r, s\rangle$, *then for some* $u \in \tilde{S}$, $(q, r, s)^u$ *is a primitive root* (mod p) *provided that* $(p-1)$ *has at most three odd prime divisors, all sufficiently large.*

Proof. Let g be a primitive root (mod p) and let us write $q \equiv g^{a_1}$, $r \equiv g^{a_2}$, $s \equiv g^{a_3} \pmod p$. Set $a = (a_1, a_2, a_3)$. Since $\gcd(a_1, a_2, a_3, p-1) = 1$, a is not the zero vector mod 2. Therefore, the orthogonal complement V of the subspace of $(\mathbb{Z}/2\mathbb{Z})^3$ generated by a has dimension two. Conditions (i) and (ii) imply that $|S_V| \geqq 7$. An element $u \in S_V$ will correspond to a primitive root $(q, r, s)^u$ if and only if $\gcd(a \cdot u, p-1) = 1$, where $a \cdot u = a_1 u_1 + a_2 u_2 + a_3 u_3$. Suppose that none of the odd divisors of $p-1$ divides the determinant corresponding to any three elements of S_V. Then for each odd prime $t | (p-1)$, at most two of the numbers $a \cdot u$, $u \in S_V$ are divisible by t. Moreover, $2 \nmid a \cdot u$ for any $u \in S_V$. Thus, for some $u_0 \in S_V$, $\gcd(a \cdot u_0, p-1) = 1$ and $(q, r, s)^{u_0}$ is a primitive root (mod p).

Proof of the Theorem. In view of Lemmas 3 and 4, it suffices to write down a set $\tilde{S}$ satisfying the given conditions. Indeed,

$$\tilde{S} = \{(1,0,2), (3,2,0); (2,1,0), (0,3,2); (0,2,1), (2,0,3); (1,3,0), (3,1,2); \\ (0,1,3), (2,3,1); (3,0,1), (1,2,3); (1,1,1)\}.$$

(The pairs between semi-colons are congruent modulo 2.) We need only verify condition (iii) as (i) and (ii) are evident.

We consider two cases:

(a) $u_1, u_2, u_3 \in S_V$ are incongruent (mod 2).

If v_1, v_2, v_3 are the reductions (mod 2) of u_1, u_2, u_3, then $\{v_1, v_2, v_3\}$ is a basis of $(\mathbb{Z}/2\mathbb{Z})^3$. This is because $v_3 \not\equiv v_1 + v_2$ as $a \cdot v_1 \not\equiv 0 \pmod 2$, $a \cdot v_2 \not\equiv 0 \pmod 2$ implies $a \cdot (v_1 + v_2) \equiv 0 \pmod 2$. Thus $\det[u_1, u_2, u_3]$ is odd and u_1, u_2, u_3 are linearly independent.

(b) $u_1 \equiv u_2 \pmod 2$. The cross product of u_1 and u_2 is a multiple of one of the six vectors $(2, -3, -1)$, $(-1, 2, -3)$, $(-3, -1, 2)$, $(-3, 1, 4)$, $(4, -3, 1)$, $(1, 4, -3)$. For each of these, the only vectors in S which are perpendicular are u_1 and u_2. Thus u_1, u_2, u_3 are linearly independent in this case as well.

This completes the proof.

Remark. The largest prime dividing any of the determinants is 19. To apply Lemma 4, it suffices to have all the odd prime divisors of $(p-1)$ greater than 19.

One can show that the set of thirteen elements above is "optimal". If $u_1, \ldots, u_{12}$ are 3-tuples of non-negative integers and $(p-1)$ has three distinct odd prime factors, q_1, q_2, q_3, then it is not hard to see that one can find a $v_2 \in (\mathbb{Z}/2\mathbb{Z})^3$, $v_2 \not\equiv 0$ such that at least six of the numbers $u_i \cdot v_2$ are $\equiv 0 \pmod 2$; say $u_i \cdot v_2 \equiv 0 \pmod 2$, for $1 \leqq i \leqq 6$. Then we can find a $v(q_1) \in (\mathbb{Z}/q_1\mathbb{Z})^3$, $v(q_1) \not\equiv 0 \pmod{q_1}$, with

$$u_7 \cdot v(q_1) \equiv u_8 \cdot v(q_1) \equiv 0 \pmod{q_1}$$

and similarly $u_9 \cdot v(q_2) \equiv u_{10} \cdot v(q_2) \equiv 0 \pmod{q_2}$, $u_{11} \cdot v(q_3) \equiv u_{12} \cdot v(q_3) \equiv 0 \pmod{q_3}$. By the Chinese remainder theorem, there is some $a = (a_1, a_2, a_3) \in (\mathbb{Z}/(p-1)\mathbb{Z})^3$ with $a \equiv v_2 \pmod 2$, $a \equiv v(q_i) \pmod{q_i}$. If g is a generator of $\mathbb{F}_p^*$, then $\mathbb{F}_p^* = \langle g^{a_1}, g^{a_2}, g^{a_3}\rangle$ but none of the twelve numbers $(g^{a_1}, g^{a_2}, g^{a_3})^{u_i}$, $1 \leqq i \leqq 12$ is a primitive root (mod p).

Finally, we remark that an analogous result can be established for the elliptic curve analogue of the Artin conjecture as formulated by Lang and Trotter [8]. Indeed, in [4], it was shown that if E is an elliptic curve over $\mathbb{Q}$ with complex multiplication by the full ring of integers in an imaginary quadratic field and rank $E(\mathbb{Q}) \geqq 6$, then there is a finite set S of rational points such that for some $a \in S$, $E(\mathbb{F}_p)$ is generated by the reduction of $a \pmod{p}$ for infinitely many primes p.

References

1. Artin, E.: The Collected Papers of Emil Artin (S. Lang and J. Tate, Eds.). Reading, Mass.: Addison-Wesley 1965; Math. Rev. **31**, # 1159
2. Bombieri, E.: Le grand crible dans la théorie analytique des nombres, Astérisque 18, Societé Mathematique de France, 1974
3. Fouvry, E., Iwaniec, H.: Primes in arithmetic progressions. Acta Arithmetica **42**, 197–218 (1983)
4. Gupta, R., Ram Murty, M.: Primitive points on elliptic curves (to appear)
5. Hooley, C.: On Artin's conjecture. J. Reine Angew. Math. **225**, 209–220 (1967)
6. Iwaniec, H.: A new form of error term in the linear sieve, Acta Arith. **37**, 307–320 (1980)
7. Iwaniec, H.: Rosser's sieve. Acta Arith. **36**, 171–202 (1980)
8. Lang, S., Trotter, H.: Primitive points on elliptic curves. Bull. Amer. Math. Soc., **83**, 289–292 (1977)

Oblatum 2-IV-1984