ACTA ARITHMETICA
180.1 (2017)

On simultaneous primitive roots

by

Mohamed Anwar and Francesco Pappalardi (Roma)

1. Introduction. Given a prime p and $a \in \mathbb{Q}^*$, we say that a is a *primitive root modulo* p if p does not divide either the numerator or the denominator of a, and the multiplicative order of a mod p equals $p-1$.

Let $S = \{a_1, \dots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ and denote

$$\mathcal{P}_S = \{p \text{ prime} \mid \text{each } a \in S \text{ is a primitive root modulo } p\}.$$

In the case where $S \subset \mathbb{Z}$, assuming the Generalized Riemann Hypothesis for suitable number fields, it was proved by K. Matthews [5] in 1976 that $\mathcal{P}_S$ is finite if and only if at least one of the following two conditions is satisfied:

(α) There exist $1 \le i_1 < \cdots < i_{2s+1} \le r$ such that $a_{i_1} \cdots a_{i_{2s+1}} \in \mathbb{Q}^{*2}$.

(β) There exist $1 \le i_1 < \cdots < i_{2s} \le r$ such that $a_{i_1} \cdots a_{i_{2s}} \in -3\mathbb{Q}^{*2}$, and for all primes $\ell \equiv 1 \bmod 3$ there exists at least one element of S which is a cube modulo ℓ.

Note that it is easy to verify without appealing to the GRH (see Proposition 1 below) that if either (α) or (β) are satisfied, then $\mathcal{P}_S$ is finite. In all other cases, not only is $\mathcal{P}_S$ infinite but it has non-zero density (under GRH). The hypothesis that all the elements of S are integers does not seem crucial in Matthews' work.

The goal of this note is to prove the conclusion of the Matthews Theorem assuming Schinzel's Hypothesis H [7]:

Hypothesis H (Schinzel, 1959). *Let $f_1, \dots, f_k \in \mathbb{Z}[x]$ be irreducible polynomials with positive leading coefficients and such that*

$$\gcd(f_1(n) \cdots f_k(n) \mid n \in \mathbb{N}) = 1.$$

Then there are infinitely many $t \in \mathbb{N}$ such that $f_1(t), \dots, f_k(t)$ are all prime.

2010 *Mathematics Subject Classification*: Primary 11N64; Secondary 11A07, 11R45.
Key words and phrases: primitive roots, Hypothesis H, applications of Chebotarev Density Theorem.
Received 4 July 2016; revised 1 February 2017.
Published online 1 August 2017.

DOI: 10.4064/aa8566-3-2017

We will prove the following

THEOREM. *Assume that Hypothesis H holds, let* $S = \{a_1, \dots, a_r\} \subset \mathbb{Q}$ *and assume that*

(1) $a_{i_1} \cdots a_{i_{2s+1}} \notin \mathbb{Q}^{*2}$ *for all* $1 \le i_1 < \cdots < i_{2s+1} \le r$;
(2) *if there exist* $1 \le i_1 < \cdots < i_{2s} \le r$ *such that* $a_{i_1} \cdots a_{i_{2s}} \in -3\mathbb{Q}^{*2}$, *then there exists a prime* $\ell \equiv 1 \bmod 3$ *such that no element of* S *is a cube modulo* ℓ.

Then the set $\mathcal{P}_S$ *is infinite.*

When $r = 1$, the statement that $\mathcal{P}_{\{a_1\}}$ is infinite is the *Artin Conjecture for primitive roots*. It was proven to hold under the assumption of the Generalized Riemann Hypothesis by C. Hooley [2] in 1967. Schinzel and Sierpiński [7, p. 199] proved that also Hypothesis H implies the Artin Conjecture.

REMARK. Suppose that $S = \{q_1 b_1^3, q_2 b_2^3, q_1 q_2 b_3^3, q_1^2 q_2 b_4^3\}$ where q_1 and q_2 are distinct primes different from 3 and $b_1, b_2, b_3, b_4 \in \mathbb{Q}^*$. Then for all primes $p \equiv 1 \bmod 3$, at least one element of S is congruent to a cube modulo p.

PROPOSITION 1. *Let* $S = \{a_1, \dots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ *be such that either* (α) *or* (β) *are satisfied. Then* $\mathcal{P}_S$ *is finite.*

Proof. If $p \in \mathcal{P}_S$, then $a_i^{(p-1)/2} \equiv -1 \bmod p$ for all $i = 1, \dots, r$. If (α) holds, then there exists $b \in \mathbb{Q}^*$ such that $a_{i_1} = b^2 a_{i_2} \cdots a_{i_{2s+1}}$. Hence

$$-1 \equiv a_{i_1}^{(p-1)/2} \equiv (b^2 a_{i_2} \cdots a_{i_{2s+1}})^{(p-1)/2} \equiv 1 \bmod p,$$

so that $p \mid 2$.

If (β) holds and if $a_{i_1} \cdots a_{i_{2s}} = -3b^2$ for some $b \in \mathbb{Q}^*$, then

$$1 \equiv (a_{i_1} \cdots a_{i_{2s}})^{(p-1)/2} \equiv \left(\frac{-3}{p}\right) \bmod p,$$

which implies that $p \equiv 1 \bmod 3$. From the second part of (β), there exist i_k such that $a_{i_k} \equiv c^3 \bmod p$, which contradicts the fact that a_{i_k} is a primitive root modulo p. ∎

2. Lemmata. Given $S = \{a_1, \dots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$, we set

$$\mathcal{L} = \{\ell \text{ prime} \mid v_\ell(a) \neq 0 \text{ for some } a \in S\}.$$

Then $\mathcal{L}$ is clearly finite. Furthermore we set

$$\mathcal{L}' = \begin{cases} \mathcal{L} \cup \{-1\} & \text{if } S \not\subseteq \mathbb{Q}^{>0}, \\ \mathcal{L} & \text{otherwise.} \end{cases}$$

We write $\mathcal{L}' = \{\ell_1, \dots, \ell_s\}$ and when $\mathcal{L}' \not\subseteq \mathbb{Q}^{>0}$ we assume that $\ell_1 = -1$. Further we set $L = 4|\ell_1 \cdots \ell_s|$.

For each $j = 1, \dots, r$, write $a_j = \ell_1^{e_{1j}} \cdots \ell_s^{e_{sj}}$. Then the matrix

$$\mathcal{E} = \begin{pmatrix} e_{11} & \cdots & e_{s1} \\ \vdots & & \vdots \\ e_{1r} & \cdots & e_{sr} \end{pmatrix}$$

has coefficients in $\mathbb{Z}$ and the first condition in the statement of the Theorem implies that the sum of any odd number of rows of $\mathcal{E}$ is not the zero vector modulo 2. We claim that this implies that the linear system

$$\mathcal{E} \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_s \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \tag{2.1}$$

admits a solution in $(\mathbb{Z}/2\mathbb{Z})^s$. Indeed, perform a Gauss elimination on the rows of the enlarged matrix obtained by attaching to $\mathcal{E}$ a column of 1's. We obtain a row echelon form. The last column has a "1" in the rows that were obtained by adding together an odd number of the original rows, and has a "0" in the rows obtained by adding together an even number of rows. The first condition in the statement implies that whenever there is a "1" in the last entry of a row, that row contains at least one more "1". Therefore the original system can be solved recursively.

We need the following

LEMMA 1. *Assume that* $(x_1, \dots, x_s) \in (\mathbb{Z}/2\mathbb{Z})^s$ *is a solution of the linear system* (2.1). *Then there exists an integer* m *invertible modulo* L (*i.e.* $\gcd(m, L) = 1$) *such that*

(i) *if* p *is prime with* $p \equiv m \bmod L$, *then* $\left(\frac{\ell_i}{p}\right) = (-1)^{x_i}$ *for all* $i = 1, \dots, s$;
(ii) $m \not\equiv 1 \bmod \ell_i$ *for all* $i = 1, \dots, s$ *such that* $\ell_i > 3$.

Furthermore conclusion (ii) *above also holds for* $\ell_i = 3$ *when* $\{-1, 3\} \not\subseteq \mathcal{L}'$, *and also when* $\{-1, 3\} \subseteq \mathcal{L}'$ *but* $x_i \neq x_1$.

Proof. We will first determine the congruence class m_4 of m modulo 4 and then its congruence class m_{ℓ_i} of m modulo each ℓ_i such that $\ell_i > 2$. If $2 \in \mathcal{L}$ we will also determine the congruence class m_8 of m modulo 8. Next we will apply the Chinese Remainder Theorem and deduce the existence of a congruence class modulo L with the required properties.

The congruence class m_4 for m modulo 4 is defined by

$$m_4 = \begin{cases} (-1)^{x_1} & \text{if } -1 \in \mathcal{L}', \\ -1 & \text{if } \{-1, 3\} \cap \mathcal{L}' = \emptyset, \\ (-1)^{x_i+1} & \text{if } 3 \in \mathcal{L}', -1 \notin \mathcal{L}' \text{ and } \ell_i = 3. \end{cases}$$

In the event that $2 \in \mathcal{L}$ and $\ell_j = 2$, let m_8 be the unique invertible congruence class modulo 8 with the properties that $m_8 \equiv m_4 \bmod 4$ and

$$(m_8^2 - 1)/8 \equiv x_j \bmod 2.$$

Note that if $p \equiv m_8 \bmod 8$ then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{x_j}.$$

For all other odd primes $\ell_i \in \mathcal{L}$, let m_{ℓ_i} be any of the $(\ell_i - 1)/2$ integers such that

$$\left(\frac{m_{\ell_i}}{\ell_i}\right) = (-1)^{x_i + (m_4-1)(\ell_i-1)/4}.$$

Note that if p is a prime with $p \equiv m_{\ell_i} \bmod \ell_i$ and $p \equiv m_4 \bmod 4$, then by the quadratic reciprocity law,

$$\begin{aligned}\left(\frac{\ell_i}{p}\right) &= (-1)^{(p-1)(\ell_i-1)/4}\left(\frac{p}{\ell_i}\right)\\ &= (-1)^{(m_4-1)(\ell_i-1)/4}\left(\frac{m_{\ell_i}}{\ell_i}\right) = (-1)^{x_i}.\end{aligned}$$

If $\ell_i > 3$, then $(\ell_i - 1)/2 > 1$. So there is always a choice of a class m_{ℓ_i} modulo ℓ_i with $m_{\ell_i} \not\equiv 1 \bmod \ell_i$.

If $\ell_i = 3$ and $-1 \notin \mathcal{L}'$, then $m_3 \equiv 2 \bmod 3$ since

$$\left(\frac{m_3}{3}\right) = (-1)^{x_i + (m_4-1)/2} = -1 = \left(\frac{2}{3}\right).$$

If $\ell_i = 3$ and $-1 = \ell_1 \in \mathcal{L}'$, then $m_3 \equiv 2 \bmod 3$ holds if and only if

$$\left(\frac{m_3}{3}\right) = (-1)^{x_i + (m_4-1)/2} = (-1)^{x_i + x_1} = -1.$$

The latter is equivalent to $x_1 \neq x_i$, and this ends the proof of the lemma. ∎

3. Proof of the Theorem. A consequence of Lemma 1 is that if $L = 4|\ell_1 \cdots \ell_s|$ and m is the integer modulo L postulated in the statement of Lemma 1, then for any prime $p \equiv m \bmod L$,

$$\left(\frac{a_j}{p}\right) = \prod_{i=1}^{s}\left(\frac{\ell_i}{p}\right)^{e_{ij}} = (-1)^{e_{1j}x_1 + \cdots + e_{sj}x_s} = -1. \tag{3.1}$$

So each a_i is a quadratic non-residue modulo p.

Let us now prove the statement of the Theorem in the case when $\{-1, 3\} \not\subseteq \mathcal{L}'$ and also when $\{-1, 3\} \subseteq \mathcal{L}'$ and there exists a solution $(x_1, \ldots, x_s) \in (\mathbb{Z}/2\mathbb{Z})^s$ of the linear system (2.1) where the components relative to -1 and to 3 are distinct.

Let $f_1(X) = m + LX$ and

$$f_2(X) = \begin{cases} (m-1)/2 + (L/2)X & \text{if } m \equiv 3 \bmod 4, \\ (m-1)/4 + (L/4)X & \text{if } m \equiv 5 \bmod 8, \\ (m-1)/8 + (L/8)X & \text{if } m \equiv 1 \bmod 8. \end{cases}$$

If $2 \notin \mathcal{L}$, we can assume that $m \not\equiv 1 \bmod 8$. So the condition $m \equiv 1 \bmod 8$ arises only when $2 \in \mathcal{L}$ (i.e. $8 \mid L$) and the polynomial $f_2(X)$ always has integer coefficients.

LEMMA 2. *Let f_1 and f_2 be as above. Then the integers*

$$f_1(0)f_2(0), \quad f_1(1)f_2(1), \quad f_1(2)f_2(2)$$

are coprime.

Proof. Let q be a prime dividing the gcd

$$\left(\frac{m(m-1)}{2^t}, \frac{(m+L)(m-1+L)}{2^t}, \frac{(m+2L)(m-1+2L)}{2^t} \right) \tag{3.2}$$

where $t = 1, 2, 3$ according to $m \equiv 3 \bmod 4$, $m \equiv 5 \bmod 8$ or $m \equiv 1 \bmod 8$.

If q is odd and $q \mid m(m-1)$ then either $q \mid m$ or $q \mid m-1$.

In the first instance $q \nmid m + L$ and $q \nmid m + 2L$ since $\gcd(m, L) = 1$. If it happened that $q \mid m - 1 + L$ and $q \mid m - 1 + 2L$ then $q \mid L$, which is a contradiction.

In the second instance observe that $q \nmid L$ by Lemma 1(ii). Therefore $q \nmid m - 1 + L$ and $q \nmid m - 1 + 2L$. If $q \mid m + L$ and $q \mid m + 2L$ then $q \mid L$, which is again a contradiction.

Next note that $m(m-1)/2^t$ is odd unless $m \equiv 1 \bmod 8$. So if $q = 2$, then $16 \mid m - 1$, and since $m + L$ is odd, this implies that $16 \mid m - 1 + L$ and the contradiction that $16 \mid L$. ∎

From Lemma 2 we deduce that f_1 and f_2 satisfy the condition in Schinzel's Hypothesis H, and so there exist infinitely many x such that $f_1(x)$ and $f_2(x)$ are both primes. Hence there exist infinitely many primes $p \equiv m \bmod L$ that have the form

$$p = \begin{cases} 1 + 2q & \text{if } m \equiv 3 \bmod 4, \\ 1 + 4q & \text{if } m \equiv 5 \bmod 8, \\ 1 + 8q & \text{if } m \equiv 1 \bmod 8, \end{cases}$$

where q is also prime.

Let p be so large that the order of no a_i divides 8. It will be enough to require that $p > \max\{|b_i^8 - c_i^8| \mid i = 1, \ldots, r\}$ where $a_i = b_i/c_i$. From this we deduce that

$$a_i^{(p-1)/q} \not\equiv 1 \bmod p.$$

Furthermore the condition

$$-1 = \left(\frac{a_i}{p}\right) \equiv a_i^{(p-1)/2} \bmod p$$

observed in (3.1) implies that $a_i^{(p-1)/2} \not\equiv 1 \bmod p$. Finally, each a_i is a primitive root modulo p, and this concludes the proof of the particular case of the Theorem.

We are now left with the case when $\{-1, 3\} \subseteq \mathcal{L}'$ and the solutions $(x_1, \dots, x_s) \in (\mathbb{Z}/2\mathbb{Z})^s$ of the linear system (2.1) are all such that components relative to -1 and to 3 are equal. Let us prove the following

LEMMA 3. *Let $\mathcal{E}$ be a matrix with s columns, r rows and entries in $\mathbb{Z}/2\mathbb{Z}$. Assume that the first two columns of $\mathcal{E}$ are non-zero and that the linear system*

$$\mathcal{E} \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_s \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

is solvable in $(\mathbb{Z}/2\mathbb{Z})^s$ and such that each solution $(x_1, \dots, x_s)$ satisfies $x_1 = x_2$. Then there exist an even number of rows of $\mathcal{E}$ such that their sum is the vector $(0, \dots, 0, 1, 1) \in (\mathbb{Z}/2\mathbb{Z})^s$.

Proof. After performing a complete Gauss elimination on the extended matrix, we obtain an extended matrix in row echelon form. We can obtain an extended matrix such that there are 1's in the first two entries of the first row. The only possibility for the above equation to produce solutions where the first two components are always equal is that $k = 2$ and $C = 0$. The equality $C = 0$ implies that the first row of our matrix was produced by the original matrix by summing an even number of rows, and this leads to the statement of the lemma. ∎

From Lemma 3 we deduce that when $\{-1, 3\} \subseteq \mathcal{L}'$ and all the solutions $(x_1, \dots, x_s) \in (\mathbb{Z}/2\mathbb{Z})^s$ of the linear system (2.1) are such that the components relative to -1 and to 3 are equal then there exist an even number of indices $1 \le i_1 < \cdots < i_{2s} \le r$ such that $a_{i_1} \cdots a_{i_{2s}} \in -3\mathbb{Q}^{*2}$.

The second condition in the statement of the Theorem implies that there exists a prime $\ell \equiv 1 \bmod 3$ such that none of $a_1, \dots, a_r$ is a perfect cube modulo ℓ. Now we need the following:

LEMMA 4. *Let $a_1, \dots, a_r \in \mathbb{Q}^* \setminus \{\pm 1\}$ and suppose that*

(a) *$a_{i_1} \cdots a_{i_{2t+1}} \notin \mathbb{Q}^{*2}$ for all $1 \le i_1 < \cdots < i_{2t+1} \le r$;*
(b) *there exist $1 \le j_1 < \cdots < j_{2t} \le r$ such that $a_{j_1} \cdots a_{j_{2t}} \in -3\mathbb{Q}^{*2}$;*
(c) *there exists a prime $\ell \equiv 1 \bmod 3$ such that each of $a_1, \dots, a_r$ is a cubic non-residue modulo ℓ.*

Then there exists another prime $q \equiv 1 \bmod 3$ such that each of $a_1, \dots, a_r$ is both a cubic non-residue and a quadratic non-residue modulo q.

Proof. Let

$$K_0 = \mathbb{Q}(\sqrt{-3}), \quad K_1 = K_0(a_1^{1/3}, \dots, a_r^{1/3}), \quad K_2 = \mathbb{Q}(a_1^{1/2}, \dots, a_r^{1/2}).$$

We have $K_0 \subset K_2$ by hypothesis (b). Furthermore the field extensions K_1/K_0 and K_2/K_0 are abelian and linearly disjoint by [4, Theorem 8.1]. Let λ be a prime of K_0 above ℓ and consider the Artin symbol $\sigma_\lambda \in \mathrm{Gal}(K_1/K_0)$. By definition $\sigma_\lambda(a_i^{1/3}) \neq a_i^{1/3}$ for all $i = 1, \dots, r$. Similarly let $p \equiv 1 \bmod 3$ be a prime such that $\left(\frac{a_i}{p}\right) = -1$ for all $i = 1, \dots, r$. The existence of such a p is guaranteed by Lemma 1. If π is a prime of K_0 above p, then the Artin symbol $\sigma_\pi \in \mathrm{Gal}(K_2/K_0)$ satisfies $\sigma_\pi(a_i^{1/2}) = -a_i^{1/2}$ for all $i = 1, \dots, r$. Since

$$\mathrm{Gal}(K_1K_2/K_0) \cong \mathrm{Gal}(K_1/K_0) \times \mathrm{Gal}(K_2/K_0),$$

by the Chebotarev Density Theorem (see for example [6, p. 552]), there exists a prime η of K_0 such that $(\sigma_\lambda, \sigma_\pi) = \sigma_\eta$. Finally, the prime $q = N(\eta) \in \mathbb{Z}$ will have the required properties. ∎

LEMMA 5. *Let $S = \{a_1, \dots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ satisfy the hypotheses of Lemma 4, and let $q \equiv 1 \bmod 3$ be a prime such that each of $a_1, \dots, a_r$ is both a cubic non-residue and a quadratic non-residue modulo q. Let η be a primary prime in $\mathbb{Z}[\omega]$ ($\omega = (-1 + \sqrt{-3})/2$) with norm q. Then there exists $L' \in \mathbb{Z}$ such that for all primes $\pi \in \mathbb{Z}[\omega]$ such that $\pi \equiv \eta \bmod L'$, if $p = N(\pi)$, then each of $a_1, \dots, a_r$ is both a cubic non-residue and a quadratic non-residue modulo p.*

Proof. Let us show that one can take

$$L' = 12 \prod_{\substack{\ell \text{ prime:} \\ \exists a \in S,\, v_\ell(a) \neq 0}} \ell = 3L.$$

We want to show that any π is a primary prime in $\mathbb{Z}[\omega]$ such that $\pi \equiv \eta \bmod L'$ has the required properties.

To this end, set

$$\mathfrak{L} = \{\omega, 1-\omega\} \cup \{\lambda \in \mathbb{Z}[\omega] \mid \lambda \text{ primary prime and } \exists a \in S, v_\lambda(a) \neq 0\}$$

and write $\mathfrak{L} = \{\lambda_1, \dots, \lambda_s\}$, where $\lambda_1 = \omega$, $\lambda_2 = 1 - \omega$. We have

$$a_i = \pm \lambda_1^{e_{1i}} \cdots \lambda_s^{e_{si}}, \qquad \left[\frac{a_j}{\eta}\right]_3 = \omega^{t_j} \quad (\text{with } t_j \in \{\pm 1\}).$$

For any $i = 3, \dots, s$ we see that $\pi \equiv \eta \bmod L'$ implies $\pi \equiv \eta \bmod \lambda_i$. So by

cubic reciprocity (see for example [1, 3])

$$\left[\frac{\lambda_i}{\eta}\right]_3 = \left[\frac{\lambda_i}{\pi}\right]_3.$$

On the other hand, $\pi \equiv \eta \bmod 9$ implies

$$\left[\frac{\omega}{\eta}\right]_3 = \left[\frac{\omega}{\pi}\right]_3 \quad \text{and} \quad \left[\frac{1-\omega}{\eta}\right]_3 = \left[\frac{1-\omega}{\pi}\right]_3.$$

So, automatically we have

$$\left[\frac{a_j}{\eta}\right]_3 = \left[\frac{a_j}{\pi}\right]_3 \quad \forall j = 1, \dots, r,$$

which implies that none of the a_i's is a cube modulo $N(\pi)$.

We also claim that if $p = N(\pi)$, then for all $i = 1, \dots, r$,

$$\left(\frac{a_i}{q}\right) = \left(\frac{a_i}{q}\right) = -1.$$

Indeed, since $\pi = \eta + 3L\alpha$ for a suitable $\alpha \in \mathbb{Z}[\omega]$, we have $p = N(\pi) \equiv q \bmod 3L$, and by applying one more time the quadratic reciprocity law we obtain the claim. ∎

If $\eta, L' \in \mathbb{Z}[(1+\sqrt{-3})/2]$ are the elements in Lemma 5, then let

$$f(X) = N(\eta + L'X) = N(L')X^2 + L'\operatorname{Tr}(\eta)X + q \in \mathbb{Z}[X].$$

It is clear from the definition of L' and η that $f(X) \equiv 1 \bmod 3$ and whenever $x \in \mathbb{N}$ is such that $p = f(x)$ is prime, then each of $a_1, \dots, a_r$ is both a cubic and a quadratic non-residue modulo p. Furthermore let

$$g(X) = \begin{cases} (f(X)-1)/6 & \text{if } \ell \equiv 3 \bmod 4, \\ (f(X)-1)/12 & \text{if } \ell \equiv 5 \bmod 8, \\ (f(X)-1)/24 & \text{if } \ell \equiv 1 \bmod 8. \end{cases}$$

Much as we did above, we can check that the conditions of Schinzel's Hypothesis H are satisfied for f and g, and therefore there exist infinitely many x such that $f(x)$ and $g(x)$ are both primes. These primes p have the form

$$p = \begin{cases} 1 + 6q & \text{if } \ell \equiv 3 \bmod 4, \\ 1 + 12q & \text{if } \ell \equiv 5 \bmod 8, \\ 1 + 24q & \text{if } \ell \equiv 1 \bmod 8, \end{cases}$$

where q is also prime and moreover none of the a_i's is either a square or a cube modulo p.

Let now p be so large that the order of no a_i divides 24. Since in this case for each i we have $a_i^{(p-1)/2} \equiv -1 \bmod p$ and $a_i^{(p-1)/3} \not\equiv 1 \bmod p$, each a_i is a primitive root modulo p, and this concludes the proof of the Theorem.

Acknowledgments. This paper was inspired by A. Granville at the Centre de Recherches Mathématiques of Montréal in January 2006. The authors would like to thank Denis R. Akhmetov and Sergei Konyagin for some useful comments.

References

[1] S. D. Adhikari, *The early reciprocity laws: from Gauss to Eisenstein*, in: Cyclotomic Fields and Related Topics (Pune, 1999), Bhaskaracharya Pratishthana, Pune, 2000, 55–74.
[2] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 225 (1967), 209–220.
[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, New York, 1990.
[4] S. Lang, *Algebra*, Grad. Texts in Math. 211, Springer, New York, 2002.
[5] K. R. Matthews, *A generalisation of Artin's conjecture for primitive roots*, Acta Arith. 29 (1976), 113–146.
[6] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Universitext, Springer, New York, 2001.
[7] A. Schinzel et W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), 185–208; erratum, ibid. 5 (1958), 259.

Mohamed Anwar, Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre
Largo S. L. Murialdo 1
I-00191 Roma, Italy
E-mail: amohamed@mat.uniroma3.it
pappa@mat.uniroma3.it