On simultaneous primitive roots

Francesco Pappalardi

November 28, 2006

Abstract

Given finitely many non zero rational numbers which are not ± 1, we prove, under the assumption of Hypothesis H of Schinzel, necessary and sufficient conditions for the existence of infinitely many primes modulo which all the given numbers are simultaneously primitive roots. A stronger result where the density of the primes in consideration was computed was proved under the assumption of the Generalized Riemann Hypothesis by K. Matthew in 1976.

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

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

In the case where $S \subset \mathbf{Z}$, assuming the Generalized Riemann Hypothesis for suitable number fields, it was proved by K. Matthews in 1976 [Mat76] that $\mathcal{P}_S$ is finite if and only if at least one of the two following conditions is satisfied:

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

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

In all other cases, not only $\mathcal{P}_S$ is 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 second part of the second condition is verified for example for the sets S of the form $S = \{q_1 b_1^3, q_2 b_2^3, q_1 q_2 b_3^3, q_1^2 q_2 b_4^3\}$ where q_1 and q_2 are distinct primes different from 3 and $b_1, b_2, b_3, b_4 \in \mathbf{Q}^*$.

The goal of this note is to prove the conclusion of Matthews Theorem assuming the Schinzel's Hypothesis H in [SS58]. We will prove the following

Theorem. *Let $S = \{a_1, \dots, a_r\} \subset \mathbf{Q}$ and assume*

1. *For each $1 \le i_1 < \cdots < i_{2s+1} \le r$ one has that $a_{i_1} \cdots a_{i_{2s+1}} \notin (\mathbf{Q}^*)^2$;*
2. *If there exist $1 \le i_1 < \cdots < i_{2s} \le r$ such that $a_{i_1} \cdots a_{i_{2s}} \in -3(\mathbf{Q}^*)^2$, then there exists a prime $l \equiv 1 \bmod 3$ such that none of the elements of S is a cube modulo l.*

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

We recall the statement of the famous Conjecture:

Hypothesis H (Schinzel, 1959) *Let $f_1, \dots, f_k \in \mathbf{Z}[x]$ be irreducible polynomials with positive leading coefficients and such that $\gcd(f_1(n)\cdots f_k(n) \mid n \in \mathbf{N}) = 1$. Then there are infinitely many $t \in \mathbf{N}$ such that $f_1(t), \dots, f_k(t)$ are all prime.*

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 in 1967 [Hoo67]. It was also considered by Schinzel and Sierpinski in [SS58, page 199] as an example of application of Hypothesis H that they proved to imply Artin Conjecture.

Let $\mathcal{L} = \{l \text{ prime} \mid v_l(a) \neq 0 \text{ for some } a \in S\}$. Then $\mathcal{L}$ is clearly finite. Furthermore set

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

We write $\mathcal{L}' = \{l_1, \dots, l_s\}$ and when $\mathcal{L}' \not\subseteq \mathbf{Q}^{>0}$ we assume that $l_1 = -1$. Further we set $L = 4|l_1 \cdots l_s|$.

For each $j = 1, \dots, r$, write $a_j = l_1^{e_{1j}} \cdot l_2^{e_{2j}} \cdots l_s^{e_{sj}}$. Then the matrix

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

has coefficients in $\mathbf{Z}$ and the first condition in the statement implies that the sum of an odd number of rows of $\mathcal{E}$ is never the zero vector modulo 2. We claim that this implies that the linear system

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

admits a solution in $(\mathbf{Z}/2\mathbf{Z})^s$. Indeed perform a complete Gaussian Elimination on the rows of the enlarged matrix obtained attaching to $\mathcal{E}$ the column of 1's. We obtain a reduced row echelon form. The last column has 1 in the rows that were obtained adding together an odd number of the original rows and 0 in the rows that were obtained adding together an even number of rows. The first condition in the statement implies that whenever there is a 1 in the last entry, the rest of the row contains some other 1 entries and therefore the original system can be solved recursively.

We now need the following

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

(i) *if p is prime with $p \equiv m \bmod L$, then $\left(\frac{l_i}{p}\right) = (-1)^{x_i}$ for all $i = 1, \dots, s$;*

(ii) *$m \not\equiv 1 \bmod l_i$ for all $i = 1, \dots, s$ such that $l_i > 3$.*

Furthermore conclusion (ii)*. above also holds for $l_i = 3$ 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 a congruence class for m modulo 4 and then its congruence class modulo each l_i such that $l_i > 2$. If $2 \in \mathcal{L}$ we will also define a class modulo 8. Then we will apply the Chinese Reminder 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 the following:

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

In the event that $2 \in \mathcal{L}$ and that $l_j = 2$, then let m_8 be the unique invertible congruence class modulo 8 with the properties that $m_8 \equiv m_4 \bmod 4$ and when $p \equiv m_8 \bmod 8$ then $\left(\frac{2}{p}\right) = (-1)^{x_j}$.

For all other odd primes l_i in $\mathcal{L}$, note that by the quadratic reciprocity law:

$$\left(\frac{l_i}{p}\right) = (-1)^{(p-1)(l_i-1)/4} \left(\frac{p}{l_i}\right).$$

Therefore for $p \equiv m_4 \bmod 4$ we have $(l_i - 1)/2$ choices for a congruence class m_{l_i} modulo l_i such that if $p \equiv m_{l_i} \bmod l_i$, then $\left(\frac{l_i}{p}\right) = (-1)^{x_i}$. Indeed it is enough to chose any class M such that $\left(\frac{M}{l_i}\right) = (-1)^{x_i+(m_4-1)(l_i-1)/4}$.

If $l_i > 3$, then there is always a choice for such a class m_{l_i} with $m_{l_i} \neq 1$ while if $l_i = 3$, then in order to have $m_3 = 2$ one needs to have

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

Identity (2) is automatically verified when $-1 \notin \mathcal{L}'$ as a consequence of the definition of m_4 (since $(-1)^{(m_4-1)/2} = (-1)^{x_i+1}$ in this case) while when $l_1 = -1 \in \mathcal{L}'$ then (2) is verified if and only if $x_1 \neq x_i$. This ends the proof of the Lemma. □

An immediate consequence of Lemma 1 is that for any prime $p \equiv m \bmod L$,

$$\left(\frac{a_j}{p}\right) = \prod_{i=1}^{s} \left(\frac{l_i}{p}\right)^{e_{ji}} = (-1)^{e_{j1}x_1+\ldots+e_{jr}x_s} = -1.$$

So each a_i is a quadratic non residue modulo p.

Let us now deduce the statement of the Theorem in the case when $\{-1,3\} \nsubseteq \mathcal{L}'$ and also in the case when $\{-1,3\} \subseteq \mathcal{L}'$ and it exists a solution $(x_1,\ldots,x_s) \in (\mathbf{Z}/2\mathbf{Z})^s$ of the linear system (1) where the components relative to -1 and to 3 are distinct. Let $f_1(X) = m + LX$ where $L = 4|l_1 \cdots l_s|$ and m is the congruence class postulated by Lemma 1. Furthermore let

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

We claim that the three integers

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

are always coprime. Indeed let q is a prime dividing the gcd

$$\left(\frac{m(m-1)}{(m-1,8)}, \frac{(m+L)(m-1+L)}{(m-1,8)}, \frac{(m+2L)(m-1+2L)}{(m-1,8)}\right).$$

If $q=2$, then $2 \mid (m-1)/(m-1,8)$ but $2 \nmid (m-1+L)/(m-1,8)$ because $16 \nmid L$ therefore $2 \mid (m+L)$ and this contradicts the fact that m is odd. Similarly if $q|m(m-1)$ and q is odd then either $q \mid m$ or $q \mid m-1$. In the first instance $q \nmid m+L$ and $q \nmid m+2L$ and 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 $q \nmid m-1+L$ and $q \nmid m-1+2L$ because of the properties of m postulated in the Lemma. If $q \mid (m+L)$ and $q \mid (m+2L)$ then $q \mid L$ which is again a contradiction.

Therefore the conditions for Schinzel's Hypothesis H in [SS58] are satisfied and so there exists infinitely many x such that $f_1(x)$ and $f_2(x)$ are both primes. These primes p verify $p \equiv m \bmod L$ and have the form

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

where q is also prime.

We want to conclude by showing that all the $a_1, \ldots, a_r$ are primitive roots modulo such primes. Let p be sufficiently large so that none of the a_i's can have as order a divisor of 8 (It will be enough to require that $p > \max\{|b_i - c_i|^8, i = 1, \ldots, r\}$ where $a_i = b_i/c_i$). From the condition

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

we deduce that the order of a_i cannot be a divisor of $(p-1)/2$. Therefore each a_i is a primitive root modulo p and this concludes the proof of the particular case of the Theorem.

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

Lemma 2. *Let $\mathcal{E}$ be a matrix with s columns, r rows and entries in $\mathbf{Z}/2\mathbf{Z}$. Assume that the first two columns of $\mathcal{E}$ is 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 $(\mathbf{Z}/2\mathbf{Z})^s$ and such that each solution $(x_1, \ldots, x_s)$ verifies $x_1 = x_2$. Then there exists an even number of rows of $\mathcal{E}$ such that their sum is the vector $(1, 1, 0, \ldots, 0) \in (\mathbf{Z}/2\mathbf{Z})^r$.

Proof. After performing a complete Gaussian Elimination, we will obtain an extended matrix in reduced form such that there will 1's in the first two entries of the first row. Therefore any solution of the system will verify a linear equation of the form:

$$X_1 + X_2 + \ldots + X_k = C$$

where $C \in \mathbf{Z}/2\mathbf{Z}$ and the variables which do not appear in the equation are independent. The only possibility for the above equation to produce solutions where the first two components are always equal is that $k = 2$ and that $C = 0$. The equality $C = 0$ implies that the first row of the reduced matrix was produced by the original matrix summing an even number of rows, and this leads to the statement of the lemma. □

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

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

Lemma 3. *Let $a_1 \ldots a_r \in \mathbf{Q}^* \setminus \{\pm 1\}$ and suppose that*

(a) *for every $1 \leq i_1 < \ldots < i_{2t+1} \leq r$, $a_{i_1} \cdots a_{i_{2t+1}} \notin (\mathbf{Q}^*)^2$;*

(b) *there exists $1 \leq j_1 < \ldots < j_{2t} \leq r$ such that $a_{j_1} \cdots a_{j_{2t}} \in -3(\mathbf{Q}^*)^2$;*

(c) *there exists a prime $l \equiv 1 \bmod 3$ such that each of $a_1, \ldots, a_r$ is a cubic non residue modulo l.*

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

Proof. Let

$$K_0 = \mathbf{Q}(\sqrt{-3}), \quad K_1 = K_0(a_1^{1/3}, \ldots, a_r^{1/3}) \quad \text{and} \quad K_2 = \mathbf{Q}(a_1^{1/2}, \ldots, a_r^{1/2}).$$

We have that $K_0 \subset K_2$ in virtue of hypothesis (b) in the statement. Furthermore the two field extensions K_1/K_0 and K_2/K_0 are abelian and linearly disjoint. 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 $i = 1, \ldots, r$. Similarly let $p \equiv 1 \bmod 3$ be a prime such that $\left(\frac{a_i}{p}\right) = -1$ for all $i = 1 \ldots, r$. 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 $\sigma_\pi \in \mathrm{Gal}(K_1/K_0)$ verifies $\sigma_\pi(a_i^{1/2}) = -a_i^{1/2}$ for all $i = 1, \ldots, r$. 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 [Rib02, page 552]), there exists a prime η of K_0 such that $(\sigma_\lambda, \sigma_\pi) = \sigma_\eta$. Finally the prime $q = N(\eta) \in \mathbf{Z}$ will have the required properties. □

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

Proof. Let us show that as L' one can take

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

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

To this end, set

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

and write $\mathfrak{L} = \{\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_s\}$, where $\lambda_1 = \omega$, $\lambda_2 = 1-\omega$. We have

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

For any $i = 3, \ldots, s$ we have that $\pi \equiv \eta \bmod L'$ implies $\pi \equiv \eta \bmod \lambda_i$. So by cubic reciprocity (see for example [Adh00, IR90])

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

While $\pi \equiv \eta \bmod 9$ implies

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

So, automatically we have that

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

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 $i = 1, \ldots, r$

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

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

If $\eta, \alpha \in \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ are the elements in Lemma 4, then let

$$f(X) = N(\eta + \alpha X) = N(\alpha)X^2 + \mathrm{Tr}(\alpha\eta)X + q \in \mathbf{Z}[X].$$

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

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

In a very similar way as we did above, we can check that the conditions of Schinzel's Hypothesis H in [SS58] are satisfied for f and g and therefore there exists infinitely many x such that $f(x)$ and $g(x)$ are both primes. These primes p have the form

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

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 sufficiently large so that none of the a_i's can have as order a divisor of 24. Since in this case for each i, $a_i^{(p-1)/2} \equiv -1 \bmod p$ 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 on the Theorem.

Acknowledgements: This paper was inspired by a suggestion of A. Granville at the Centre de Recherches Mathématiques of Montréal in January 2006. The paper was translated in russian by Dr. Denis R. Akhmetov.

References

[Adh00] Sukumar Das Adhikari. The early reciprocity laws: from Gauss to Eisenstein. In *Cyclotomic fields and related topics (Pune, 1999)*, pages 55–74. Bhaskaracharya Pratishthana, Pune, 2000.

[Hoo67] Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Mat76] Keith R. Matthews. A generalisation of Artin's conjecture for primitive roots. *Acta Arith.*, 29(2):113–146, 1976.

[Rib02] Paulo Ribenboim. *Classical theory of algebraic numbers*, *Universitext*. Springer-Verlag, New York, 2001.

[SS58] A. Schinzel and W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith. 4 (1958), 185–208; erratum*, 5:259, 1958.