ОБ ОДНОВРЕМЕННО ПЕРВООБРАЗНЫХ КОРНЯХ

Франческо Паппаларди

Аннотация. Для конечного числа ненулевых рациональных чисел, не равных ± 1, в предположении гипотезы H Шинцеля устанавливаются необходимые и достаточные условия существования бесконечного числа простых чисел, являющихся первообразными корнями по модулю всех заданных рациональных чисел одновременно. В предположении обобщенной гипотезы Римана К. Мэттьюс в 1976 году доказал более сильный результат, вычислив плотность рассматриваемых простых чисел.

Пусть $S = \{a_1, \ldots, a_r\} \subset \mathbf{Q}^* \setminus \{\pm 1\}$. Обозначим

$$\mathcal{P}_S = \{p \text{ — простое } \mid \forall\, a \in S,\ a \text{ — первообразный корень по модулю } p\}\,.$$

В случае $S \subset \mathbf{Z}$ в предположении обобщенной гипотезы Римана (для подходящего числа полей) К. Мэттьюс в 1976 году доказал [Mat76], что множество $\mathcal{P}_S$ — ограничено, если и только если выполняется по крайней мере одно из следующих условий:

(α) Существуют $1 \le i_1 < \cdots < i_{2s+1} \le r$ такие, что $a_{i_1} \cdots a_{i_{2s+1}} \in (\mathbf{Q}^*)^2$;

(β) Существуют $1 \le i_1 < \cdots < i_{2s} \le r$ такие, что $a_{i_1} \cdots a_{i_{2s}} \in -3(\mathbf{Q}^*)^2$, и для всякого целого $l \equiv 1 \bmod 3$ существует по крайней мере один элемент множества S, являющийся кубом по модулю l.

Во всех других случаях множество $\mathcal{P}_S$ не просто бесконечно, но и имеет ненулевую плотность (в предположении ОГР). По всей вероятности гипотеза о том, что все элементы множества S — целые числа, не является существенной в работе Мэттьюса.

Вторая часть второго условия выполняется, например, для всех множеств S вида $S = \{q_1 b_1^3, q_2 b_2^3, q_1 q_2 b_3^3, q_1^2 q_2 b_4^3\}$, где q_1 и q_2 — различные простые числа отличные от 3 и $b_1, b_2, b_3, b_4 \in \mathbf{Q}^*$.

Цель данной заметки — доказать заключение теоремы Мэттьюса в предположении шинцелевской гипотезы H из [SS58]. Мы докажем следующую теорему.

Теорема 1. *В предположении гипотезы H, пусть* $S = \{a_1, \ldots, a_r\} \subset \mathbf{Q}$. *Предположим, что:*

1) *для каждого набора* $1 \le i_1 < \cdots < i_{2s+1} \le r$ *имеем* $a_{i_1} \cdots a_{i_{2s+1}} \notin (\mathbf{Q}^*)^2$;
2) *если существуют* $1 \le i_1 < \cdots < i_{2s} \le r$ *такие, что* $a_{i_1} \cdots a_{i_{2s}} \in -3(\mathbf{Q}^*)^2$, *то существует* $l \equiv 1 \bmod 3$ *такое, что ни один элемент множества* S *не является кубом по модулю* l.

Тогда множество $\mathcal{P}_S$ *неограниченно.*

Напомним формулировку знаменитой гипотезы.

Гипотеза H (Schinzel, 1958) *Пусть* $f_1, \ldots, f_k \in \mathbf{Z}[x]$ *— несократимые полиномы с положительными старшими коэффициентами такие, что* $\gcd(f_1(n) \cdots f_k(n) \mid n \in \mathbf{N}) = 1$. *Тогда существует бесконечное множество натуральных* t *таких, что все* $f_1(t), \ldots, f_k(t)$ *— простые числа.*

В случае $r = 1$ утверждение о том, что множество $\mathcal{P}_{\{a_1\}}$ — бесконечно, является *предположением Артина о первообразных корнях.* В предположении обобщенной гипотезы Римана его справедливость была установлена Ч. Хули в 1967 году [Hoo67]. Этот случай рассмотрели также Шинцель и Серпинский [SS58, страница 199] как пример приложения гипотезы H. Они доказали, что гипотеза H влечет предположение Артина.

Пусть $\mathcal{L} = \{l$ — простое $\mid v_l(a) \neq 0$ для некоторого $a \in S\}$. Тогда множество $\mathcal{L}$, очевидно, ограничено. Положим

$$\mathcal{L}' = \begin{cases} \mathcal{L} \cup \{-1\}, & \text{если } S \not\subseteq \mathbf{Q}^{>0}; \\ \mathcal{L} & \text{в противном случае.} \end{cases}$$

Мы будем использовать запись $\mathcal{L}' = \{l_1, \ldots, l_s\}$ и подразумевать, что $l_1 = -1$, если $\mathcal{L}' \not\subseteq \mathbf{Q}^{>0}$. Далее, введем $L = 4|l_1 \cdots l_s|$.

Для каждого $j = 1, \ldots, r$ обозначим $a_j = l_1^{e_{1j}} \cdot l_2^{e_{2j}} \cdots l_s^{e_{sj}}$. Тогда матрица

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

имеет коэффициенты из $\mathbf{Z}$, и из первого условия теоремы следует, что сумма нечетного числа строк матрицы $\mathcal{E}$ никогда не является нулевым вектором по модулю 2. Мы утверждаем, что в таком случае линейная система

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

имеет решение из $(\mathbf{Z}/2\mathbf{Z})^s$. В самом деле, выполнив полное гауссовское исключение в строках расширенной матрицы, полученной присоединением к матрице $\mathcal{E}$ столбца единиц, получим сокращенную форму, в которой последний столбец содержит единицы в строках, полученных сложением нечетного числа исходных строк, и нули в строках, полученных сложением четного числа строк. Из первого услови теоремы вытекает, что если в конце какой-либо строки сокращенной формы стоит единица, то остаток данной строки содержит по крайней мере еще одну единицу, и значит, исходная система может быть решена рекурсивно.

Теперь нам понадобится следующая

Лемма 1. *Предположим, что* $(x_1, \ldots, x_s) \in (\mathbf{Z}/2\mathbf{Z})^s$ *— решение линейной системы* (1)*. Тогда существует обратимое целое* m *по модулю* L *такое, что:*

i) *если* p *— простое и* $p \equiv m \bmod L$*, то* $\left(\frac{l_i}{p}\right) = (-1)^{x_i}$ *для всех* $i = 1, \ldots, s$*;*

ii) $m \not\equiv 1 \bmod l_i$ *для всех* $i = 1, \ldots, s$ *таких, что* $l_i > 3$*.*

Кроме того, заключение ii) *справедливо также для* $l_i = 3$*, если* $\{-1, 3\} \not\subseteq \mathcal{L}'$ *или если* $\{-1, 3\} \subseteq \mathcal{L}'$ *и* $x_i \neq x_1$*.*

Доказательство. Определим сначала класс вычетов для m по модулю 4, а затем класс вычетов для m по модулю каждого l_i такого, что $l_i > 2$. Если $2 \in \mathcal{L}$, то определим также класс вычетов по модулю 8. Затем применим Китайскую теорему об остатках и получим существование класса вычетов по модулю L с требуемыми свойствами.

Класс вычетов для m по модулю 4 определим следующим образом:

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

В случае когда $2 \in \mathcal{L}$ и $l_j = 2$, определим m_8 как единственный обратимый класс вычетов по модулю 8 со свойствами (a) $m_8 \equiv m_4 \bmod 4$ и (b) если $p \equiv m_8 \bmod 8$, то $\left(\frac{2}{p}\right) = (-1)^{x_j}$.

Заметим, что для всех других нечетных простых l_i из $\mathcal{L}$ по закону квадратичной взаимности имеем

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

Поэтому для $p \equiv m_4 \bmod 4$ существует $(l_i - 1)/2$ вариантов класса вычетов m_{l_i} по модулю l_i такого, что если $p \equiv m_{l_i} \bmod l_i$, то $\left(\frac{l_i}{p}\right) = (-1)^{x_i}$. В самом деле, достаточно выбрать произвольный класс M такой, что $\left(\frac{M}{l_i}\right) = (-1)^{x_i+(m_4-1)(l_i-1)/4}$.

Если $l_i > 3$, то всегда можно выбрать такой класс m_{l_i} с $m_{l_i} \neq 1$, а если $l_i = 3$, то для того, чтобы было $m_3 = 2$, необходимо выполнение условия

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

Тождество (2) выполняется автоматически, когда $-1 \notin \mathcal{L}'$, как следствие определения m_4 (так как в этом случае $(-1)^{(m_4-1)/2} = (-1)^{x_i+1}$), а если $l_1 = -1 \in \mathcal{L}'$, то (2) выполняется тогда и только тогда, когда $x_1 \neq x_i$. Этим завершается доказательство. $\square$

Немедленным следствием леммы 1 является тот факт, что для любого простого $p \equiv m \bmod L$

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

Таким образом, каждое a_i — квадратичный невычет по модулю p.

Сейчас мы докажем утверждение теоремы в случае, когда $\{-1, 3\} \nsubseteq \mathcal{L}'$, а также в случае, когда $\{-1, 3\} \subseteq \mathcal{L}'$ и когда существует решение $(x_1, \ldots, x_s) \in (\mathbf{Z}/2\mathbf{Z})^s$ линейной системы (1) у которого компоненты, соответствующие -1 и 3, различны. Пусть $f_1(X) = m + LX$, где $L = 4|l_1 \cdots l_s|$ и m — класс вычетов, постулированный леммой 1. Далее, пусть

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

Мы утверждаем, что три целых числа

$$f_1(0)f_2(0), \quad f_1(1)f_2(1) \quad \text{и} \quad f_1(2)f_2(2)$$

всегда взаимно просты. В самом деле, пусть q — простое число, делящее наибольший общий делитель

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

Если $q = 2$, то $2 \mid (m-1)/(m-1,8)$, но $2 \nmid (m-1+L)/(m-1,8)$, потому что $16 \nmid L$, поэтому $2 \mid (m+L)$, а это противоречит тому, что m — нечетное. Аналогично, если $q|m(m-1)$ и q — нечетное, то либо $q \mid m$, либо $q \mid m-1$. В первом случае $q \nmid m+L$ и $q \nmid m+2L$, и если еще $q \mid (m-1+L)$ и $q \mid (m-1+2L)$, то $q \mid L$, что является противоречием. Во втором случае $q \nmid m-1+L$ и $q \nmid m-1+2L$ вследствие свойств m, постулированных в лемме 1. Если дополнительно $q \mid (m+L)$ и $q \mid (m+2L)$, то $q \mid L$, что опять является противоречием.

Таким образом, условия шинцелевской гипотезы H из [SS58] выполнены, и значит, существует бесконечное множество таких x, для которых $f_1(x)$ и $f_2(x)$ — оба простые. Эти простые p удовлетворяют соотношению $p \equiv m \bmod L$ и представляются в виде

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

где q — тоже простое.

Завершим доказательство демонстрацией того факта, что по модулю таких простых чисел все $a_1, \ldots, a_r$ — первообразные корни. Пусть p — настолько большое, что ни одно из a_i-х не имеет своим порядком никакой делитель 8-и (для этого достаточно потребовать выполнение неравенства $p > (\max_{i=1,\ldots,r} |b_i - c_i|)^8$, где $a_i = b_i/c_i$). Из условия

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

заключаем, что порядок a_i-го не может быть делителем числа $(p-1)/2$, поэтому каждое a_i — первообразный корень по модулю p, и этим завершается доказательство частных случаев теоремы.

Остается рассмотреть последний случай, когда $\{-1, 3\} \subseteq \mathcal{L}'$ и все решения $(x_1, \ldots, x_s) \in (\mathbf{Z}/2\mathbf{Z})^s$ линейной системы (1) таковы, что компоненты, соответствующие -1 и 3, совпадают. Прежде всего докажем следующую лемму.

Лемма 2. *Пусть $\mathcal{E}$ — матрица с s столбцами, r строками и данными из $\mathbf{Z}/2\mathbf{Z}$. Предположим, что первые два столбца матрицы $\mathcal{E}$ — ненулевые и что линейная система*

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

разрешима в $(\mathbf{Z}/2\mathbf{Z})^s$ так, что каждое решение $(x_1, \ldots, x_s)$ удовлетворяет условию $x_1 = x_2$. Тогда существует четное число строк матрицы $\mathcal{E}$, сумма которых является вектором $(1, 1, 0, \ldots, 0) \in (\mathbf{Z}/2\mathbf{Z})^r$.

Доказательство. После выполнения полного гауссовского исключения получим расширенную матрицу в сокращенной форме такой, что в первой строке на первых двух местах будут стоять единицы. Поэтому любое решение системы будет удовлетворять линейному уравнению вида

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

где $C \in \mathbf{Z}/2\mathbf{Z}$, а переменные, не входящие в это уравнение, будут независимы. Случай $k = 2$ и $C = 0$ — единственная возможность получения решений данного уравнения, первые две компоненты которых всегда совпадают. Равенство $C = 0$ подразумевает, что первая строка сокращенной матрицы получен из исходной матрицы суммированием четного числа строк, и это приводит к утверждению леммы. □

Если $\{-1, 3\} \subseteq \mathcal{L}'$ и все решения $(x_1, \ldots, x_s) \in (\mathbf{Z}/2\mathbf{Z})^s$ линейной системы (1) таковы, что компоненты, соответствующие -1 и 3, равны, то из леммы 2 вытекает существование четного числа индексов $1 \leq i_1 < \cdots < i_{2s} \leq r$ таких, что $a_{i_1} \cdots a_{i_{2s}} \in -3(\mathbf{Q}^*)^2$.

Второе условие теоремы влечет существование простого $l \equiv 1 \bmod 3$ такого, что ни одно из чисел $a_1, \ldots, a_r$ не является полным кубом по модулю l. Теперь нам необходима следующая

Лемма 3. *Пусть* $a_1 \dots a_r \in \mathbf{Q}^* \setminus \{\pm 1\}$. *Предположим, что:*

- $\forall\, 1 \le i_1 < \ldots < l_{2t+1} \le r$ *имеем* $a_{i_1} \cdots a_{i_{2t+1}} \notin (\mathbf{Q}^*)^2$;
- $\exists\, 1 \le i_1 < \ldots < l_{2t} \le r$ *такие, что* $a_{i_1} \cdots a_{i_{2t}} \in -3(\mathbf{Q}^*)^2$;
- $\exists$ *простое* $l \equiv 1 \bmod 3$ *такое, что все* $a_1, \ldots, a_r$ — *кубические невычеты по модулю* l.

Тогда существует другое простое $q \equiv 1 \bmod 3$ *такое, что все* $a_1, \ldots, a_r$ — *кубические и квадратичные невычеты по модулю* q.

Доказательство. Пусть

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

В силу второго предположения леммы $K_0 \subset K_2$. Кроме того, расширения K_1/K_0 и K_2/K_0 — абелевы и линейно независимы. Возьмем теперь простое λ из K_0, превосходящее l, и рассмотрим символ Артина $\sigma_\lambda \in \mathrm{Gal}(K_1/K_0)$. По определению $\sigma_\lambda(a_i^{1/3}) \ne a_i^{1/3}$ для всех $i = 1, \ldots, r$. Аналогично, пусть $p \equiv 1 \bmod 3$ — простое такое, что $\left(\frac{a_i}{p}\right) = -1$ для всех $i = 1 \ldots, r$. Существование такого p гарантируется леммой 1. Заметим, что если π — простое из K_0, превосходящее p, то символ Артина $\sigma_\pi \in \mathrm{Gal}(K_1/K_0)$ удовлетворяет равенству $\sigma_\pi(a_i^{1/2}) = -a_i^{1/2}$ для всех $i = 1, \ldots, r$. По теореме плотности Чеботарева (см., например, [Rib02, страница 552])

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

и значит, существует простое η из K_0 такое, что $(\sigma_\lambda, \sigma_\pi) = \sigma_\eta$. Рациональное простое $q = N(\eta)$ будет обладать всеми требуемыми свойствами. □

Лемма 4. *Пусть для* $S = \{a_1 \dots a_r\} \subset \mathbf{Q}^* \setminus \{\pm 1\}$ *выполняются все гипотезы леммы* 3 *и* $q \equiv 1 \bmod 3$ — *такое простое число, по модулю которого все* $a_1, \ldots, a_r$ — *кубические и квадратичные невычеты. Далее, пусть* η — *первостепенно простое в* $\mathbf{Z}[\omega]$ $(\omega = (-1 + \sqrt{-3})/2)$ *по норме* q. *Тогда существует* $L' \in \mathbf{Z}$ *такое, что для всех простых* π *из* $\mathbf{Z}[\omega]$, *удовлетворяющих условию* $\pi \equiv \eta \bmod \alpha$, *имеем: если* $p = N(\pi)$, *то все* $a_1, \ldots, a_r$ — *кубические и квадратичные невычеты по модулю* p.

Доказательство. Покажем, что в качестве L' можно взять

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

Для этой цели положим

$$\mathfrak{L} = \{\omega, 1 - \omega\} \cup \{\lambda \in \mathbf{Z}[\omega],\ \lambda \text{ — первостепенно простое и } \exists\, a \in S,\, v_\lambda(a) \ne 0\}$$

и запишем $\mathfrak{L} = \{\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_s\}$, где $\lambda_1 = \omega$, $\lambda_2 = 1 - \omega$. Имеем

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

Далее, для любого $i = 3, \ldots, s$ из свойства $\pi \equiv \eta \bmod L'$ следует, что $\pi \equiv \eta \bmod \lambda_i$. Таким образом, по кубической взаимности (см., например, [Adh00, IR90])

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

тогда как свойство $\pi \equiv \eta \bmod 9$ влечет

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

Следовательно, автоматически имеем

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

и значит, никакое a_i не является кубом по модулю $N(\pi)$.

Мы также утверждаем, что если $p = N(\pi)$, то для всех $i = 1, \ldots, r$

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

В самом деле, так как $\pi = \eta + 3L\alpha$ для подходящего $\alpha \in \mathbf{Z}[\omega]$, мы имеем $p = N(\pi) \equiv q \bmod 3L$ и, применяя еще раз закон квадратичной взаимности, получаем утверждение леммы. $\square$

Если $\eta, \alpha \in \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ из леммы 4, то положим

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

Из определения α и η ясно, что $f(X) \equiv 1 \bmod 3$ и если $x \in \mathbf{N}$ такое, что $p = f(x)$ — простое, то все $a_i, \ldots, a_r$ — кубические и квадратичные невычеты по модулю p. Далее, пусть

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

Очень похожим образом, как сделано выше, можно проверить, что для f и g выполняются условия шинцелевской гипотезы H из [SS58], и значит, существует бесконечное множество таких x, для которых $f(x)$ и $g(x)$ — оба простые. Эти простые p представляются в виде

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

где q — тоже простое, причем ни одно из a_i-х не является ни квадратом, ни кубом по модулю p.

Пусть теперь p является настолько большим, что ни одно a_i не имеет своим порядком никакой делитель числа 24. Так как в этом случае для каждого i справедливы соотношения $a_i^{(p-1)/2} \equiv -1 \bmod p$ и $a_i^{(p-1)/3} \not\equiv 1 \bmod p$, каждое a_i — первообразный корень по модулю p, и этим завершается доказательство теоремы.

Благодарности: Это доказательство появилось благодаря предложению А. Грэнвилля (A. Granville, Centre de Recherches Mathematiques, Montreal, Canada), сделанному в январе 2006 года. Автор благодарен Д. Р. Ахметову за его ценную помощь в редактировании рукописи.

Список литературы

[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.

Francesco Pappalardi, Dipartimento di Matematica, Università Roma Tre, Largo S. L. Murialdo 1, I–00146 Roma, ITALIA

E-mail address: pappa@mat.uniroma3.it