It is clear that explicit zero-free regions for \( \zeta(s) \) can be obtained at least in those cases where the integrals

\[
\int_0^1 \omega^{s-1} G(s, \omega) \, d\omega
\]

are of the form \( I(q) J(x_1) \), in which case the inequality of Theorem 2 takes the form

\[
\sum_{x=1}^{N} \frac{1}{\lambda_x} \sum_{x=1}^{N} |q_{\lambda_x} J(x_1)|^2 < \frac{1}{|I(q)|^2 (1 - 2\beta)}.
\]

The integral will be separable when \( X \in \mathbb{Q}^N \), 0 < \( x_1 < \ldots < x_N \leq 1 \), and when \( g \in \mathfrak{S} \) has the form

\[
g(x) = \sum a_r \lambda_r (c, x), \quad 0 < c_r \leq 1,
\]

with \( \lambda_r \) having the form

\[
\lambda_r = \frac{\cos 2\pi r}{\sigma}, \quad r \in \mathbb{Z}, \ r \geq 2.
\]

This follows by the same reasoning given in Theorem 2.

We remark that the single greatest impediment to the estimation of the size of \( \sum \) appearing in Theorem 1 is the lack of an effective construction of the orthonormal functions \( \mathcal{F}_k \), 1 < \( k \leq N \). A systematic procedure for constructing such functions has been given, but it is ineffective in the sense that the spectrum of the matrix \( A \mathcal{F}_k \mathcal{F}_k \) is largely unknown, so that good estimates of the sum in Theorem 1 and Theorem 2 are not obtained.

Finally, we observe that the methods of the present paper can be readily adapted to the study of the zeros of Dirichlet \( L \)-series, where, in this case, we would begin with the integral

\[
\int_0^1 \omega^{s-1} \sum_{n=1}^{\infty} \chi(n) f(n\omega) \, d\omega.
\]

Any zero-free region like that given in Theorem 2 would have important consequences for the distribution of prime numbers.

References


University of California

Santa Barbara, California

Received on 10. 3. 1975 (823)

On the construction of non-congruence subgroups

by

JULIET BRITTO (Bombay)

The existence of subgroups of finite index in the modular group which are different from its “congruence subgroups” was first pointed out by Klein ([5], § 1, p.63) and several mathematicians have since dealt with the explicit construction of such subgroups (see [7], [8], and [9]). If one looks for “non-congruence subgroups” in analogous situations, one is led naturally in the light of the well-known solution of the “Congruence subgroup problem” and especially [10], to consider the other interesting case namely, that of the group \( \text{SL}(2, \mathcal{O}) \), where \( \mathcal{O} \) is the ring of algebraic integers in an imaginary quadratic field over the field \( \mathbb{Q} \) of rational numbers. The problem of constructing “non-congruence subgroups” of \( \text{SL}(2, \mathbb{Z} \langle \sqrt{-1} \rangle) \) has recently been dealt with in a purely algebraic fashion by A. Drillick [2]. We are thankful to Professor S. Raghavan for his guidance during the preparation of this note. We are also thankful to Professor K. G. Ramanathan for his encouragement and to Professor W. Magnus for having given us an opportunity to see the dissertation of Drillick.

In this note, we deal with the construction of non-congruence subgroups of \( \text{SL}(2, \mathcal{O}) \), i.e. subgroups of finite index but different from “congruence subgroups”, when \( \mathcal{O} \) is the ring of integers in an imaginary quadratic field \( \mathbb{Q} \langle \sqrt{-d} \rangle \) with \( d = 1, 2, 3, 7, 11, 5, 6, 16 \). In the first five cases, the field is euclidean and B. Fine [3] has given an explicit presentation for \( \text{PSL}(2, \mathcal{O}) \); in the remaining cases, we use the presentation given by Swan [11].

Our proof is based on the same ideas as of Drillick and perhaps a little simpler.

Let \( \text{SL}(2, \mathcal{O}) \) denote the group of 2-rowed matrices, with entries in \( \mathcal{O} \) and determinant 1, and \( \text{PSL}(2, \mathcal{O}) \) the group \( \langle \pm I \rangle \), where \( I \) is the 2-rowed identity matrix. For any ideal \( \mathfrak{q} \subset \mathcal{O} \), let \( \text{SL}(2, \mathcal{O}/\mathfrak{q}) \) denote the group of 2-rowed matrices, with entries in the quotient ring \( \mathcal{O}/\mathfrak{q} \) and determinant 1, and \( \text{PSL}(2, \mathcal{O}/\mathfrak{q}) \) the quotient group \( \langle \pm I \rangle \).
Let
\[ \Gamma(q) = \{ T \in \text{SL}(2, \mathbb{O}) \text{ such that } T = I \mod q \} \]
and
\[ \Gamma(q) = \{ T \in \text{SL}(2, \mathbb{O}) \text{ such that } T = \pm I \mod q \}. \]

Then \( \Gamma(q) \) is called the principal congruence subgroup modulo \( q \) in \( \text{SL}(2, \mathbb{O}) \). Any subgroup of \( \text{SL}(2, \mathbb{O}) \) containing \( \Gamma(q) \) for some ideal \( q \) of \( \mathbb{O} \) is called a congruence subgroup and is necessarily of finite index. Clearly
\[ \text{SL}(2, \mathbb{O})/\Gamma(q) \simeq \text{SL}(2, \mathbb{O}/q), \]
\[ \Gamma(q)/\langle \pm I \rangle \simeq \Gamma(q). \]

**Lemma 1.** Let \( p \) be any prime ideal of \( \mathbb{O} \) and \( t \) any natural number. Then the order of the group \( \Gamma(p^t)/\Gamma(p^t) \) is a power of \( p \) where \( p \) is the rational prime belonging to \( p \).

**Proof.** We know from [4] that \( \Gamma(q) \) has in \( \text{SL}(2, \mathbb{O}) \) the index given by
\[ [\text{SL}(2, \mathbb{O}):\Gamma(q)] = (Nq)^3 \prod_{p|q} \left(1 - \frac{1}{(Np)^t}\right) \]
where \( p \) runs over all prime ideals dividing \( q \) and \( Nq \) (respectively \( Np \)) denotes the order of \( \mathbb{O}/q \) (resp. \( \mathbb{O}/p \)). The homomorphism \( \gamma: \text{SL}(2, \mathbb{O}/p^t) \to \text{SL}(2, \mathbb{O}/p) \) induced by the natural map \( \mathbb{O}/p^t \to \mathbb{O}/p \) is surjective and the kernel is \( \Gamma(p^t)/\Gamma(p^t) \). Hence \( \Gamma(p^t)/\Gamma(p^t) \) has order \( (Np)^{t-3} \). We know that
\[ Np = \frac{p^2}{p} \text{ if } p \text{ is prime,} \]
\[ \frac{1}{p} \text{ otherwise.} \]
Thus \( \Gamma(p^t)/\Gamma(p^t) \) is a \( p \)-group.

**Lemma 2.** The alternating group \( A_n \), \( n \geq 7 \), is not isomorphic to any composition factor in a composition series for \( \text{SL}(2, \mathbb{O}/q) \).

**Proof.** Let \( q = q_1^{a_1} \cdots q_k^{a_k} \), where \( q_i \) are distinct prime ideals and \( a_i > 0 \) are integers for \( 1 \leq i \leq k \). As is well-known, \( \text{SL}(2, \mathbb{O}/q) \) is the direct product of \( \text{SL}(2, \mathbb{O}/q_i^{a_i}) \) for \( 1 \leq i \leq k \) and any composition factor in a composition series for \( \text{SL}(2, \mathbb{O}/q) \) is also a composition factor in a composition series for \( \text{SL}(2, \mathbb{O}/q_i^{a_i}) \) for some \( i, 1 \leq i \leq k \). Hence it is enough to prove the lemma when \( q = q_i^{a_i} \) a prime ideal of \( \mathbb{O}, t > 0 \) any integer.

**Case 1.** \( 2 \not| p \). Consider the normal series
\[ \text{SL}(2, \mathbb{O})/\Gamma(q^t) \supset \Gamma(q)/\Gamma(q^t) \supset \langle I \rangle. \]

In view of Lemma 1, \( \Gamma(p^t)/\Gamma(p^t) \) has order a power of 2, hence its composition factors are of order 2. Now
\[ \text{SL}(2, \mathbb{O})/\Gamma(p^t)/\Gamma(p^t) \simeq \text{SL}(2, \mathbb{O}/p) \]
and the order of \( \text{SL}(2, \mathbb{O}/p) \)
\[ = \begin{cases} 6 & \text{when } 2 \text{ splits in } \mathbb{O}, \\ 60 & \text{when } 2 \text{ remains prime.} \end{cases} \]

Hence \( A_n \), for \( n \geq 7 \), is not isomorphic to any composition factor.

**Case 2.** \( 2 \mid p \). Consider the normal series
\[ \text{SL}(2, \mathbb{O})/\Gamma(p^t) \supset \Gamma(p)/\Gamma(p^t) \supset \Gamma(p)/\Gamma(p) \supset \langle I \rangle. \]

In view of Lemma 1, \( \Gamma(p)/\Gamma(p^t) \) is a \( p \)-group. Hence its composition factors are all cyclic of order \( p \). Now
\[ \text{SL}(2, \mathbb{O})/\Gamma(p^t)/\Gamma(p)/\Gamma(p) \simeq \text{SL}(2, \mathbb{O}/p) \simeq \text{PSL}(2, \mathbb{O}/p). \]

When \( Np = 3 \), the order of \( \text{PSL}(2, \mathbb{O}/p) \) is 12; hence \( A_n \), \( n \geq 7 \), is not isomorphic to any composition factor. When \( Np > 3 \), \( \text{PSL}(2, \mathbb{O}/p) \) is simple and \( A_n \), \( n \geq 7 \), is not isomorphic to \( \text{PSL}(2, F) \), where \( F \) is a field with \( p \) or \( p^2 \) elements; in fact for a field \( F \) with \( q = p^t \) elements (and \( p \) a prime), it is well-known that the order of \( \text{PSL}(2, F) \) is \( q(q^2 - 1)/(q - 1) \) and \( n!(q^2 - 1) \) is impossible for \( p > t > 3 \) or \( t = 2, p > 5 \), or \( t = 1, p > 5 \). This completes the proof of the lemma.

**Lemma 3.** Let the symmetric group \( S_n \) or the alternating group \( A_n \) for some \( n \geq 7 \), be the quotient of \( \text{SL}(2, \mathbb{O}) \) by a subgroup \( K \). Then \( K \) is a non-congruence subgroup.

**Proof.** (i) Let, if possible, \( A_n \simeq \text{SL}(2, \mathbb{O}/K) \) for some \( n \geq 7 \), with \( K \supset \Gamma(q) \) for some ideal \( q \). Then any composition series for \( \text{SL}(2, \mathbb{O}/q) \) contains a factor isomorphic to \( A_n \) for some \( n \geq 7 \), which is a contradiction to Lemma 2.

(ii) Let, if possible, \( S_n \simeq \text{SL}(2, \mathbb{O}/K) \) for some \( q \) ideal \( q \) and for some \( n \geq 7 \). Then \( A_n \simeq H/K \), for a normal subgroup \( H \) of \( \text{SL}(2, \mathbb{O}) \). The normal series
\[ \text{SL}(2, \mathbb{O})/\Gamma(q) \supset H/\Gamma(q) \supset K/\Gamma(q) \supset \langle I \rangle \]
has a simple factor isomorphic to \( A_n \), for some \( n \geq 7 \), a contradiction to Lemma 2. Hence the kernel \( K \) is a non-congruence subgroup.

**Remark.** Even if we have a homomorphism \( \eta \) of a normal subgroup \( N \) of \( \text{SL}(2, \mathbb{O}) \) onto \( A_n \) or \( S_n \) for some \( n \geq 7 \), the kernel \( K \) of \( \eta \) is a non-congruence subgroup of \( \text{SL}(2, \mathbb{O}) \).

**Lemma 4.** If \( \text{SL}(2, \mathbb{O}) \) contains one non-congruence subgroup then it contains infinitely many such subgroups.

**Proof.** Let \( G \) be a non-congruence subgroup of \( \text{SL}(2, \mathbb{O}) \). Then \( G \cap \Gamma(q) \) for any ideal \( q \) of \( \mathbb{O} \) is of finite index in \( \text{SL}(2, \mathbb{O}) \) and is evidently a non-congruence subgroup. Let \( S \) be an infinite subset of the set of rational primes. For each \( p \) in \( S \), let \( p \) be a prime ideal in \( \mathbb{O} \) containing \( p \). We assert that \( G \cap \Gamma(p) \) are distinct for infinitely many \( p \)'s in \( S \). Let, if possible,
Theorem. Let \( d \) be the ring of integers of \( \mathbb{Q}(\sqrt{-d}) \), where \( d = 1, 2, 3, 7, 11, 15 \). Then \( \text{SL}(2, \mathbb{O}) \) contains infinitely many non-congruence subgroups.

Proof. In view of Lemma 1, it is enough to exhibit one non-congruence subgroup of \( \text{SL}(2, \mathbb{O}) \). For the construction of one such subgroup, we use an explicit presentation for \( \text{PSL}(2, \mathbb{O}) \) given in [3] and [11] for the \( d \)'s mentioned.

In the sequel, we mean by a product \( \sigma \cdot \sigma \) of two permutations \( \sigma_1, \sigma_2 \) on a symbols, the permutation obtained by applying \( \sigma_1 \) first and then \( \sigma_2 \).

We deal with the various \( d \)'s one by one, as follows.

**Case 1:** \( d = 1 \).

\[
\text{PSL}(2, \mathbb{O}) = \{ a, b, c, d; ab = (ab)^2 = (ba)^2 = (ab) \cdot (ba) = \text{identity} \}
\]

The map which sends \( a, b, c, d \) to \((14)(25)(67), (16)(24)(65), (17)(23)(56), (18)(25)(49)\) respectively clearly extends to a homomorphism of \( \text{PSL}(2, \mathbb{O}) \) into \( S_3 \). We assert that it is onto. In fact the image contains \((52), (5271346), (2i, (a la ta) \cdot (25), (w lu a) \cdot (5271346))\) and hence \( S_3 \), by [6], p. 49.

**Case 2:** \( d = 2 \).

\[
\text{PSL}(2, \mathbb{O}) = \{ a, b, c, d; ab = (ab)^2 = (ba)^2 = (ab) \cdot (ba) \cdot (ba) = \text{identity} \}
\]

Since for every \( n \geq 9 \), \( S_3 \) is generated by two elements \( a, b \) of order 2 and 3 respectively [1], it is a quotient of \( \text{PSL}(2, \mathbb{O}) \); a map \( \varphi \) with \( \varphi(a) = a, \varphi(b) = b \) and \( \varphi(ab) = b \) will do. Thus \( S_3 \), for every \( n \geq 9 \), is a quotient of \( \text{SL}(2, \mathbb{O}) \) and the kernel is a non-congruence subgroup.

**Case 3:** \( d = 3 \).

Let \( G^* \) be the commutator subgroup of \( \text{PSL}(2, \mathbb{O}) \). Then

\[
G^* = \{ j, m, t, u; j^2 = m^2 = t^2 = u^2 = (jtmu)^2 = (jtmu)^3 \}
\]

Let \( \varphi \) be the map which sends \( m, t, u, j \) to \((13)(24), (12)(34)(56), (17)(23)(56), (16)(24)(35)\) respectively. Since \( \varphi(j) = (14)(25)(67), \varphi(m)(\varphi(j) \varphi(u) = (147), \varphi(u)(\varphi(m) \varphi(j) = (175)(263), \varphi(m)(\varphi(t) = (14)(23)(56), \varphi \) extends to a homomorphism of \( G^* \) into \( S_3 \). Since \( \varphi(u) = (173)(42)(56), \varphi(u)^3 = (56). \) Also \( \varphi(\text{um}) \varphi(\text{um}) = (1364756). \) Hence \((56)(1364756) \in \varphi(G^*)\). Thus \( S_3 \) is a quotient group of \( G^* \) hence also of the commutator subgroup \( G \) of \( \text{SL}(2, \mathbb{O}) \). Since \( G \) is of finite index in \( \text{SL}(2, \mathbb{O}) \), we get a non-congruence subgroup of \( \text{SL}(2, \mathbb{O}) \), by the Remark following Lemma 3.

**Case 4:** \( d = 7 \).

\[
\text{PSL}(2, \mathbb{O}) = \{ a, b, c, d; ab = (ab)^2 = (ba)^2 = (ab) \cdot (ba) \cdot (ba) = \text{identity} \}
\]

If we set \( \varphi(a) = (12)(34)(56), \varphi(b) = (15)(19)(27)(63), \varphi(c) = (12)(34)(56) \) then clearly \( \varphi(a) \varphi(b) = \varphi(c) \varphi(b) = \varphi(a) \varphi(b) \varphi(c) = (15)(19)(27)(63) \) and \( \varphi(c) = (12)(34)(56) \) \times \( \varphi(b) \varphi(c) = (15)(19)(27)(63) \); hence \( \varphi \) extends to a homomorphism of \( \text{PSL}(2, \mathbb{O}) \) into \( S_3 \). We show that \( \varphi \) is surjective as follows. In fact,

\[
\]

\[
(15)(19)(27)(63) = (15)(19)(27)(63),
\]

hence

\[
(15)(19)(27)(63)^2 = (15)(19)(27)(63) \in \varphi \text{SL}(2, \mathbb{O})
\]

Also

\[
(15)(19)(27)(63) = (15)(19)(27)(63),
\]

\[
(15)(19)(27)(63) = (15)(19)(27)(63),
\]

\[
(15)(19)(27)(63) = (15)(19)(27)(63),
\]

\[
(15)(19)(27)(63) = (15)(19)(27)(63),
\]

Since \((56) \) and \((369182754) \) generate \( S_3 \), \( \varphi \text{SL}(2, \mathbb{O}) = S_3 \). Hence it follows that \( S_3 \) is a quotient group of \( \text{SL}(2, \mathbb{O}) \) and the kernel is a non-congruence subgroup by Lemma 3.

**Case 5:** \( d = 9 \).

\[
\text{PSL}(2, \mathbb{O}) = \{ a, b, c, d; ab = (ab)^2 = (ba)^2 = (ab) \cdot (ba) \cdot (ba) = \text{identity} \}
\]

The map which sends \( a, b, c, d \) to \((13)(24), (12)(34)(56), (17)(23)(56), (18)(25)(49)\) respectively extends to a homomorphism of \( \text{PSL}(2, \mathbb{O}) \) into \( S_3 \). Further, \((12)(34)(56)(78)(3678) = (125)(347), (265)(347)(1245) = (125)(347) \) and hence

\[
(125)(347)^2 = (125)(347),
\]

From \((125)(347) = (16)(245), \) we have

\[
(16)(245)^2 = (16)(245),
\]

Moreover,

\[
(16)(245)^3 = (16)(245),
\]

and so

\[
(16)(245)^3 = (16)(245),
\]
Since (16) and (16842357) generate $S$, $\varphi(\text{PSL}(2, \omega)) = S$, hence $S$ is also a quotient group of $\text{SL}(2, \omega)$ and the kernel is a non-congruence subgroup.

$d = 5$.

$$\text{PSL}(2, \omega) = \{T, U, A, B, C; TU = UT, A^2 = B^2 = (TA)^3 = (AB)^3 = (AUBU^{-1})^3 = \text{identity}; ACA = TCT^{-1}, UBU^{-1}CB = TCT^{-1} \}.$$  

Since $S_n$, for any $n \geq 9$, is generated by two elements $\alpha, \beta$ of order 2 and 3 respectively, the map $\varphi$ with $\varphi(\alpha) = \varphi(B) = \varphi(U) = \varphi(C) = \text{identity}, \varphi(\alpha \beta) = \varphi(\beta \alpha)$, $\varphi(T) = \beta \alpha$ extends to a homomorphism of $\text{PSL}(2, \omega)$ onto $S_n$, for $n \geq 9$. Hence $S_n$, for $n \geq 9$, are quotients of $\text{SL}(2, \omega)$ and the kernels are non-congruence subgroups. Thus for all the rings $\omega$, mentioned in the theorem, $\text{SL}(2, \omega)$ contains infinitely many non-congruence subgroups (in view of Lemma 4) and the proof of the theorem is complete.

References


Centre of Advanced Study in Mathematics
University of Bombay

Received on 29th March 1976