Bollettino
Unione Matematica Italiana

Marilena Massa

The Probabilistic Zeta Function of the Alternating Group $\mathrm{Alt}(p+1)$

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **10-B** (2007), n.3, p. 581–591.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2007_8_10B_3_581_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2007.

Bollettino U. M. I.
(8) **10**-B (2007), 581-591

The Probabilistic Zeta Function of the Alternating Group $\mathrm{Alt}(p+1)$.

MARILENA MASSA

Sunto. – *Si studia l'irriducibilità del polinomio di Dirichlet $P_G(s)$ nel caso in cui G sia il gruppo alterno di grado $p+1$, con p primo, e si prova che $P_G(s)$ è irriducibile per infinite scelte di p.*

Summary. – *We study the irreducibility of the Dirichlet polynomial $P_G(s)$ when G is the alternating group on $p+1$ elements with p prime and we prove that $P_G(s)$ is irreducible for infinitely many choiches of p.*

1. – Introduction.

Let G be a finite group; if $t \in \mathbb{N}$, then $\Phi_G(t)$ is the number of ordered t-uples of elements of G that generate G. Φ_G is called the Eulerian function of the finite group G and it satisfies the following equality proved by Hall (see [6]):

$$\Phi_G(t) = \sum_{1 \leq H \leq G} \mu_G(H)|H|^t. \tag{1}$$

μ_G is called the Möbius function of the subgroup lattice of G and it is defined inductively in this way: $\mu_G(G) = 1$ and $\sum_{H \leq K \leq G} \mu_G(K) = 0$ if $H < G$.

Note that the probability that a random t-uple generates G is given by

$$\mathrm{Prob}_G(t) = \frac{\Phi_G(t)}{|G|^t}. \tag{2}$$

By (1), we may write

$$\mathrm{Prob}_G(t) = \sum_{1 \leq H \leq G} \frac{\mu_G(H)}{|G:H|^t} \tag{3}$$

This means that it is possible to define a complex function $P_G(s)$, with the property that $P_G(t) = \mathrm{Prob}_G(t)$ for any $t \in \mathbb{N}$, by associating a Dirichlet poly-

nomial with G as follows:

$$P_G(s) = \sum_{n=1}^{\infty} \frac{a_n(G)}{n^s} \qquad \text{with} \qquad a_n(G) = \sum_{|G:H|=n} \mu_G(H). \tag{4}$$

Note that $a_n(G) \neq 0$ implies that n divides $|G|$.

The inverse complex function of $P_G(s)$ is usually called the probabilistic zeta function of G (see Mann [8], Boston [2] and Shareshian [10]).

The ring of Dirichlet polynomials with integer coefficients R is a factorial domain and so we ask whether it is possible to obtain information on the structure of the group G from the factorization of $P_G(s)$ in R. An important role in the factorization of $P_G(s)$ is played by the normal subgroups of G. In fact, for any $N \trianglelefteq G$, the polynomial $P_{G/N}(s)$ divides $P_G(s)$ (see [3], Section 2.2) and this allows to write $P_G(s)$ as a product of Dirichlet polynomials corresponding to the factors in a chief series of G. A relevant question is whether it is possibile to reconstruct these polynomials from the factorization into irreducible elements of $P_G(s)$ and, hopefully, to recognize with this method the isomorphism type of the chief factors. In this context, it is important to understand whether there exist factorizations of $P_G(s)$ which do not come from normal subgroups and how they eventually look like. In particular, this lead Boston [2] to ask whether it is true that $P_G(s)$ is an irreducible Dirichlet polynomial when G is a simple group. This is not true in general: if $p = 2^t - 1$ is a Mersenne prime with $t \equiv 3 \pmod 4$, then $P_{PSL(2,p)}(s)$ is reducible [4]. No other counterexample is known and the feeling is that $P_G(s)$ is irreducible for many classes of simple groups. For example in [4] it is proved that $P_{\mathrm{Alt}(p)}(s)$ is irreducible if $p \geq 5$ is a prime number. It is interesting to discuss the irreducibility of $P_{\mathrm{Alt}(n)}(s)$, for other choices of n. The key remark in discussing the case $n = p$ is that the irreducible factors of $P_G(s)$ must divide also $P_G^{(p)}(s) = \sum_r a_{p^r}(G)/p^{rs}$. This remains true for arbitrary values of n, by taking p to be the largest prime with $p \leq n$; the problem is that if the gap $n - p$ is a large number, then $P_G^{(p)}(s)$ is too complicated to be really of help (for example it is not in general irreducible as in the case $p = n$). So in this paper we study as a test example the case $n - p = 1$: in this case $P_G^{(p)}(s)$ turns out to be the product of two irreducible polynomials and this makes the problem more difficult to be discussed and give more hints on which difficulties one meets when dealing with the general case. The indication that comes from this analysis is that the classification of maximal subgroups of the alternating group allows in general to compute $P_G^{(p)}(s)$ quite easily, but even when the gap $n - p$ is small, it is difficult to control the divisibility of $P_G(s)$ by the irreducible factors of $P_G^{(p)}(s)$; several number theoretical results related to the prime factorization of the binomial coefficients $\binom{n}{i}$ for $p \leq i \leq n$ are needed. Using information of this kind we prove that $P_{\mathrm{Alt}(p+1)}(s)$ is irreducible for infinitely many choices of the prime p.

2. – Preliminaries.

DEFINITION 1. – *A Dirichlet polynomial with integer coefficients is a series of the form*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad s \in \mathbb{C}$$

with these properties: $a_n \in \mathbb{Z}\ \forall n \geq 1$ *and* $|\{n : a_n \neq 0\}| < \infty$.

Let R be the ring of Dirichlet polynomials with integer coefficients. Let Π be the set of all prime numbers; we associate an indeterminate x_p with any $p \in \Pi$. Let X_Π be the set of all these indeterminates. The map which sends $1/p^s$ to x_p gives rise to a ring isomorphism between R and $\mathbb{Z}[X_\Pi]$. In particular, this implies that R is a unique factorial domain and it is possible to translate well-known facts about polynomial rings as results on Dirichlet polynomials.

LEMMA 1 (see [4] Lemma 3). – *Let* $n \in \mathbb{N}$ *with* $n > 1$. *Then* $\left(1 - \frac{n}{n^s}\right)$ *is reducible in* R *if and only if* n *is a power in* $\mathbb{Z}$.

Let π be the set of all prime numbers. Note that we may define a ring endomorphism of R as follows:

$$\begin{array}{rccc} \varphi_\pi : & R & \longrightarrow & R \\ & f(s) = \displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s} & \longmapsto & f^{(\pi)}(s) = \displaystyle\sum_{n=1}^{\infty} \frac{b_n}{n^s} \end{array}$$

where

$$b_n = \begin{cases} 0 & \text{if } \exists\ p \in \pi \text{ prime s.t. } p \text{ divides } n \\ a_n & \text{otherwise} \end{cases}$$

3. – The alternating groups $\mathrm{Alt}\,(p+1)$ with p prime.

Let Λ be the set of $n \in \mathbb{N}$ such that $n - 1 = p$ is a prime number, n is not a power and $n \notin \{6, 12, 24\}$. The exceptional cases $n = 6$, $n = 12$ and $n = 24$ will be discussed at the end of the paper.

LEMMA 2. – *If* $n \in \Lambda$ *and* $G = \mathrm{Alt}\,(n)$ *then*

$$P_G^{(p)}(s) = \left(1 - \frac{(p+1)}{(p+1)^s}\right)\left(1 - \frac{(p-2)!}{(p-2)!^s}\right).$$

PROOF. – The series $P_G^{(p)}(s)$ depends only on the subgroups H of G such that $\mu_G(H) \neq 0$ and $(|G:H|, p) = 1$. As was noticed by Hall in [6], if $\mu_G(H) \neq 0$, then H is an intersection of maximal subgroups. So we need to study the maximal subgroups of G containing a Sylow p-subgroup of G.

Obviously, the intransitive maximal subgroups of G with index coprime with p are point-stabilizers. On the other hand, if M is a transitive maximal subgroup of G containing a p-cycle then M is a 2-transitive group. By the classification of 2-transitive groups and the hypothesis on n we deduce that $M \cong PSL(2,p)$. Let us consider the subgroups of G that are intersections of the maximal subgroups of G with index coprime with p and let us see which among these have the same property. First of all observe that the subgroups obtained as intersection of two stabilizers in G of two distinct points of $\Omega = \{1, \ldots, n\}$ cannot contain a cycle of length p, therefore a cyclic subgroup of order p. On the other hand, if we intersect two subgroups of G isomorphic to $PSL(2,p)$, the resulting subgroup will not contain a cyclic subgroup of order p: all the maximal subgroups of G isomorphic to $PSL(2,p)$ are conjugated, hence, given $P \in \mathrm{Syl}(G)$, there exists a unique subgroup $H \cong PSL(2,p)$ with $P \leq H$. Moreover, given $P \in \mathrm{Syl}(G)$, there exists a unique $\omega \in \Omega$ such that $P \leq G_\omega$; furthermore $H \cap G_\omega = H_\omega = N_G(P)$.

If H is a subgroup of G with $\mu_G(H) \neq 0$ and $(|G:H|, p) = 1$, then one of the following holds:

- $H = G_\omega$, $\omega \in \Omega$, is a point-stabilizer, $\mu_G(H) = -1$ and $|G:H| = p+1$. Note that there are $p+1$ subgroups of this type.
- $H \cong PSL(2,p)$. $PSL(2,p)$ is maximal in G and all the subgroups of G isomorphic to $PSL(2,p)$ are conjugated, hence there exist $(p-2)!$ subgroups $H \cong PSL(2,p)$ and such that $|G:H| = (p-2)!$. Moreover these subgroups have Möbius equal to -1.
- $H = H_\omega$, obtained as intersection of a point-stabilizer and a subgroup H isomorphic to $PSL(2,p)$. We observe that there exists a bijection among the subgroups H_ω and the Sylow p-subgroups of G and so G has $(p+1)(p-2)!$ subgroups H_ω. Moreover, $|G:H_\omega| = (p+1)(p-2)!$ and $\mu_G(H_\omega) = 1$.
  We deduce that:

$$P_G^{(p)}(s) = 1 - \frac{(p+1)}{(p+1)^s} - \frac{(p-2)!}{((p-2)!)^s} + \frac{(p+1)(p-2)!}{((p+1)(p-2)!)^s}$$

$$= \left(1 - \frac{(p+1)}{(p+1)^s}\right)\left(1 - \frac{(p-2)!}{(p-2)!^s}\right) \qquad \square$$

LEMMA 3. – *Let $n \in \Lambda$ and $G = \mathrm{Alt}(n)$. $P_G(s)$ is irreducible if $1 - \dfrac{(p-2)!}{(p-2)!^s}$ and $1 - \dfrac{(p+1)}{(p+1)^s}$ do not divide $P_G(s)$.*

PROOF. – Let $R^{(p)} = \{\sum_r b_r/r^s \mid b_r = 0 \text{ if } p \text{ divides } r\}$. Since p^2 does not divide $|G|$, there exists $Q(s) \in R^{(p)}$ such that

$$P_G(s) = P_G^{(p)}(s) + \frac{1}{p^s}Q(s).$$

Assume that $P_G(s) = A(s)B(s)$ is a non trivial factorization: we may assume $A(s) \in R^{(p)}$; in particular $A(s)$ must be a common divisor of $P_G^{(p)}(s)$ and $Q(s)$. By the previous lemma

$$P_G^{(p)}(s) = \left(1 - \frac{(p+1)}{(p+1)^s}\right)\left(1 - \frac{(p-2)!}{(p-2)!^s}\right)$$

and, by Lemma 1, $1 - \dfrac{(p+1)}{(p+1)^s}$ and $1 - \dfrac{(p-2)!}{(p-2)!^s}$ are irreducible because $(p+1)$ and $(p-2)!$ are not powers (to see that $(p-2)!$ is not a power in $\mathbb{Z}$ it is sufficient to note that, by [7] Theorem 418, there exists a prime q such that $\dfrac{n}{2} < q \leq (p-2)$). Hence $A(s)$ coincides either with $1 - \dfrac{(p-2)!}{(p-2)!^s}$ or with $1 - \dfrac{(p+1)}{(p+1)^s}$. □

First of all we will prove that $1 - \dfrac{(p-2)!}{(p-2)!^s}$ does not divide $P_G(s)$.

LEMMA 4. – *If $n \in \Lambda$ and $G = \mathrm{Alt}(n)$ then, when $m = \binom{n}{4}$, we have $a_m(G) = -m$.*

Before the proof of the lemma, it is useful to recall this theorem.

THEOREM 1 (see [5] Theorem 5.2). – *Let $G = \mathrm{Alt}(\Omega)$ with $\Omega = \{1, \ldots, n\}$ and let K be a subgroup of G.*

Let $n \geq 10$ and $r \leq \dfrac{n}{2}$. Suppose that $1 < |G : K| < \binom{n}{r}$.

Then one of the following conditions holds:

(a) *there exists $\Delta \subseteq \Omega$ with $|\Delta| < r$ such that $G_{(\Delta)} \subseteq K \subseteq G_{\{\Delta\}}$, where*
$G_{\{\Delta\}} = (\mathrm{Sym}(\Delta) \times \mathrm{Sym}(\Omega - \Delta)) \cap \mathrm{Alt}(\Omega) = \{g \in G | \Delta^g = \Delta\}$
$G_{(\Delta)} = (\mathrm{Sym}(\Omega - \Delta)) \cap \mathrm{Alt}(\Omega) = \mathrm{Alt}(\Omega - \Delta) = \{g \in G | \delta^g = \delta \quad \forall \delta \in \Delta\}$;

(b) *$n = 2m$ and $|G : K| = \dfrac{1}{2}\binom{n}{m}$.*

Now the proof of the lemma.

PROOF. – Let $m = \binom{n}{4}$ and $K \cong (\mathrm{Sym}(4) \times \mathrm{Sym}(n-4)) \cap G$. Then $|G : K| = m$. Now, we prove that all the subgroups of G that have index equal to $\binom{n}{4}$ are of type $(\mathrm{Sym}(4) \times \mathrm{Sym}(n-4)) \cap G$.

Let K be a subgroup of G of index $m = \binom{n}{4}$. We apply the Theorem 1 with $r = 5$. Furthermore, because of our choices of n, the condition (b) of the theorem is never satisfied. Hence:

1. if $|\Delta| = 4$ then $G_{\{\Delta\}} = (\mathrm{Sym}(4) \times \mathrm{Sym}(n-4)) \cap G$ and $G_{(\Delta)} \subseteq K \subseteq G_{\{\Delta\}}$. We deduce that $K = G_{\{\Delta\}} = (\mathrm{Sym}(4) \times \mathrm{Sym}(n-4)) \cap G$.
2. if $i = |\Delta| \leq 3$ it is not difficult to see that $\binom{n}{4}$ divides $\dfrac{n!}{(n-i)!}$, which is impossible.

Therefore, we can conclude that the only subgroups of G of index equal to $\binom{n}{4}$ are the subgroups of type $K = (\mathrm{Sym}(4) \times \mathrm{Sym}(n-4)) \cap G$. These subgroups are maximal and so they have Möbius equal to -1. The distinct subgroups of G of type $K = (\mathrm{Sym}(4) \times \mathrm{Sym}(n-4)) \cap G$ are $m = \binom{n}{4}$, the number of distinct subsets with 4 elements in a set with n elements. By definition of $a_m(G)$, we deduce that $a_m(G) = -m$. □

THEOREM 2. – *Let $G = \mathrm{Alt}(n)$ with $n \in \Lambda$, then $P_G(s)$ is not divisible by $1 - \dfrac{(p-2)!}{(p-2)!^s}$.*

PROOF. – Let $(p-2)! = m$, $P_G(s) = \displaystyle\sum_{r \in \mathbb{N}} \frac{a_r}{r^s}$ and $r^* = \binom{n}{4}$. Assume by contradiction that $P_G(s)$ is divisible by $\left(1 - \dfrac{m}{m^s}\right)$. Then $P_G(s) = \left(1 - \dfrac{m}{m^s}\right) Q(s)$ where $Q(s) = \displaystyle\sum_{r \in \mathbb{N}} \frac{b_r}{r^s}$, from which $P_G(s) = \displaystyle\sum_{r \in \mathbb{N}} \frac{b_r}{r^s} - \sum_{r \in \mathbb{N}} \frac{b_r m}{(rm)^s}$. It is not difficult to see that the quantity $m = (p-2)! = (n-3)!$ does not divide $\binom{n}{4} = r^*$. Hence $a_{r^*} = b_{r^*}$. By Lemma 4, $a_{r^*} \neq 0$ and so $b_{r^*} \neq 0$. Furthermore, there exists t maximal with the property $b_t \neq 0$ and r^* divides t. By definition of t, $b_{mt} = 0$ and so $\dfrac{a_{mt}}{(mt)^s} = \dfrac{b_{mt}}{(mt)^s} - \dfrac{b_t m}{(mt)^s} = -\dfrac{b_t m}{(mt)^s}$. By $b_t \neq 0$, it follows that $a_{mt} \neq 0$. Then mt divides $|G| = \dfrac{n!}{2}$. In particular, mr^* divides $\dfrac{n!}{2}$. Therefore, $(p-2)$ divides 12, but this is impossible, hence the thesis. □

Now, we shall show that $\left(1 - \dfrac{n}{n^s}\right)$ does not divide $P_G(s)$ for infinitely many choices of $n \in \Lambda$.

Let π be the set of prime numbers smaller than p and that do not divide n and let q be the largest prime smaller than p. In addition, let be $A(s) = \left(1 - \dfrac{n}{n^s}\right)$ and $C(s) = P_G^{(\pi)}(s)$.

We want to prove that $A(s)$ does not divide $P_G(s)$ for infinitely many choices of $n \in \Lambda$. In order to do this, it is sufficient to show that $A(s)$ does not divide $C(s)$ for infinitely many choices of $n \in \Lambda$.

First of all, note that $\frac{n}{2} < q < n-1 = p$ (see [7] Theorem 418). By [5] Theorem 3.3E, G does not have transitive maximal subgroups with index coprime with q; hence, the maximal subgroups H of G that have index coprime with q are of the type $(\mathrm{Sym}(r) \times \mathrm{Sym}(s)) \cap G$ where $r+s=n$ and $r \geq q$.

Therefore, being $q \in \pi$, the maximal subgroups of G that give a non-zero contribution to $C(s)$ must have index of the type $\binom{n}{i}$ with $0 < i < n/2$. In order to handle these subgroups, we need the following two results.

LEMMA 5. – *Let a and b be two positive integers and let k be a prime*

1. *if $\binom{a}{b} = k^t r$ with $(k,r)=1$ then $k^t \leq a$.*
2. *if $a = \sum_{i=0}^{s} c_i k^i$ and $b = \sum_{i=0}^{s} d_i k^i$ with $0 \leq c_i, d_i \leq (k-1)$, then k does not divide $\binom{a}{b}$ if and only if $0 \leq d_i \leq c_i \leq (k-1)$ for each i.*

The lemma is a consequence of a well known theorem of Kummer (see [9] as reference).

THEOREM 3 (see [1] Section 4). – *For any positive integer m, let $\Omega(m)$ be the number of the primes that occur in the factorization of m. There exist infinite primes p such that $\Omega(p^2-1) \leq 21$. More precisely, for any $m \in \mathbb{R}$, let $A_m = \{p \in \mathbb{N} : p \text{ prime}, p \leq m \text{ and } \Omega(p^2-1) \leq 21\}$. If m is large enough, then*

$$|A_m| \geq\geq \frac{m}{log^3 m}$$

REMARK 1. – Let $A_m^* = \{p \in A_m : p+1 \text{ is not a power}\}$. It can be easily proved that any prime $p \in A_m - A_m^*$ is a Mersenne prime, i.e $p = 2^a - 1$ with $a \in \mathbb{N}_0$; with a quick computation we get that $|A_m - A_m^*| \leq log_2(m+1)$. Therefore, $|A_m^*|$ satisfies asymptotically the same lower bound as $|A_m|$.

THEOREM 4. – *There exist infinitely many choices of $n \in \Lambda$ that satisfy the following property: if $\binom{n}{i}$ is a π'-number and $0 < i < n/2$, then $i = 1$ or $i = 2$.*

PROOF. – Let $\Lambda_1 = \{n = p+1 \in \Lambda \mid \Omega(p^2-1) \leq 21\}$. There exists υ in $\mathbb{N}$ such that if $n \in \Lambda_1$ then the following property holds: if $\binom{n}{i}$, for $0 < i < n/2$, is a π'-number then $i \leq \upsilon$. In fact, since $\binom{n}{i}$ is a π'-number, whenever $0 < i < n/2$, it follows that

$$\binom{n}{i} = p_1^{a_1} \dots p_t^{a_t} \qquad \text{with} \qquad p_i \notin \pi$$

By definition of π, the condition $p_i \notin \pi$ implies that $p_i = p$ or p_i divides $(p+1)$ and, so, (p^2-1), from which it must be $t \leq 22$. By the Lemma 5, $p_i^{a_i} \leq n$ for any i. Therefore,

$$\binom{n}{i} \leq n^{22}$$

and this implies $i \leq \upsilon$ for a suitable υ, independently of the choice of n.

Now, let Λ_2 be the set of $n \in \Lambda_1$ such that $(p-1)$ is divisible by an odd prime power larger than υ. Assume $n \in \Lambda_2$ and denote with r^t the largest odd prime power that divides $(p-1)$; let $0 < i < n/2$ with $\binom{n}{i}$ a π'-number. In particular, since $r \in \pi$ we get that r does not divide $\binom{n}{i}$; then, from the Lemma 5, it follows that we can write $n = 2 + r^t(a_0 + a_1 r + \dots)$ and $i = x + r^t y$ with $x \in \{0,1,2\}$ and $y \geq 0$. If $y = 0$ then $i = 1$ or $i = 2$ and if $y > 0$ then $i \geq r^t$ and, so, $i > \upsilon$, but this second possibility is in contradiction with the hypothesis $\binom{n}{i}$ π'-number. Therefore, we have proved that the elements of Λ_2 satisfy the condition required by the theorem.

In order to prove the theorem, it is sufficient to verify that Λ_2 is infinite, i.e. the number a_m of the primes p such that $p \leq m$, with m real number, and $p+1 = n \in \Lambda_2$ goes to infinite when m goes to infinite. First of all, note that if p is a prime such that $p \leq m$, then $p+1 = n \in \Lambda_2$ if and only if $p \in A_m^*$ and the largest odd prime power that divides $(p-1)$ is greater than υ. Now, we give a bound of the number β_m of the primes $p \in A_m^*$ and such that the largest odd prime power that divides $(p-1)$ is smaller than υ. In this case, $(p-1) = ab$ where a is an odd divisor of $\upsilon!$ and b is a 2-power smaller than m. The possibilities for a are finitely many and the possible choices for b are at most $\log_2 m$. It follows that $\beta_m \leq c \log m$ with c a constant and, so, for m sufficiently large,

$$a_m \geq |A_m^*| - \beta_m \geq\geq \frac{m}{\log^3 m} - c \log m.$$

Therefore, a_m goes to infinite while m increases. □

THEOREM 5. – *For infinitely many choices of $n \in \Lambda$, we get that $\left(1 - \frac{n}{n^s}\right)$ does not divide the series $C(s)$.*

PROOF. – From the previous theorem we deduce that there exist infinitely many choices of $n \in \Lambda$ such that $\binom{n}{i}$ is a π'-number and $0 < i < n/2$ if and only if $i = 1$ o $i = 2$. Write down the series $C(s)$ for these n. The maximal subgroups of G that give a contribution to this series are those that have index $\binom{n}{1}$ and $\binom{n}{2}$. There are exactly $\binom{n}{1}$ subgroups of index $\binom{n}{1}$ and $\binom{n}{2}$ subgroups of index $\binom{n}{2}$. Moreover, these subgroups have Möbius equal to -1. In order to complete the computation of the series $C(s)$, we need the intersections of these maximal subgroups.

The subgroups that can be obtained as intersection of maximal intransitive

subgroups are of the kind $(\mathrm{Sym}(n_1)\times\cdots\times\mathrm{Sym}(n_r))\cap G$ and have index of the type $\binom{n}{n_1\ \dots\ n_r}$ with $n_1+\ldots+n_r=n$. Furthermore, among these, only that ones have index a π'-number can give contribution to the series $C(s)$. Hence, all the maximal subgroups that contain them must have index a π'-number. It follows that the subgroups H of G that satisfy these conditions are of the type $(\mathrm{Sym}(n-2)\times\mathrm{Sym}(1)\times\mathrm{Sym}(1))\cap G$. They satisfy the following properties: $\mu_G(H)=2$, $|G:H|=n(n-1)$ and they are exactly $n(n-1)/2$.
From what written above, we may write down explicitly the series $C(s)$.

$$C(s)=P_G^{(\pi)}(s)=1-\frac{n}{n^s}-\frac{\binom{n}{2}}{\binom{n}{2}^s}+\frac{n(n-1)}{(n(n-1))^s}$$

Now, we study the divisibility of this series by $\left(1-\frac{n}{n^s}\right)$. If this series is divisible by $\left(1-\frac{n}{n^s}\right)$ then also $-\frac{\binom{n}{2}}{\binom{n}{2}^s}+\frac{n(n-1)}{(n(n-1))^s}=-\frac{\binom{n}{2}}{\binom{n}{2}^s}\left(1-\frac{2}{2^s}\right)$ will be divisible by $\left(1-\frac{n}{n^s}\right)$, which is impossible. □

So we have proved the following

THEOREM 6. – *For infinitely many choices of $n\in\mathcal{A}$, if $G=\mathrm{Alt}(n)$ then $P_G(s)$ is irreducible.*

Now let us analyze the cases excluded before, i.e. the cases for which $n\in\{6,12,24\}$.

• $G=\mathrm{Alt}(6)$

In this case

$$P_G(s)=1-\frac{12}{6^s}-\frac{10}{10^s}-\frac{30}{15^s}+\frac{60}{30^s}+\frac{36}{36^s}+\frac{45}{45^s}+\frac{240}{60^s}+\frac{90}{90^s}-\frac{240}{120^s}-\frac{900}{180^s}+\frac{720}{360^s}$$

If $P_G(s)$ is reducible then $P_G(s)$ will be divisible by $P_G^{(5)}(s)=1-\frac{12}{6^s}+\frac{36}{36^s}$. So

$$P_G(s)=P_G^{(5)}(s)Q(s)$$

and, in particular,

$$P_G(-1)=P_G^{(5)}(-1)Q(-1)$$

but this is impossible because $P_G^{(5)}(-1)=1225$ does not divide $P_G(-1)=360\cdot 265$.

• $G=\mathrm{Alt}(12)$

The difference with respect to the general case is that the transitive subgroups isomorphic to $PSL(2,11)$ are not maximal; they are contained in maximal

subgroups isomorphic to M_{12}. As a consequence, the series $P_G^{(11)}(s)$ is more complicated; namely:

$$P_G^{(11)}(s) = 1 - \frac{12}{12^s} - \frac{5040}{2520^s} + \frac{60480}{30240^s} + \frac{362880}{362880^s} - \frac{4354560}{4354560^s}$$

from which

$$P_G^{(11)}(s) = \left(1 - \frac{12}{12^s}\right)\left(1 - \frac{5040}{2520^s} + \frac{362880}{362880^s}\right)$$

The two series in the factorization of $P_G^{(11)}(s)$ are both irreducible and, therefore, to prove that $P_G(s)$ is irreducible it is sufficient to show that the two series do not divide it. In order to see that $B(s) = 1 - \frac{5040}{2520^s} + \frac{362880}{362880^s}$ does not divide $P_G(s)$, we can use a technique similar to that used in the proof of the Theorem 2: if we put $r^* = \binom{12}{5}$ then $a_{r^*} = -r^* \neq 0$ and, if $B(s)$ divides $P_G(s)$, then $|G|$ will be divisible by mr^* where $m = 362880$, which is impossible. In order to see that $A(s) = 1 - \frac{12}{12^s}$ does not divide $P_G(s)$, it is sufficient to prove that it does not divide $P_G^{(\pi)}(s)$ where $\pi = \{5, 7\}$, i.e. $P_G^{(\pi)}(s) = 1 - \frac{12}{12^s} - \frac{66}{66^s} + \frac{132}{132^s} - \frac{792}{792^s}$.

• $G = \mathrm{Alt}\,(24)$

The subgroups isomorphic to $PSL(2, 23)$ are contained in maximal transitive subgroups isomorphic to M_{24} and we can not argue as in the general case. First of all, note that if $\pi_1 = \{13, 23\}$ then $P_G^{(\pi_1)}(s) = 1 - \frac{24}{24^s}$. In addition, $P_G^{(\pi_1)}(s)$ cannot divide $P_G(s)$ (it is sufficient to see that $1 - \frac{24}{24^s}$ does not divide $P_G^{(\pi_2)}(s) = 1 - \frac{24}{24^s} - \frac{12 \cdot 23}{(12 \cdot 23)^s} + \frac{23 \cdot 24}{(23 \cdot 24)^s}$ where $\pi_2 = \{11, 19\}$). Now, let $x = \frac{1}{23^s}$ and $y = \frac{1}{13^s}$. The series $P_G(s)$ is of the type $a_0 + a_1 x + a_2 y + a_3 xy$ where $a_0 = 1 - \frac{24}{24^s}$ and a_1, a_2, a_3 are Dirichlet series that do not involve terms divisible by 13 or 23. Note that a_0 is irreducible and since it does not divide $P_G(s)$ it is possible to factorize $P_G(s)$ only in this two ways: $(a_0 + bx)(1 + cy)$ or $(1 + bx)(a_0 + cy)$. But these two ways cannot occur. In fact, consider, for example, the first way of factorization: let $bx = \sum_n \frac{\beta_n}{n^s}$ and $cy = \sum_n \frac{\gamma_n}{n^s}$. Consider $m_1 = \frac{24!}{13!}$, it is easy to see that $\mathrm{Alt}\,(13)$ is a subgroup of $\mathrm{Alt}\,(24)$ such that $\mu_{\mathrm{Alt}\,(24)}\mathrm{Alt}\,(13) \neq 0$ and that all the subgroups H of $\mathrm{Alt}\,(24)$ with this index and such that $\mu_{\mathrm{Alt}\,(24)}(H) \neq 0$ are conjugated to $\mathrm{Alt}\,(13)$; this implies $a_{m_1}(G) \neq 0$ and so, since m_1 is divisible by 23 but not by 13, it must be $\beta_{m_1} \neq 0$; analogously, if $m_2 = |G : M_{24}|$, then $\gamma_{m_2} \neq 0$. Then there exists $n \geq m_1 m_2$ with $a_n(G) \neq 0$, and this implies $2m_1 m_2 \leq 24!$, false.

REFERENCES

[1] K. Alladi - R. Solomon - A. Turull, *Finite simple groups of bounded subgroup chain length*, J. Algebra, **231** (2000), 374-386.

[2] Nigel Boston, *A probabilistic generalization of the Riemann zeta function*, Analytic number theory, Vol. 1 (Allerton Park, IL, 1995) **138** (1996), 155-162.

[3] KENNETH S. BROWN, *The coset poset and probabilistic zeta function of a finite group*, J. Algebra, **225**, no. 2 (2000), 989-1012.
[4] ERIKA DAMIAN - ANDREA LUCCHINI - FIORENZA MORINI, *Some properties of the probabilistic zeta function of finite simple groups*, Pacific J. Math., **215** (2004), 3-14.
[5] JOHN D. DIXON - BRIAN MORTIMER, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.
[6] PHILIP HALL, *The eulerian functions of a group*, Quart. J. Math., no. 7 (1936), 134-151.
[7] G. H. HARDY - E. M. WRIGHT, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.
[8] AVINOAM MANN, *Positively finitely generated groups*, Forum Math. 8, no. 4 (1996), 429-459.
[9] P. RIBENBOIM, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1989, 23-24.
[10] JOHN SHARESHIAN, *On the probabilistic zeta function for finite groups*, J. Algebra **210**, no. 2 (1998), 703-707.

Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano Bicocca
Via Cozzi 53, 20125 Milano
E-mail: marilena.massa@unimib.it

Pervenuta in Redazione
il 21 gennaio 2006 e in forma rivista il 17 maggio 2006