On the number of permutations admitting an m-th root

Nicolas POUYANNE

Département de mathématiques
Université de Versailles - Saint-Quentin
45, avenue des Etats-Unis
78035 Versailles Cedex
pouyanne@math.uvsq.fr

Submitted: August 28, 2001; Accepted: December 20, 2001.
MR Subject Classification: Primary 05A15, 05A16; Secondary 68W40

Abstract

Let m be a positive integer, and $p_n(m)$ the proportion of permutations of the symmetric group $\mathfrak{S}_n$ that admit an m-th root. Calculating the exponential generating function of these permutations, we show the following asymptotic formula

$$p_n(m) \underset{n\to+\infty}{\sim} \frac{\pi_m}{n^{1-\varphi(m)/m}},$$

where φ is the Euler function and π_m an explicit constant.

1. Introduction

The question consists in estimating the number of permutations of the symmetric group $\mathfrak{S}_n$ which admit an m-th root when n is large. Turán gave an upperbound when m is a prime number [Tu] and Blum found an asymptotically equivalent form for $m = 2$ [Bl]. In the general case, Bender applied a theorem of Hardy, Littlewood and Karamata to the exponential generating function of these permutations to obtain an asymptotic equivalent of the partial sums of the required numbers [Be]. In [BoMcLWh], it is shown that the sequence tends monotonically to zero in the case when m is prime.

Whether a permutation of $\mathfrak{S}_n$ admits an m-th root can be read on the partition of n determined by the lengths of the permutation's cycles, because the class of such permutations is stable under conjugacy in $\mathfrak{S}_n$. This characterisation, already mentioned in [Be] is established in section **2**.

The computation of the exponential generating function (EGF) P_m of these permutations follows from the preceding result. This EGF splits in a natural way as a product of two others EGF:

$$P_m = C_m \times R_m.$$

Singularity analysis provides the asymptotics of the coefficients of $C_m = \sum_n c_n(m)X^n$ because C_m has a finite number of algebraic singularities on its circle of convergence. This asymptotics turns to be of the following form

$$c_n(m) \underset{n\to+\infty}{\sim} \frac{\kappa_m}{n^{1-\frac{\varphi(m)}{m}}},$$

where κ_m is an explicit constant and φ the Euler function. This formula was already established in [BoGl] only when m is a prime number.

On the contrary, the singularities of $R_m = \sum_n r_n(m)X^n$ form a dense subset of its circle of convergence; this prevents transfer theorems to apply to R_m and to the whole series P_m. Nevertheless, the series with positive coefficients $\sum_n r_n(m)$ converges. Now, since

$$\frac{p_n(m)}{c_n(m)} = \sum_{k=o}^{n} \frac{c_{n-k}(m)}{c_n(m)} r_k(m),$$

and since $c_{n-k}(m)/c_n(m)$ tends to 1 as n tends to infinity for every k, the asymptotics of the $p_n(m)$ will follow from an interchange of limits.

Lebesgue's dominated convergence theorem for the counting measure on the natural numbers does not directly apply because $c_{n-k}(m)/c_n(m)$ is too large when k is not far from n (if k equals n, its value is $n^{1-\varphi(m)/m}$ up to a positive factor). If the sequences $\big(c_{n-k}(m)/c_n(m)\big)_n$ were monotonic, the result would be a consequence of Lebesgue's monotonic convergence theorem (for the counting measure once again). Unfortunately, this is not the case. We approximate the $c_n(m)$ by the coefficients $d_n(m)$ of the expansion in power series of the principal part D_m of C_m in a neighbourhood of its dominant singularity 1. The sequences $\big(d_{n-k}(m)/d_n(m)\big)_n$ are this time monotonic, so that

$$\lim_{n\to+\infty} \sum_{k=0}^{n} \frac{d_{n-k}(m)}{d_n(m)} r_k(m) = \sum_{n\geq 0} r_n(m).$$

Now, the approximation of the $c_n(m)$ by the $d_n(m)$ is good enough to ensure the application of dominated convergence theorem; this last fact implies the announced result.

In an appendix, we give an explicit formula giving the number $c_n(m) \times n!$ of permutations of $\mathfrak{S}_n$ whose canonical decomposition has only cycles of length prime to m (these permutations are m-th powers).

2. What does an m-th power look like in $\mathfrak{S}_n$?

Every permutation has a canonical decomposition (unique up to order) as a product of cycles of disjoint supports. These cycles commute. Therefore, a permutation is an m-th power if and only if it is a product of m-th powers of cycles with disjoint supports. Then, it suffices to check what the m-th power of a cycle looks like.

Lemma. *The m-th power of a cycle of length l is a product of* $\gcd(l,m)$ *cycles of length* $l/\gcd(l,m)$ *with disjoint supports.*

In algebraic terms, this lemma can be understood in the following way: if c is a cycle of length l, the order of the element c^m in the symmetric group is $l/\gcd(l,m)$.

In order to establish the shape of an m-th power of $\mathfrak{S}_n$, let us introduce the notation $l^\infty \wedge m$: if l and m are integers, $\gcd(l^n,m)$ does not depend on n, provided n is large enough; $l^\infty \wedge m$ is defined as this common value of $\gcd(l^n,m)$, $n \gg 1$. In terms of decomposition in prime factors, $l^\infty \wedge m$ is the part of m having a common divisor with l: let $m = \pm\prod p^{v_p(m)}$ be the decomposition of m in primes, the products ranges over all primes numbers p, the valuations $v_p(m)$ are nonnegative integers, almost all of them are zero. Then, $l^\infty \wedge m = \prod p^{v_p(m)}$ where the product ranges over all primes p such that p divides l. At last, one can see the number $l^\infty \wedge m$ as the least positive divisor d of m such that l and m/d are coprimes.

Proposition. *A permutation $\sigma \in \mathfrak{S}_n$ has an m-th root if and only if for every positive integer l, the number of l-cycles in the canonical decomposition of σ is a multiple of $l^\infty \wedge m$.*

Proof. Let $\delta = l^\infty \wedge m$. Then δ divides m, and $\gcd(m/\delta, l) = 1$. For every positive integer k, with the help of the lemma, a product of $k\delta$ cycles with disjoint supports is the m-th power of a cycle of length $lk\delta$. Doing this for every l, one sees that the condition is sufficient. Now, let c be a cycle of length k. Then, thanks to the lemma, c^m is the product of $\gcd(k,m)$ cycles of length $l = k/\gcd(k,m)$. To catch the necessity of the condition, it is enough to show that $\gcd(k,m)$ is a multiple of δ, *i.e.* that for every prime p, one has $v_p(\gcd(k,m)) \geq v_p(\delta)$. It follows from the definition of $l^\infty \wedge m$ that

$$v_p(\delta) = \begin{cases} 0 & \text{if } p \text{ divides } \gcd(l,m) \\ v_p(m) & \text{if } p \text{ does not divide } \gcd(l,m). \end{cases}$$

Suppose that p is a prime divisor of $\gcd(l,m)$. In particular, $v_p(l) \neq 0$ Then, $v_p(m) < v_p(k)$ since $v_p(l) = v_p(k) - \min\{v_p(m), v_p(k)\}$. This implies that $v_p(\gcd(k,m)) = v_p(m) = v_p(\delta)$. On the other hand, if the prime p does not divide $\gcd(l,m)$, then $v_p(\delta) = 0 \leq v_p(\gcd(k,m))$ and the proof is complete.

Examples. 1: In the case where m is a prime number, the recipe to build an m-th power in $\mathfrak{S}_n$ is the following: compose arbitrarily cycles of length not divisible by m with groups of m cycles of same length divisible by m (all cycles with disjoint supports).

2: The notations for partitions are the standard ones. If the partition associated to a permutation σ is $(2^6, 3^{27}, 4^2, 5, 6^{18}, 7^2)$, then σ is the 18-th power of a permutation whose partition is $(4^3, 5, 7^2, 8, 27^3, 104)$. In general, a permutation admits many m-th roots, which do not have necessarily the same partition.

3. The exponential generating function of the m-th powers

We adopt the following notations :

$$P_m = \sum_{n \geq 0} p_n(m) X^n$$

$$C_m = \sum_{n \geq 0} c_n(m) X^n$$

$$R_m = \sum_{n \geq 0} r_n(m) X^n.$$

$P_m \in \mathbf{Q}[[X]]$ is the exponential generating function (EGF, formal series) of the m-th powers in the groups $\mathfrak{S}_n$. This means that the number of m-th powers in $\mathfrak{S}_n$ is $p_n(m) \times n!$ for each n. In the same way, C_m is the EGF of the permutations having only cycles of length prime to m in their canonical decomposition (they admit a m-th root) and R_m the EGF of the *rectangular m-th powers*, that is the m-th powers with only cycles of length having a common factor with m (the adjective rectangular is chosen because of the form of the Ferrers diagram associated to such a permutation : a sequence of rectangular blocks of height greater than 1).

Now, the standard way to compute these series [FlSe] leads to the following expressions, according to the previous proposition:

$$P_m = C_m \times R_m = \prod_{l \geq 1} e_{l^\infty \wedge m}\left(\frac{X^l}{l}\right). \tag{1}$$

In the last formula, $l^\infty \wedge m$ is defined in **2-** and e_d denotes the formal series (or the entire function) defined for $d \geq 1$ by

$$e_d(X) = \sum_{n \geq 0} \frac{X^{nd}}{(nd)!} = \frac{1}{d} \sum_{\zeta} \exp(\zeta X).$$

The last sum is extended to all d-th (complex) roots of 1. Note that for $d = 1$ this series is the exponential and for $d = 2$ the hyperbolic cosine.

3.1. Isolating the numbers l prime to m, one finds

$$C_m = \exp\left(\sum_{\substack{l \geq 1 \\ \gcd(l,m)=1}} \frac{X^l}{l}\right). \tag{2}$$

If the decomposition into prime numbers of m is $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ with all α_i greater or equal to one, let $q(m) = p_1 \dots p_r$ be the *quadratfrei radical** of m (a positive integer is said to be quadratfrei if and only if it has no square factor). For conciseness, we shall write q in place of $q(m)$ if the situation is unambiguous. Formula (2) shows that

$$C(m) = C(q).$$

If m is the power of a prime number, $\gcd(k, m) = 1$ if and only if k is not divisible by the prime q, which gives the expression $C_m = \sqrt[q]{1 - X^q}/(1 - X)$. Furthermore, if p is a prime number and q a quadratfrei number prime to p, formula (2) shows that

$$C_{pq}(X) = C_q(X) \times C_q(X^p)^{1/p}. \tag{3}$$

We note μ the Möbius function on the positive integers, defined by $\mu(m) = 0$ if m has a square prime factor, and $\mu(q) = (-1)^r$ if q is a quadratfrei number with r prime factors (in particular, $\mu(1) = 1$). The function μ is multiplicative in the following sense : if m_1 and m_2 are coprime numbers, then $\mu(m_1 m_2) = \mu(m_1)\mu(m_2)$ (see [HaWr]).

Proposition. *For every positive m, the EGF of the permutations having only cycles of length prime to m in their canonical decomposition is*

$$C_m = \prod_{k|m} \left(1 - X^k\right)^{-\mu(k)/k}$$

Proof. Induction with formula (3).

Note that one can write the proposition with the product being extended only to all divisors of the quadratfrei radical q of m. Indeed, only the quadratfrei divisors of m have a non trivial contribution.

3.2. The contribution of the rectangular m-th powers to the series P_m is the product extended to the l which have a common factor with m, *i.e.*

$$R_m = \prod_{\substack{l \geq 1 \\ \gcd(l,m) \neq 1}} e_{l^\infty \wedge m}\left(\frac{X^l}{l}\right). \tag{4}$$

* In terms of commutative algebra, the radical of an ideal I is the set of all elements of the ring some positive power of which belongs to I; in the present situation, $q(m)$ is the positive generator of the radical of the ideal of $\mathbf{Z}$ generated by m.

4. Main theorem

We now aim to calculate an asymptotic equivalent of the coefficients of $P_m = C_m R_m$. Singularity analysis will allow us to establish such an asymptotics for the coefficients of C_m, because the radius of convergence of the associated analytic function it defines is 1, with a finite number of algebraic singularities on the unit circle. Unfortunately, the series R_m admits the unit circle as a natural boundary: the singularities of R_m form a dense subset of the unit circle.

The argument given to reach the desired asymptotics uses the convergence of the series of coefficients of R_m, and a combination of monotonic and dominated convergences round C_m, together with a new occurence of singularity analysis.

4.1. Convergence of the series $\sum_n r_n(m)$

The infinite product

$$R_m(1) = \prod_{\substack{l \geq 1 \\ \gcd(l,m) \neq 1}} e_{l^\infty \wedge m}\left(\frac{1}{l}\right)$$

converges because its general term is $1 + \mathcal{O}(1/l^2)$ as l tends to infinity.

Moreover, $e_d(X^l/l) = 1 + \frac{1}{l^d d!} X^{ld} + \cdots$, which shows that just a finite number of factors of the infinite product R_m are enough to calculate the n-th coefficient $r_n(m)$ (roughly speaking, one needs less than the first $\lceil n/2 \rceil$ terms of the product).

If t is a positive integer, let $R_m^t = \sum r_n^t(m) X^n$ be the product of the first t terms of the product R_m. The series R_m^t has an infinite radius of convergence; in particular, the series $\sum_n r_n^t(m)$ converges to $R_m^t(1)$. Then, all terms being nonnegative, if t is greater than $\lceil n/2 \rceil$, one has successively

$$\sum_{k=0}^{n} r_k(m) = \sum_{k=0}^{n} r_k^t(m) \leq \sum_{k=0}^{+\infty} r_k^t(m) = R_m^t(1) \leq R_m(1).$$

The last inequality is due to the fact that the e_d are greater than 1 on the nonnegative real numbers. Since the terms $r_n(m)$ are all positive, the series $\sum_n r_n(m)$ converges and thanks to Abel's theorem*, one has at last

$$\sum_{n \geq 0} r_n(m) = R_m(1). \tag{5}$$

Remark. The series R_m admits the unit circle as a natural boundary. We illustrate this phenomenon on the particular case where $m = 2$. The general case, more complicated to write, is conceptually of the same kind.

---

* We refer to the following theorem of Abel: if the series $\sum a_n$ converges, then the power series $\sum a_n z^n$ is uniformly convergent on $[0, 1]$.

For $m = 2$, the series is

$$R_2 = \prod_{n\geq 1} \cosh\left(\frac{X^{2n}}{2n}\right) = \exp\left(\sum_{m\geq 1} \frac{(-1)^{m-1}\tau_{m-1}}{m2^{2m+1}} \mathrm{Li}_{2m}(X^{4m})\right), \tag{6}$$

where $\mathrm{Li}_n(X) = \sum X^k/k^n$ is the n-th polylogarithm and τ_m are the tangent numbers, defined by the expansion $\tan X = \sum \tau_m X^{2m+1}$. The n-th polylogarithm has a singularity at 1, with principal part $(1-z)^{n-1}\log 1/(1-z)$ up to a factor. Thus every primitive $4m$-th root of unity ζ is a singularity of R_2 with principal part $(1-z/\zeta)^{2m-1}\log 1/(1-z/\zeta)$ up to a factor, so that R_2 is singular at a dense subset of points on the unit circle.

4.2. Asymptotics of the $c_n(m)$

We use a restricted notion of order of a singularity: we will say that an analytic function f has order $\alpha \in \mathbf{R} \setminus \mathbf{Z}_-$ at its (isolated) singularity ζ if

$$f(z) = \frac{\mathrm{c}}{\left(1 - \frac{z}{\zeta}\right)^{\alpha}}\big(1 + \mathcal{O}(z-\zeta)\big)$$

in a neighbourhood of ζ which avoids the ray $[\zeta, +\infty[$, where c is a non zero constant (c is the value at ζ of the function $z \mapsto (1-\frac{z}{\zeta})^{\alpha} f(z)$).

All the singularities of C_m are on the unit circle : they are the q-th roots of unity, where q is the quadratfrei radical of m. The order of the singularity 1 is clearly $\sum \mu(k)/k$, where the sum extends to all divisors of q. Let φ be the Euler function, *i.e.* $\varphi(q)$ is the number of all positive integers less or equal to q and prime to q. Because of the Möbius inversion formula (see [HaWr]), since $q = \sum \varphi(k)$ where k ranges over all divisors of q, one finds $\sum \mu(k)/k = \varphi(q)/q$. An elementary calculation of the same kind, using the multiplicativity of the arithmetical functions φ and μ leads to the following result.

Lemma. *If ζ is a primitive k-th root of unity (where k divides q), then C_m has at ζ a singularity of order* $\dfrac{\mu(k)}{\varphi(k)}\dfrac{\varphi(q)}{q}$.

Note once more that one could state this result without the use of q, writing directly m instead of q. Indeed, μ is zero on non-quadratfrei numbers, and $\varphi(q)/q = \varphi(m)/m$.

Proposition. *For every positive integer m, the number $c_n(m) \times n!$ of permutations of $\mathfrak{S}_n$ having only cycles of length prime to m in their canonical decomposition satisfies*

$$c_n(m) \underset{n\to+\infty}{\sim} \frac{\kappa_m}{n^{1-\frac{\varphi(m)}{m}}},$$

where κ_m is the following constant depending only on the quadratfrei radical q of m

$$\kappa_m = \frac{1}{\Gamma\left(\frac{\varphi(m)}{m}\right)} \prod_{k|m} k^{-\frac{\mu(k)}{k}}.$$

Proof. C_m defines an analytic (single-valued) function in any simply connected domain that avoids its singularities. The lemma shows that the singularity of C_m at 1 determines alone the asymptotics of $c_n(m)$ *via* transfer theorem *. The constant $\kappa_m \times \Gamma\left(\frac{\varphi(m)}{m}\right)$ is the value at 1 of the function $z \mapsto (1-z)^{\varphi(m)/m} C_m(z)$.

For a formula giving the exact value of $c_n(m)$, see the appendix. Figure 1 shows the first thousand values of kappa, with m on the x-axis and κ_m on the y-axis.

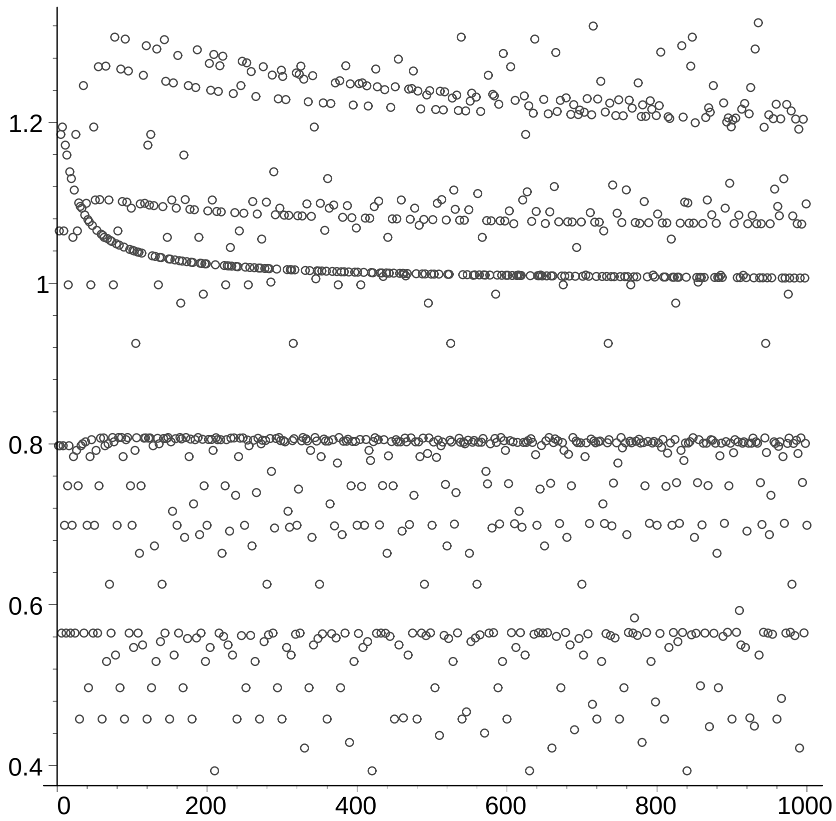

Figure 1: The function $m \mapsto \kappa_m$

4.3. Statement and proof of the main theorem

The situation is the following: we look for the asymptotics of the coefficients $p_n(m)$ of the formal series $P_m = C_m R_m$ where the coefficients $c_n(m)$ are equivalent to $n^{-1+\varphi(m)/m}$ up to a constant factor, and the series of coefficients $r_n(m)$ converges.

* By transfer theorem, we mean analysis of singularities that consists in deducing the asymptotics of the coefficients of a power series from the local analysis of its singularities when they involve only powers and logarithms. For a detailed study, see [FlSe].

Theorem. *Let m be a positive integer. The number $p_n(m) \times n!$ of permutations of $\mathfrak{S}_n$ which admit a m-th root satisfies*

$$p_n(m) \underset{n\to+\infty}{\sim} \frac{\pi_m}{n^{1-\frac{\varphi(m)}{m}}}$$

where π_m is the positive constant

$$\pi_m = \kappa_m R_m(1) = \frac{1}{\Gamma\left(\frac{\varphi(m)}{m}\right)} \prod_{k|m} k^{-\frac{\mu(k)}{k}} \prod_{\substack{l\geq 1 \\ \gcd(l,m)\neq 1}} e_{l^\infty \wedge m}\left(\frac{1}{l}\right).$$

Proof. For simplicity, we note $p_n = p_n(m)$, and similarly for c_n and r_n. We deduce from the formula $P_m = C_m R_m$ that $p_n = \sum c_{n-k} r_k$, where k ranges over $\{0, \ldots, n\}$. Since c_{n-k}/c_n tends to 1 as n tends to infinity for every k (see the asymptotics of c_n), it is enough to show that the following interchanging of limits is valid:

$$\lim_{n\to+\infty} \sum_{k=0}^{n} \frac{c_{n-k}}{c_n} r_k = \sum_{n\geq 0} r_n.$$

Let D_m be the series $D_m = \kappa_m \times \Gamma(\varphi(m)/m) \times (1-X)^{-\varphi(m)/m} = \sum_{n\geq 0} d_n X^n$, principal term of the series C_m in a neighbourhood of 1 (see proof of the previous proposition). For each integer k, the sequence $(d_{n-k}/d_n)_n$ decreases (compute it explicitely, d_n is a generalised binomial number up to a factor) and converges to one. Then, by monotonic convergence theorem,

$$\lim_{n\to+\infty} \sum_{k=0}^{n} \frac{d_{n-k}}{d_n} r_k = \sum_{n\geq 0} r_n.$$

On the other hand, the formal series $C_m - D_m$ defines a function analytic on the unit disk, whose singularities are those of C_m except 1 which becomes of order $\varphi(m)/m - 1$. If $m \neq 1$, the singularity that determines the asymptotics of its coefficient has order α strictly less than $\varphi(m)/m$ (the previous lemma gives α explicitely). As a consequence, $1 - d_n/c_n$ tends to zero as n tends to $+\infty$. In particular, there exist two positive constants A and B such that

$$\forall n \geq 0, \quad A \leq \frac{d_n}{c_n} \leq B.$$

Then, for all n and k (with $k \leq n$), one has

$$\frac{c_{n-k}}{c_n} \leq \frac{B}{A} \frac{d_{n-k}}{d_n}.$$

The conclusion follows now from the dominated convergence theorem.

Figure 2 shows the first thousand values of the function $m \mapsto \pi_m$, with m on the x-axis and π_m on the y-axis.

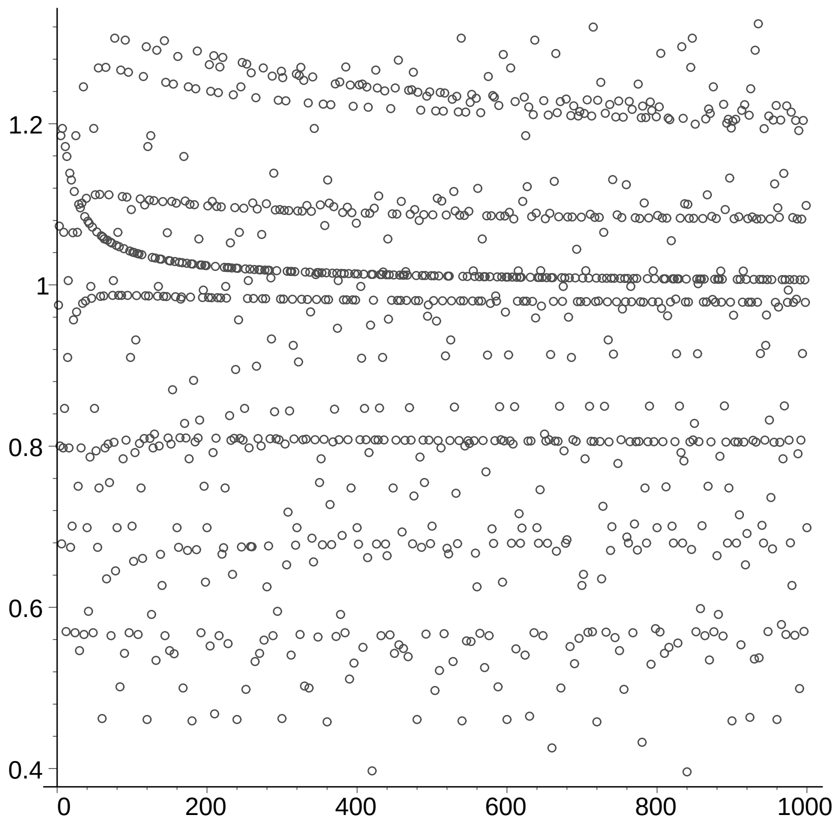

Figure 2: The function $m \mapsto \pi_m$

Remarks.
i) When m is the power of a prime number q, there is another way to catch the interchange of limits because one can explicitly write the coefficients $c_n(m) = c_n(q)$ as products and quotients of integers (see section **5-** : under this assumption, $b_n(q)$ equals $c_n(q)$). It is just a matter of elementary computation to see that for every k, the "congruence subsequences" of $c_{n-k}(q)/c_n(q)$ are monotonic :

$$\forall k \geq 0, \quad \forall r \in \{0, \dots, q-1\}, \quad \text{the sequence } \left(\frac{c_{nq+r-k}(q)}{c_{nq+r}(q)} \right)_n \quad \text{is monotonic.}$$

Putting together the common asymptotics these congruence subsequences give is enough to prove the theorem.
ii) The expression of P_m with the help of polylogarithms such as in formula (6) would give an alternative proof of the theorem, and a way to obtain further asymptotics of the numbers $p_n(m)$, using a hybrid method of singular analysis and of Darboux's method as it is described in [FlGoPa].

5. Appendix

Let $b_n(m)\times n!$ be the number of permutations of $\mathfrak{S}_n$ which admit no cycle of length divisible by m in their canonical decomposition. Calculating the exponential generating function of these permutations leads to a recurrence formula for the $b_n(m)$; finally, one finds

$$b_n(m) = \prod_{\substack{1\le k\le n \\ m|k}} \left(1-\frac{1}{k}\right)$$

(see [BeGo]). One can calculate these numbers with the induction formula:

$$\begin{cases} b_n(m) &=& b_{n-1}(m) & \text{if } n\notin m\mathbf{N}^* \\ b_n(m) &=& b_{n-1}(m)(1-\frac{1}{n}) & \text{if } n\in m\mathbf{N}^* \end{cases}$$

If $\mathcal{B}_m$ (*resp.* $\mathcal{C}_m$) denotes the set of all permutations (of any $\mathfrak{S}_n$) which admit no cycle of length divisible by m (*resp.* having only cycles of length prime to m) in their canonical decomposition, then $\mathcal{C}_m = \bigcup \mathcal{B}_d$, where the union is extended to all divisors d of q greater than or equal to 2. Once more, q denotes the quadratfrei radical of m. The sieve formula gives $\#(\mathcal{C}_m) = \sum -\mu(d)\#(\mathcal{B}_d)$, the sum being extended to the same d as before; μ is the Möbius function. This implies the following result.

Proposition. *The number $c_n(m)\times n!$ of permutations of $\mathfrak{S}_n$ having only cycles of length prime to m satisfies*

$$c_n(m) = \sum_{\substack{d\ge 2\\ d|m}} -\mu(d)b_n(d) = \sum_{\substack{d\ge 2\\ d|m}} -\mu(d) \sum_{\substack{k\in d\mathbf{Z}\\ 1\le k\le n}} \left(1-\frac{1}{k}\right).$$

6. Aknowledgements

Je remercie tout particulièrement Abdelkader Mokkadem et Jean-François Marckert d'avoir suscité puis soutenu mes premiers pas sur le sujet, ainsi que Philippe Flajolet pour m'avoir permis de me repérer dans le paysage des disciplines qui lui sont connexes.

References

[Be] E. A. Bender, Asymptotics methods in enumeration, *SIAM Rev. 16* (1974), 485-515.

[BeGo] E. A. Bertram and B. Gordon, Counting special permutations, *European J. Combin. 10(3)* (1989), 221-226.

[Bl] J. Blum, Enumeration of the square permutations in S_n, *J. Combin. Theory Ser. A17* (1974), 156-161.

[BoGl] E.D. Bolker and A.M. Gleason, Counting permutations, *J. Combin. Theory Ser. A29(2)* (1980), 236-242.

[BoMcLWh] M. Bóna, A. McLennan and D. White, Permutations with roots, *Random Structures & algorithms 17(2)* (2000), 157-167.

[FlGoPa] P. Flajolet, X. Gourdon, D. Panario, The complete analysis of a polynomial factorization algorithm over finite fields, *J. of Algorithms*, to appear.

[FlOd] P. Flajolet and A.M. Odlyzko, Singularity analysis of generating functions, *SIAM Journal on Discrete Mathematics 3(2)* (1990), 216-240.

[FlSe] P. Flajolet and R. Sedgewick, The average case analysis of algorithms: complex asymptotics and generating functions, *INRIA research report 2026* (1993).

[HaWr] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Science Publications.

[Tu] P. Turán, On some connections between combinatorics and group theory, *Colloq. Math. Soc. János Bolyai, P. Erdös, A. Rényi and V. T. Sós, eds.*, North Holland, Amsterdam (1970), 1055-1082.