Asymptotic Behavior of Friable Permutations

Owen Mireles Briones *

April 5, 2021

Abstract

In number theory, the function $\psi(x,y)$ counts the amount of y-friable integers not exceeding x. A theorem of de Brujin and Alladi relates the asymptotic value of ψ to Dickman's function ρ. In this note, we use ρ to estimate the limit of the probability that a uniformly chosen permutation of S_n contains only short cycles, a quantity akin to friable numbers for permutations. The main tool is the Saddle Point Method.

1 Introduction

An integer n is called y-friable if its largest prime factor is not greater than y. Denote by $\psi(x,y)$ the number of y-friable integers not exceeding x. The question of evaluating this quantity is crucial in numerous arithmetical problems, and the techniques employed to tackle it are instructive from several points of view.

For instance, the following theorem, found in [3], is obtained from a standard, albeit careful, execution of the Saddle Point Method.

Theorem 1.1. *Let ρ be Dickman's function. Uniformly for $x \geq y \geq 2$, define $u = \frac{\ln x}{\ln y}$. We have*

$$\psi(x,y) = x\rho(u) + O\left(\frac{m}{\ln y}\right).$$

The permutations of the symmetric group of n elements S_n can be decomposed uniquely into cycles. This fact facilitates the interpretation of cycles as the prime factors of permutations. We can define *y-friable permutations* as those in which all their factoring cycles have length at most y.

The problem we will solve is:

Problem 1.2. *Let $\alpha = O\left(\frac{\log n}{n}\right)$. Let $p_{n,\alpha}$ be the probability that uniformly random permutation σ of S_n is αn-friable. Then,*

$$p_{n,\alpha} = (1 + o(1))\psi\left(\frac{1}{\alpha}\right),$$

where ψ is Dickman's function and $o(1)$ depends on n.

Remark 1.3. *As it will be seen later, the Saddle Point Method breaks when α is too large.*

*Department of Mathematics, Stony Brook University, Stony Brook, NY, USA. Email: owen.mirelesbriones@stonybrook.edu.

As in the case of friable numbers, the main tool is the Saddle Point Method, which is used to estimate integrals. Let us describe it briefly, sans technicalities.

Let U be a domain, and γ its boundary. Consider a nonconstant meromorphic function $f : \mathbb{C} \to \mathbb{C}$ with a pole w in U. To approximate the residue of f at w it suffices to calculate $\int_\gamma f(z)dz$ roughly. Write $\int_\gamma f(z)dz = \int_\gamma \exp(I(z))dz$ for the appropriate function I. Suppose z_0 is a critical point of I, then it *must be* a saddle point of f, since otherwise $\exp(I(z))$ would be constant, by the Maximum/Minimum Modulus Principle. If we can suitably deform γ to pass through z_0, then f will have a maximum on γ at z_0, and it will rapidly decrease away from it. Thus, it is the hope that $\int_\gamma f(z)dz \sim f(z_0)$.

Acknowledgements. I would like to thank my advisor, Robert Hough, who recommended me this problem, for pointing me in fruitful directions. Also, Appendix A of his paper [1] contains the slight modification of the regular Saddle Point Method that we use in this write up.

2 Preliminaries

2.1 Notation

While most notation is standard to analysis, some parts may require clarification.

$\Re(z)$ denotes the real part of the complex number z.

Big O and small o notation are employed; they are taken to depend on n as it grows. Since α may ultimately depend on n as well, if a more refined analysis is required, α will appear in the expressions, e.g. $O(n^3\alpha^4)$.

In some parts $\gg$ and $\ll$ are used. $A \ll B$ means $A = O(B)$, while $A \gg B$ should be interpreted as $B = O(A)$.

Finally, abusing notation, αn might be used in place of $\lfloor \alpha n \rfloor$ whenever we need an integer, depending on context. For example, $\sum_{k=1}^{\alpha n} k$ would mean $\sum_{k=1}^{\lfloor \alpha n \rfloor} k$ under this convention.

2.2 Cycle Generating Function

This discussion follows Chapter 4.7 of [4].

For any $a = (a_1, \ldots, a_k) \in \mathbb{N}^k$ such that $a_1 + 2a_2 + \ldots + ka_k = k$, let $c(a)$ denote the number of permutations σ of S_n that contain a_1 cycles of length 1, a_2 cycles of length 2, etc.

The generating function

$$\phi_n(x) = \sum_{a_1+2a_2+\ldots+ka_k=k} c(a) x_1^{a_1} x_2^{a_2} \cdots$$

is called *the cycle index of the symmetric group* S_n.

The following *grand generating function*, where x is a sequence,

$$C(x,t) = \sum_{k=1}^{\infty} \phi_k(x) \frac{t^k}{k!}$$

can be shown to have the closed form

$$C(x,t) = \exp\left(\sum_{k\geq 1} \frac{x_k t^k}{k} \right).$$

2.3 Dickman's Function

The following material is taken from Section 4, Chapter 5 of Part III of [3].

Dickman discovered the function bearing its name in 1930. It is continuous at $u = 1$, differentiable for $u > 1$, satisfies the *delay differential equation*

$$u\rho'(u) + \rho(u-1) = 0, \qquad \text{for } u > 1,$$

and has the initial condition $\rho(u) = 1$ for $0 \leq u \leq 1$. By making $\rho(u) = 0$ when $u < 0$, we can extend ρ effectively to all of $\mathbb{R}$.

We first introduce an auxiliary quantity.

For $u > 1$, let $\xi = \xi(u)$ be the unique real, non-zero root of the equation

$$e^{\xi} = 1 + u\xi, \qquad u > 0, u \neq 1.$$

Lemma 2.1. *We can implicitly differentiate ξ with respect to u to obtain*

$$\xi'(u) = \frac{\xi}{1 + u(\xi - 1)}.$$

Also, for $u \geq 3$, ξ has the following expansion

$$\xi(u) = \ln(u \ln u) + O\left(\frac{\ln_2 u}{\ln u}\right)$$

This theorem of de Brujin and Alladi states the right order of ρ.

Theorem 2.2. *Define $I(s)$ as the function*

$$I(s) = \int_0^s \frac{e^t - 1}{t} dt, \qquad s \in \mathbb{C}.$$

Let γ be the Euler-Mascheroni constant.

We have

$$\rho(u) = \sqrt{\frac{\xi'(u)}{2\pi}} e^{\gamma - u\xi + I(\xi)} \left\{1 + O\left(\frac{1}{u}\right)\right\}.$$

3 Friable Permutations

3.1 Summary of the Solution

Computing $p_{n,\alpha}$ amounts to counting the number of αn-friable permutations and dividing by $n!$. As is common practice in combinatorics, we will find a generating function $G(t)$ whose n-th coefficient is $p_{n,\alpha}$. We will then recover the coefficients through Cauchy's integral formula. The main, and final, step is employing the Saddle Point Method to estimate the resulting integral.

3.2 Setting up the Integral

Let $\bar{x}$ be the sequence defined by making $x_j = 1$ when $j \leq \alpha n$ and $x_j = 0$ otherwise. We observe that the coefficient of t^n in $C(\bar{x}, t)$ is actually $p_{n,\alpha}$, and we can isolate it through Cauchy's integral formula.

Define with foresight

$$F(t) = \sum_{k=1}^{\alpha n} \frac{R^k e^{2\pi ikt}}{k} - 2\pi int.$$

If Γ is the circle with radius R centered at 0, we have

$$\begin{aligned} p_{n,\alpha} &= \frac{1}{2\pi i} \int_\Gamma \frac{C(\bar{x}, z)}{z^{n+1}} dz \\ &= \int_{-1/2}^{1/2} \frac{\exp\left(\sum_{k=1}^{\alpha n} \frac{R^k e^{2\pi ikt}}{k} - 2\pi int\right)}{R^n} dt \\ &= \int_{-1/2}^{1/2} \frac{\exp(F(t))}{R^n} dt. \end{aligned}$$

We ignore the intersection of the circle and the ray $\Re(z) \leq 0$, as it has measure zero.

3.3 The Saddle Point Method

3.3.1 Finding a Critical Point

To use the Saddle-Point Method, we first have to solve the *stationary-phase equation* $F'(0) = 0$; this is equivalent to finding an R that makes 0 a critical point of F.

When $R = 1$, zero is not a critical point of F; thus, we can assume $R \neq 1$, and compute

$$F'(0) = 2\pi i \frac{R^{\alpha n+1} - R}{R - 1} - 2\pi in.$$

Then, R has to satisfy

$$0 = R^{\alpha n+1} - (n+1)R + n.$$

It is not hard to note this equation has a real solution $R = R(\alpha, n) = 1 + \beta$ such that $\beta > 0$ and $\lim_{n\to\infty} \beta = 0$. We write $\beta = Bn^{-1} + O(n^{-2})$, and compute the first order Taylor expansion at $n = \infty$ of the previous equation:

$$0 = \left(e^{\alpha B} - B - 1\right) + O(n^{-1}).$$

We force $B > 0$ to be the unique positive solution to $e^{\alpha B} = 1 + B$.

We make the change of variables $\alpha B = \xi$ and $\alpha = 1/u$. Translating the contents of Lemma 2.1, we have

$$B = \frac{1}{\alpha} \log\left(\frac{1}{\alpha} \log \frac{1}{\alpha}\right) + \frac{1}{\alpha} O\left(\frac{\log_2(1/\alpha)}{\log(1/\alpha)}\right) = \frac{1}{\alpha} \log\left(\frac{1}{\alpha} \log \frac{1}{\alpha}\right) + O\left(\frac{1}{\alpha}\right).$$

3.3.2 The Leading Coefficient

Define $S = F(0)$. We need to estimate

$$p_{n,\alpha} = \frac{\exp(S)}{R^n}\int_{-1/2}^{1/2} \exp\left(F(t) - F(0)\right) dt$$
$$= \frac{\exp(S)}{R^n}\int_{-1/2}^{1/2} \exp\left(\sum_{k=1}^{\alpha n} \frac{R^k\left(e^{2i\pi kt} - 1\right)}{k} - 2i\pi nt\right) dt.$$

In what follows, we will compute asymptotics for S, R^n, and the integral.

Since $R = (1 + Bn^{-1} + O(n^{-2}))$, $R^n = e^B + o(1)$.

We claim $S = \sum_{k=1}^{\alpha n} R^k/k = \log(\alpha n) + \gamma + \int_0^{\alpha B} \frac{e^s-1}{s}ds + o(1)$, where γ is the Euler-Mascheroni constant.

Note $R^k = (1+\beta)^k = \exp(k\log(1+\beta)) = \exp(kBn^{-1} + O(kn^{-2}))$. Hence,

$$\sum_{k=1}^{\alpha n} \frac{R^k - 1}{k} = \sum_{k=1}^{\alpha n} \frac{e^{kBn^{-1}} - 1}{k} + \sum_{k=1}^{\alpha n} \frac{e^{kBn^{-1}+O(kn^{-2})} - e^{kBn^{-1}}}{k}.$$

Observe that the left-hand side is $S - \log(\alpha n) - \gamma + o(1)$.

On the right-hand side, the left summand is

$$\sum_{k=1}^{\alpha n} \frac{e^{kBn^{-1}} - 1}{k} = \sum_{k=1}^{\alpha n} \frac{1}{\alpha n} \frac{(e^{k(\alpha n)^{-1}})^{\alpha B} - 1}{k(\alpha n)^{-1}}.$$

This is $\int_0^1 \frac{e^{\alpha bs}-1}{s}ds + o(1)$, since it is a partial Riemann sum. By a change of variables,

$$\int_0^1 \frac{e^{\alpha bs} - 1}{s}ds = \int_0^{\alpha b} \frac{e^s - 1}{s}ds.$$

The right summand is

$$\left|\sum_{k=1}^{\alpha n} \frac{e^{kBn^{-1}+O(kn^{-2})} - e^{kBn^{-1}}}{k}\right| \le \sum_{k=1}^{\alpha n} \frac{e^{kBn^{-1}}\left|e^{O(kn^{-2})} - 1\right|}{k}$$
$$\le \sum_{k=1}^{\alpha n} \frac{e^{\alpha B}\left|e^{O(n^{-1})} - 1\right|}{k} = e^{\alpha B}\left|e^{O(n^{-1})} - 1\right| \left(\sum_{k=1}^{\alpha n} \frac{1}{k}\right) = o(1),$$

since it is easy to see that $e^{O(n^{-1})} - 1$ is $o((\log n)^{-1})$.

3.3.3 Main Term of the Integral

For the integral, set $A = \frac{\alpha^{-1/9}}{\alpha^{1/2}n}$ and $D = n^{-1/3}$, as they will be useful. Define

$$M = \int_{-1/2}^{1/2} \exp\left(\frac{1}{2}F''(0)t^2\right) dt,$$

$$M_1 = \int_{|t|\le A} \left(\exp\left(F(t) - F(0)\right) - \exp\left(\frac{1}{2}F''(0)t^2\right)\right) dt,$$

$$
\begin{aligned}
M_2 &= \int_{A\le|t|\le 1/2} \exp\left(\frac{1}{2}F''(0)t^2\right) dt,\\
M_3 &= \int_{A\le|t|\le D} \exp\left(F(t)-F(0)\right) dt.\\
M_4 &= \int_{D\le|t|\le 1/2} \exp\left(F(t)-F(0)\right) dt.
\end{aligned}
$$

We will show that M dominates all the other M_j, for $j = 1, 2, 3, 4$. This will help us conclude

$$
\int_{-1/2}^{1/2} \exp\left(F(t)-F(0)\right) dt = M + M_1 - M_2 + M_3 + M_4 = (1+o(1))M.
$$

We first analyze M. It is a Gaussian integral, since

$$
\begin{aligned}
F''(0) &= -4\pi^2 \left(\frac{\alpha n R^{\alpha n+2} - (\alpha n+1)R^{\alpha n+1} + R}{(R-1)^2}\right)\\
&= -4\pi^2 \left(\frac{e^{\alpha B}(\alpha B-1)+1}{B^2}\right)(1+o(1))^2\\
&= -4\pi^2 \left(\frac{\alpha+\alpha B-1}{B}\right)(1+o(1))n^2.
\end{aligned}
$$

Recalling the dependence of B on α, note

$$
\frac{\alpha+\alpha B-1}{B} = (1+o(1))\alpha.
$$

Thus, the standard deviation of the Gaussian integral is $O(\alpha^{-1/2}n^{-1})$, and hence most of its mass concentrates around 0 in a neighborhood of size $\alpha^{-1/2}n^{-1}$. We have

$$
\begin{aligned}
\int_{-1/2}^{1/2} \exp\left(\frac{1}{2}F''(0)t^2\right) dt &= (1+o(1))\sqrt{\frac{B(\alpha+\alpha B-1)^{-1}}{2\pi}}\frac{1}{n}\\
&= (1+o(1))\sqrt{\frac{\alpha^2 B(\alpha+\alpha B-1)^{-1}}{2\pi}}\frac{1}{\alpha n}\\
&= M.
\end{aligned}
$$

3.3.4 Discarding Error Terms

We begin with M_1.

By Taylor's Theorem, we know for every $0 < t < A$ there is $0 < \xi_t < t$ such that

$$
F(t) - F(0) = \frac{1}{2}F''(0)t^2 + \frac{1}{6}F'''(\xi_t)t^3,
$$

since the first derivative vanishes due to our choice of R.

Also, recalling our estimate for B, note that

$$
\begin{aligned}
|F'''(\xi_t)| &= \left|-8\pi^3 i \sum_{k=1}^{\alpha n} k^2 e^{2\pi i k\xi} R^k\right| \le 8\pi^3 \sum_{k=1}^{\alpha n} k^2 R^k\\
&= 8\pi^3 \frac{R(-((\alpha n)^2(R-1)^2 - 2\alpha n(R-1) + R + 1)R^{\alpha n} + R + 1)}{1-R^3}\\
&= \left(\frac{2-2\alpha-2\alpha B-2\alpha B^2+\alpha^2B^2+\alpha^2B^3}{B^3}\right)n^3(1+o(1))\\
&= \alpha^2 n^3(1+o(1)).
\end{aligned}
$$

Thus,

$$
\begin{aligned}
|M_1| &= \left| \int_{|t|\le A} \left(\exp\left(\frac{1}{2}F''(0)t^2 + \frac{1}{6}F'''(\xi_t)t^3 \right) - \exp\left(\frac{1}{2}F''(0)t^2 \right) \right) dt \right| \\
&= \left| \int_{|t|\le A} \exp\left(\frac{1}{2}F''(0)t^2 \right) \left[\exp\left(\frac{1}{6}F'''(\xi_t)t^3 \right) - 1 \right] dt \right| \\
&\le \left[\exp\left(\frac{1}{6}\alpha^2 n^3 (1+o(1))A^3 \right) - 1 \right] \int_{|t|\le A} \exp\left(\frac{1}{2}F''(0)t^2 \right) dt \\
&= \left[\frac{1}{6}\alpha^2 n^3 (1+o(1))A^3 + O\left(\alpha^4 n^6 A^6\right) \right] \int_{|t|\le A} \exp\left(\frac{1}{2}F''(0)t^2 \right) dt \\
&= o(M).
\end{aligned}
$$

This last equality is true because $\alpha^2 n^3(1+o(1))A^3 = (1+o(1))\alpha^{1/6} = o(1)$, and $\int_{|t|\le A} \exp\left(\frac{1}{2}F''(0)t^2\right) dt$ is $(1+o(1))M$ since the domain $\{|t| \le A\}$ contains $\sim \alpha^{-1/9}$ standard deviations of M and $\alpha^{-1/9} \to \infty$.

M_2 is the most direct quantity to drop. By known theory of Gaussian integrals, a two-sided tail of ℓ standard deviations away from the mean is $O(e^{-\ell^2/2})$ times the whole integral. Thus, $M_2 = o(M)$, as A is about $\alpha^{-1/9}$ standard deviations away and $\alpha^{-2/9}$ dominates $\log n$.

For M_3 and M_4 we will use Lemma 12 of [2].

Lemma 3.1. *For $t \in [-\frac{1}{2}, \frac{1}{2}]$, the sum $\Re\left(\sum_{k=1}^{\alpha n}(R^k \exp(2\pi i k x) - 1)/k\right)$ is upper bounded by*

$$
-8\frac{R^{\alpha n+1}}{\alpha n(R-1)} \cdot \frac{t^2}{(R-1)^2 + 4\pi^2 t^2} + \frac{2R}{\alpha n(R-1)}.
$$

Remark 3.2. *The previous lemma can be simplified when observing that*

$$
\frac{R^{\alpha n+1}}{\alpha n(R-1)} = (1+o(1))\frac{\exp(\alpha B)}{\alpha B},
$$

and also

$$
\frac{2R}{\alpha n(R-1)} = (1+o(1))\frac{2R}{\alpha B} = o(1).
$$

Continuing, we look at M_3. We have, for some constant $C > 0$,

$$
\begin{aligned}
M^{-1}|M_3| &\le M^{-1} \int_{A\le|t|\le D} |\exp(F(t) - F(0))|\, dt \\
&= M^{-1} \int_{A\le|t|\le D} \exp\left(\Re\left(\sum_{k=1}^{\alpha n} (R^k \exp(2\pi i k x) - 1)/k \right) \right) dt \\
&\le M^{-1}[D-A] \exp\left(-8\frac{R^{\alpha n+1}}{\alpha n(R-1)} \cdot \frac{A^2}{(R-1)^2 + 4\pi^2 D^2} + \frac{2R}{\alpha n(R-1)} \right) \\
&\le C(1+o(1)) \exp\left(-\frac{\exp(\alpha B)}{\alpha B} \cdot \frac{\alpha^{-1-2/9} n^{-2}}{B^2 n^{-2} + 4\pi^2 n^{-2/3}} + o(1) - \log(M) \right) \\
&\le C(1+o(1)) \exp\left(-\frac{\exp(\alpha B)}{\alpha B} \cdot \frac{\alpha^{-1-2/9} n^{-2}}{8\pi^2 n^{-2/3}} + o(1) - \log(M) \right) \\
&= o(1).
\end{aligned}
$$

Recall that $M \sim \alpha^{-1/2}n^{-1}$ and $\alpha \ll \log n/n$. The last line is true because, as n grows,

$$
\begin{aligned}
\frac{\exp(\alpha B)}{\alpha B} \cdot \frac{\alpha^{-1-2/9}n^{-2}}{8\pi^2 n^{-2/3}} + \log(M) &\gg \frac{\frac{1}{\alpha}\log\left(\frac{1}{\alpha}\right)}{\log\left(\frac{1}{\alpha}\log\left(\frac{1}{\alpha}\right)\right)} \cdot \frac{\frac{1}{\alpha^{1+2/9}}}{n^{4/3}} - \log(\sqrt{\alpha}n) \\
&\gg \frac{n^{2/3}\frac{1}{\alpha^{2/9}}}{(\log n)^2 \log\left(\frac{1}{\alpha}\log\left(\frac{1}{\alpha}\right)\right)} - \log(\sqrt{\alpha}n) \\
&\to \infty.
\end{aligned}
$$

For M_4, an analogous argument works, with some constants C_1, C_2,

$$
\begin{aligned}
M^{-1}|M_4| &\leq M^{-1}\int_{D\leq|t|\leq 1/2} |\exp\left(F(t)-F(0)\right)|\,dt \\
&\leq C_1(1+o(1))\exp\left(-\frac{\exp(\alpha B)}{\alpha B}\cdot\frac{D^2}{2C_2} + o(1) - \log(M)\right) \\
&\leq C_1(1+o(1))\exp\left(-\frac{\exp(\alpha B)}{\alpha B}\cdot\frac{1}{2C_2 n^{2/3}} + o(1) - \log(M)\right) \\
&= o(1).
\end{aligned}
$$

Again, the exponent of the last line satisfies

$$
\begin{aligned}
\frac{\exp(\alpha B)}{\alpha B}\cdot\frac{1}{2C_2 n^{2/3}} + \log(M) &\gg \frac{\frac{1}{\alpha}\log\left(\frac{1}{\alpha}\right)}{\log\left(\frac{1}{\alpha}\log\left(\frac{1}{\alpha}\right)\right)} \cdot \frac{1}{n^{2/3}} - \log(\sqrt{\alpha}n) \\
&\gg \frac{n^{1/3}}{(\log n)\log\left(\frac{1}{\alpha}\log\left(\frac{1}{\alpha}\right)\right)} - \log(\sqrt{\alpha}n) \\
&\to \infty.
\end{aligned}
$$

4 Conclusion

We can now match the terms of $p_{n,\alpha}$ with those of Dickman's function ρ in Theorem 2.2. We will be using the correspondence $\alpha B = \xi$ and $\alpha^{-1} = u$ from here on. First,

$$
\xi'(u) = \frac{\xi}{1+u(\xi-1)} = \frac{\alpha^2 B}{\alpha + \alpha B - 1}.
$$

After processing all the error terms, we end with the expression,

$$
\begin{aligned}
p_{n,\alpha} &= (1+o(1))\frac{\exp(S)}{R^n}\cdot M \\
&= (1+o(1))\exp\left(-B + \log(\alpha n) + \gamma + \int_0^{\alpha B}\frac{e^s-1}{s}dx\right)\sqrt{\frac{\alpha^2 B}{2\pi(\alpha+\alpha B-1)}\frac{1}{\alpha n}} \\
&= (1+o(1))\exp\left(\gamma - B + I(\alpha B)\right)\sqrt{\frac{\alpha^2 B}{2\pi(\alpha+\alpha B-1)}} \\
&= (1+o(1))\exp\left(\gamma - u\xi - I(\xi)\right)\sqrt{\frac{\xi'(u)}{2\pi}} = (1+o(1))\rho(u) \\
&= (1+o(1))\cdot\rho\left(\frac{1}{\alpha}\right).
\end{aligned}
$$

References

[1] Robert Hough. Mixing and cut-off in cycle walks. *Electronic Journal of Probability*, 22:P1 – P49, 2017.

[2] Eugenijus Manstavičius and Robertas Petuchovas. Local probabilities for random permutations without long cycles. *The Electronic Journal of Combinatorics*, pages P1–58, 2016.

[3] Gérald Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, third edition, 2008.

[4] Herbert S. Wilf. *generatingfunctionology*. Academic Press, Inc., 1994.