American Journal of Computational Mathematics, 2023, 13, 230-235
https://www.scirp.org/journal/ajcm
ISSN Online: 2161-1211
ISSN Print: 2161-1203

Average Probability of an Element Being a Generator in the Cyclic Group

Yoshihiro Tanaka

Faculty of Economics, Hokkaido University, Sapporo, Japan
Email: tanaka@econ.hokudai.ac.jp

How to cite this paper: Tanaka, Y. (2023) Average Probability of an Element Being a Generator in the Cyclic Group. *American Journal of Computational Mathematics*, 13, 230-235.
https://doi.org/10.4236/ajcm.2023.132012

Received: March 15, 2023
Accepted: June 5, 2023
Published: June 8, 2023

Abstract

All elements in the cyclic group $C(n)=\{g^0(=e),g,g^2,\cdots,g^{n-1}\}$ are generated by a generator *g*. The number of generators of $g^i, i\in S(n)$ of $C(n)$, namely $|S(n)|$ is known to be Euler's totient function $\varphi(n)$; however, the average probability of an element being a generator has not been discussed before. Several analytic properties of $\varphi(n)$ have been investigated for a long time. However, it seems that some issues still remain unresolved. In this study, we derive the average probability of an element being a generator using previous classical studies.

Keywords

Generator, Cyclic Group, Euler Product

1. Introduction

A cyclic group $C(n)$ is an elementary commutative group, and if $n=p$ (prime), $C(p)$ is known as one of the classifications of finite simple groups.

Every element in the cyclic group $C(n)=\{g^0(=e),g,g^2,\cdots,g^{n-1}\}$ is generated by a generator *g*. Euler's totient function $\varphi(n)$ is defined by

$$\varphi(n)=\left|\{1\le k\le n \mid \gcd(k,n)=1\}\right|. \quad (1)$$

Euler's totient function $\varphi(n)$ plays an intrinsically important role in the public key cipher RSA, which is essential in electronic commerce [1].

The average probability of an element being a generator has not been discussed before. Several analytic properties of $\varphi(n)$ have been investigated for a long time (e.g., [2] [3]). However, it seems that some issues still remain unresolved.

Dirichlet [4] considered the mean values of sequences of integer values analytically; however, their understanding can be somewhat challenging because of their unfamiliarity.

In this paper, we derive the average probability of an element being a generator using the studies by Dirichlet [4] and Dirichlet and Dedekind [5].

Throughout this paper, for a real number *t*, [*t*] denotes the integer part of *t*.

2. Preliminaries

As for the possibility that two arbitrary natural numbers are coprime, the following result is mentioned in [6]. We prove the result for the sake of convenience.

Lemma 1. The probability that two arbitrary natural numbers are coprime is $\frac{6}{\pi^2}$.

Proof. Since the probability that two arbitrary natural numbers have a prime p as a common divisor is $1-\frac{1}{p^2}$, the probability that two arbitrary natural numbers are coprime is $\prod_{p:\text{prime}}\left(1-\frac{1}{p^2}\right)$. Noting that by the Euler product formula

$$\prod_{p:\text{prime}}\left(1\Big/\left(1-\frac{1}{p^2}\right)\right)=\sum_{n=1}^{\infty}\frac{1}{n^2}=\zeta(2),$$

it holds that

$$\prod_{p:\text{prime}}\left(1-\frac{1}{p^2}\right)=\zeta(2)^{-1}=\frac{6}{\pi^2}. \tag{2}$$

□

We also mention the following result.

Theorem 2. Choose two arbitrary natural numbers *a* and *b*, and consider an arithmetic progression $\{a, a+b, a+2b, \cdots\}$. Then, the probability that the arithmetic progression includes an infinite number of primes is $\frac{6}{\pi^2}$.

Proof. The proof follows from Lemma 1 and Dirichlet's theorem on arithmetic progressions [7]. □

3. Main Result

In general, the cyclic group $C(n)=\left\{g^0(=e), g, g^2, \cdots, g^{n-1}\right\}$ generated by a generator g has generators $g^i, i\in S(n)\subset\{1,2,\cdots,n-1\}$. Then, $C(n)$ is expressed as $C(n)=\left\{g^0(=e), g^i, g^{2i}, \cdots, g^{(n-1)i}\right\}$.

As for $|S(n)|$, which is the number of generators of the cyclic group $C(n)$, we prove the following lemma.

Lemma 3. $|S(n)|=\varphi(n)$.

Proof. Let g be a generator. If g^k is a generator, it follows that $g=\left(g^k\right)^z=g^{kz}$, namely, $g^{kz-1}=e$.

As we can write $kz-1=qn+r$, $r<n$,

$$g^{kz-1}=g^{qn+r}=\left(g^n\right)^q\cdot g^r=g^r=e.$$

As $r=0$ because $r<n$,

$$kz=1,\ \text{mod } n. \tag{3}$$

Equation (3) implies that the Diophantine equation $kz+nu=1$ has integer solutions z and u, which means k and n are coprimes by Bezout's lemma. The converse is obvious.

Therefore, the theorem holds from the definition (1) of Euler's totient function $\varphi(n)$. □

Consider $\mathrm{P}(x)=\dfrac{\varphi(x)}{x}$ for x (integer). We can see that $\mathrm{P}(1)=1$, $\mathrm{P}(p)=\dfrac{p-1}{p}$ for p: prime, and $\mathrm{P}(x)>x^{-\frac{1}{2}}$ for $x>6$, $\mathrm{P}(x)>x^{-\frac{1}{3}}$ for $x>30$ (see [8]).

We can define $E(\mathrm{P}(X))$, the average probability of $\mathrm{P}(x)$ as follows.

$$E(\mathrm{P}(X))=\lim_{x\to\infty}\frac{1}{x}\cdot\sum_{i=1}^{x}\mathrm{P}(i)=\lim_{x\to\infty}\frac{1}{x}\cdot\sum_{i=1}^{x}\frac{|S(i)|}{i}=\lim_{x\to\infty}\frac{1}{x}\cdot\sum_{i=1}^{x}\frac{\varphi(i)}{i}.$$

Let $\psi(x)=\sum_{i=1}^{x}\varphi(i)$.

Then, the following result holds.

Theorem 4. $E(\mathrm{P}(X))=\dfrac{6}{\pi^2}=0.6079271\cdots$.

Proof. First, we derive $\varphi(n)$ along the lines of Dirichlet [4]. It is well-known that

$$\sum_{\delta|n}\varphi(\delta)=n \tag{4}$$

for example, in [5]. Summing up both sides for $n,n-1,\cdots,1$,

$$\sum_{s=1}^{n}\left[\frac{n}{s}\right]\varphi(s)=\frac{1}{2}n^2+\frac{1}{2}n. \tag{5}$$

For $\left[\dfrac{n}{s}\right]=t$, it follows that

$$\left(\psi\left(\left[\frac{n}{t}\right]\right)-\psi\left(\left[\frac{n}{t+1}\right]\right)\right)t=\left(\varphi\left(\left[\frac{n}{t+1}\right]+1\right)+\cdots+\varphi\left(\left[\frac{n}{t}\right]\right)\right)t$$

because $\left[\dfrac{n}{t+1}\right]<s\le\left[\dfrac{n}{t}\right]$. We regard the right hand side as $\varphi\left(\left[\dfrac{n}{t}\right]\right)t$ if $\left[\dfrac{n}{t+1}\right]+1=\left[\dfrac{n}{t}\right]$, and as 0 if $\left[\dfrac{n}{t+1}\right]=\left[\dfrac{n}{t}\right]$.

Therefore, (4) turns out to be

$$\sum_{s=1}^{n}\left[\frac{n}{s}\right]\varphi(s)=\sum_{s=1}^{n}\psi\left(\left[\frac{n}{s}\right]\right). \tag{6}$$

Hence,

$$\sum_{s=1}^{n}\psi\left(\left[\frac{n}{s}\right]\right)=\frac{1}{2}n^2+\frac{1}{2}n. \tag{7}$$

We put

$$\psi(n)=\frac{3}{\pi^2}n^2+\zeta\chi(n),\ \ \exists\zeta \text{ for } n. \tag{8}$$

By (7),

$$\psi(n)=-\sum_{s=2}^{n}\psi\left(\left[\frac{n}{s}\right]\right)+\frac{1}{2}n^2+\frac{1}{2}n. \tag{9}$$

By (8),

$$-\sum_{s=2}^{n}\psi\left(\left[\frac{n}{s}\right]\right)=-\sum_{s=2}^{n}\left(\frac{3}{\pi^2}\left[\frac{n}{s}\right]^2+\zeta\chi\left(\left[\frac{n}{s}\right]\right)\right)$$

$$=-\frac{3}{\pi^2}\sum_{s=2}^{n}\left(\frac{n}{s}-\varepsilon\right)^2-\sum_{s=2}^{\infty}\zeta\chi\left(\left[\frac{n}{s}\right]\right),\ \ 0\le\varepsilon<1$$

$$=-\frac{3n^2}{\pi^2}\sum_{s=2}^{n}\frac{1}{s^2}+\frac{6n}{\pi^2}\sum_{s=2}^{n}\frac{\varepsilon}{s}-\frac{3}{\pi^2}\sum_{s=2}^{n}\varepsilon^2-\sum_{s=2}^{\infty}\zeta\chi\left(\left[\frac{n}{s}\right]\right)$$

$$=-\frac{3n^2}{\pi^2}\left(\frac{\pi^2}{6}-1+\tau\right)+\frac{6n}{\pi^2}\sum_{s=2}^{n}\frac{\varepsilon}{s}-\frac{3}{\pi^2}\sum_{s=2}^{n}\varepsilon^2-\sum_{s=2}^{\infty}\zeta\chi\left(\left[\frac{n}{s}\right]\right)$$

$$=-\frac{1}{2}n^2+\frac{3}{\pi^2}n^2+Pn\log n+B\sum_{s=2}^{\infty}\chi\left(\frac{n}{s}\right),\ \ \exists P,\exists B$$

Substituting this back into (9),

$$\psi(n)=\frac{3}{\pi^2}n^2+Pn\log n+A\sum_{s=2}^{\infty}\chi\left(\frac{n}{s}\right),\ \ \exists P,\exists A \tag{10}$$

From (8) and (10),

$$\zeta\chi(n)=Pn\log n+A\sum_{s=2}^{\infty}\chi\left(\frac{n}{s}\right)$$

$$\zeta=\frac{Pn\log n}{\chi(n)}+\frac{A}{\chi(n)}\sum_{s=2}^{\infty}\chi\left(\frac{n}{s}\right).$$

We can write

$$\chi(n)=n^{\delta},$$

where δ is a constant satisfying

$$\sum_{s=2}^{n}\frac{1}{s^{\delta}}<\sum_{s=2}^{\infty}\frac{1}{s^{\delta}}=q,\ \ 1<\delta<2.$$

Hence,

$$\zeta=\frac{Pn\log n}{\chi(n)}+\frac{A}{n^{\delta}}\sum_{s=2}^{\infty}\left(\frac{n}{s}\right)^{\delta}=\frac{Pn\log n}{n^{\delta}}+Aq$$

for $\forall k>0$, $\dfrac{Pn\log n}{n^{\delta}}<k$, $n\ge N$,

Which implies

$$A' < k + Aq \,, \quad \exists A' \,.$$

Especially, if we use δ satisfying

$$\sum_{s=2}^{\infty} \frac{1}{s^{\delta}} = 1 \,, \tag{11}$$

we obtain

$$A' < A \,, \quad n \gg N \,.$$

Therefore, it follows that

$$\psi(n) = \frac{3}{\pi^2} n^2 + A' n^{\delta} \,, \quad 1 < \delta < 2 \,.$$

Thus,

$$\varphi(x) = \psi(x) - \psi(x-1) = \frac{3}{\pi^2}\left(x^2 - (x-1)^2\right) + A'\left(x^{\delta} - (x-1)^{\delta}\right)$$
$$= \frac{6}{\pi^2} x + o(x), \quad x : \text{integer}$$

this is because $(x-1)^{\delta} = x^{\delta} + \delta x^{\delta-1}(-1) + \cdots$ by the Taylor expansion.

Hence,

$$E(\mathrm{P}(X)) = \lim_{x\to\infty} \frac{1}{x} \cdot \sum_{i=1}^{x} \frac{\varphi(i)}{i} = \frac{6}{\pi^2} + \lim_{x\to\infty} \frac{1}{x} \cdot x \cdot o(1) = \frac{6}{\pi^2} \,. \tag{12}$$

□

We conducted an elementary computational experiment, in which we computed $\frac{1}{x} \cdot \sum_{i=1}^{x} \frac{\varphi(i)}{i}, x = 1, \cdots, 120$ using Python (**Figure 1**). **Figure 1** shows the validity of the result.

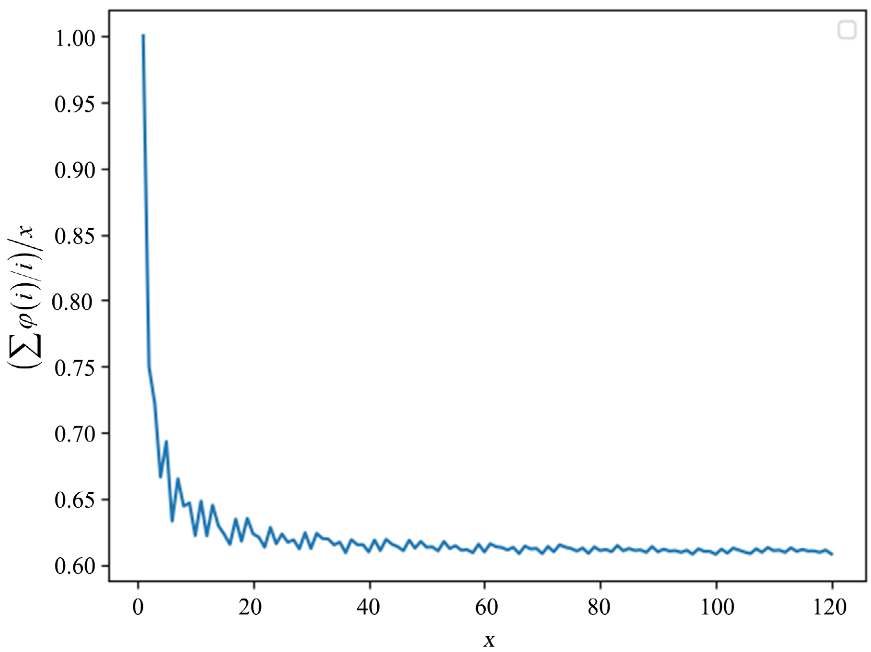

Figure 1. Average probability of an element being a generator.

4. Conclusions

In this study, we have proved that the average probability of an element being a generator in the cyclic group is $6/\pi^2$. It is interesting that this value is equal to the value of Lemma 1. This is evident in the following discussion.

Consider $(j,k), j=1,\cdots,x; k=1,\cdots,x$. Note that (j,j) is coprime for $j=1$ and not coprime for $j=2,\cdots,x$. Then,

$$\begin{aligned}
&\Pr\{(j,k) \text{ are coprime integers} \mid j=1,\cdots,x; k=1,\cdots,x\}\\
&=\sum_{k=1}^{x}\Pr\{((j,k), j\le k) \text{ are coprime integers} \mid j=1,\cdots,k\}\\
&\quad+\sum_{j=1}^{x}\Pr\{((j,k), j\ge k) \text{ are coprime integers} \mid k=1,\cdots,j\}\\
&\quad-\sum_{j=1}^{x}\Pr\{(j,j) \text{ are coprime integers}\}\\
&=\frac{1}{2}\left(1+\frac{1}{x}\right)\cdot\frac{1}{x}\cdot\sum_{k=1}^{x}\frac{\varphi(k)}{k}+\frac{1}{2}\left(1+\frac{1}{x}\right)\cdot\frac{1}{x}\cdot\sum_{j=1}^{x}\frac{\varphi(j)}{j}-\frac{1}{x^2}\\
&=\frac{1}{x}\cdot\sum_{i=1}^{x}\frac{\varphi(i)}{i}+\frac{1}{x^2}\cdot\sum_{i=1}^{x}\frac{\varphi(i)}{i}-\frac{1}{x^2}\\
&\xrightarrow[x\to\infty]{}\lim_{x\to\infty}\frac{1}{x}\cdot\sum_{i=1}^{x}\frac{\varphi(i)}{i}=E(\mathrm{P}(X))
\end{aligned}$$

We would like to further clarify the asymptotic property of $\mathrm{P}(x)=\varphi(x)/x$ itself, which seems like $\varphi(x)/x \xrightarrow{P} 6/\pi^2$ when $x\to\infty$, in our future work.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Wang, S.D. (2022) A Study of the Use of Euler Totient Function Is RSA Cryptosystem and the Future of RSA Cryptosystem. *Journal of Physics*: *Conference Series*, **2386**, Article ID: 012030. https://doi.org/10.1088/1742-6596/2386/1/012030

[2] Haukkanen, P. (2002) On an Inequality Related to the Legendre Totient Function. *Journal of Inequalities in Pure and Applied Mathematics*, **3**, Article 37.

[3] Zhai, W.G. (2020) On a Sum Involving the Euler Function. *Journal of Number Theory*, **211**, 199-219. https://doi.org/10.1016/j.jnt.2019.10.003

[4] Dirichlet, G.L. (1849) Über die Bestimmung der mittleren Werthe in der Zahlentheorie. Verlag nicht ermittelbar, Berlin. (Reprinted in G. Lejeune Dirichlet's Werke, Chelsea Publishing Company, New York, 1969).

[5] Dirichlet, G.L. and Dedekind, R. (1879) Vorlesungen über Zahlentheorie Braunschweig. Cambridge University Press, Cambridge.

[6] Chen, Y.-P. (2012) A Probabilistic Look at Series Involving Euler's Totient Function. *Integers*, **12**, 649-657. https://doi.org/10.1515/integers-2011-0125

[7] Dirichlet, G.L. (1837) Beweis des Satzes, dass jede unbegrentze arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Abhandlungen der Königlichen Preussischen Akademie der Wissenschaften zu Berlin*, **48**, 45-71. arXiv:0808.1408v2 (2014).

[8] Kendall, R. and Osborn, R. (1965) Two Simple Lower Bounds for the Euler ϕ-Function. *Texas Journal of Science*, **17**, 324-326.