This page is here to make the page numbers come out correctly.

Do not print this page.

The Probability that the GCD of Products of Ideals in a Number Ring is B-smooth

A Thesis Presented to

The Faculty of the Mathematics Program

California State University Channel Islands

In (Partial) Fulfillment

of the Requirements for the Degree

Masters of Science

by

Adrian Vazquez

May, 2023

Signature page for the Masters in Mathematics Thesis of Adrian Vazquez

APPROVED FOR THE MATHEMATICS PROGRAM

Brian Sittinger — 05/16/2023

Brian Sittinger (May 16, 2023 12:45 PDT)

Dr. Brian Sittinger, Thesis Advisor — Date

05/16/2023

Dr. Ivona Grzegorczyk, Thesis Committee — Date

05/17/2023

Jill Leafstedt (May 17, 2023 12:48 PDT)

Dr. Jill Leafstedt, AVP Extended University — Date

Non-Exclusive Distribution License

In order for California State University Channel Islands (CSUCI) to reproduce, translate and distribute your submission worldwide through the CSUCI Institutional Repository, your agreement to the following terms is necessary. The author(s) retain any copyright currently on the item as well as the ability to submit the item to publishers or other repositories.

By signing and submitting this license, you (the author(s) or copyright owner) grants to CSUCI the nonexclusive right to reproduce, translate (as defined below), and/or distribute your submission (including the abstract) worldwide in print and electronic format and in any medium, including but not limited to audio or video.

You agree that CSUCI may, without changing the content, translate the submission to any medium or format for the purpose of preservation.

You also agree that CSUCI may keep more than one copy of this submission for purposes of security, backup and preservation.

You represent that the submission is your original work, and that you have the right to grant the rights contained in this license. You also represent that your submission does not, to the best of your knowledge, infringe upon anyone's copyright. You also represent and warrant that the submission contains no libelous or other unlawful matter and makes no improper invasion of the privacy of any other person.

If the submission contains material for which you do not hold copyright, you represent that you have obtained the unrestricted permission of the copyright owner to grant CSUCI the rights required by this license, and that such third party owned material is clearly identified and acknowledged within the text or content of the submission. You take full responsibility to obtain permission to use any material that is not your own. This permission must be granted to you before you sign this form.

IF THE SUBMISSION IS BASED UPON WORK THAT HAS BEEN SPONSORED OR SUPPORTED BY AN AGENCY OR ORGANIZATION OTHER THAN CSUCI, YOU REPRESENT THAT YOU HAVE FULFILLED ANY RIGHT OF REVIEW OR OTHER OBLIGATIONS REQUIRED BY SUCH CONTRACT OR AGREEMENT.

The CSUCI Institutional Repository will clearly identify your name(s) as the author(s) or owner(s) of the submission, and will not make any alteration, other than as allowed by this license, to your submission.

The Probability that the GCD of Products of Ideals in a Number Ring is B-smooth

Title of Item

Mathematics Masters Thesis

3 to 5 keywords or phrases to describe the item

Adrian Vazquez

Author(s) Name (Print)

Adrian Vazquez (affiliate)

Digitally signed by Adrian Vazquez (affiliate)
Date: 2023.05.15 22:56:34 -07'00'

Author(s) Signature Date

Acknowledgements

First and foremost, I would like to express my sincerest gratitude to my thesis advisor Dr. Brian Sittinger, whose patience, guidance, and expertise were critical to my success in my independent studies courses and this thesis. I would also like to thank Dr. Ivona Grzegorczyk for her advice in academic matters and for serving in my thesis committee.

I give a very special thanks to my colleague Chris Luk for encouraging me to apply to a graduate program. I also give a special thanks to Cecelia Feit, Charles Yi, and Thomas To for their glowing letters of recommendation. I express my deepest gratitude to Gilbert Gutierrez and Hoang Tran for lending me their support and expertise during the execution of the AN/ALR-67 Task Orders.

From California State University Northridge, I am deeply indebted to Dr. Jason Lo who revealed to me the beauty of algebra, and to Dr. Majid Mojirsheibani for revealing the beauty of probability theory. From Los Angeles Mission college, I also thank professors George Cracuin, Debbie Wong, Emil Sargsyan, and Agnes Marsubian.

Finally, I give a very special thanks to A. D. Aleksandrov, A. N. Kolmogorov, M. A. Lavrent'ev for authoring *Mathematics: Its Content, Methods and Meaning*, and the anonymous person who recommended that I read it. This book is the primary reason that I decided to study mathematics.

Abstract

As an extension of a result of Benkoski that the probability of r positive integers being relatively k-prime equals $\frac{1}{\zeta(rk)}$, Cheon and Kim in 2016 derived the probability that the k-greatest common divisor (k-GCD) of products of positive integers is B-smooth. We start by providing a more concise proof to this result. Then, we generalize this result to any given ring of algebraic integers.

Contents

1. Overview

1.1. **Introduction.** In 1737, Euler derived a closed form of the sum of the reciprocals of the squares of rational integers $\zeta(2)$, which was later generalized as a complex function in 1859 by Riemann. In 1849, Dirichlet [5] proved the probability that two random integers are relatively prime is $\frac{1}{\zeta(2)}$, where ζ denotes the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Subsequently in 1900, Lehmer [9] extended Dirichlet's result by proving that the probability that k integers are relatively prime is $\frac{1}{\zeta(k)}$. In 1970 Nymann provided another result by using Inclusion-Exclusion Principle [13]. In 1976, Benkoski [3] published a proof showing that the probability that k integers are relatively r-prime is $\frac{1}{\zeta(rk)}$. In 2010, Sittinger [18] published a more concise proof of Benkoski's theorem using methods developed by Nymann and extended the result to the algebraic integers. More recently, Cheon and Kim published a proof for the probability that the GCD and k-GCD of products of positive integers is B-smooth [4].

Definition 1.1.1. *Let B be a fixed positive integer. A positive integer x is* ***B-smooth (or B-friable)*** *if x has no prime divisor greater than B.*

Example 1.1.2. *Let $B = 20$. Then 57 is 20-smooth, because $57 = 3 \cdot 19$ and both 3 and 19 are less than 20. However 46 is not 20-smooth, because $46 = 2 \cdot 23$ and 23 is a prime number greater than 20.*

In this thesis, we provide more concise proofs of Cheon and Kim's results by applying element enumeration arguments. We then use this method to generalize their results to the ring algebraic integers.

1.2. **B-smooth Numbers in Cryptography.** Currently given sufficiently large integers, there is no known efficient non-quantum prime factorization algorithm. The difficulty of the prime factorization problem is leveraged when building cryptographic schemes that are difficult to crack (using even the most efficient algorithm, the General Number Field Sieve running on hundreds of specialized computers. One can imagine the near impossibility of randomly guessing the factorization).

With the rise of cybercrime, espionage, and the world's reliance on computers and digital information, it has become more critical to ensure that secure cryptography schemes exist in order to protect data privacy and integrity. To this end, factorization algorithms are constantly evolving in order to attack or prove the effectiveness of cryptography schemes that employ the difficulty of the prime factorization problem (some of these prime factorization algorithms can be applied on discrete logarithm problem-based cryptography).

Example 1.2.1. *In the RSA algorithm we use large integers with only two prime factors, p and q, preferably of similar length. RSA-130 is the integer with 130 digits:*

$$1807082088687404805951656164405905566278102516769401349170127021450056662540244048387341127590812303371781887966563182013214880557.$$

It can be shown that RSA-130 has prime factorization pq, where

$$p = 3968599945959745429016112616288378606757644911281006483255515724 3,$$

$$q = 455344986467359721884036868972744088643563012632050696009990445 99.$$

Since the history of factorization algorithms is rich and deep, we provide a condensed history of factorization algorithms and describe how smooth numbers and their error estimates play a central role in their discovery.

The most naïve approach to factorization is called trial division (sometimes called direct search factorization) which was described by Fibonacci in his book *Liber Abaci* [11]. In this algorithm, an integer N is systematically divided by all integers in $[2, \sqrt{N}]$ until we find the factorization. While this algorithm is guaranteed to produce the correct result every time, it would be completely impractical for factoring large integers in a reasonable amount of time. Subsequently, mathematicians have devised algorithms which exploit the properties of integers in order to reduce the amount of computations required. In turn, this reduces the time needed to find the factorization.

On April 7 1643, Fermat responded to a letter from Mersenne asking for a method to factor the integer $N = 100895598169 = 898423 \cdot 112303$ within a day [17]. Fermat discovered a method of factoring integers by utilizing the observation that any odd integer N can be written as a difference of squares $N = a^2 - b^2 = (a + b)(a - b)$ where a, b are non-trivial. Fermat's Factorization Method works by selecting values for $a \geq \sqrt{N}$ until $\sqrt{a^2 - N}$ is an integer, yielding b. However since $\sqrt{N} = 317640$, this means Fermat would have needed to take 187723 square roots. Consequently, it is possible that Fermat must have known some of the optimizations that can be applied to his method.

In 1981, Dixon discovered an algorithm based on solving the congruence of squares problem: Find integers x, y such that $x^2 \equiv y^2 \bmod N$ [6]. In essence, instead of searching for

the square of an integer as Fermat did, Dixon instead searches for integers that have small prime factors.

Dixon's algorithm takes as an input a value B (for which there exists an optimum value), a list of random integers in $[1, N]$, and the composite integer we wish to factor N [6]. Using B, we build what is called a factor base, that is, all primes that are B-smooth. Next, we search for all positive integers x such that $x^2 \bmod N$ is B-smooth, meaning its factors are in the factor base. After a sufficient number of such values for x are found, Dixon finds a set that satisfies the congruence of squares through the use of linear algebra, noticing that for every pair (x, y) there is a 50% chance that $\gcd(N, x + y)$ factors N. With a result from Pomerance's Multiplicative Independence for Random Integers, Dixon rigorously proves the expected runtime of his algorithm [8].

The quadratic sieve discovered by Pomerance is an optimization on Dixon's algorithm. Dixon's algorithm casts a wide net when attempting to search for B-smooth numbers by random sampling from a list of integers; however the quadratic number sieve optimizes this stage of Dixon's algorithm. As Pomerance describes, when attempting to recognize B-smooth numbers, there are fewer than B primes up to B [15]. This means that the number of trial divisions is at most $\max(\log_2 n, \pi(B))$, where π is the prime counting function. Pomerance describes how this search for suitable B-smooth numbers can be optimized by utilizing a method similar to the Sieve of Eratosthenes and we can identify a B-smooth number in $\log \log B$ steps on average.

In 1983, the quadratic sieve held the record for the largest factored number, namely one that had 71 digits and took 9.5 hours to factor [16]. In 1994, this algorithm factored RSA-129 (having 129 digits, and used 600 computers and 600 internet volunteers). However, Pomerance would later go on to describe that in April 1996, Pollard's general number sieve successfully factored RSA-130 (130 digits) in 15% of the time that the quadratic number sieve would have taken [14].

The general number sieve, in broad terms, requires the selection of two polynomials $F(x, y)$, $G(x, y)$ with which we search for coprime pairs of integers a, b such that the integers $F(a, b)$ and $G(a, b)$ are both B-smooth [2]. Then the probability of finding such pairs (which depends on the choice of polynomials) is inversely proportional to the runtime of the algorithm. In other words, the higher this probability is, the faster the algorithm runs.

We have now seen that finding efficient ways of identifying B-smooth numbers is critical to reducing the amount of operations in factoring algorithms. This results in reducing the computation time and resources, and improving the chances of solving the prime factorization problem that is at the core of many encryption schemes.

Other applications of smooth numbers include: cracking weak cryptography schemes, creating strong hashing functions, primality testing, and error-correcting functions [12].

2. Probability that the GCD of Products of Positive Integers is B-smooth

We now provide concise proofs for the probability that the GCD and k-GCD are B-smooth by using counting arguments. Appendix A contains detailed versions of Cheon and Kim's original proofs using the Inclusion-Exclusion Principle.

In this section, we find the probability that the greatest common divisor (GCD) of m products of n positive integers (all randomly chosen in a uniform and independent manner) is B-smooth.

We fix a positive integer N. Next, we randomly, uniformly, and independently choose integers $r_{ij} \in [1, N]$ for each integer $1 \leq i \leq m$ and $1 \leq j \leq n$ where $m \geq 2$ and $n \geq 1$. Our goal is to compute the probability that an ordered m-tuple (r_{ij}) satisfies the following condition:

$$\gcd\Big(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj}\Big)$$

is relatively prime to the first l primes greater than B.

Before stating the main theorem for this section, we establish the following useful lemma that we use in the ensuing derivation.

Lemma 2.0.1. *If n and k are positive integers, then*

$$\frac{1}{n}\Big\lfloor\frac{n}{k}\Big\rfloor = \frac{1}{k} + O\Big(\frac{1}{n}\Big).$$

Proof. By the definition of the floor function, $0 \leq x - \lfloor x \rfloor < 1$ for any real number x. Hence we can write

$$0 \leq \frac{n}{k} - \Big\lfloor\frac{n}{k}\Big\rfloor < 1.$$

Then, rearranging this inequality and dividing all three parts by n, we obtain

$$0 \leq \frac{1}{k} - \frac{1}{n}\Big\lfloor\frac{n}{k}\Big\rfloor < \frac{1}{n}.$$

The claim now directly follows. □

Now, we are ready to state and prove the main theorem of this section.

Theorem 2.0.2. *Fix positive integers B and N, and let $p_1, p_2, ...$ be the primes greater than B in increasing order. The probability of the GCD of products of random positive integers is not divisible by the first l primes greater than B is given by*

$$\prod_{i=1}^{l}\Big[1-\Big(1-\Big(1-\frac{1}{p_i}\Big)^n\Big)^m\Big].$$

Proof. We first find the probability that

$$\gcd\Big(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj}\Big)$$

is coprime to the first l primes greater than B. Note that for any prime p, there are $(N-\lfloor\frac{N}{p}\rfloor)^n$ products of n positive integers each of which is at most N that are not divisible by p. Hence, there are $N^n-(N-\lfloor\frac{N}{p}\rfloor)^n$ products of n positive integers each of which is at most N that are divisible by p. Therefore, there are

$$N^{mn}-\Big(N^n-\Big(N-\Big\lfloor\frac{N}{p}\Big\rfloor\Big)^n\Big)^m$$

m-tuples of products of n positive integers each of which is at most N that are not divisible by p.

Hence, the probability that an ordered m-tuple of products of n positive integers each of which is at most N are not divisible by p is equal to

$$\frac{N^{mn}-\Big(N^n-\Big(N-\Big\lfloor\frac{N}{p}\Big\rfloor\Big)^n\Big)^m}{N^{mn}}=1-\Big(1-\Big(1-\frac{1}{N}\Big\lfloor\frac{N}{p}\Big\rfloor\Big)^n\Big)^m.$$

Then, since divisibility by finitely many primes yields independent events, the probability that the GCD of m products of random positive integers at most N are not divisible by the

first l primes greater than B is equal to

$$\prod_{i=1}^{l}\Big[1-\Big(1-\Big(1-\frac{1}{N}\Big\lfloor\frac{N}{p_i}\Big\rfloor\Big)^n\Big)^m\Big].$$

Since we ultimately want to let $N\to\infty$, we now use the above Lemma to estimate the error from removing the floor function from our probability statement. This gives us

$$\begin{aligned}&\prod_{i=1}^{l}\Big[1-\Big(1-\Big(1-\Big(\frac{1}{p_i}+O\Big(\frac{1}{N}\Big)\Big)\Big)^n\Big)^m\Big]\\&=\prod_{i=1}^{l}\Big[1-\Big(1-\Big(1-\frac{1}{p_i}\Big)^n\Big)^m\Big]+O\Big(\frac{1}{N^{nm}}\Big).\end{aligned}$$

Finally letting $N\to\infty$ now gives us the desired result. □

We have found the probability that the GCD of products of random integers is not divisible by the first l primes greater than B. We now use this result to find the probability that the GCD of products of random integers is not divisible by *all* primes greater than B, thereby giving the probability that this GCD is B-smooth.

Theorem 2.0.3. *Suppose that each positive integer r_{ij} is chosen uniformly and independently from $\{1,2,...,N\}$. Then, the probability that $\gcd(\prod_{j=1}^{n}r_{1j},...,\prod_{j=1}^{n}r_{mj})$ is B-smooth converges (as $N\to\infty$) to*

$$\prod_{p>B}\Big[1-\Big(1-\Big(1-\frac{1}{p}\Big)^n\Big)^m\Big].$$

Proof. Letting $P(l,N)$ denote the probability in Theorem 2.0.2 (and for convenience setting $P(0,N)=1$, we define $g_N(l)=P(l-1,n)-P(l,n)$. Then, we see that $g_N(l)$ is precisely the probability that $\gcd(\prod_{j=1}^{n}r_{1j},...,\prod_{j=1}^{n}r_{mj})$ is coprime to $p_1,...,p_{l-1}$ and divisible by p_l for

uniformly and independently chosen r_{ij}'s from $\{1, 2, ..., N\}$. In particular, note that $g_N(l)$ is non-negative. We claim that we can move the limit to infinity past the summation sign:

$$\lim_{N\to\infty} \sum_{k=1}^{\infty} g_N(k) = \sum_{k=1}^{\infty} \lim_{N\to\infty} g_N(k).$$

In order to accomplish this, we use the Dominated Convergence Theorem (for series). Now we need to show that $g_N(l)$ is bounded above by $g(l) = \frac{n^m}{p_l^m}$ and $\sum_{l=1}^{\infty} g(l)$ converges.

We start by showing that $g_N(l)$ is bounded. We observe that

$$g_N(l) \leq \Pr\Big(p_l \Big| \gcd\Big(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj}\Big)\Big).$$

Computing the numerator to the probability on the last line, we find that

$$\begin{aligned}\Big|\{(r_{ij}) : p_l \mid \prod_{j=1}^{n} r_{1j}\Big|^m &= \frac{(N^n - |\{(r_{1j}) : p_l \nmid \prod_{j=1}^{n} r_{1j}\}|)^m}{N^{mn}} \\ &= \frac{(N^n - |\{r_{11} : p_l \nmid r_{11}\}|^n)^m}{N^{mn}}.\end{aligned}$$

Therefore, it follows that

$$\begin{aligned}g_N(l) &\leq \frac{(N^n - |\{r_{11} : p_l \nmid r_{11}\}|^n)^m}{N^{mn}} \\ &= \Big[1 - \Big(1 - \frac{1}{N}\Big\lfloor\frac{N}{p_l}\Big\rfloor\Big)^n\Big]^m \\ &\leq \Big[1 - \Big(1 - \frac{1}{p_l}\Big)^n\Big]^m \\ &\leq \frac{n^m}{p_l^m},\end{aligned}$$

where the last inequality directly follows from Bernoulli's inequality. Moreover $\sum_{l=1}^{\infty} g(l)$ converges, because we can bound this series from above with a convergent p-series (noting

that $m \geq 2$):

$$\sum_{l=1}^{\infty} g(l) = n^m \sum_{l=1}^{\infty} \frac{1}{p_l^m} < n^m \sum_{j=1}^{\infty} \frac{1}{j^m}.$$

Having satisfied the hypotheses of the Dominated Convergence Theorem, we observe that since $\sum_{k=1}^{l} g_N(k)$ is a telescoping sum, we obtain

$$\sum_{k=1}^{l} g_N(k) = \sum_{k=1}^{l} (P(k-1,n) - P(k,n)) = 1 - P(l,N),$$

and thus

$$\lim_{N\to\infty} \sum_{k=1}^{\infty} g_N(k) = 1 - \prod_{p>B} \Big[1 - \Big(1 - \Big(1 - \frac{1}{p_i}\Big)^n\Big)^m\Big].$$

Then since $\displaystyle\sum_{k=1}^{\infty} \lim_{N\to\infty} g_N(k)$ represents the complement of the probability we wanted to compute, the Dominated Convergence Theorem yields the desired assertion. □

Having derived the probability that the GCD of products of randomly chosen positive integers is B-smooth, we now find more convenient bounds for this product representation.

Theorem 2.0.4. *The probability that* $\gcd(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj})$ *is B-smooth is bounded above by*

$$\frac{1}{\zeta(m)} \prod_{p\leq B} \Big(1 - \frac{1}{p^m}\Big)^{-1},$$

and is bounded below by

$$\prod_{B<p\leq \hat{n}} \Big[1 - \Big(1 - \Big(1 - \frac{1}{p}\Big)^n\Big)^m\Big] \cdot \prod_{\hat{n}<p\leq \hat{r}} \Big(1 - \Big(\frac{n}{p}\Big)^m\Big) \cdot \frac{1}{\zeta(s)},$$

where $\hat{n} = \max\{n, B\}$, $\hat{r} = \max\{\hat{n}, \lfloor n^{\frac{m}{m-1}} + 1 \rfloor\}$, *and* $s = m(1 - \log_{\hat{r}} n) > 1$.

Remark. It is understood that for the lower bound, the first finite product is equal to 1 if $B = \hat{n}$, and the second finite product is equal to 1 if $\hat{n} = \hat{r}$.

Proof. We start by deriving the upper bound. Since $(1-\frac{1}{p})^n$ decreases as a function of n as $1-\frac{1}{p} \in (0,1)$, we obtain

$$\prod_{B<p\leq\hat{n}} \left[1-\left(1-\left(1-\frac{1}{p}\right)^n\right)^m\right] \leq \prod_{p>B}\left(1-\frac{1}{p^m}\right) = \frac{1}{\zeta(m)}\prod_{p\leq B}\left(1-\frac{1}{p^m}\right)^{-1},$$

where the rightmost equality uses the infinite product representation of the Riemann zeta function.

Next, we derive the lower bound for our probabilistic expression. We start by splitting the product at $\hat{n}$. We apply Bernoulli's inequality in the form $(1-x)^n \geq 1-nx$ where $x \in [0,1]$ and $n \geq 1$, and we take $x = \frac{1}{p}$ where $p > \hat{n}$ is a prime number. This yields

$$\prod_{B<p\leq\hat{n}} \left[1-\left(1-\left(1-\frac{1}{p}\right)^n\right)^m\right] \geq \prod_{B<p\leq\hat{n}} \left[1-\left(1-\left(1-\frac{1}{p}\right)^n\right)^m\right] \cdot \prod_{p>\hat{n}}\left(1-\left(\frac{n}{p}\right)^m\right).$$

It remains to find a lower bound for $\prod_{p>\hat{n}}(1-(\frac{n}{p})^m)$. By the definition of s, we have $p \geq \hat{r}$ is equivalent to $(\frac{n}{p})^m \leq \frac{1}{p^s}$. Using this fact in conjunction to the infinite product representation for the Riemann zeta function, we obtain

$$\begin{aligned}
\prod_{p>\hat{n}}\left(1-\left(\frac{n}{p}\right)^m\right) &= \prod_{\hat{n}<p\leq\hat{r}}\left(1-\left(\frac{n}{p}\right)^m\right) \cdot \prod_{p>\hat{r}}\left(1-\left(\frac{n}{p}\right)^m\right) \\
&\geq \prod_{\hat{n}<p\leq\hat{r}}\left(1-\left(\frac{n}{p}\right)^m\right) \cdot \prod_{p>\hat{r}}\left(1-\frac{1}{p^s}\right) \\
&\geq \prod_{\hat{n}<p\leq\hat{r}}\left(1-\left(\frac{n}{p}\right)^m\right) \cdot \frac{1}{\zeta(s)}.
\end{aligned}$$

The claimed lower bound now directly follows.

It remains to show that $s > 1$. We observe that since $r = \lfloor n^{\frac{m}{m-1}}+1 \rfloor$ and $\hat{r} = \max\{n, B, r\}$, we have $\hat{r} \geq r > n^{\frac{m}{m-1}}$. Hence, we conclude that $s = m(1-\log_{\hat{r}} n) > 1$ as required. $\square$

3. Probability that the k-GCD of Products of Positive Integers is B-smooth

In this section we extend the previous results to the k-GCD, and provide a more concise proof to Cheon and Kim's proof.

Definition 3.0.1. *Fix a positive integer k. The k-**GCD** of n nonzero integers $x_1, \ldots, x_n$, written $\gcd_k(x_1, \ldots, x_n)$, is the largest integer whose k^{th} power divides each of $x_1, \ldots, x_n$.*

Remark. When $k = 1$, the k-GCD reduces to the classic GCD.

Definition 3.0.2. *When $\gcd_k(x_1, x_2, \ldots, x_n) = 1$ we say that $x_1, x_2, \ldots, x_n$ are **relatively k-prime**.*

Example 3.0.3. *As k varies, it is possible that the k-GCD of a set of nonzero integers can change.*

For instance, although $\gcd(2^7, 2^6 \cdot 3, 2^8 \cdot 5) = 64$, we see that $\gcd_2(2^7, 2^6 \cdot 3, 2^8 \cdot 5) = 8$, while $\gcd_3(2^7, 2^6 \cdot 3, 2^8 \cdot 5) = 4$ and $\gcd_6(2^7, 2^6 \cdot 3, 2^8 \cdot 5) = 2$.

However since $\gcd_8(2^7, 2^6 \cdot 3, 2^8 \cdot 5) = 1$, we find that $2^7, 2^6 \cdot 3, 2^8 \cdot 5$ are relatively 8-prime.

We start by fixing a positive integer N. Next, we randomly, uniformly, and independently choose integers $r_{ij} \in [1, N]$ for each integer $1 \leq i \leq m$ and $1 \leq j \leq n$ where $m \geq 2$ and $n \geq 1$. We want to find the probability that an ordered m-tuple (r_{ij}) such that

$$\gcd{}_k\Big(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj}\Big)$$

is coprime to the first l primes greater than B.

Before stating the main theorem for this section, we establish the following lemmas that we use in the ensuing derivation below. We first need the following terminology from elementary number theory.

Definition 3.0.4. *Let a, n be integers and p be a prime number. We say that p^a* ***exactly divides*** *n, written as $p^a \,||\, n$, if $p^a \mid n$ but $p^{a+1} \nmid n$.*

Lemma 3.0.5. *Fix positive integers k and N. Let $Q_{p^k}(N)$ the number of ordered n-tuples of positive integers in which each entry is at most N such that p^k does not divide the product of these entries. Then, we have*

$$Q_{p^k}(N) = \sum_{a_1+\ldots+a_n<k} \Big[\prod_{j=1}^{n} \Big(\Big\lfloor \frac{N}{p^{a_j}} \Big\rfloor - \Big\lfloor \frac{N}{p^{a_j+1}} \Big\rfloor \Big) \Big].$$

Proof. Since the number of positive integers at most N that are divisible by p^j (for some prime p and positive integer j) equals $\lfloor \frac{N}{p^j} \rfloor$, it follows that the number of positive integers at most N where p^j *exactly* divides the positive integer is equal to

$$\Big\lfloor \frac{N}{p^j} \Big\rfloor - \Big\lfloor \frac{N}{p^{j+1}} \Big\rfloor.$$

Next, the number of ordered n-tuples $(m_1, \ldots, m_n)$ of positive integers in which each entry is at most N satisfying the conditions $p^{a_j} \,||\, m_j$ for each $j = 1, \ldots, n$ is given by the quantity

$$\prod_{j=1}^{n} \Big(\Big\lfloor \frac{N}{p^{a_j}} \Big\rfloor - \Big\lfloor \frac{N}{p^{a_j+1}} \Big\rfloor \Big).$$

Therefore, we conclude that $Q_{p^k}(N)$ is given as follows:

$$Q_{p^k}(N) = \sum_{a_1+\ldots+a_n<k} \Big[\prod_{j=1}^{n} \Big(\Big\lfloor \frac{N}{p^{a_j}} \Big\rfloor - \Big\lfloor \frac{N}{p^{a_j+1}} \Big\rfloor \Big) \Big].$$

□

We now give a less cumbersome representation for $Q_{p^k}(N)$ by estimating the error from removing the floor functions from its expression.

Lemma 3.0.6. *Using the same notation as in Lemma 3.0.5, we have the following estimate:*

$$Q_{p^k}(N) = \Big(N - \frac{N}{p}\Big)^n \Big(1 + \frac{{}_nH_1}{p} + ... + \frac{{}_nH_{k-1}}{p^{k-1}}\Big) + O(1),$$

where ${}_nH_j = \binom{n-1+j}{j}$.

Proof. Applying the basic estimate $\lfloor x \rfloor = x + O(1)$ to the result from Lemma 3.0.5, we obtain

$$\begin{aligned} Q_{p^k}(N) &= \sum_{a_1+...+a_n<k} \Big[\prod_{j=1}^{n} \Big(\frac{N}{p^{a_j}} - \frac{N}{p^{a_j+1}} + O(1)\Big)\Big] \\ &= \Big(N - \frac{N}{p}\Big)^n \sum_{a_1+...+a_n<k} \frac{1}{p^{a_1+...+a_n}} + O(1). \end{aligned}$$

Next for each non-negative integer less than k, there are ${}_nH_j = \binom{n-1+j}{j}$ solutions in non-negative integers to the equation $a_1 + ... + a_n = j$. Hence we conclude that

$$Q_{p^k}(N) = \Big(N - \frac{N}{p}\Big)^n \Big(1 + \frac{{}_nH_1}{p} + ... + \frac{{}_nH_{k-1}}{p^{k-1}}\Big) + O(1),$$

as required. □

Now, we are ready to state and prove the main theorem of this section.

Theorem 3.0.7. *Fix positive integers B and N, and let $p_1, p_2, ...$ be the primes greater than B in increasing order. The probability of the k-GCD of products of random integers is not divisible by the first l primes greater than B is given by*

$$\prod_{i=1}^{l} \Big[1 - \Big(1 - \Big(1 - \frac{1}{p_i}\Big)^n \Big(1 + \frac{{}_nH_1}{p} + ... + \frac{{}_nH_{k-1}}{p^{k-1}}\Big)\Big)^m\Big].$$

Proof. Letting $Q_{p^k}(N)$ denote the number of n positive integers each of which is at most N that are not divisible by p^k, there are $N^n - Q_{p^k}(N)$ products of n positive integers each of which is at most N that are divisible by p^k. Therefore, there are

$$N^{mn} - (N^n - Q_{p^k}(N))^m$$

ordered m-tuples of products of n positive integers each of which is at most N that are not divisible by p^k. Hence, the probability that an ordered m-tuples of products of n positive integers each of which is at most N that are not divisible by p^k is equal to

$$\frac{N^{mn} - (N^n - Q_{p^k}(N))^m}{N^{mn}} = 1 - \Big(1 - \frac{Q_{p^k}(N)}{N^n}\Big)^m.$$

Now, we use Lemma 3.0.6 to rewrite the latter probability as follows:

$$1 - \Big[1 - \Big(1 - \frac{1}{p}\Big)^n \Big(1 + \frac{{}_nH_1}{p} + ... + \frac{{}_nH_{k-1}}{p^{k-1}}\Big)\Big]^m + O\Big(\frac{1}{N^{mn}}\Big).$$

Then, since divisibility by finitely many primes are independent events, we deduce that the probability that an ordered m-tuples of products of n positive integers each of which is at most N that are not divisible by p_1^k, ..., p_l^k is equal to

$$\prod_{i=1}^{l} \Big[1 - \Big(1 - \Big(1 - \frac{1}{p_i}\Big)^n \Big(1 + \frac{{}_nH_1}{p_i} + \ldots + \frac{{}_nH_{k-1}}{p_i^{k-1}}\Big)\Big)^m + O\Big(\frac{1}{N^{mn}}\Big)\Big]$$
$$= \prod_{i=1}^{l} \Big[1 - \Big(1 - \Big(1 - \frac{1}{p_i}\Big)^n \Big(1 + \frac{{}_nH_1}{p_i} + \ldots + \frac{{}_nH_{k-1}}{p_i^{k-1}}\Big)\Big)^m\Big] + O\Big(\frac{1}{N^{mn}}\Big).$$

Letting $N \to \infty$ now gives us the desired result. □

We have found the probability that the k-GCD of products of random integers is not divisible by the first l primes greater than B. We now use this result to find the probability

that the k-GCD of products of random integers is not divisible by *all* primes greater than B, thereby giving the probability that this k-GCD is B-smooth.

Theorem 3.0.8. *Suppose that each r_{ij} is chosen uniformly and independently from $\{1, 2, ..., N\}$. Then, the probability that $\gcd_k(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj})$ is B-smooth converges (as $N \to \infty$) to*

$$\prod_{p>B} \left[1 - \left(1 - \left(1 - \frac{1}{p_i}\right)^n \left(1 + \frac{{}_nH_1}{p} + ... + \frac{{}_nH_{k-1}}{p^{k-1}}\right)\right)^m\right].$$

Proof. Let $P(l, N)$ denote the probability in Theorem 3.0.7 (and for convenience setting $P(0, N) = 1$). We define $g_N(l) = P(l-1, n) - P(l, n)$. Then, we see that $g_N(l)$ is precisely the probability that k- $\gcd(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj})$ is coprime to $p_1, \ldots, p_{l-1}$ and divisible by p_l for uniformly and independently chosen r_{ij}'s from $\{1, 2, ..., N\}$. In particular, note that $g_N(l)$ is non-negative. We claim that we can move the limit to infinity past the summation sign:

$$\lim_{N\to\infty} \sum_{s=1}^{\infty} g_N(s) = \sum_{s=1}^{\infty} \lim_{N\to\infty} g_N(s).$$

In order to accomplish this, we use the Dominated Convergence Theorem (for series). Now, we need to show that $g_N(l)$ is bounded above by $g(l) = \frac{n^m}{p_l^{km}}$ and $\sum_{l=1}^{\infty} g(l)$ converges.

We start by showing that $g_N(l)$ is bounded. We observe that

$$g_N(l) \leq \Pr\left(p_l^k \,\middle|\, \gcd\left(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj}\right)\right).$$

Computing the numerator to the probability on the last line, we find that

$$\left|\{(r_{ij}) : p_l^k \mid \prod_{j=1}^{n} r_{1j}\}\right|^m = \frac{(N^n - |\{(r_{1j}) : p_l^k \nmid \prod_{j=1}^{n} r_{1j}\}|)^m}{N^{mn}}$$
$$= \frac{(N^n - |\{r_{11} : p_l^k \nmid r_{11}\}|^n)^m}{N^{mn}}.$$

Therefore, it follows that

$$\begin{aligned} g_N(l) &\leq \frac{(N^n - |\{r_{11} : p_l^k \nmid r_{11}\}|^n)^m}{N^{mn}} \\ &= \left[1 - \left(1 - \frac{1}{N}\left\lfloor \frac{N}{p_l^k} \right\rfloor\right)^n\right]^m \\ &\leq \left[1 - \left(1 - \frac{1}{p_l^k}\right)^n\right]^m \\ &\leq \frac{n^m}{p_l^{km}}, \end{aligned}$$

where the last inequality directly follows from Bernoulli's inequality. Moreover $\sum_{l=1}^{\infty} g(l)$ converges, because we can bound this series from above with a convergent p-series (noting that $m \geq 2$):

$$\sum_{l=1}^{\infty} g(l) = n^m \sum_{l=1}^{\infty} \frac{1}{p_l^{km}} < n^m \sum_{j=1}^{\infty} \frac{1}{j^{km}}.$$

Having satisfied the hypotheses of the Dominated Convergence Theorem, we observe that since $\sum_{s=1}^{l} g_N(s)$ is a telescoping sum, we obtain

$$\sum_{s=1}^{l} g_N(s) = \sum_{s=1}^{l} (P(s-1,n) - P(s,n)) = 1 - P(l,N),$$

and thus

$$\lim_{N\to\infty} \sum_{s=1}^{\infty} g_N(s) = 1 - \prod_{p>B} \left[1 - \left(1 - \left(1 - \frac{1}{p_i}\right)^n \left(1 + \frac{{}_nH_1}{p} + ... + \frac{{}_nH_{k-1}}{p^{k-1}}\right)\right)^m\right].$$

Then since $\sum_{s=1}^{\infty} \lim_{N\to\infty} g_N(s)$ represents the complement of the probability we wanted to compute, the Dominated Convergence Theorem yields the desired assertion. $\square$

4. Background Material for the Algebraic Integer Case

We now provide some key concepts involving algebraic integers that we use for the remainder of the proofs in this paper. Unsurprisingly, the derivations of these results have the similar flow and form to their rational integer counterparts, and by choosing particular values, yields the rational integer cases. For further details, please see [10].

Definition 4.0.1. *A complex number is an* ***algebraic number*** *if it is a zero of a polynomial with rational coefficients.*

Definition 4.0.2. *A number is an* ***algebraic integer*** *if it is a zero of a monic polynomial with integer coefficients.*

The set of all algebraic integers forms a ring and is denoted by $\mathbb{A}$.

Definition 4.0.3. *The* ***(algebraic) number ring****, denoted by* $\mathcal{O}$*, is the ring of algebraic integers of the algebraic field* K *given by* $\mathcal{O} = K \cap \mathbb{A}$.

Definition 4.0.4. *We say that an ideal* $\mathfrak{p}$ *in a number ring* $\mathcal{O}$ *is* ***prime*** *if whenever* $\mathfrak{ab} \subseteq \mathfrak{p}$ *for some ideals* $\mathfrak{a}, \mathfrak{b}$ *in* $\mathcal{O}$ *implies* $\mathfrak{a} \subseteq \mathfrak{p}$ *or* $\mathfrak{b} \subseteq \mathfrak{p}$.

Definition 4.0.5. *A* ***Dedekind domain*** *is a Noetherian, integrally closed, integral domain of Krull dimension 1.*

Remark. There are alternative ways to define a Dedekind domain.

Theorem 16 in [10] states that every ideal in a Dedekind domain is uniquely factors into prime ideals and Theorem 14 in [10] states that every number ring is a Dedekind domain. Thus, every ideal of a number ring uniquely factors into prime ideals. We use this fact to ensure uniqueness whenever we count ideals.

Definition 4.0.6. *Let $\mathfrak{a}$ be a nonzero ideal of a number ring $\mathcal{O}$. We define the* ***ideal norm*** *of $\mathfrak{a}$ as $\mathfrak{N}(\mathfrak{a}) := |\mathcal{O}/\mathfrak{a}|$.*

Example 4.0.7. *Let $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$ and $\mathfrak{a} = \langle 3 \rangle$ (that is, the ideal generated by 3). Then, $\mathfrak{N}(\langle 3 \rangle) = \left|\mathbb{Z}[\sqrt{-5}]/\langle 3 \rangle\right| = 3^2$.*

Observe that every element of $\mathbb{Z}[\sqrt{-5}]$ is of the form $a + b\sqrt{-5}$ where $a, b \in \mathbb{Z}$. Thus, elements in $\mathbb{Z}[\sqrt{-5}]/\langle 3 \rangle$ have the form $a + b\sqrt{-5} + \langle 3 \rangle$, where $a, b \in \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$ (3 choices for each). Thus $\left|\mathbb{Z}[\sqrt{-5}]/\langle 3 \rangle\right|$ has exactly 3^2 elements.

Not only is the norm on ideals finite, it also gives a completely multiplicative function. That is, for any ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}$, we have

$$\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}).$$

Having defined the norm, we can now give the number ring generalization of the Riemann zeta function.

Definition 4.0.8. *Let $\mathcal{O}$ be an algebraic number ring. The* ***Dedekind zeta function*** *of $\mathcal{O}$ is given by*

$$\zeta_{\mathcal{O}}(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s},$$

where the sum is over all non-zero ideals of $\mathcal{O}$.

Equivalently, the Dedekind zeta function can be defined by the Dirichlet series

$$\zeta_{\mathcal{O}}(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

where c_n is the number of ideals with norm n. The following theorem states that the Dedekind zeta function can be represented by the Euler product indexed by all prime *ideals* of $\mathcal{O}$,

Theorem 4.0.9.

$$\zeta_{\mathcal{O}}(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}\ prime} (1 - \mathfrak{N}(\mathfrak{p})^{-s})^{-1}.$$

Proof. Refer to Theorem 42 in [10]. □

Remark. As with the Riemann zeta Function, the Dedekind zeta Function converges for all $\mathrm{Re}(s) > 1$.

Definition 4.0.10. *Fix $r \in \mathbb{N}$. We say that nonzero ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k \subseteq \mathcal{O}$ are* ***relatively r-prime*** *if $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k \not\subseteq \mathfrak{b}^r$ for any nonzero and proper ideal $\mathfrak{b}$.*

Definition 4.0.11. *Let $H(n)$ denote the number of ideals in $\mathcal{O}$ with norm less than or equal to n.*

Note that n need not be an integer. The following theorem provides an estimate that we repeatedly use in the derivations that follow.

Theorem 4.0.12. *There exists $c > 0$ such that $H(n) = cn + O(n^{1-\epsilon})$ where $\epsilon = [K : \mathbb{Q}]^{-1}$.*

Proof. Refer to Theorem 39 in [10]. □

Remark. If $K = \mathbb{Q}$ so that $\mathcal{O} = \mathbb{Z}$, then H reduces to the floor function.

5. Probability that the GCD of Products of Algebraic Integers is B-smooth

Definition 5.0.1. *Let B be a fixed positive integer and $\mathcal{O}$ be an algebraic number ring. A nonzero ideal $\mathfrak{a}$ in $\mathcal{O}$ is B-**smooth** (B-**friable**) if $\mathfrak{a}$ has no prime ideal factor whose norm is greater than B.*

Remark. In the case where $\mathcal{O}$ is a PID, we can replace ideals with elements, then check that the elements have no prime factors with an absolute value of their norm that is greater than B.

Example 5.0.2. *Let $\mathcal{O} = \mathbb{Z}[i]$, the ring of Gaussian integers. Since $\mathbb{Z}[i]$ is a PID, we use the element norm $N(a+bi) = a^2 + b^2$ instead of the ideal norm. Taking $B = 15$, $7 + 6i$ is not 15-smooth, because its prime factorization is $(2+i)(4+i)$, and $N(4+i) = 17 > 15$. On the other hand, $9 - 3i$ is 15-smooth, because its prime factorization is $3(3-i)$, with norms $N(3) = 9$ and $N(3-i) = 10$, both less than 15.*

For the remainder of this section, we are going to find the probability that the greatest common divisor (GCD) of m products of n nonzero ideals in an algebraic number ring $\mathcal{O}$ (all randomly chosen in a uniform and independent manner) is B-smooth.

We fix a positive integer N. Next, we randomly, uniformly, and independently, choose ideals $\mathfrak{a}_{ij}$ whose norms at most N for each integer $1 \leq i \leq m$ and $1 \leq j \leq n$ where $m \geq 2$ and $n \geq 1$. We want to find the probability that an ordered m-tuple $(\mathfrak{a}_{ij})$ such that

$$\gcd\Big(\prod_{j=1}^{n} \mathfrak{a}_{1j}, ..., \prod_{j=1}^{n} \mathfrak{a}_{mj}\Big)$$

is coprime to the first l prime ideals (arranged in non-decreasing order by norm) having norm greater than B. We start with the following error bound.

Lemma 5.0.3. *If k is a positive integer, then there exists a constant $\epsilon > 0$ such that for all sufficiently large n:*

$$\frac{1}{H(n)} H\Big(\frac{n}{k}\Big) = \frac{1}{k} + O\Big(\frac{1}{n^{\epsilon}}\Big).$$

Proof. Since we know from Theorem 4.0.12 that $H(x) = cx + O(x^{1-\epsilon})$ for some constants $c, \epsilon > 0$, there exists a constant $A > 0$ such that for all sufficiently large x:

$$|H(x) - cx| < Ax^{1-\epsilon}.$$

By using this inequality, we deduce for all sufficiently large n that

$$\frac{1}{H(n)} H\Big(\frac{n}{k}\Big) \leq \frac{\frac{cn}{k} + A(\frac{n}{k})^{1-\epsilon}}{cn - An^{1-\epsilon}} = \frac{\frac{cn}{k}(1 + \frac{Ak^{\epsilon}}{c} n^{-\epsilon})}{cn(1 - \frac{A}{c} n^{-\epsilon})}.$$

Applying the geometric series to the right side of the inequality above, we obtain for all sufficiently large n:

$$\frac{1}{H(n)} H\Big(\frac{n}{k}\Big) = \frac{1}{k}\Big(1 + \frac{Ak^{\epsilon}}{c} n^{-\epsilon}\Big)\Big(1 + O\Big(\frac{1}{n^{\epsilon}}\Big)\Big) = \frac{1}{k} + O\Big(\frac{1}{n^{\epsilon}}\Big),$$

and that is what we wanted to prove. □

Theorem 5.0.4. *Fix positive integers B and N and a number ring $\mathcal{O}$. Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ be the prime ideals in $\mathcal{O}$ with norm greater than B arranged in non-decreasing order by norm. Then, the probability of the GCD of products of random ideals is not divisible by the first l*

prime ideals greater than B is given by

$$\prod_{i=1}^{l}\Big[1-\Big(1-\Big(1-\frac{1}{\mathfrak{N}(\mathfrak{p}_i)}\Big)^n\Big)^m\Big].$$

Proof. For any prime ideal $\mathfrak{p}$, there are $\big[H(N)-H\big(\frac{N}{\mathfrak{N}(\mathfrak{p})}\big)\big]^n$ products of ideals with norm at most N that are not divisible by $\mathfrak{N}(\mathfrak{p})$. Hence, there are $H(N)^n-\big[H(N)-H\big(\frac{N}{\mathfrak{N}(\mathfrak{p})}\big)\big]^n$ products of ideals with norm at most N that are divisible by $\mathfrak{N}(\mathfrak{p})$. Therefore, there are

$$H(N)^{nm}-\Big[H(N)^n-\Big(H(N)-H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p})}\Big)\Big)^n\Big]^m$$

ordered m-tuples of products of ideals, each of which has norm at most N and is not divisible by $\mathfrak{N}(\mathfrak{p})$. Then, the probability that an ordered m-tuple of products of ideals, each of which has norm at most N and is not divisible by $\mathfrak{N}(\mathfrak{p})$ is equal to

$$\frac{H(N)^{nm}-\Big[H(N)^n-\Big(H(N)-H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p})}\Big)\Big)^n\Big]^m}{H(N)^{nm}}=1-\Big[1-\Big(1-\frac{1}{H(N)}H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p})}\Big)\Big)^n\Big]^m.$$

Then since divisibility by finitely many primes yields independent events, we find that the probability that the GCD of m products of random ideals with norm at most N are not divisible by the first l prime ideals:

$$\prod_{i=1}^{l}\Big[1-\Big(1-\Big(1-\frac{1}{H(N)}H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p})}\Big)\Big)^n\Big)^m\Big].$$

We now examine what happens to our probability as $N\to\infty$. Using the estimate for $H(n)$ from Lemma 5.0.3 then gives us

$$\begin{aligned}&\prod_{i=1}^{l}\Big[1-\Big(1-\Big(1-\frac{1}{\mathfrak{N}(\mathfrak{p}_i)}+O\Big(\frac{1}{N^\epsilon}\Big)\Big)^n\Big)^m\Big]\\&=\prod_{i=1}^{l}\Big[1-\Big(1-\Big(1-\frac{1}{\mathfrak{N}(\mathfrak{p}_i)}\Big)^n\Big)^m\Big]+O\Big(\frac{1}{N^\epsilon}\Big).\end{aligned}$$

Finally, letting $N \to \infty$ gives us the desired result. $\square$

Remark. Setting $\mathcal{O} = \mathbb{Z}$, prime ideals are substituted for the prime integers, and $\epsilon = 1$, yields the same result as for the integers case.

As in the case for the integers, this only provides the probability for the first l prime ideals greater than B. Using the Dominated Convergence Theorem, we can take the limit as l approaches infinity.

Theorem 5.0.5. *The probability that the GCD of products of random ideals of algebraic integers in a given number ring $\mathcal{O}$ is B-smooth converges to*

$$\prod_{\mathfrak{N}(\mathfrak{p})>B} \left[1 - \left(1 - \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right)^n\right)^m\right].$$

Proof. Let $P(l, N)$ denote the probability in Theorem 5.0.4 (and for convenience setting $P(0, N) = 1$). We define $g_N(l) = P(l-1, n) - P(l, n)$. Then, we see that $g_N(l)$ is precisely the probability that $\gcd(\prod_{j=1}^n \mathfrak{a}_{1j}, ..., \prod_{j=1}^n \mathfrak{a}_{mj})$ is coprime to $\mathfrak{p}_1, ..., \mathfrak{p}_{l-1}$ and divisible by $\mathfrak{p}_l$ for uniformly and independently chosen $\mathfrak{a}_{ij}$'s from $\{1, 2, ..., N\}$. In particular, note that $g_N(l)$ is non-negative. We claim that we can move the limit to infinity past the summation sign:

$$\lim_{N\to\infty} \sum_{k=1}^{\infty} g_N(k) = \sum_{k=1}^{\infty} \lim_{N\to\infty} g_N(k).$$

In order to accomplish this, we use the Dominated Convergence Theorem (for series). Now we need to show that $g_N(l)$ is bounded above by $g(l) = \frac{n^m}{\mathfrak{N}(\mathfrak{p}_l)^m}$ and $\sum_{l=1}^{\infty} g(l)$ converges.

We start by showing that $g_N(l)$ is bounded. We observe that

$$g_N(l) \leq \Pr\left(\mathfrak{p}_l \middle| \gcd\left(\prod_{j=1}^n \mathfrak{a}_{1j}, \ldots, \prod_{j=1}^n \mathfrak{a}_{mj}\right)\right).$$

Computing the numerator to the probability on the last line, we find that

$$\Big|\{(\mathfrak{a}_{ij}) : \mathfrak{p}_l \mid \prod_{j=1}^{n} \mathfrak{a}_{1j}\}\Big|^m = \frac{(H(N)^n - |\{(\mathfrak{a}_{1j}) : \mathfrak{p}_l \nmid \prod_{j=1}^{n} \mathfrak{a}_{1j}\}|)^m}{H(N)^{mn}}$$

$$= \frac{(H(N)^n - |\{\mathfrak{a}_{11} : \mathfrak{p}_l \nmid \mathfrak{a}_{11}\}|^n)^m}{H(N)^{mn}}.$$

Therefore, it follows for all sufficiently large N that

$$\begin{aligned} g_N(l) &\leq \frac{(H(N)^n - |\{\mathfrak{a}_{11} : \mathfrak{p}_l \nmid \mathfrak{a}_{11}\}|^n)^m}{H(N)^{mn}} \\ &\leq \Big(1 - \Big(1 - \frac{1}{H(N)} H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p}_l)}\Big)\Big)^n\Big)^m \\ &= \Big(1 - \Big(1 - \Big(\frac{1}{\mathfrak{N}(\mathfrak{p}_l)} + \frac{A}{N^\epsilon}\Big)\Big)^n\Big)^m \text{ for some } A > 0 \\ &\leq \Big(1 - \Big(1 - \frac{2}{\mathfrak{N}(\mathfrak{p}_l)}\Big)^n\Big)^m. \end{aligned}$$

The latter expression is bounded above by $g(l) = \frac{(2n)^m}{\mathfrak{N}(\mathfrak{p}_l)^m}$ by Bernoulli's inequality in the form $1 - (1-x)^t \leq xt$ for $t \geq 1$ and $0 \leq x \leq 1$. Moreover $\sum_{l=1}^{\infty} g(l)$ converges, because we can bound this series from above with a constant multiple of the Dedekind zeta function (with $m \geq 2$):

$$\sum_{l=1}^{\infty} g(l) \leq (2n)^m \sum_{l=1}^{\infty} \frac{1}{\mathfrak{N}(\mathfrak{p}_l)^m} \leq (2n)^m \zeta_{\mathcal{O}}(m) < \infty.$$

Having satisfied the hypotheses of the Dominated Convergence Theorem, we observe that since $\sum_{k=1}^{l} g_N(k)$ is a telescoping sum, we obtain

$$\sum_{k=1}^{l} g_N(k) = \sum_{k=1}^{l} (P(k-1,n) - P(k,n)) = 1 - P(l,N),$$

and thus

$$\lim_{N\to\infty} \sum_{k=1}^{\infty} g_N(k) = 1 - \prod_{\mathfrak{N}(\mathfrak{p})>B} \Big[1 - \Big(1 - \Big(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\Big)^n\Big)^m\Big].$$

Since $\sum_{k=1}^{\infty} \lim_{N\to\infty} g_N(k)$ represents the complement of the probability we wanted to compute, the Dominated Convergence Theorem yields the desired assertion. $\square$

6. Probability that the k-GCD of Products of Algebraic Integers is B-smooth

Definition 6.0.1. *Fix a positive integer k. The **k-GCD** of n prime ideals $\mathfrak{a}_1$, $\mathfrak{a}_2$,..., $\mathfrak{a}_n$ in a number ring $\mathcal{O}$, written $\gcd_k(\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n)$, is the largest prime ideal whose k^{th} power divides each of $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$.*

Observe that when $k = 1$, the k-GCD reduces to the standard GCD of ideals.

Lemma 6.0.2. *Fix positive integers k and N. Let $Q_{\mathfrak{p}^k}(N)$ the number of ordered n-tuples of nonzero ideals in a number ring $\mathcal{O}$, in which each entry has norm at most N such that $\mathfrak{p}^k$ does not divide the product of these entries. Then, we have*

$$Q_{\mathfrak{p}^k}(N) = \sum_{a_1+\ldots+a_n<k} \Big[\prod_{j=1}^{n} \Big(H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p})^{a_j}}\Big) - H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p})^{a_j+1}}\Big)\Big)\Big].$$

Proof. Since the number of nonzero ideals with norm at most N that are divisible by $\mathfrak{N}(\mathfrak{p})^j$ (for some nonzero prime ideal $\mathfrak{p}$ and positive integer j) equals $H\big(\frac{N}{\mathfrak{N}(\mathfrak{p})^j}\big)$, it follows that the number of nonzero prime ideals at most N where $\mathfrak{N}(\mathfrak{p})^j$ *exactly* divides the nonzero ideal is equal to

$$H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p})^j}\Big) - H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p})^{j+1}}\Big).$$

Next, the number of ordered n-tuples $(m_1, ..., m_n)$ of nonzero ideals in which entry is at most N satisfying the conditions $\mathfrak{p}^{a_j} \mid\mid m_j$ for each $j = 1, ..., n$ is given by the quantity

$$\prod_{j=1}^{n} H\left(\frac{N}{\mathfrak{N}(\mathfrak{p})^j}\right) - H\left(\frac{N}{\mathfrak{N}(\mathfrak{p})^{j+1}}\right).$$

Therefore, we conclude that $Q_{\mathfrak{p}^k}(N)$ is given as follows:

$$Q_{\mathfrak{p}^k}(N) = \sum_{a_1+...+a_n<k} \left[\prod_{j=1}^{n} H\left(\frac{N}{\mathfrak{N}(\mathfrak{p})^j}\right) - H\left(\frac{N}{\mathfrak{N}(\mathfrak{p})^{j+1}}\right)\right].$$

□

We now give a less cumbersome representation for $Q_{p^k}(N)$ by estimating the error from removing the ideal counting functions from its expression.

Lemma 6.0.3. *Using the same notation as in the Lemma 6.0.2, we have the following estimate:*

$$Q_{\mathfrak{p}^k}(N) = H(N)^n\left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right)^n\left(1 + \frac{{}_nH_1}{\mathfrak{N}(\mathfrak{p})} + ... + \frac{{}_nH_{k-1}}{\mathfrak{N}(\mathfrak{p})^{k-1}}\right) + O(1),$$

where ${}_nH_j = \binom{n-1-j}{j}$.

Proof. Applying Lemma 5.0.3 to Lemma 6.0.2, for some $\epsilon > 0$, we obtain

$$\begin{aligned} Q_{\mathfrak{p}^k}(N) &= \sum_{a_1+...+a_n<k} H(N)^n\Big[\prod_{j=1}^{n} \frac{1}{\mathfrak{N}(\mathfrak{p})^j} - \frac{1}{\mathfrak{N}(\mathfrak{p})^{j+1}} + O\left(\frac{1}{N^\epsilon}\right)\Big] \\ &= H(N)^n\left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right)^n \sum_{a_1+...+a_n<k} \frac{1}{\mathfrak{N}(\mathfrak{p})^{a_1+...+a_n}} + O(1). \end{aligned}$$

Next for each non-negative integer less than k, there are ${}_nH_j = \binom{n-1+j}{j}$ solutions in non-negative integers to the equation $a_1 + ... + a_n = j$. Hence we conclude that

$$Q_{\mathfrak{p}^k}(N) = H(N)^n\Big(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\Big)^n\Big(1 + \frac{{}_nH_1}{\mathfrak{N}(\mathfrak{p})} + ... + \frac{{}_nH_{k-1}}{\mathfrak{N}(\mathfrak{p})^{k-1}}\Big) + O(1),$$

as required. □

Now, we are ready to state and prove the main theorem of this section.

Theorem 6.0.4. *Fix positive integers B and N, and let $\mathfrak{p}_1, \mathfrak{p}_2, ...$ be the prime ideals in a number ring $\mathcal{O}$ with norm greater than B in increasing order. Then, the probability of the k-GCD of products of random nonzero ideals in a number ring $\mathcal{O}$ is not divisible by the first l prime ideals with norm greater than B is given by*

$$\prod_{i=1}^{l}\Big[1 - \Big(1 - \Big(1 - \frac{1}{\mathfrak{N}(\mathfrak{p}_i)}\Big)^n\Big(1 + \frac{{}_nH_1}{\mathfrak{N}(\mathfrak{p}_i)} + \ldots + \frac{{}_nH_{k-1}}{\mathfrak{N}(\mathfrak{p}_i)^{k-1}}\Big)\Big)^m\Big].$$

Proof. Let $Q_{\mathfrak{p}^k}(N)$ denote the number of n non zero ideals each of which have norm at most N that are not divisible by $\mathfrak{p}^k$, there are $H(N)^n - Q_{\mathfrak{p}^k}(N)$ products of n nonzero ideals each of which has norm at most N that are divisible by $\mathfrak{p}^k$. Therefore, there are

$$H(N)^{mn} - (H(N)^n - Q_{\mathfrak{p}^k}(N))^m$$

ordered m-tuples of products of n nonzero ideals each of which is at most N that are not divisible by $\mathfrak{p}^k$.

Hence, the probability that an ordered m-tuples of products of n nonzero ideals each of which has norm at most N that are not divisible by $\mathfrak{p}^k$ is equal to

$$\frac{H(N)^{mn} - (H(N)^n - Q_{\mathfrak{p}^k}(N))^m}{H(N)^{mn}} = 1 - \Big(1 - \frac{Q_{\mathfrak{p}^k}(N)}{H(N)^n}\Big)^m.$$

Now, we use the result of Lemma 6.0.3 to rewrite the latter probability as follows:

$$1-\Big[1-\Big(1-\frac{1}{\mathfrak{N}(\mathfrak{p})}\Big)^n\Big(1+\frac{{}_nH_1}{\mathfrak{N}(\mathfrak{p})}+...+\frac{{}_nH_{k-1}}{\mathfrak{N}(\mathfrak{p})^{k-1}}\Big)\Big]^m+O\Big(\frac{1}{H(N)^{nm}}\Big).$$

Then, since divisibility by finitely many nonzero prime ideals give independent events, we deduce that the probability that an ordered m-tuples of products of n nonzero ideals each of which is at most N that are not divisible by $\mathfrak{p}_1^k,\dots,\mathfrak{p}_l^k$ is equal to

$$\begin{aligned}&\prod_{i=1}^{l}\left[1-\Big[1-\Big(1-\frac{1}{\mathfrak{N}(\mathfrak{p}_i)}\Big)^n\Big(1+\frac{{}_nH_1}{\mathfrak{N}(\mathfrak{p}_i)}+...+\frac{{}_nH_{k-1}}{\mathfrak{N}(\mathfrak{p}_i)^{k-1}}\Big)\Big]^m+O\Big(\frac{1}{H(N)^{nm}}\Big)\right]\\&=\prod_{i=1}^{l}\Big[1-\Big(1-\Big(1-\frac{1}{\mathfrak{N}(\mathfrak{p}_i)}\Big)^n\Big(1+\frac{{}_nH_1}{\mathfrak{N}(\mathfrak{p}_i)}+\dots+\frac{{}_nH_{k-1}}{\mathfrak{N}(\mathfrak{p}_i)^{k-1}}\Big)\Big)^m\Big]+O\Big(\frac{1}{H(N)^{mn}}\Big).\end{aligned}$$

Letting $N\to\infty$ now gives us the desired result. □

We have so far found the probability that the k-GCD of products of random nonzero ideals in a number ring $\mathcal{O}$ is not divisible by the first l nonzero prime ideals greater than B. We now use this result to find the probability that the k-GCD of products of random nonzero ideals is not divisible by *all* non zero prime ideals with norm greater than B, thereby giving the probability that this k-GCD is B-smooth.

Theorem 6.0.5. *Suppose that each $\mathfrak{a}_{ij}$ is randomly, independently, and uniformly chosen from $\mathcal{O}$. The probability that $\gcd_k(\prod_{j=1}^n\mathfrak{a}_{ij},\dots,\prod_{j=1}^n\mathfrak{a}_{mj})$ is B-smooth converges as $N\to\infty$ to*

$$\prod_{\mathfrak{N}(\mathfrak{p})>B}\Big[1-\Big(1-\Big(1-\frac{1}{\mathfrak{N}(\mathfrak{p})}\Big)^n\Big(1+\frac{{}_nH_1}{\mathfrak{N}(\mathfrak{p})}+\dots+\frac{{}_nH_{k-1}}{\mathfrak{N}(\mathfrak{p})^{k-1}}\Big)\Big)^m\Big].$$

Proof. Let $P(l,N)$ denote the probability in Theorem 6.0.4 (and for convenience setting $P(0,N)=1$). We define $g_N(l)=P(l-1,n)-P(l,n)$. Then, we see that $g_N(l)$ is precisely

the probability that $\gcd_k(\prod_{j=1}^n \mathfrak{a}_{1j}, ..., \prod_{j=1}^n \mathfrak{a}_{mj})$ is coprime to $\mathfrak{p}_1, \ldots, \mathfrak{p}_{l-1}$ and divisible by $\mathfrak{p}_l$ for uniformly and independently chosen $\mathfrak{a}_{ij}$'s from $\{1, 2, ..., N\}$. In particular, note that $g_N(l)$ is non-negative. We claim that we can move the limit to infinity past the summation sign:

$$\lim_{N\to\infty} \sum_{s=1}^{\infty} g_N(s) = \sum_{s=1}^{\infty} \lim_{N\to\infty} g_N(s).$$

In order to accomplish this, we use the Dominated Convergence Theorem (for series). Now we need to show that $g_N(l)$ is bounded above by $g(l) = \frac{n^m}{\mathfrak{N}(\mathfrak{p}_l)^m}$ and $\sum_{l=1}^{\infty} g(l)$ converges.

We start by showing that $g_N(l)$ is bounded. We observe that

$$g_N(l) \leq \Pr\Big(\mathfrak{p}_l^k \Big| \gcd\Big(\prod_{j=1}^n \mathfrak{a}_{1j}, \ldots, \prod_{j=1}^n \mathfrak{a}_{mj}\Big)\Big).$$

Computing the numerator to the probability on the last line, we find that

$$\begin{aligned}\Big|\{(\mathfrak{a}_{ij}) : \mathfrak{p}_l^k \mid \prod_{j=1}^n \mathfrak{a}_{1j}\}\Big|^m &= \frac{(H(N)^n - |\{(\mathfrak{a}_{1j}) : \mathfrak{p}_l^k \nmid \prod_{j=1}^n \mathfrak{a}_{1j}\}|)^m}{H(N)^{mn}} \\ &= \frac{(H(N)^n - |\{\mathfrak{a}_{11} : \mathfrak{p}_l^k \nmid \mathfrak{a}_{11}\}|^n)^m}{H(N)^{mn}}.\end{aligned}$$

Therefore, it follows that

$$\begin{aligned} g_N(l) &\leq \frac{(H(N)^n - |\{\mathfrak{a}_{11} : \mathfrak{p}_l^k \nmid \mathfrak{a}_{11}\}|^n)^m}{H(N)^{mn}} \\ &\leq \Big[1 - \Big(1 - \frac{1}{H(N)} H\Big(\frac{N}{\mathfrak{N}(\mathfrak{p}_l)^k}\Big)\Big)^n\Big]^m \\ &\leq \Big[1 - \Big(1 - \Big(\frac{1}{\mathfrak{N}(\mathfrak{p}_l)^k} + \frac{A}{N^\varepsilon}\Big)\Big)^n\Big]^m \text{ for some } A > 0 \\ &\leq \Big(1 - \Big(1 - \frac{2}{\mathfrak{N}(\mathfrak{p}_l)^k}\Big)^n\Big)^m. \end{aligned}$$

The latter expression is bounded above by $g(l) = \frac{(2n)^m}{\mathfrak{N}(\mathfrak{p}_l)^{km}}$ from Bernoulli's inequality in the form $1-(1-x)^t \leq xt$ for $t \geq 1$ and $0 \leq x \leq 1$.

Moreover $\sum_{l=1}^{\infty} g(l)$ converges, because we can bound this series from above with a constant multiple of the Dedekind zeta function (with $m \geq 2$)

$$\sum_{l=1}^{\infty} g(l) \leq (2n)^m \sum_{l=1}^{\infty} \frac{1}{\mathfrak{N}(\mathfrak{p}_l)^{km}} \leq (2n)^m \zeta_O(km) < \infty.$$

Having satisfied the hypotheses of the Dominated Convergence Theorem, we observe that since $\sum_{s=1}^{l} g_N(s)$ is a telescoping sum, we obtain

$$\sum_{s=1}^{l} g_N(s) = \sum_{s=1}^{l} (P(s-1,n) - P(s,n)) = 1 - P(l,N),$$

and thus

$$\lim_{N\to\infty} \sum_{s=1}^{\infty} g_N(s) = 1 - \prod_{\mathfrak{N}(\mathfrak{p})>B} \Big(1 - \Big[1 - \Big(1 - \frac{1}{\mathfrak{N}(\mathfrak{p}_i)}\Big)^n \Big(1 + \frac{{}_nH_1}{\mathfrak{N}(\mathfrak{p})} + \ldots + \frac{{}_nH_{k-1}}{\mathfrak{N}(\mathfrak{p})^{k-1}}\Big)\Big]^m\Big).$$

Then since $\sum_{s=1}^{\infty} \lim_{N\to\infty} g_N(s)$ represents the complement of the probability we wanted to compute, the Dominated Convergence Theorem yields the desired assertion. □

7. Conclusions and Future Work

We have used element counting techniques to provided more concise proofs for the probability that the GCD and k-GCD of products of rational integers are B-smooth. We then extended these results to the ring of algebraic integers. We showed that the more general k-GCD case for the algebraic integers can be used to yield the GCD and k-GCD cases for the rational integers.

Avenues for future work include finding upper and lower bound estimates for the algebraic integer cases, and researching applications in ideal lattices and in the cryptanalysis of cryptographic multilinear maps.

8. Appendix: A Proofs based on the Inclusion-Exclusion Principle

8.1. **Probability that the GCD of Products of Positive Integers is B-smooth Using the Inclusion-Exclusion Principle.** For purposes of comparison to the previous proofs, we now show Cheong and Kim's original proof via the Inclusion-Exclusion Principle in detail.

Theorem 8.1.1. *Fix positive integers B and N, and let $p_1, p_2, ...$ be the primes greater than B in increasing order. If $X_l = \{p_1, p_2, ..., p_l\}$, then*

$$T(l,N) = \sum_{P \subset X_l} (-1)^{|P|} \Big[\sum_{Q \subset P} (-1)^{|Q|} \Big(\sum_{R \subset Q} (-1)^{|R|} \Big\lfloor \frac{N}{\prod_{p \in R} p} \Big\rfloor \Big)^n \Big]^m.$$

Proof. By hypothesis, we want to find the value of

$$T(l,N) = \Big| \Big\{ (r_{ij}) : \gcd\Big(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj} \Big) \text{ is coprime to } p \in X_l \Big\} \Big|.$$

In order to accomplish this, we use the Inclusion-Exclusion Principle to enumerate the number of ordered pairs that are not in a subset containing elements not coprime to some $p \in X_l$. Hence,

$$\begin{aligned} T(l,N) &= \sum_{P \subset X_l} (-1)^{|P|} \left| \Big\{ (r_{ij}) : \prod_{p \in P} p \,\Big|\, \gcd\Big(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj} \Big) \Big\} \right| \\ &= \sum_{P \subset X_l} (-1)^{|P|} \left| \Big\{ (r_{ij}) : \prod_{p \in P} p \,\Big|\, \prod_{j=1}^{n} r_{1j} \Big\} \right|^m. \end{aligned}$$

Again, applying the Inclusion-Exclusion Principle yields

$$\begin{aligned} \left| \Big\{ (r_{ij}) : \prod_{p \in P} p \,\Big|\, \prod_{j=1}^{n} r_{1j} \Big\} \right| &= \sum_{Q \subset P} (-1)^{|Q|} \Big| \Big\{ (r_{1j}) : p \nmid \prod_{j=1}^{n} r_{1j} \text{ for all } p \in Q \Big\} \Big| \\ &= \sum_{Q \subset P} (-1)^{|Q|} \left(\sum_{R \subset Q} (-1)^{|R|} \left\lfloor \frac{N}{\prod_{p \in R} p} \right\rfloor \right)^n. \end{aligned}$$

Therefore, we conclude that

$$T(l,N) = \sum_{P\subset X_l} (-1)^{|P|}\left[\sum_{Q\subset P}(-1)^{|Q|}\Big(\sum_{R\subset Q}(-1)^{|R|}\Big\lfloor\frac{N}{\prod_{p\in R}p}\Big\rfloor\Big)^n\right]^m.$$

□

Theorem 8.1.2. *The probability of the GCD of products of random integers is not divisible by the first l primes greater than B is given by*

$$\lim_{N\to\infty}\frac{T(l,N)}{N^{nm}} = \prod_{i=1}^{l}\Big(1-\Big[1-\Big(1-\frac{1}{p^i}\Big)^n\Big]^m\Big).$$

Proof. By the work done in the section, we see that $\dfrac{T(l,N)}{N^{nm}}$ is equal to

$$\begin{aligned}&\frac{1}{N^{nm}}\sum_{P\subset X_l}(-1)^{|P|}\Big[\sum_{Q\subset P}(-1)^{|Q|}\Big(\sum_{R\subset Q}(-1)^{|R|}\Big\lfloor\frac{N}{\prod_{p\in R}p}\Big\rfloor\Big)^n\Big]^m\\ &=\sum_{P\subset X_l}(-1)^{|P|}\Big[\sum_{Q\subset P}(-1)^{|Q|}\Big(\sum_{R\subset Q}(-1)^{|R|}\frac{1}{\prod_{p\in R}p}\Big)^n\Big]^m+O\Big(\frac{1}{N^{nm}}\Big).\end{aligned}$$

Next, factoring the principal term above yields

$$\begin{aligned}&\sum_{P\subset X_l}(-1)^{|P|}\Big[\sum_{Q\subset P}(-1)^{|Q|}\Big(\sum_{R\subset Q}(-1)^{|R|}\frac{1}{\prod_{p\in R}p}\Big)^n\Big]^m+O\Big(\frac{1}{N^{nm}}\Big)\\ &=\prod_{i=1}^{l}\Big(1-\Big[1-\Big(1-\frac{1}{p_i}\Big)^n\Big]^m\Big)+O\Big(\frac{1}{N^{mn}}\Big).\end{aligned}$$

Finally, taking the limit as $N\to\infty$ yields the desired conclusion. □

8.2. Probability that the k-GCD of Products of Positive Integers is B-smooth using the Inclusion-Exclusion Principle.

Theorem 8.2.1. *Let p be a prime number and r_{ij} be nonzero integers for each $1\le i\le m$ and $1\le j\le n$. Then $p \mid \gcd_k(\prod_{j=1}^n r_{1j},\dots,\prod_{j=1}^n r_{mj})$ if and only if $p^k \mid \prod_j r_{ij}$ for some i.*

Proof. Suppose that $p \mid a$ where $a = \gcd_k(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj})$. This is true if and only if $p \mid a$. Then this is equivalent to $p^k \mid a^k$ as well as $p^k \mid \prod_j r_{ij}$ for some i. $\square$

Theorem 8.2.2. *Let $p_1, p_2, \ldots$ be the prime numbers larger than B in increasing order. Then, we have*

$$\lim_{N\to\infty} \frac{T_k(l,n)}{N^{mn}} = \prod_{i=1}^{l} \Big(1 - \Big[1 - \Big(1 - \frac{1}{p_i}\Big)^n \Big(1 + \frac{nH_1}{p_i} + \ldots + \frac{nH_{k-1}}{p_i^{k-1}}\Big)\Big]\Big).$$

Proof. Let $X_l = \{p_1, \ldots, p_l\}$ and $1 \le r_{ij} \le N$. Using the Inclusion-Exclusion Principle,

$$\frac{T_k(l,n)}{N^{nm}} = \sum_{P \subset X_l} (-1)^{|P|} \Big(\sum_{Q \subset P} \Pr\Big[p^k \nmid \prod_{j=1}^n r_{1j} \ \text{ for all } p \in Q\Big]\Big)^m.$$

Let $p^a \,||\, x$ denote $p^a \mid x$ and $p^{a+1} \nmid x$ and let $a_p, j \in Q$ and $1 \le j \le n$.

Remark. Suppose a tuple satisfies $a_{p,1} + \ldots + a_{p,n} < k$ with $a_{p,1} + \ldots + a_{p,n} + 1 = k$, then using the exactly divides symbol $||$ guarantees $p^k \nmid x$.

Thus,

$$\begin{aligned}\Pr\Big[p^k \nmid \prod_{j=1}^n r_{1j},\ \forall p \in Q\Big] &= \sum_{a_{p,1}+\ldots+a_{p,n}<l} \Pr\Big[p^{a_{p,j}} \,||\, r_{1j}, \ \text{ for all } p, j\Big] \\ &= \sum_{a_{p,1}+\ldots+a_{p,n}<k} \ \prod_{j=1}^n \Pr\Big[p^{a_{p,j}} \,||\, r_{1j} \text{ for all } p \in Q\Big],\end{aligned}$$

where the last term utilizes the product rule for probability. This allows us to count the innermost quantity.

Using the Inclusion-Exclusion Principle,

$$\begin{aligned}
&|\{(r_{1j}) : p^{a_{p,j}} \mid\mid r_{1j} \text{ for all } p \in Q\}| \\
&= \Big\lfloor \frac{N}{\prod_{p\in Q} p^{a_{p,j}}} \Big\rfloor - \sum_{p\in Q} \Big\lfloor \frac{N}{\prod_{p\in Q} p^{a_{p,j}}} \Big\rfloor + \ldots + (-1)^{|Q|} \Big\lfloor \frac{N}{\prod_{p\in Q} p^{a_{p,j}+1}} \Big\rfloor.
\end{aligned}$$

Next, we form an estimate of the quantity by taking the difference of the last two terms. We find that

$$\begin{aligned}
\Big\lfloor \frac{N}{\prod_{p\in Q} p^{a_{p,j}}} \Big\rfloor - \Big\lfloor \frac{N}{\prod_{p\in Q} p^{a_{p,j}+1}} \Big\rfloor &= \frac{N}{\prod_{p\in Q} p^{a_{p,j}}} - \frac{N}{\prod_{p\in Q} p^{a_{p,j}+1}} + O(1) \\
&= N \prod_{p\in Q} \Big[\frac{1}{p^{a_{p,j}}} - \frac{1}{p^{a_{p,j}+1}} \Big] + O(1).
\end{aligned}$$

Putting this all together, we obtain

$$\begin{aligned}
\Pr\Big[p^k \nmid \prod_{j=1}^{n} r_{1j},\ \forall p \in Q\Big] &= \prod_{p\in Q} \Big(\sum_{a_{p,1}+\ldots+a_{p,n}<k} \prod_{j=1}^{n} \frac{p-1}{p^{a_{p,j}+1}} \Big) + O\Big(\frac{1}{N}\Big) \\
&= \prod_{p\in Q} \Big[\Big(1-\frac{1}{p}\Big)^n \sum_{a_{p,1}+\ldots+a_{p,n}<k} \frac{1}{p^{a_{p,1}+\ldots+a_{p,n}}} \Big] + O\Big(\frac{1}{N}\Big).
\end{aligned}$$

Next, we count every composition $a_{p,1} + \ldots + a_{p,n} < k$ for $p^{a_{p,j}}$ that divides the quantity. By using combinations with repetition, the number of n-tuples of positive integers which are a solution to $a_{p,1} + \ldots + a_{p,n} = i$ is given by ${}_nH_i = \binom{n+i-1}{i}$. Applying this result yields

$$\begin{aligned}
&\prod_{p\in Q} \Big[\Big(1-\frac{1}{p}\Big)^n \Big[\sum_{a_{p,1}+\ldots+a_{p,n}<k} \frac{1}{p^{a_{p,1}+\ldots+a_{p,n}}} \Big] + O\Big(\frac{1}{N}\Big) \\
&= \prod_{p\in Q} \Big[\Big(1-\frac{1}{p}\Big)^n \Big(1 + \frac{{}_nH_1}{p} + \ldots + \frac{{}_nH_{k-1}}{p^{k-1}}\Big) \Big] + O\Big(\frac{1}{N}\Big).
\end{aligned}$$

Finally, substitute these results into the original expression and simplify. Letting $N \to \infty$, we see that the error approaches 0 as desired. $\square$

References

[1] T. M. Apostol, Introduction to Analytic Number Theory, Springer, 1976.

[2] S. Bai, Polynomial Selection for the Number Field Sieve. 2011. Australian National University, PhD dissertation. https://maths-people.anu.edu.au/~brent/pd/Bai-thesis.pdf

[3] S. J. Benkoski. The probability that k positive integers are relatively r-prime, Journal of Number Theory, **8**: 218–223, 1976.

[4] J.H. Cheon and D. Kim, Probability that the k-GCD of products of positive integers is B-smooth, Journal of Number Theory, **168**: 72-80, 2016.

[5] P.G.L. Dirichlet, Über die Bestimmung der mittleren Werthe in der Zahlentheorie, Abhandlungen der Königlich Preussischen Akademie der Wissenchaften, **2**: 69-83, 1849.

[6] J.D. Dixon, Asymptotically Fast Factorization of Integers, Mathematics of Computation, **36**: 255-260, 1981.

[7] D. Dummit and R. Foote, Abstract Algebra, Prentice Hall, 1991.

[8] A. Granville, Smooth numbers: Computational number theory and beyond, Algorithmic Number Theory, **44**: 267-323, 2008.

[9] D. N. Lehmer, Asymptotic evaluation of certain totient sums, American Journal of Mathematics, **22**: 293–335, 1900.

[10] D.A. Marcus, Number Fields. 2nd Edition, Springer, 2018.

[11] R.A. Mollin, A Brief History of Factoring and Primality Testing B.C. (Before Computers), Mathematics Magazine, **75**: 18-29, 2002.

[12] D. Naccache and I. Shparlinski, Divisibility, Smoothness and Cryptographic Applications, https://eprint.iacr.org/2008/437.pdf.

[13] J. E. Nymann, On the Probability that k Positive Integers are Relatively Prime, Journal of Number Theory, **4**: 469-473, 1972.

[14] C.Pomerance, A Tale of Two Sieves, Notices of the American Mathematical Society, **36**: 1473-1485, 1996.

[15] C. Pomerance, The Quadratic Sieve Factoring Algorithm, Advances in Cryptology, Proceedings of Eurocrypt'84, **44**: 169-182, 1985.

[16] C. Pomerance, Smooth numbers and the quadratic sieve, Algorithmic Number Theory, **44**: 69-81, 2008.

[17] P. Shiu, Fermat's Method of Factorisation, Mathematical Gazette, **99**: 97–103, 2015.

[18] B. Sittinger, The probability that random algebraic integers are relatively r-prime, Journal of Number Theory, **130** (1): 164-171, 2010.