PROBABILITY THAT THE K-GCD OF PRODUCTS OF POSITIVE INTEGERS IS B-FRIABLE

JUNG HEE CHEON, DUHYEONG KIM

Abstract. In 1849, Dirichlet [5] proved that the probability that two positive integers are relatively prime is $1/\zeta(2)$. Later, it was generalized into the case that positive integers has no nontrivial kth power common divisor. In this paper, we further generalize this result: the probability that the gcd of m products of n positive integers is B-friable is $\prod_{p>B}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]$ for $m \geq 2$. We show that it is lower bounded by $\frac{1}{\zeta(s)}$ for some $s>1$ if $B>n^{\frac{m}{m-1}}$, which completes the heuristic proof in the cryptanalysis of cryptographic multilinear maps by Cheon et al. [2]. We extend this result to the case of k-gcd: the probability is $\prod_{p>B}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\left(1+\frac{{}_nH_1}{p}+\cdots+\frac{{}_nH_{k-1}}{p^{k-1}}\right)\right\}^m\right]$, where ${}_nH_i=\binom{n+i-1}{i}$.

1. Introduction

In 1849, Dirichlet [5] proved that the probability that two positive integers are relatively prime is $1/\zeta(2)$. To be precise,

$$\lim_{N\to\infty}\frac{\left|\left\{(x_1,x_2)\in\{1,2,..,N\}^2 : \gcd(x_1,x_2)=1\right\}\right|}{N^2}=\frac{1}{\zeta(2)}.$$

Lehmer [7] and more recently Nymann [10] extended this result that the probability that the r positive integers are relatively prime is $1/\zeta(r)$.

Meanwhile, in 1885, Gegenbauer [6] proved that the probability that a positive integer is not divisible by rth power for an integer $r \geq 2$ is $1/\zeta(r)$. In 1976, Benkoski [1] combined Gegenbauer and Lehmer's results and obtain that the probability that r positive integers are relatively k-prime is $1/\zeta(rk)$. For positive integers $x_1, ..., x_r$ and k, we denote by $\gcd_k(x_1, .., x_r)$ or k-gcd of $x_1, ..., x_r$ the largest kth power that divides $x_1, ..., x_r$. If $\gcd_k(x_1, .., x_r) = 1$, we call $x_1, .., x_r$ are relatively k-prime.

Later, study on the probability of gcd was extended by changing domain from $\mathbb{Z}$ to other Principal Ideal Domains. One extension is the result of Collins and Johnson [3] in 1989 that the probability that two Gaussian integers are relatively prime is $1/\zeta_{\mathbb{Q}(i)}(2)$. In 2004, Morrison and Dong [8] extended Benkoski's result to the ring $\mathbb{F}_q[x]$ for a finite field $\mathbb{F}_q$. More recently, in 2010, Sittinger [11] extended Benkoski's result to the algebraic integers over the algebraic number field K: the probability that k algebraic integers are relative r-prime is $1/\zeta_{O_K}(rk)$ while O_K is the ring of algebraic integers in K, and $\zeta_O(rk)$ denotes the Dedekind zeta function over O_K.

Key words and phrases. gcd of products of positive integers, B-friable, k-gcd.

In this paper, we move our question to the probability that the gcd of products of positive integers is B-friable. We investigate the probability that the gcd of *products* of positive integers is B-friable. Given positive integers $m \geq 2$ and n, assume that r_{ij}'s are positive integers chosen randomly and independently in $[1, N]$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. Our theorem states that the probability that $\gcd(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj})$ is B-friable converges to $\prod_{p>B}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]$ as $N \to \infty$. This is proved by using Lebesgue Dominated Convergence Theorem and the inclusion and exclusion principle.

We show that the value of $\prod_{p>B}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]$ is lower bounded by $\prod_{B<p\leq\hat{n}}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]\cdot\prod_{\hat{n}<p\leq\hat{r}}\left\{1-\left(\frac{n}{p}\right)^m\right\}\cdot\frac{1}{\zeta(s)}$ for $\hat{n} = \max\{n, B\}$, $r = \lfloor n^{\frac{m}{m-1}} + 1\rfloor$, $\hat{r} = \max\{\hat{n}, r\}$ and $s = m(1 - \log_{\hat{r}} n) > 1$. Note that the first product term is equal to 1 if $B = \hat{n}$, and the second product term is equal to 1 if $\hat{n} = \hat{r}$. Thus our theorem proves the heuristic argument in the lemma in [2, page 10] to tell that this probability is lower bounded by $1/\zeta(s)$ in case of $B = 2n$ and $\frac{m}{\log_2 2n} > 1$. The lemma is used to guarantee the success probability of the cryptanalysis of cryptographic multilinear maps proposed by Coron et al. [4].

Finally, we extend the theorem to the case of k-gcd. When r_{ij}'s are chosen randomly and independently from $\{1, \cdots, N\}$, we show that the probability that $\gcd_k(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj})$ is B-friable converges to

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

as $N \to \infty$, where ${}_nH_i = \binom{n+i-1}{i}$. This result is another generalized form of Benkoski's.

Notations. For an integer x, if x has no prime divisor larger than B, we say that x is B-friable. For a finite set X, the number of elements of X is denoted by $|X|$. All of the error terms in this paper are only about the positive integer N, *i.e.* O is actually O_N. For positive integers $x_1, ..., x_r$, and k, we denote by $\gcd_k(x_1, ..., x_r)$ or the k-gcd of $x_1, ..., x_r$ the largest kth power that divides $x_1, ..., x_r$. Note that the usual gcd is 1-gcd. From now on, alphabet p always denotes a prime number, and $\bigsqcup$ is a disjoint union.

2. Probability that the gcd of products of positive integers is B-friable

2.1. **The gcd of products of positive integers.**

In this section, we fix the positive integers $m \geq 2$ and n. For a positive integer N, r_{ij}'s are integers uniformly and independently chosen in $[1, N]$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. The aim of this section is to compute the probability that $\gcd(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj})$ is B-friable when $N \to \infty$. Denote by $p_1, p_2, p_3....$ the prime numbers larger than B in increasing order, and define $T(\ell, N)$ be the number of ordered pairs (r_{ij}) such that $\gcd(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj})$ is coprime to $p_1, ..., p_\ell$ for $1 \leq r_{ij} \leq N$. Note that $\lim_{\ell\to\infty} T(\ell, N)/N^{mn}$ is the probability that $\gcd(\prod_{j=1}^{n} r_{1j}, ..., \prod_{j=1}^{n} r_{mj})$ is

B-friable where r_{ij} are chosen randomly and independently in $\{1,2,...,N\}$. By following two steps, we obtain the value of $\lim_{N\to\infty}\lim_{\ell\to\infty}T(\ell,N)/N^{mn}$.

Theorem 2.1. *Let $p_1,p_2,...$be the prime numbers larger than B in increasing order. Then,*

$$\lim_{N\to\infty}\frac{T(\ell,N)}{N^{mn}}=\prod_{i=1}^{\ell}\left[1-\left\{1-\left(1-\frac{1}{p_i}\right)^n\right\}^m\right]. \tag{2.1}$$

Proof. Let $X_\ell=\{p_1,p_2,...,p_\ell\}$ and $1\le r_{ij}\le N$ for a positive integer N. By the inclusion and exclusion principle,

$$\begin{aligned}&\left|\left\{(r_{ij}):\gcd(\prod_{j=1}^{n}r_{1j},...,\prod_{j=1}^{n}r_{mj})\text{ is coprime to }p_1,...,p_\ell\right\}\right|\\&=\sum_{P\subset X_\ell}(-1)^{|P|}\left|\left\{(r_{ij}):\prod_{p\in P}p\mid\gcd(\prod_{j=1}^{n}r_{1j},...,\prod_{j=1}^{n}r_{mj})\right\}\right|\\&=\sum_{P\subset X_\ell}(-1)^{|P|}\left|\left\{(r_{1j}):\prod_{p\in P}p\mid\prod_{j=1}^{n}r_{1j}\right\}\right|^m.\end{aligned}$$

where $\prod_{p\in P}p=1$ for $P=\phi$. Applying the inclusion and exclusion principle again, we obtain

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

Consequently, we have

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

Finally, using $\lfloor N/\prod_{p\in R}p\rfloor/N=1/\prod_{p\in R}p+O(1/N)$, we have

$$\begin{aligned}\frac{T(\ell,N)}{N^{mn}}&=\sum_{P\subset X_\ell}(-1)^{|P|}\left\{\sum_{Q\subset P}(-1)^{|Q|}\left(\sum_{R\subset Q}(-1)^{|R|}\frac{1}{\prod_{p\in R}p}\right)^n\right\}^m+O\left(\frac{1}{N}\right)\\&=\prod_{i=1}^{\ell}\left[1-\left\{1-\left(1-\frac{1}{p_i}\right)^n\right\}^m\right]+O\left(\frac{1}{N}\right),\end{aligned}$$

which gives the theorem as $N\to\infty$. □

Theorem 2.1 gives the probability that the gcd of products of positive integers is not divisible by the first ℓ primes greater than B. To obtain the probability that this gcd is B-friable, we need to take $\ell\to\infty$ before taking $N\to\infty$ in Theorem 2.1. To swap the orders of limits, we use the Lebesgue Dominated Convergence Theorem for counting measure on set of natural numbers, which states:

Let $\{f_n : \mathbb{N} \to \mathbb{R}\}$ be a sequence of functions. Suppose that $\lim_{n\to\infty} f_n$ exists pointwisely and there exists a function $g : \mathbb{N} \to \mathbb{R}$ s.t $|f_n| \le g$, and $\sum_{x=1}^{\infty} g(x) < \infty$. Then we have

$$\lim_{n\to\infty} \sum_{x=1}^{\infty} f_n(x) = \sum_{x=1}^{\infty} \lim_{n\to\infty} f_n(x).$$

Theorem 2.2. *When r_{ij}'s are chosen randomly and independently from $\{1, 2, ..., N\}$, the probability that $\gcd(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj})$ is B-friable converges to*

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

as $N \to \infty$.

Proof. Define $g_N(\ell) = (T(\ell-1, N) - T(\ell, N))/N^{mn}$ and $T(0, N) = N^{mn}$. Note that $g_N(\ell)$ is the probability that $\gcd(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj})$ is coprime to $p_1, ..., p_{\ell-1}$ and divisible by p_ℓ for randomly and independently chosen r_{ij}'s from $\{1, ..., N\}$, and so is non-negative.

We claim that

$$\lim_{N\to\infty} \sum_{\ell=1}^{\infty} g_N(\ell) = \sum_{\ell=1}^{\infty} \lim_{N\to\infty} g_N(\ell). \tag{2.2}$$

Since $\sum_{1\le s\le \ell} g_N(s) = 1 - T(\ell, N)/N^{mn}$, this claim gives the proof of the theorem.

To prove the claim, we show that $g_N(\ell)$ is bounded by the function $g(\ell) = \frac{n^m}{p_\ell^m}$ and $\sum_{\ell=1}^{\infty} g(\ell) \le n^m \zeta(m) < \infty$. As the final step, we have

$$\begin{aligned}
g_N(\ell) &= \Pr\left[\gcd(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj}) \text{ coprime to } p_1, ..., p_{\ell-1} \text{ and divisible by } p_\ell \right] \\
&\le \Pr\left[p_\ell \mid \gcd(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj}) \right] \\
&= \frac{\left| \left\{ (r_{1j}) : p_\ell \mid \prod_{j=1}^n r_{1j} \right\} \right|^m}{N^{mn}} = \frac{\left(N^n - \left| \left\{ (r_{1j}) : p_\ell \nmid \prod_{j=1}^n r_{1j} \right\} \right| \right)^m}{N^{mn}} \\
&= \frac{(N^n - |\{r_{11} : p_\ell \nmid r_{11}\}|^n)^m}{N^{mn}} = \left\{ 1 - \left(1 - \frac{1}{N} \left\lfloor \frac{N}{p_\ell} \right\rfloor \right)^n \right\}^m \\
&\le \left\{ 1 - \left(1 - \frac{1}{p_\ell} \right)^n \right\}^m \le \frac{n^m}{p_\ell^m},
\end{aligned}$$

where the last inequality is from Bernoulli's inequality. □

Corollary 2.3. *Let $\hat{n} = \max\{n, B\}$, $r = \lfloor n^{\frac{m}{m-1}} + 1 \rfloor$ and $\hat{r} = \max\{\hat{n}, r\}$. Then the probability that $\gcd(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj})$ is B-friable is upper bounded by*

$$\frac{1}{\zeta(m)} \cdot \prod_{p\le B} \left(1 - \frac{1}{p^m} \right)^{-1},$$

and lower bounded by

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

for $s=m(1-\log_{\hat{r}} n)>1$*. The first product term is equal to 1 if* $B=\hat{n}$*, and the second product term is equal to 1 if* $\hat{n}=\hat{r}$*.*

Proof. Since $\prod_{p>B}[1-\{1-(1-1/p)^n\}^m]$ decreases as n increases, we can obtain an inequality

$$\prod_{p>B}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]\le\prod_{p>B}\left(1-\frac{1}{p^m}\right)=\frac{1}{\zeta(m)}\cdot\prod_{p\le B}\left(1-\frac{1}{p^m}\right)^{-1}.$$

Using Bernoulli's inequality, we can also obtain

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

We can easily check that $n^m/p^m\le 1/p^s$ for prime p larger than $\hat{r}$. Therefore, we obtain

$$\begin{aligned}&\prod_{p>B}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]\\&\ge\prod_{B<p\le\hat{n}}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]\cdot\prod_{\hat{n}<p\le\hat{r}}\left\{1-\left(\frac{n}{p}\right)^m\right\}\cdot\prod_{p>\hat{r}}\left(1-\frac{1}{p^s}\right)\\&\ge\prod_{B<p\le\hat{n}}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]\cdot\prod_{\hat{n}<p\le\hat{r}}\left\{1-\left(\frac{n}{p}\right)^m\right\}\cdot\frac{1}{\zeta(s)}.\end{aligned}$$

Finally, $s=m(1-\log_{\hat{r}} n)>1$ since $\hat{r}\ge r>n^{\frac{m}{m-1}}$, and the proof is completed. □

Remark 2.4. Suppose $B=2n$, and $\frac{m}{\log_2 2n}$ is a positive integer larger than 1. Then we can check that $B>n^{\frac{m}{m-1}}$, so $\hat{r}=B\ge r\ge n$. Applying Corollary 2.3, we have

$$\prod_{p>B}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]\ge\frac{1}{\zeta(s)},$$

for $s=m(1-\log_{\hat{r}} n)=m(1-\log_{2n} n)=\frac{m}{\log_2 2n}$. This is exactly same lower bound suggested in the lemma of [2, page 10].

2.2. **Generalization to k-gcd.** Now, we extend Theorem 2.1 and 2.2 to the case of k-gcd. For a positive integer N, r_{ij}'s are chosen randomly and independently in $\{1,2,...,N\}$. We compute the probability that $\gcd_k(\prod_{j=1}^n r_{1j},...,\prod_{j=1}^n r_{mj})$ is B-friable when $N\to\infty$. Define $T_k(\ell,N)$ be the number of ordered pairs (r_{ij}) such that $\gcd_k(\prod_{j=1}^n r_{1j},...,\prod_{j=1}^n r_{mj})$ is coprime to $p_1,...,p_\ell$ for $1\le r_{ij}\le N$. Note that $\lim_{\ell\to\infty}T_k(\ell,N)/N^{mn}$ is the probability that $\gcd_k(\prod_{j=1}^n r_{1j},...,\prod_{j=1}^n r_{mj})$ is B-friable where r_{ij}'s are chosen randomly and independently in $\{1,2,...,N\}$. Similarly to Theorem 2.1 and 2.2, we obtain the value of $\lim_{N\to\infty}\lim_{\ell\to\infty}T_k(\ell,N)/N^{mn}$ by following two steps.

Theorem 2.5. *Let $p_1, p_2, ...$ be the prime numbers larger than B in increasing order. Then,*

$$\lim_{N\to\infty} \frac{T_k(\ell, N)}{N^{mn}} = \prod_{i=1}^{\ell} \left[1 - \left\{ 1 - \left(1 - \frac{1}{p_i}\right)^n \left(1 + \frac{{}_nH_1}{p_i} + \cdots \frac{{}_nH_{k-1}}{p_i^{k-1}}\right) \right\}^m \right].$$

Proof. Similarly to Theorem 2.1, we apply the inclusion and exclusion principle. Note that $\prod_{p\in P} p \mid \gcd_k(\prod_{j=1}^n r_{1j}, ..., \prod_{j=1}^n r_{mj})$ if and only if $\prod_{p\in P} p^k \mid \prod_j r_{ij}$ for any i. For $X_\ell = \{p_1, ..., p_\ell\}$ and $1 \le r_{ij} \le N$, we can get

$$\frac{T_k(\ell, N)}{N^{mn}} = \sum_{P\subset X_\ell} (-1)^{|P|} \left(\sum_{Q\subset P} (-1)^{|Q|} \Pr\left[p^k \nmid \prod_{j=1}^n r_{1j} \text{ for all } p \in Q \right] \right)^m.$$

Let $p^a \parallel x$ denotes that $p^a \mid x$ and $p^{a+1} \nmid x$, and $a_{p,j}$'s be the non-negative integers for $p \in Q$ and $1 \le j \le n$. Note that the number of n-tuples of non-negative integers $(a_{p,1}, ..., a_{p,n})$ satisfying $a_{p,1} + \cdots + a_{p,n} = i$ is ${}_nH_i = \binom{n+i-1}{i}$. Then we have

$$\begin{aligned} \Pr\left[p^k \nmid \prod_{j=1}^n r_{1j} \text{ for all } p \in Q \right] &= \sum_{a_{p,1}+\cdots a_{p,n}<k} \Pr\left[p^{a_{p,j}} \parallel r_{1j} \text{ for all } p, j\right] \\ &= \sum_{a_{p,1}+\cdots a_{p,n}<k} \prod_{j=1}^n \Pr\left[p^{a_{p,j}} \parallel r_{1j} \text{ for all } p \in Q\right]. \end{aligned}$$

Using inclusion and exclusion principle,

$$\begin{aligned} &|\{(r_{1j}) : p^{a_{p,j}} \parallel r_{1j} \text{ for all } p \in Q\}| \\ &= \left\lfloor \frac{N}{\prod_{p\in Q} p^{a_{p,j}}} \right\rfloor - \sum_{q\in Q} \left\lfloor \frac{N}{q \cdot \prod_{p\in Q} p^{a_{p,j}}} \right\rfloor + \cdots + (-1)^{|Q|} \left\lfloor \frac{N}{\prod_{p\in Q} p^{a_{p,j}+1}} \right\rfloor \\ &= N \prod_{p\in Q} \left(\frac{1}{p^{a_{p,j}}} - \frac{1}{p^{a_{p,j}+1}} \right) + O(1). \end{aligned}$$

Therefore, we obtain

$$\begin{aligned} \Pr\left[p^k \nmid \prod_{j=1}^n r_{1j}, \forall p \in Q \right] &= \prod_{p\in Q} \left(\sum_{a_{p,1}+\cdots+a_{p,n}<k} \prod_{j=1}^n \frac{p-1}{p^{a_{p,j}+1}} \right) + O\left(\frac{1}{N}\right) \\ &= \prod_{p\in Q} \left\{ \left(1 - \frac{1}{p}\right)^n \sum_{a_{p,1}+\cdots+a_{p,n}<k} \frac{1}{p^{a_{p,1}+\cdots+a_{p,n}}} \right\} + O\left(\frac{1}{N}\right) \\ &= \prod_{p\in Q} \left(1 - \frac{1}{p}\right)^n \left(1 + \frac{{}_nH_1}{p} + \cdots + \frac{{}_nH_{k-1}}{p^{k-1}}\right) + O\left(\frac{1}{N}\right), \end{aligned}$$

which gives the theorem when substituting in above equation and taking the limit $N \to \infty$. □

Theorem 2.6. *When r_{ij}'s are chosen randomly and independently from $\{1,2,...,N\}$, the probability that* $\gcd_k(\prod_{j=1}^n r_{1j},...,\prod_{j=1}^n r_{mj})$ *is B-friable converges to*

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

as $N\to\infty$.

Proof. The statement is proved by exactly the same way with Theorem 2.2. Since

$$\begin{aligned}\frac{T_k(\ell-1,N)-T_k(\ell,N)}{N^{mn}} &\le \Pr\left[p_\ell \mid \gcd{}_k(\prod_{j=1}^n r_{1j},...,\prod_{j=1}^n r_{mj})\right]\\ &= \Pr\left[p_\ell^k \mid \gcd(\prod_{j=1}^n r_{1j},...,\prod_{j=1}^n r_{mj})\right]\\ &\le \Pr\left[p_\ell \mid \gcd(\prod_{j=1}^n r_{1j},...,\prod_{j=1}^n r_{mj})\right]\\ &\le \frac{n^m}{p_\ell^m},\end{aligned}$$

we can apply Lebesgue Dominated Convergence Theorem in the same way to Theorem 2.2 to obtain the theorem. □

Theorem 2.6 is a generalized form of Benkoski's theorem [1] and Theorem 2.2. As we mentioned in Introduction, Benkoski's theorem is that the probability that r positive integers are relatively k-prime is $1/\zeta(rk)$. When $k=1$, $1+\frac{{}_nH_1}{p}+\cdots+\frac{{}_nH_{k-1}}{p^{k-1}}=1$, so the result is same with Theorem 2.2. Also when $B=n=1$, the same condition with Benkoski's theorem, $\left(1-\frac{1}{p}\right)^n\left(1+\frac{{}_nH_1}{p}+\cdots+\frac{{}_nH_{k-1}}{p^{k-1}}\right)=1-\frac{1}{p^k}$. Therefore,

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

This is exactly the same result of Benkoski.

The value of $\prod_{p>B}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\left(1+\frac{{}_nH_1}{p}+\cdots+\frac{{}_nH_{k-1}}{p^{k-1}}\right)\right\}^m\right]$ can be lower bounded by the case of $k=1$. Therefore, we can conclude

$$\begin{aligned}&\prod_{p>B}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\left(1+\frac{{}_nH_1}{p}+\cdots+\frac{{}_nH_{k-1}}{p^{k-1}}\right)\right\}^m\right]\\ &\ge \prod_{B<p\le\hat{n}}\left[1-\left\{1-\left(1-\frac{1}{p}\right)^n\right\}^m\right]\cdot\prod_{\hat{n}<p\le\hat{r}}\left\{1-\left(\frac{n}{p}\right)^m\right\}\cdot\frac{1}{\zeta(s)},\end{aligned}$$

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

References

1. S.J. Benkoski, The probability that k integers are relatively r-prime, Journal of Number Theory. vol. 8, 218-223, 1973.

2. J. Cheon, K. Han, C. Lee, H. Ryu, and D. Stehle, Cryptanalysis of the multilinear map over the integers, Available at https://eprint.iacr.org/2014/906.pdf, 2014.
3. G. E. Collins and J. R. Johnson, The probability of relative primality of Gaussian integers, International Symposium Symbolic and Algebraic Computation, Springer-Vrlag, 252-258, 1989.
4. J. Coron, T. Lepoint, and M. Tibouchi, Practical Multilinear Maps over the Integers. CRYPTO (1) 2013: 476-493
5. G. Dirichlet, Über die Bestimmung der mittleren Werte in der Zahlentheorie, Abhandlungen Koniglich Preuss, Akad. Wiss., 1849.
6. L. Gegenbauer, Asymptotische Gesetze der Zahlentheorie, Denkshcriften Akad. Wien 49, 37-80, 1885.
7. D. N. Lehmer, Asymptotic evaluation of certain totient sums, Amer. J. Math. vol. 22, 293-355, 1900.
8. K. Morrison and Z. Dong, The probability that random polynomials are relatively r-prime, 2004. Available at http://www.calpoly.edu/∼kmorriso/Research/RPFF04-2.pdf.
9. I. Niven, H. Zuckerman and H. Montgomery, Introduction to the theory of numbers, the fifth edition, John Wiley and Sons, 1991.
10. J. E. Nymann, On the probability that k positive integers are relatively prime, Journal of Number Theory. vol. 4, 469-473, 1970.
11. Brain D. Sittinger, The probability that random algebraic integers are relatively r-prime, Journal of Number Theory. vol. 130, 164-171, 2009.

Department of Mathematical Sciences, Seoul National University, Seoul 151-747, Korea

E-mail address: jhcheon@snu.ac.kr, doodoo1204@snu.ac.kr