8-9-2014

The Non-Existence of a Covering System with all Moduli Distinct, Large and Square-Free

Melissa Kate Bechard
University of South Carolina - Columbia

The Non-Existence of a Covering System with all Moduli Distinct, Large and Square-Free

by

Melissa Kate Bechard

Bachelor of Science
James Madison University 2010

Master of Arts
Wake Forest University 2012

Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in

Mathematics

College of Arts and Sciences

University of South Carolina

2014

Accepted by:

Michael Filaseta, Co-Director of Thesis

Ognian Trifonov, Co-Director of Thesis

Lacy Ford, Vice Provost and Dean of Graduate Studies

Abstract

The work in this thesis is based on a paper written by Bob Hough in 2013. This thesis addresses the conjecture posed by Erdős that the least modulus for a covering system can be arbitrarily large. Hough proves the least modulus cannot be arbitrarily large. In this thesis, we present Hough's proof for the case of square-free moduli.

Table of Contents

Chapter 1

1.1 Introduction

A covering system is a finite collection of congruences, $x \equiv a \pmod{q}$, such that every integer satisfies at least one of the congruences. In this thesis we only consider moduli that are distinct and square-free. Let M be the smallest moduli in a system of congruences, with moduli $M = q_1 < q_2 < \ldots < q_k$. We show for sufficiently large M, that some integer remains uncovered by the system of congruences. We show this result in a series of steps. We begin by considering primes on a specific interval, and the moduli which are composed of those primes on this interval. Since each modulus is square-free, we can easily apply the Chinese Remainder Theorem to further break down the moduli. We show the result by proving several lemmas, including the Lovász Local Lemma.

1.2 Definitions and Notations

In this section, we provide the definitions and notations that we use throughout the thesis.

Definition 1.2.1. Let $\delta > 0, \theta > 0$, and $K > 3$ be fixed, with $\theta + (K+1)\delta < 1/2$.

Definition 1.2.2. $P_{-1} = 1$, $P_0 = \sqrt{\log M}$, and $P_{i+1} = e^{P_i^{\delta}}$, where $i \geq 0$.

Definition 1.2.3. $T_i = \exp\left((\log P_i)^K\right)$ for $i \geq 0$.

Definition 1.2.4. $Q_{-1} = 1$ and $Q_i = \prod_{p \leq P_i} p$ for $i \geq 0$, where p denotes a prime.

Definition 1.2.5. $\mathcal{N}_{i+1} = \left\{ q \in \mathbb{Z}^+ : q \text{ divides } \prod_{P_i < p \leq P_{i+1}} p \right\}$.

Definition 1.2.6. $\mathcal{N}_{i+1}^* = \mathcal{N}_{i+1} - \{1\}$.

Definition 1.2.7. M_{i+1}, is the set of moduli created by going from divisors of Q_i to divisors of Q_{i+1}, where each modulus can be uniquely written as $q'q$, with $q'|Q_i$ and $q \in \mathcal{N}_{i+1}^*$.

Definition 1.2.8. If q is a modulus in our system of congruences, we define a_q to be the unique number in $\{0, 1, \ldots, q-1\}$ for which $a_q \bmod q$ is the residue class covered by the congruence.

Definition 1.2.9. $R_{-1} = R_0 = \mathbb{Z}$, $R_i = \{x \in \mathbb{Z} : x \not\equiv a_q \pmod{q}, \text{for all } q|Q_i\}$.

Definition 1.2.10. $R_{i,r} = R_i \cap (r \bmod Q_{i-1})$.

Definition 1.2.11. For $r \in R_i$ and $q \in \mathcal{N}_{i+1}$, we define $A_{q,r}$ as the set of residue classes modulo qQ_i, which are $r \bmod Q_i$ and which are covered by some congruence $x \equiv a_{qq'} \pmod{qq'}$, where $q'|Q_i$.

Definition 1.2.12. $X_q(r) = |A_{q,r}|$.

Definition 1.2.13. $S_i \subset R_i$ such that if $a \in S_i$ and $b \equiv a \pmod{Q_i}$, then $b \in S_i$.

Definition 1.2.14. $R_i^* = S_{i-1} \cap R_i$.

Definition 1.2.15. $R_i^* \bmod Q_i$ represents the set of distinct residue classes modulo Q_i in R_i^*.

Definition 1.2.16. $E_{i,sup}$, $E_{i,GCD}$ and $E_{i,tail}$ are subsets of $R_i^* \bmod Q_i$ which will be defined in Lemma 1.6.6.

Definition 1.2.17. $R_i' = (R_i^* \bmod Q_i) \setminus E_{i,sup} \cup E_{i,GCD} \cup E_{i,tail}$.

Definition 1.2.18. $\ell_m(n) = |\{(n_1, n_2, \ldots, n_m) \in \mathbb{N}^m : \operatorname{lcm}(n_1, n_2, \ldots, n_m) = n\}|$.

We also use the notation, $G_{i+1,r}$ and $E_{q',B}$, which are defined in Section 1.6, as well as R'' and R''', which are defined in Section 1.7.

Note that $R_i' \subseteq (R_i^* \bmod Q_i) \subseteq (R_i \bmod Q_i)$. We later choose a set $R_i'' \subseteq R_i'$, and then we choose S_i so that $(S_i \bmod Q_i) \subseteq R_i''$.

1.3 Preliminary Lemmas used in the Main Theorem

We now prove several lemmas necessary to prove our desired result.

Lemma 1.3.1. *$\ell_m(n_1n_2) = \ell_m(n_1)\ell_m(n_2)$ where $n_1, n_2 \in \mathbb{Z}^+$ and $\gcd(n_1, n_2) = 1$. Moreover, at prime powers, $\ell_m(p^j) = (j+1)^m - j^m$, for $j \geq 0$.*

Proof. Fix an m. Let $A_m(n) = \{(d_1, d_2, \ldots, d_m) \in \mathbb{N}^m : \operatorname{lcm}(d_1, d_2, \ldots, d_m) = n\}$. We define a map $\phi : A_m(n_1n_2) \to A_m(n_1) \times A_m(n_2)$. Let $(c_1, c_2, \ldots, c_m) \in A_m(n_1n_2)$. Notice, each c_j can be written uniquely as $c_j = a_jb_j$ where $a_j = \gcd(c_j, n_1)$, and $b_j = \gcd(c_j, n_2)$. We then have $a_j \mid n_1$ and $b_j \mid n_2$, as well as $\operatorname{lcm}(a_1, a_2, \ldots, a_m) = n_1$ and $\operatorname{lcm}(b_1, b_2, \ldots, b_m) = n_2$. Define

$$\phi(c_1, c_2, \ldots, c_m) = ((a_1, a_2, \ldots, a_m), (b_1, b_2, \ldots, b_m)).$$

Notice ϕ is one-to-one. Let $(a_1, a_2, \ldots, a_m) \in A_m(n_1)$, and $(b_1, b_2, \ldots, b_m) \in A_m(n_2)$. Then since $\gcd(n_1, n_2) = 1$ we have $(a_1b_1, a_2b_2, \ldots, a_mb_m) \in \mathbb{N}^m$ with

$$\operatorname{lcm}(a_1b_1, a_2b_2, \ldots, a_mb_m) = n_1n_2.$$

Hence, $(a_1b_1, a_2b_2, \ldots, a_mb_m) \in A_m(n_1n_2)$, and the map ϕ is surjective. Then since we have a one-to-one correspondence between $A_m(n_1n_2)$ and $A_m(n_1) \times A_m(n_2)$, and the sets are finite, they must have the same size. Therefore, $\ell_m(n_1n_2) = |A_m(n_1n_2)| = |A_m(n_1) \times A_m(n_2)| = \ell_m(n_1)\ell_m(n_2)$. Furthermore,

$$\begin{aligned}\ell_m(p^j) &= \left|\left\{(a_1, a_2, \ldots, a_m) : \operatorname{lcm}(a_1, a_2, \ldots, a_m) = p^j\right\}\right| \\ &= \left|\left\{(p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_m}) : \operatorname{lcm}(p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_m}) = p^j \text{ and } \alpha_i \leq j\right\}\right|.\end{aligned}$$

Notice, at least one of $\alpha_1, \alpha_2, \ldots, \alpha_m$ is j, otherwise the lcm would be smaller. So, to count the number of possibilities for the α_i's, we have $(j+1)^m$ total possibilities, where each $\alpha_i \in \{0, 1, \ldots j\}$, and then j^m possibilities, where none of the α_i's equals j. Thus, $\ell_m(p^j) = (j+1)^m - j^m$. □

Since we are only concerned with the square-free case, we note a consequence of this lemma is that $\ell_m(p) = 2^m - 1$. This will be used in Lemma 1.3.3.

Lemma 1.3.2. *If $a > 1$ and $x > 0$ are real numbers, then $(1+x)^a > 1 + ax$.*

Proof. Consider $f(x) = a\log(1+x) - \log(1+ax)$. We then have

$$\begin{aligned} f'(x) &= \frac{a}{1+x} - \frac{a}{1+ax} \\ &= \frac{ax(a-1)}{ax^2 + (a+1)x + 1}. \end{aligned}$$

Notice, $f'(x) = 0 \Leftrightarrow x = 0$. And for $x > 0$ we have $f'(x) > 0$. Therefore, $f(x)$ is increasing for $x > 0$. Notice, $f(0) = a\log(1) - \log(1) = 0$. Since $f(x)$ is increasing for $x > 0$ and $f(0) = 0$ we have $f(x) > 0$ for $x > 0$. This gives us $a\log(1+x) - \log(1+ax) > 0$, which implies $a\log(1+x) > \log(1+ax)$, or $(1+x)^a > 1 + ax$. □

Lemma 1.3.3. *For some constant $C > 0$, the following inequalities hold. For $i \geq 0$,*

$$\sum_{n \in \mathcal{N}_{i+1}} \frac{1}{n} \leq C \frac{\log P_{i+1}}{\log P_i}. \tag{1.1}$$

For $m \geq 1$ and $i \geq -1$,

$$\sum_{\substack{n \in \mathcal{N}_{i+1} \\ n > T_{i+1}}} \frac{\ell_m(n)}{n} < \exp\Big(-(\log P_{i+1})^{K-1} \Big) \Big(C \log P_{i+1} \Big)^{2^m e}. \tag{1.2}$$

For $m \geq 1$ and $i \geq 0$,

$$\sum_{n | Q_i} \frac{\ell_m(n)}{n} \leq \Big(C \log P_i \Big)^{2^m}. \tag{1.3}$$

Proof. By the multiplicity of $\ell_m(n)$, and for $\theta \in [0,1)$, we have

$$\sum_{n\in\mathcal{N}_{i+1}} \frac{\ell_m(n)}{n^{1-\theta}} = \prod_{P_i<p\leq P_{i+1}} \left(1+\frac{\ell_m(p)}{p^{1-\theta}}\right). \tag{1.4}$$

For $s>1$ we have

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

which gives us

$$\prod_{p\leq z} \left(1-\frac{1}{p^2}\right)^{-1} \sim \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \tag{1.5}$$

We use the fact

$$\prod_{p\leq z} \left(1-\frac{1}{p}\right) \sim \frac{C}{\log z} \text{ for some constant } C. \tag{1.6}$$

Then, for some constant C' we have the following equation,

$$\begin{aligned}
\prod_{p\leq z} \left(1+\frac{1}{p}\right) &= \prod_{p\leq z} \left(\frac{\left(1-\frac{1}{p^2}\right)}{\left(1-\frac{1}{p}\right)}\right) \\
&= \frac{\prod\limits_{p\leq z}\left(1-\frac{1}{p^2}\right)}{\prod\limits_{p\leq z}\left(1-\frac{1}{p}\right)} \\
&= \prod_{p\leq z}\left(1-\frac{1}{p^2}\right)\prod_{p\leq z}\left(1-\frac{1}{p}\right)^{-1} \\
&\sim \left(\frac{1}{\sum\limits_{n=1}^{\infty}\frac{1}{n^2}}\right)\prod_{p\leq z}\left(1-\frac{1}{p}\right)^{-1} \\
&= \frac{1}{\frac{\pi^2}{6}}\prod_{p\leq z}\left(1-\frac{1}{p}\right)^{-1} \\
&= \frac{6}{\pi^2}\prod_{p\leq z}\left(1-\frac{1}{p}\right)^{-1} \\
&\sim \frac{\log z}{C'}.
\end{aligned} \tag{1.7}$$

The first asymptotic holds by (1.5), while the last step is true by (1.6). Notice, when $m=1$ and $\alpha=0$ we have

$$\sum_{n\in\mathcal{N}_{i+1}} \frac{1}{n} = \sum_{n\in\mathcal{N}_{i+1}} \frac{\ell_m(n)}{n^{1-\alpha}}$$

$$= \prod_{P_i < p \leq P_{i+1}} \left(1 + \frac{\ell_m(p)}{p^{1-\alpha}}\right).$$

This equality holds by the multiplicity of $\ell_m(p)$ shown in equation (1.4). Furthermore,

$$\begin{aligned}
\prod_{P_i < p \leq P_{i+1}} \left(1 + \frac{\ell_m(p)}{p^{1-\alpha}}\right) &= \prod_{P_i < p \leq P_{i+1}} \left(1 + \frac{1}{p}\right) \\
&= \frac{\prod_{p \leq P_{i+1}} \left(1 + \frac{1}{p}\right)}{\prod_{p \leq P_i} \left(1 + \frac{1}{p}\right)} \\
&\sim \frac{\frac{\log P_{i+1}}{C'}}{\frac{\log P_i}{C'}}.
\end{aligned}$$

The first equality holds since $m = 1$ and $\alpha = 0$, while the asymptotic holds by (1.7).

Thus, we have

$$\sum_{n \in \mathcal{N}_{i+1}} \frac{1}{n} \sim \frac{\frac{\log P_{i+1}}{C'}}{\frac{\log P_i}{C'}} = \frac{\log P_{i+1}}{\log P_i}.$$

In particular, statement (1.1) follows.

Let $\alpha \in [0, 1]$. Since $n > T_{i+1}$, we have $\frac{n}{T_{i+1}} > 1$. We then have

$$\begin{aligned}
\sum_{\substack{n \in \mathcal{N}_{i+1} \\ n > T_{i+1}}} \frac{\ell_m(n)}{n} &\leq \sum_{\substack{n \in \mathcal{N}_{i+1} \\ n > T_{i+1}}} \frac{\ell_m(n)}{n} \left(\frac{n}{T_{i+1}}\right)^{\alpha} \\
&\leq \sum_{n \in \mathcal{N}_{i+1}} \frac{\ell_m(n)}{n} \left(\frac{n}{T_{i+1}}\right)^{\alpha} \\
&= T_{i+1}^{-\alpha} \sum_{n \in \mathcal{N}_{i+1}} \frac{\ell_m(n)}{n^{1-\alpha}}.
\end{aligned}$$

This gives us the inequality

$$\sum_{\substack{n \in \mathcal{N}_{i+1} \\ n > T_{i+1}}} \frac{\ell_m(n)}{n} \leq T_{i+1}^{-\alpha} \sum_{n \in \mathcal{N}_{i+1}} \frac{\ell_m(n)}{n^{1-\alpha}}. \tag{1.8}$$

Let $\alpha = \dfrac{1}{\log P_{i+1}}$, and recall $T_{i+1} = \exp\left((\log P_{i+1})^K\right)$. We deduce

$$\begin{aligned} T_{i+1}^{-\alpha} &= \exp\left(\log T_{i+1}^{-\alpha}\right) \\ &= \exp\left(-\alpha \log T_{i+1}\right) \\ &= \exp\left(-\alpha \log\left(\exp\left((\log P_{i+1})^K\right)\right)\right) \\ &= \exp\left(-\alpha \left(\log P_{i+1}\right)^K\right) \\ &= \exp\left(-\frac{1}{\log P_{i+1}} \left(\log P_{i+1}\right)^K\right) \\ &= \exp\left(-\left(\log P_{i+1}\right)^{K-1}\right). \end{aligned} \tag{1.9}$$

Additionally, for $\alpha = \dfrac{1}{\log P_{i+1}}$ and $P_i < p \leq P_{i+1}$, we obtain

$$\begin{aligned} \frac{1}{p^{1-\alpha}} &= \frac{1}{p} \cdot p^{\alpha} \\ &= \frac{1}{p} \cdot p^{\frac{1}{\log P_{i+1}}} \\ &= \frac{1}{p} \cdot \exp\left(\log\left(p^{\frac{1}{\log P_{i+1}}}\right)\right) \\ &= \frac{1}{p} \cdot \exp\left(\frac{1}{\log P_{i+1}} \log p\right) \\ &\leq \frac{e}{p}. \end{aligned} \tag{1.10}$$

By equation (1.8), we have

$$\begin{aligned} \sum_{\substack{n \in \mathcal{N}_{i+1} \\ n > T_{i+1}}} \frac{\ell_m(n)}{n} &\leq T_{i+1}^{-\alpha} \sum_{n \in \mathcal{N}_{i+1}} \frac{\ell_m(n)}{n^{1-\alpha}} \\ &= T_{i+1}^{-\alpha} \prod_{P_i < p \leq P_{i+1}} \left(1 + \frac{\ell_m(p)}{p^{1-\alpha}}\right), \end{aligned}$$

where the equality holds by equation (1.4). By Lemma 1.3.1, $\ell_m(p) = 2^m - 1 < 2^m$. This gives us

$$T_{i+1}^{-\alpha} \prod_{P_i < p \leq P_{i+1}} \left(1 + \frac{\ell_m(p)}{p^{1-\alpha}}\right) < T_{i+1}^{-\alpha} \prod_{P_i < p \leq P_{i+1}} \left(1 + \frac{2^m}{p^{1-\alpha}}\right).$$

Together, we have

$$\sum_{\substack{n\in\mathcal{N}_{i+1}\\ n>T_{i+1}}} \frac{\ell_m(n)}{n} < T_{i+1}^{-\alpha} \prod_{P_i<p\le P_{i+1}} \left(1+\frac{2^m}{p^{1-\alpha}}\right).$$

Then, by (1.10), we see that

$$\begin{aligned}\sum_{\substack{n\in\mathcal{N}_{i+1}\\ n>T_{i+1}}} \frac{\ell_m(n)}{n} &\le T_{i+1}^{-\alpha} \prod_{P_i<p\le P_{i+1}} \left(1+\frac{2^m e}{p}\right)\\ &< T_{i+1}^{-\alpha} \prod_{P_i<p\le P_{i+1}} \left(1+\frac{1}{p}\right)^{2^m e},\end{aligned}$$

where the last inequality holds by Lemma 1.3.2. Applying equation (1.9) gives

$$\begin{aligned}T_{i+1}^{-\alpha} \prod_{P_i<p\le P_{i+1}} \left(1+\frac{1}{p}\right)^{2^m e} &= \exp\left(-\left(\log P_{i+1}\right)^{K-1}\right) \prod_{P_i<p\le P_{i+1}} \left(1+\frac{1}{p}\right)^{2^m e}\\ &\le \exp\left(-\left(\log P_{i+1}\right)^{K-1}\right) \left(C\log P_{i+1}\right)^{2^m e}.\end{aligned}$$

Hence, $\displaystyle\sum_{\substack{n\in\mathcal{N}_{i+1}\\ n>T_{i+1}}} \frac{\ell_m(n)}{n} < \exp\left(-\left(\log P_{i+1}\right)^{K-1}\right) \left(C\log P_{i+1}\right)^{2^m e}$, and we have shown statement (1.2).

To show statement (1.3) we use the inequality

$$\begin{aligned}\sum_{n|Q_i} \frac{\ell_m(n)}{n} &= \prod_{p\le P_i} \left(1+\frac{\ell_m(p)}{p}\right)\\ &\le \prod_{p\le P_i} \left(1+\frac{2^m}{p}\right)\\ &\le \prod_{p\le P_i} \left(1+\frac{1}{p}\right)^{2^m}\\ &\le \left(C\log P_i\right)^{2^m},\end{aligned}$$

where the first inequality holds by Lemma 1.3.1, the second by Lemma 1.3.2, and the last inequality holds by (1.7). □

Lemma 1.3.4. *For $n \in \mathbb{Z}^+$, let $\omega(n)$ be the number of distinct prime divisors of n. Let $q \in \mathcal{N}_{i+1}$ with $q \leq T_{i+1}$, for some integer $i \geq 0$. Fix $A > 0$ and $\theta > 0$ with $\theta + K\delta < 1$. Then,*

$$\sum_{\substack{d \in \mathcal{N}_{i+1} \\ d|q, d \neq 1}} \frac{A^{\omega(d)}}{d^{1-\theta}} \leq \frac{2AP_i^{\theta+K\delta-1}}{\log P_i}.$$

Proof. Let $d = 1$. Then we have $\omega(d) = 0$, which gives us $\dfrac{A^{\omega(d)}}{d^{1-\theta}} = 1$. Therefore,

$$1 + \sum_{\substack{d \in \mathcal{N}_{i+1} \\ d|q, d \neq 1}} \frac{A^{\omega(d)}}{d^{1-\theta}} = \sum_{\substack{d \in \mathcal{N}_{i+1} \\ d|q}} \frac{A^{\omega(d)}}{d^{1-\theta}} = \prod_{\substack{P_i < p \leq P_{i+1} \\ p|q}} \left(1 + \frac{A}{p^{1-\theta}}\right). \tag{1.11}$$

Note the second equality comes from the fact that $d \in \mathcal{N}_{i+1}$ is square-free. Observe that

$$\begin{aligned} \log\left(\prod_{\substack{P_i < p \leq P_{i+1} \\ p|q}} \left(1 + \frac{A}{p^{1-\theta}}\right)\right) &= \sum_{\substack{P_i < p \leq P_{i+1} \\ p|q}} \log\left(1 + \frac{A}{p^{1-\theta}}\right) \\ &\leq \sum_{\substack{P_i < p \leq P_{i+1} \\ p|q}} \frac{A}{p^{1-\theta}} \\ &\leq \sum_{\substack{P_i < p \leq P_{i+1} \\ p|q}} \frac{A}{P_i^{1-\theta}} \\ &\leq \frac{A\omega(q)}{P_i^{1-\theta}}, \end{aligned} \tag{1.12}$$

where the first inequality is true since $\log(1 + x) \leq x$ for all $x \geq 0$. Additionally, we have $q \in \mathcal{N}_{i+1}$ implies each prime divisor of q is greater than or equal to P_i. Since $q \leq T_{i+1}$ by assumption, and $T_{i+1} = \exp\left((\log P_{i+1})^K\right)$, we have

$$P_i^{\omega(q)} \leq q \leq T_{i+1} = \exp\left((\log P_{i+1})^K\right).$$

Applying the logarithm to this inequality we obtain

$$\omega(q) \log P_i \leq (\log P_{i+1})^K.$$

Recall that $P_{i+1} = e^{P_i\delta}$. We deduce

$$\omega(q) \leq \frac{(\log P_{i+1})^K}{\log P_i} = \frac{P_i^{K\delta}}{\log P_i}. \tag{1.13}$$

From (1.12) and (1.13) we obtain

$$\log\left(\prod_{\substack{P_i<p\leq P_{i+1}\\ p|q}}\left(1+\frac{A}{p^{1-\theta}}\right)\right) \leq \frac{A}{P_i^{1-\theta}}\frac{P_i^{K\delta}}{\log P_i} = \frac{AP_i^{\theta+K\delta-1}}{\log P_i}. \tag{1.14}$$

Exponentiating both sides of (1.14), and applying equation (1.11), we find

$$1+\sum_{\substack{d\in\mathcal{N}_{i+1}\\ d|q,d\neq 1}}\frac{A^{\omega(d)}}{d^{1-\theta}} \leq \exp\left(\frac{AP_i^{\theta+K\delta-1}}{\log P_i}\right). \tag{1.15}$$

Since $\theta+K\delta<1$ by assumption, we have $\theta+K\delta-1$ is negative. So, for large M, and therefore, large P_i, we have $0<\dfrac{AP_i^{\theta+K\delta-1}}{\log P_i}<1$. Applying the Taylor series expansion of e^X, with $X=\dfrac{AP_i^{\theta+K\delta-1}}{\log P_i}$, we have

$$\begin{aligned} e^X &= 1+X+\frac{X^2}{2!}+\frac{X^3}{3!}+\dots \\ &\leq 1+X+\frac{X}{2}+\frac{X}{2^2}+\dots \\ &= 1+X\left(\sum_{i=0}^{\infty}\left(\frac{1}{2^i}\right)\right) \\ &= 1+2X. \end{aligned}$$

Therefore, (1.15) gives us

$$1+\sum_{\substack{d\in\mathcal{N}_{i+1}\\ d|q,d\neq 1}}\frac{A^{\omega(d)}}{d^{1-\theta}} \leq 1+2\left(\frac{AP_i^{\theta+K\delta-1}}{\log P_i}\right).$$

Subtracting one from both sides yields the desired inequality. □

1.4 Lovász Local Lemma

The Lovász Local Lemma provides a general way to prove events with little dependencies, have a positive probability that none of the events occur. In our case, the

lemma is useful to show for a set of residue classes A_i, that satisfy some conditions, the probability that some integer is not covered by any of the residue classes is non-zero.

Lemma 1.4.1 (Lovász Local Lemma)**.** *Let $A_1, A_2, \ldots, A_n$ be events. Let $D = (V, E)$ be a directed graph with $|V| = n$. Assume all $1 \leq i \leq n$ has A_i independent of the sigma-algebra generated by the events $\{A_i : (i,j) \notin E\}$. If there exists $x_1, x_2, \ldots x_n \in \mathbb{R}$ with $0 \leq x_i < 1$ where all $1 \leq i \leq n$ satisfy $P(A_i) \leq x_i \prod_{(i,j)\in E} (1 - x_j)$, then for all $1 \leq m \leq n$ we have*

$$P\left(\bigcap_{i=1}^{n} A_i^c\right) \geq P\left(\bigcap_{i=1}^{m} A_i^c\right) \cdot \prod_{j=m+1}^{n} (1 - x_j)\,.$$

Furthermore,

$$P\left(\bigcap_{i=1}^{n} A_i^c\right) \geq \prod_{j=1}^{n} (1 - x_j)\,.$$

Proof. We suppose the conditions of the lemma are satisfied.

Claim 1.4.2. *Let k be a positive integer. For any $S \subseteq \{1, \ldots, n\}$ where $|S| = k - 1$, and for $i \notin S$, where $1 \leq i \leq n$, we have $P\left(A_i \mid \bigcap_{j\in S} A_j^c\right) \leq x_i$.*

Proof of Claim. We prove this claim using induction. Let $k = 1$. Then $S = \emptyset$, so $\mathrm{P}\left(A_i \mid \bigcap_{j\in S} A_j^c\right) = \mathrm{P}(A_i) \leq x_i$. And, since $\mathrm{P}(A_i) + \mathrm{P}(A_i^c) = 1$, we also have $\mathrm{P}\left(A_i^c \mid \bigcap_{j\in S} A_j^c\right) \geq 1 - x_i$. Assume the claim holds for all $1 \leq k' < k$. Notice, $\mathrm{P}\left(\bigcap_{j\in S} A_j^c\right) \geq \prod_{j\in S} (1 - x_j) > 0$, when $|S| = k - 1$. This gives us $\mathrm{P}\left(A_i^c \mid \bigcap_{j\in S} A_j^c\right)$ is defined, so we are not dividing by zero.

Define $S_1 = \{j \in S : (i,j) \in E\}$, and $S_2 = S \setminus S_1$. Notice, S_2 is independent of A_i. So, if $S_1 = \emptyset$, then all events in S are independent of A_i. This implies

$$\mathrm{P}\left(A_i \mid \bigcap_{j\in S} A_j^c\right) = \mathrm{P}(A_i) \leq x_i,$$

establishing the claim in this case. Now, consider the case that $S_1 \neq \emptyset$, and write $S_1 = \{j_1 < j_2 < \ldots < j_r\}$. By the definition of conditional probability we have

$$\begin{aligned} \mathrm{P}\left(A_i \mid \bigcap_{j\in S} A_j^c\right) &= \frac{\mathrm{P}\left(A_i \cap \bigcap_{j\in S} A_j^c\right)}{\mathrm{P}\left(\bigcap_{j\in S} A_j^c\right)} \\ &= \frac{\frac{1}{\mathrm{P}\left(\bigcap_{j\in S_2} A_j^c\right)}}{\frac{1}{\mathrm{P}\left(\bigcap_{j\in S_2} A_j^c\right)}} \cdot \frac{\mathrm{P}\left(A_i \cap \bigcap_{j\in S} A_j^c\right)}{\mathrm{P}\left(\bigcap_{j\in S} A_j^c\right)} \\ &= \frac{\mathrm{P}\left(A_i \cap \bigcap_{j\in S_1} A_j^c \mid \bigcap_{j\in S_2} A_j^c\right)}{\mathrm{P}\left(\bigcap_{j\in S_1} A_j^c \mid \bigcap_{j\in S_2} A_j^c\right)}. \end{aligned} \tag{1.16}$$

We justify that the denominator of this last expression, which we call d(RHS), is positive. We apply the inductive step to obtain

$$\begin{aligned} \mathrm{d(RHS)} &= \mathrm{P}\left(A_{j_1}^c \mid \bigcap_{j\in S_2} A_j^c\right) \times \mathrm{P}\left(A_{j_2}^c \mid A_{j_1}^c \cap \bigcap_{j\in S_2} A_j^c\right) \\ &\qquad \times \cdots \times \mathrm{P}\left(A_{j_r}^c \mid A_{j_1}^c \cap A_{j_2}^c \cap \ldots \cap A_{j_{r-1}}^c \cap \bigcap_{j\in S_2} A_j^c\right) \\ &\geq (1-x_{j_1})\,(1-x_{j_2}) \cdots (1-x_{j_r}) \\ &= \prod_{\ell=1}^{r} (1-x_{j_\ell}) \\ &= \prod_{j\in S_1} (1-x_j)\,. \end{aligned} \tag{1.17}$$

Recall that $0 \leq x_j < 1$ for each j, so d(RHS) > 0. Examining the numerator of the last expression in (1.16), and using the fact that S_2 is independent of A_i, which implies S_2 is independent of A_i^c, we have the following,

$$\begin{aligned} \mathrm{P}\left(A_i \cap \bigcap_{j\in S_1} A_j^c \mid \bigcap_{j\in S_2} A_j^c\right) &\leq \mathrm{P}\left(A_i \mid \bigcap_{j\in S_2} A_j^c\right) \\ &= \mathrm{P}\left(A_i\right) \\ &\leq x_i \prod_{(i,j)\in E} (1-x_j)\,, \end{aligned} \tag{1.18}$$

where the last inequality holds by our assumption. Combining what we found in equations (1.17) and (1.18), and applying this to equation (1.16) we have

$$\begin{aligned} \mathrm{P}\left(A_i \mid \bigcap_{j\in S} A_j^c\right) &= \frac{\mathrm{P}\left(A_i \cap \bigcap_{j\in S_1} A_j^c \mid \bigcap_{j\in S_2} A_j^c\right)}{\mathrm{P}\left(\bigcap_{j\in S_1} A_j^c \mid \bigcap_{j\in S_2} A_j^c\right)} \\ &\leq x_i \prod_{\substack{(i,j)\in E \\ j\notin S}} (1-x_j) \\ &\leq x_i, \end{aligned}$$

where the last inequality is true since each $0 \leq x_j \leq 1$. □

Notice, a consequence of the claim is

$$\mathrm{P}\left(A_i^c \,\middle|\, \bigcap_{j\in S} A_j^c\right) \geq 1 - x_i. \tag{1.19}$$

Also,

$$\prod_{j=m+1}^{n} \mathrm{P}\left(A_j^c \,\middle|\, \bigcap_{i=1}^{j-1} A_i^c\right) = \prod_{j=m+1}^{n} \frac{\mathrm{P}\left(\bigcap_{i=1}^{j} A_i^c\right)}{\mathrm{P}\left(\bigcap_{i=1}^{j-1} A_i^c\right)}.$$

Multiplying the above by $\mathrm{P}\left(\bigcap_{i=1}^{m} A_i^c\right)$ gives us the following equation,

$$\mathrm{P}\left(\bigcap_{i=1}^{m} A_i^c\right) \prod_{j=m+1}^{n} \mathrm{P}\left(A_j^c \,\middle|\, \bigcap_{i=1}^{j-1} A_i^c\right) = \mathrm{P}\left(\bigcap_{i=1}^{n} A_i^c\right).$$

From 1.19, we obtain

$$\mathrm{P}\left(\bigcap_{i=1}^{n} A_i^c\right) = \mathrm{P}\left(\bigcap_{i=1}^{m} A_i^c\right) \prod_{j=m+1}^{n} \mathrm{P}\left(A_j^c \,\middle|\, \bigcap_{i=1}^{j-1} A_i^c\right) \geq \mathrm{P}\left(\bigcap_{i=1}^{m} A_i^c\right) \prod_{j=m+1}^{n} (1-x_j),$$

and we have proven the first assertion in the lemma.

In particular, taking $m = 1$ gives us

$$\mathrm{P}\left(\bigcap_{i=1}^{n} A_i^c\right) \geq \mathrm{P}\left(A_1^c\right) \prod_{j=2}^{n} (1-x_j)$$

$$= (1 - \mathrm{P}(A_1)) \prod_{j=2}^{n} (1 - x_j)$$

$$\geq \prod_{j=1}^{n} (1 - x_j),$$

since $P(A_1) \leq x_1$. Thus, the second assertion in the lemma also holds. □

The symmetric version of the Lovász Local Lemma, which can be shown to be a consequence of Lemma 1.4.1, is

Lemma 1.4.3 (symmetric version of Lovász Local Lemma)**.** *Let $A_1, A_2, \ldots A_k$ be events. Assume each event occurs with probability at most p and such that each event is independent of all the other events except for at most d of them. If $e \cdot p\,(d+1) < 1$, then $P\,(\cap A_i^c) > 0$, where e is the base of the natural logarithm.*

We now provide an example using this version.

Example 1.4.4. Given a hypergraph G where each edge has at least k vertices. Assume that each edge intersects at most d other edges. Using the Lemma 1.4.3, we show if $e(d+1) < 2^{k-1}$, then G is 2-colorable.

Let $G = (V, E)$ be a hypergraph, and let C be a coloring set for G. C is a proper coloring of G if and only if every $e \in E$, where e is incident to at least two vertices, there exists two vertices incident to e that can be colored different colors from C. Thus, we do not want an edge to be monochromatic when $|C| = 2$. Define A_i to be the event that edge i is monochromatic under a random 2-coloring. Assume edge i has k vertices. Then, we have $\mathrm{P}(A_i) = \dfrac{2}{2^k} = \dfrac{1}{2^{k-1}}$. Since every edge has at least k vertices, we have $\max\limits_i \{\mathrm{P}(A_i)\} \leq \dfrac{1}{2^{k-1}}$.

Assuming $e(d+1) < 2^{k-1}$, we have $e(d+1)\dfrac{1}{2^{k-1}} < 2^{k-1}\dfrac{1}{2^{k-1}} = 1$. Applying the Lovász Local Lemma, we have $\mathrm{P}\left(\bigcap\limits_i A_i^c\right) > 0$. Since A_i is the event that edge i is monochromatic, the intersection of the complements of A_i over all i gives the event

that no edge is monochromatic. Thus, $\mathrm{P}\left(\bigcap_i A_i^c\right) > 0$ implies a proper 2-coloring exists.

1.5 Main Theorem

Theorem 1.5.1. *For all M that are larger than a fixed constant, we have for all $i \geq 0$,*

$$|R_i \bmod Q_i| \geq Q_i \exp\left(-(\log P_i)^2\right).$$

Furthermore, there exists a set $S_{i-1} \subset R_{i-1}$, determined modulo Q_{i-1}, such that S_{i-1} and $R_i^* := S_{i-1} \cap R_i$ satisfy the following properties.

1. *(Large size)*

$$|S_{i-1} \bmod Q_{i-1}| \geq Q_{i-1} \cdot \exp\left(-2(\log P_{i-1})^2\right)$$

2. *(Large fibres)*

$$|R_i^* \bmod Q_i| \geq \frac{Q_i}{Q_{i-1}} \cdot |S_{i-1} \bmod Q_{i-1}| \cdot \exp\left(-(\log P_i)^2\right)$$

3. *(Uniform fibres)*

   $\forall r \in S_{i-1}$ *we have*

$$|R_{i,r} \bmod Q_i| \asymp \frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|},$$

   where for $A, B > 0$, $A \asymp B$ means $C_1 B < A < C_2 B$ for constants C_1 and C_2.

4. *(Uniformity within fibres)*

   $\forall r \in S_{i-1}$ *and all $q \in \mathcal{N}_i^*$ such that $q \leq T_i$,*

$$\max_{b \bmod q} \left\{|R_{i,r} \cap (b \bmod q) \bmod Q_i|\right\} \leq \frac{2}{q} |R_{i,r} \bmod Q_i|.$$

In particular, the first two items imply that R_i^* satisfies

$$|R_i^* \bmod Q_i| \geq \frac{Q_i}{\exp\left(\frac{3}{2}(\log P_i)^2\right)},$$

since M is assumed to be sufficiently large.

Proof. We prove this theorem using induction. Consider the case when $i = 0$. Recall, $R_0 = \mathbb{Z}$ and $P_0 = \sqrt{\log M}$. We then have

$$\begin{aligned} |R_0 \bmod Q_0| &= |\mathbb{Z} \bmod Q_0| \\ &= Q_0 \\ &\geq \frac{Q_i}{\exp\left(\left(\log\sqrt{\log M}\right)^2\right)} \\ &= Q_0 \cdot \exp\left(-\left(\log P_0\right)^2\right). \end{aligned}$$

Hence, the first part of the theorem holds. Choose $S_{-1} = \mathbb{Z}$. Recall, $Q_{i-1} = 1$ and $P_{-1} = 1$. This gives us

$$|S_{-1} \bmod Q_{-1}| = |\mathbb{Z} \bmod 1| = 1. \tag{1.20}$$

We then have the following

$$\begin{aligned} |S_{-1} \bmod Q_{-1}| &= 1 \\ &\geq \frac{1}{\exp\left(2\left(\log(1)\right)^2\right)} \\ &= \frac{1}{\exp\left(2\left(\log P_{-1}\right)^2\right)} \\ &= Q_{-1} \cdot \exp\left(-2\left(\log P_{-1}\right)^2\right), \end{aligned}$$

which proves statement (1). Observe $R_0^* = S_{-1} \cap R_0 = \mathbb{Z}$. Applying equation (1.20) we have

$$\begin{aligned} |R_0^* \bmod Q_0| &= |\mathbb{Z} \bmod Q_0| \\ &= Q_0 \\ &\geq \frac{Q_0 \cdot 1}{1 \cdot \exp\left(\left(\log\sqrt{\log M}\right)^2\right)} \end{aligned}$$

$$= \frac{Q_0 \cdot |S_{-1} \bmod Q_{-1}|}{Q_{-1} \cdot \exp\left(-\left(\log\sqrt{\log M}\right)^2\right)}$$
$$= \frac{Q_0}{Q_{-1}} \cdot |S_{-1} \bmod Q_{-1}| \cdot \exp\left(-\left(\log P_0\right)^2\right),$$

which proves statement (2). Observe

$$R_{0,r} = R_0 \cap (r \bmod Q_{-1}) = \mathbb{Z} \cap (r \bmod 1) = \mathbb{Z}. \tag{1.21}$$

We deduce

$$|R_{0,r} \bmod Q_0| = |\mathbb{Z} \bmod Q_0|$$
$$= \frac{|\mathbb{Z} \bmod Q_0|}{|\mathbb{Z} \bmod 1|}$$
$$= \frac{|R_0^* \bmod Q_0|}{|S_{-1} \bmod Q_{-1}|},$$

which by choosing $C_1 < 1$ and $C_2 > 1$ statement (3) follows. Furthermore, when $q \in \mathcal{N}_0^* = \left(\left\{q \in \mathbb{Z}^* : q \text{ divides } \prod_{1 \le p < \sqrt{\log M}} p\right\} - 1\right)$, we have $q \mid Q_0$. So, for $r \in S_{-1}$, and $q \in \mathcal{N}_0^*$ with $q \le T_0$, we have

$$|R_{0,r} \cap (b \bmod q) \bmod Q_0| = |\mathbb{Z} \cap (b \bmod q) \bmod Q_0|$$
$$= \frac{Q_0}{q}$$
$$\le \frac{2}{q} \cdot Q_0$$
$$= \frac{2}{q} \cdot |R_{0,r} \bmod Q_0|,$$

where the first and last steps applied equation (1.21), while the second step used the fact that $q \mid Q_0$. Thus, statement (4) holds.

Assume the statements in the theorem hold up to i. We now prove several lemmas to establish the statements with i replaced with $i + 1$. □

1.6 Further Lemmas Leading Towards the Main Theorem

Lemma 1.6.1. *There is an absolute constant $C > 0$ such that for all $q \in \mathcal{N}_{i+1}$ and all positive integers $m \leq \sqrt{\log\log P_i}$, we have*

$$\frac{1}{|R_i^* \bmod Q_i|} \sum_{r \in R_i^* \bmod Q_i} X_q(r)^m \leq \exp\left((2\log P_{i-1})^2\right) (C \log P_i)^{2^m}. \tag{1.22}$$

In particular, for all $i \geq 0$, we have

$$\frac{1}{|R_i^* \bmod Q_i|} \sum_{r \in R_i^* \bmod Q_i} \sum_{\substack{q \in \mathcal{N}_{i+1} \\ 1 < q \leq T_{i+1}}} \frac{X_q(r)}{q} \leq C^3 \log P_{i+1} \exp\left((2\log P_{i-1})^2\right) (\log P_i). \tag{1.23}$$

Proof. After finding all moduli, $q|Q_i$, we consider the residue classes that are not covered. A new set of moduli, M_{i+1}, is created by going from divisors of Q_i to divisors of Q_{i+1}, where each modulus can be written as $q'q$, where $q'|Q_i$ and $q \in \mathcal{N}_{i+1}^*$. For $q \in \mathcal{N}_{i+1}^*$ fixed, $A_{q,r}$ is the set of residue classes modulo qQ_i that are r modulo Q_i and covered by the new moduli in M_{i+1} that are of the form $q'q$, where $q'|Q_i$. Recall our congruences are of the form $x \equiv a_{qq'} \pmod{qq'}$, which is equivalent to $x \equiv a_{qq'} \pmod{q}$ and $x \equiv a_{qq'} \pmod{q'}$. For $q'|Q_i$, the congruence $x \equiv a_{qq'} \pmod{qq'}$ will cover a number that is r modulo Q_i if and only if $a_{qq'} \equiv r \pmod{q'}$. Additionally, each of the residue classes of $A_{q,r}$ are incongruent modulo q, which implies the system $x \equiv a_{qq'} \pmod{q}$ and $x \equiv r \pmod{q'}$ will cover exactly one residue class of $A_{q,r}$. Recall, $X_q(r) = |A_{q,r}|$. Letting q' vary, we obtain

$$X_q(r) \leq \sum_{\substack{q'|Q_i \\ a_{qq'} \equiv r \pmod{q'}}} 1.$$

Note, we have an inequality since varying q' may result in congruences covering the same residue class of $A_{q,r}$. This gives us

$$X_q(r)^m \leq \sum_{\substack{q_1'|Q_i \\ a_{qq_1'} \equiv r \pmod{q_1'}}} \sum_{\substack{q_2'|Q_i \\ a_{qq_2'} \equiv r \pmod{q_2'}}} \cdots \sum_{\substack{q_m'|Q_i \\ a_{qq_m'} \equiv r \pmod{q_m'}}} 1. \tag{1.24}$$

We rewrite the q'_j's, where $j = 1, \ldots, m$, in equation (1.24) as $q'_j = q'_{j_0} q'_{j_1}$, where $q'_{j_0} \mid Q_{i-1}$ and $q'_{j_1} \in \mathcal{N}_i$. Let $\widetilde{q_0} = \operatorname{lcm}(q'_{10}, q'_{20}, \ldots, q'_{m0})$ and $\widetilde{q_1} = \operatorname{lcm}(q'_{11}, q'_{21} \ldots q'_{m1})$. Since for each j, we have $q'_{j0} \mid Q_{i-1}$ so q'_{j0} is square-free. Hence, the highest power of q'_{j0} is one so that $\widetilde{q_0} \mid Q_{i-1}$. Also, each $q_{j1} \in \mathcal{N}_i$ which means $\widetilde{q_1} \in \mathcal{N}_i$. Thus, rewriting equation (1.24) gives

$$\begin{aligned}
X_q(r)^m \leq & \sum_{\substack{q'_1 \mid Q_i \\ a_{qq'_1} \equiv r \pmod{q'_1}}} \sum_{\substack{q'_2 \mid Q_i \\ a_{qq'_2} \equiv r \pmod{q'_2}}} \cdots \sum_{\substack{q'_m \mid Q_i \\ a_{qq'_m} \equiv r \pmod{q'_m}}} 1 \\
= & \sum_{q'_{10} \mid Q_{i-1}} \sum_{\substack{q'_{11} \in \mathcal{N}_i \\ a_{qq'_{10}q'_{11}} \equiv r \pmod{q'_{10}q'_{11}}}} \sum_{q'_{20} \mid Q_{i-1}} \sum_{\substack{q'_{21} \in \mathcal{N}_i \\ a_{qq'_{20}q'_{21}} \equiv r \pmod{q'_{20}q'_{21}}}} \\
& \cdots \sum_{q'_{m0} \mid Q_{i-1}} \sum_{\substack{q'_{m1} \in \mathcal{N}_i \\ a_{qq'_{m0}q'_{m1}} \equiv r \pmod{q'_{m0}q'_{m1}}}} 1 \\
= & \sum_{\widetilde{q_0} \mid Q_{i-1}} \sum_{\widetilde{q_1} \in \mathcal{N}_i} \sum_{\substack{q'_{10} \mid Q_{i-1}, \ldots, q'_{m0} \mid Q_{i-1} \\ \operatorname{lcm}(q'_{10}, \ldots, q'_{m0}) = \widetilde{q_0}}} \sum_{\substack{q'_{11} \in \mathcal{N}_i, \ldots, q'_{m1} \in \mathcal{N}_i \\ \operatorname{lcm}(q'_{11}, \ldots, q'_{m1}) = \widetilde{q_1} \\ a_q q'_{j0} q'_{j1} \equiv r \pmod{q'_{j0}q'_{j1}} \ \forall j}} 1.
\end{aligned}$$

Therefore,

$$\begin{aligned}
& \sum_{r \in R_i^* \bmod Q_i} X_q(r)^m \\
& \leq \sum_{\widetilde{q_0} \mid Q_{i-1}} \sum_{\widetilde{q_1} \in \mathcal{N}_i} \sum_{\substack{q'_{10} \mid Q_{i-1}, \ldots, q'_{m0} \mid Q_{i-1} \\ \operatorname{lcm}(q'_{10}, \ldots, q'_{m0}) = \widetilde{q_0}}} \sum_{\substack{q'_{11} \in \mathcal{N}_i, \ldots, q'_{m1} \in \mathcal{N}_i \\ \operatorname{lcm}(q'_{11}, \ldots, q'_{m1}) = \widetilde{q_1}}} \sum_{\substack{r \in R_i^* \bmod Q_i \\ a_q q'_{j0} q'_{j1} \equiv r \pmod{q'_{j0}q'_{j1}} \ \forall j}} 1.
\end{aligned} \tag{1.25}$$

Define

$$S(\widetilde{q_0}, \widetilde{q_1}) = \max_{c \in \mathbb{Z}} \left\{ \sum_{\substack{r \in R_i^* \bmod Q_i \\ r \equiv c \pmod{\widetilde{q_0}\widetilde{q_1}}}} 1 \right\}.$$

Note that although j is changing in the last sum of equation (1.25), and there may not be a solution to the congruence, we want the maximum number of solutions counted, which results in $S(\widetilde{q_0}, \widetilde{q_1})$ as an upper bound on this last sum in equation (1.25).

Recalling $\ell_m(n) = |\{(n_1, n_2, \ldots, n_m) \in \mathbb{N}^m : \operatorname{lcm}(n_1, n_2, \ldots, n_m) = n\}|$, we then have

$$\sum_{r \in R_i^* \bmod Q_i} X_q(r)^m \leq \sum_{\widetilde{q_0} | Q_{i-1}} \sum_{\widetilde{q_1} \in \mathcal{N}_i} \ell_m(\widetilde{q_0})\, \ell_m(\widetilde{q_1})\, S(\widetilde{q_0}, \widetilde{q_1}).$$

We now look at the case when $\widetilde{q_1} \leq T_i$ and when $\widetilde{q_1} > T_i$ to bound $S(\widetilde{q_0}, \widetilde{q_1})$. Thus, we are interested in using the estimate

$$\begin{aligned}\sum_{r \in R_i^* \bmod Q_i} X_q(r)^m \leq & \sum_{\widetilde{q_0} | Q_{i-1}} \sum_{\substack{\widetilde{q_1} \in \mathcal{N}_i \\ \widetilde{q_1} \leq T_i}} \ell_m(\widetilde{q_0})\, \ell_m(\widetilde{q_1})\, S(\widetilde{q_0}, \widetilde{q_1}) \\ & + \sum_{\widetilde{q_0} | Q_{i-1}} \sum_{\substack{\widetilde{q_1} \in \mathcal{N}_i \\ \widetilde{q_1} > T_i}} \ell_m(\widetilde{q_0})\, \ell_m(\widetilde{q_1})\, S(\widetilde{q_0}, \widetilde{q_1}).\end{aligned} \tag{1.26}$$

For the case when $\widetilde{q_1} \leq T_i$, we recall $r \in R_i^* = R_i \cap S_{i-1}$ implies $r \in R_i$ and $r \in S_{i-1} \subset R_{i-1}$. Since S_{i-1} is a set of residue classes modulo Q_{i-1}, and $S_{i-1} \cap R_i$ extends to classes modulo Q_i by adding multiples of Q_{i-1}, we have $r \in R_i^*$ implies $r = c_0 + kQ_{i-1}$ where $c_0 \in S_{i-1}$ and $k \in \mathbb{Z}$. So, $r \equiv c_0 \pmod{Q_{i-1}}$. Furthermore, $\widetilde{q_0} \mid Q_{i-1}$ gives us that $r \equiv c_0 \pmod{\widetilde{q_0}}$. We are interested when $r \equiv c \pmod{\widetilde{q_0}\widetilde{q_1}}$, which is equivalent to $r \equiv c \pmod{\widetilde{q_0}}$ and $r \equiv c \pmod{\widetilde{q_1}}$. So, since $r \equiv c_0 \pmod{\widetilde{q_0}}$, we have $c \equiv c_0 \pmod{\widetilde{q_0}}$. First restricting to when $c \equiv c_0 \pmod{\widetilde{q_0}}$, and then summing over all such c_0, gives the following,

$$\sum_{\substack{r \in R_i^* \bmod Q_i \\ r \equiv c \pmod{\widetilde{q_0}\widetilde{q_1}}}} 1 = \sum_{\substack{c_0 \in S_{i-1} \bmod Q_{i-1} \\ c_0 \equiv c \pmod{\widetilde{q_0}}}} \sum_{\substack{r \in R_i^* \bmod Q_i \\ r \equiv c \pmod{\widetilde{q_1}} \\ r \equiv c_0 \pmod{Q_{i-1}}}} 1.$$

Then by the induction hypothesis of Theorem 1.5.1 statement (4), since $\widetilde{q_1} \leq T_i$, we have

$$\begin{aligned}\sum_{\substack{r \in R_i^* \bmod Q_i \\ r \equiv c \pmod{\widetilde{q_1}} \\ r \equiv c_0 \pmod{Q_{i-1}}}} 1 &= |R_{i,c_0} \cap (c \bmod \widetilde{q_1}) \bmod Q_i| \\ &\leq \max_{c \bmod \widetilde{q_1}} |R_{i,c_0} \cap (c \bmod \widetilde{q_1}) \bmod Q_i| \\ &\leq \frac{2}{\widetilde{q_1}} |R_{i,c_0} \bmod Q_i|.\end{aligned}$$

Then by the induction hypothesis of Theorem 1.5.1 statement (3), we have

$$\frac{2}{\widetilde{q_1}}|R_{i,c_0} \bmod Q_i| \leq c_t \frac{2}{\widetilde{q_1}} \left(\frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|} \right),$$

for some constant c_t. Combining both results, and summing over c_0, we have

$$\begin{aligned} \sum_{\substack{r \in R_i^* \bmod Q_i \\ r \equiv c \pmod{\widetilde{q_0}\widetilde{q_1}}}} 1 &= \sum_{\substack{c_0 \in S_{i-1} \bmod Q_{i-1} \\ c_0 \equiv c \pmod{\widetilde{q_0}}}} \sum_{\substack{r \in R_i^* \bmod Q_i \\ r \equiv c \pmod{\widetilde{q_1}} \\ r \equiv c_0 \pmod{Q_{i-1}}}} 1 \\ &\leq \sum_{\substack{c_0 \in S_{i-1} \bmod Q_{i-1} \\ c_0 \equiv c \pmod{\widetilde{q_0}}}} c_t \frac{2}{\widetilde{q_1}} \left(\frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|} \right). \end{aligned} \tag{1.27}$$

The number of terms in this last sum is at most $\dfrac{Q_{i-1}}{\widetilde{q_0}}$. Applying this to (1.27) gives

$$\sum_{\substack{r \in R_i^* \bmod Q_i \\ r \equiv c \pmod{\widetilde{q_0}\widetilde{q_1}}}} 1 \leq \frac{2c_t Q_{i-1}}{\widetilde{q_0}\widetilde{q_1}} \left(\frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|} \right).$$

We deduce

$$\begin{aligned} &\sum_{\widetilde{q_0} | Q_{i-1}} \sum_{\substack{\widetilde{q_1} \in \mathcal{N}_i \\ \widetilde{q_1} \leq T_i}} \ell_m(\widetilde{q_0}) \ell_m(\widetilde{q_1}) S(\widetilde{q_0}, \widetilde{q_1}) \\ &\qquad \leq \sum_{\widetilde{q_0} | Q_{i-1}} \sum_{\widetilde{q_1} \in \mathcal{N}_i} \ell_m(\widetilde{q_0}) \ell_m(\widetilde{q_1}) \frac{2c_t Q_{i-1}}{\widetilde{q_0}\widetilde{q_1}} \left(\frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|} \right) \\ &\qquad = (2c_t Q_{i-1}) \left(\frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|} \right) \sum_{\widetilde{q_0} | Q_{i-1}} \sum_{\widetilde{q_1} \in \mathcal{N}_i} \frac{\ell_m(\widetilde{q_0})}{\widetilde{q_0}} \cdot \frac{\ell_m(\widetilde{q_1})}{\widetilde{q_1}} \\ &\qquad = (2c_t Q_{i-1}) \left(\frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|} \right) \sum_{\widetilde{q_0} | Q_{i-1}} \sum_{\widetilde{q_1} \in \mathcal{N}_i} \frac{\ell_m(\widetilde{q_0}\widetilde{q_1})}{\widetilde{q_0}\widetilde{q_1}}, \end{aligned}$$

where Lemma 1.3.1 was used in the last step. Analogous to rewriting the q_j''s in equation (1.24) by splitting them into $q_{j0}' \mid Q_{i-1}$ and $q_{j1}' \in \mathcal{N}_\backslash$, we rewrite $\widetilde{q_0}\widetilde{q_1} = \widetilde{q}$

where $\widetilde{q} \mid Q_i$. Applied to the above gives

$$\begin{aligned}
&\sum_{\widetilde{q_0}|Q_{i-1}} \sum_{\substack{\widetilde{q_1}\in\mathcal{N}_i \\ \widetilde{q_1}\leq T_i}} \ell_m\left(\widetilde{q_0}\right)\ell_m\left(\widetilde{q_1}\right) S\left(\widetilde{q_0},\widetilde{q_1}\right) \\
&\qquad\qquad \leq \left(2c_t Q_{i-1}\right)\left(\frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|}\right) \sum_{\widetilde{q_0}|Q_{i-1}} \sum_{\widetilde{q_1}\in\mathcal{N}_i} \frac{\ell_m\left(\widetilde{q_0}\widetilde{q_1}\right)}{\widetilde{q_0}\widetilde{q_1}} \\
&\qquad\qquad = \left(2c_t Q_{i-1}\right)\left(\frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|}\right) \sum_{\widetilde{q}|Q_i} \frac{\ell_m\left(\widetilde{q}\right)}{\widetilde{q}} \\
&\qquad\qquad \leq \left(2c_t Q_{i-1}\right)\left(\frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|}\right) \left(C\log P_i\right)^{2^m},
\end{aligned} \tag{1.28}$$

where the last step used Lemma 1.3.3 equation (1.3). Applying the induction hypothesis of Theorem 1.5.1 statement (1) to (1.28), which gives us

$$\frac{Q_{i-1}}{|S_{i-1} \bmod Q_{i-1}|} \leq \exp\left(2\left(\log P_{i-1}\right)^2\right),$$

we then have

$$\begin{aligned}
&\sum_{\widetilde{q_0}|Q_{i-1}} \sum_{\substack{\widetilde{q_1}\in\mathcal{N}_i \\ \widetilde{q_1}\leq T_i}} \ell_m\left(\widetilde{q_0}\right)\ell_m\left(\widetilde{q_1}\right) S\left(\widetilde{q_0},\widetilde{q_1}\right) \\
&\qquad\qquad \leq 2c_t|R_i^* \bmod Q_i| \exp\left(2\left(\log P_{i-1}\right)^2\right)\left(C\log P_i\right)^{2^m}.
\end{aligned} \tag{1.29}$$

This gives us the estimate we want for $\widetilde{q_1} \leq T_i$.

Consider when $\widetilde{q_1} > T_i$. We gain an upper bound on $S\left(\widetilde{q_0},\widetilde{q_1}\right)$ by starting with

$$\sum_{\substack{r\in R_i^* \\ r\equiv c \pmod{\widetilde{q_o}\widetilde{q_1}}}} 1 \leq \sum_{\substack{0\leq r\leq Q_i-1 \\ r\equiv c \pmod{\widetilde{q_0}\widetilde{q_1}}}} 1 = \frac{Q_i}{\widetilde{q_0}\widetilde{q_1}}.$$

The inequality holds since we are including more or the same number of residue classes going from the first sum to the second sum, and the equality holds since we have simply computed the number of terms in the second sum. Notice, this inequality

does not depend on c, so we can apply the maximum over all c to get

$$\begin{aligned}
&\sum_{\widetilde{q_0}|Q_i-1} \sum_{\substack{\widetilde{q_1}\in\mathcal{N}_{i+1} \\ \widetilde{q_1}>T_i}} \ell_m\left(\widetilde{q_0}\right)\ell_m\left(\widetilde{q_1}\right) S\left(\widetilde{q_0},\widetilde{q_1}\right) \\
&\qquad \leq \sum_{\widetilde{q_0}|Q_i-1} \sum_{\substack{\widetilde{q_1}\in\mathcal{N}_{i+1} \\ \widetilde{q_1}>T_i}} \ell_m\left(\widetilde{q_0}\right)\ell_m\left(\widetilde{q_1}\right) \frac{Q_i}{\widetilde{q_0}\widetilde{q_1}} \\
&\qquad \leq Q_i \sum_{\widetilde{q_0}|Q_i-1} \frac{\ell_m\left(\widetilde{q_0}\right)}{\widetilde{q_0}} \sum_{\substack{\widetilde{q_1}\in\mathcal{N}_i \\ \widetilde{q_1}>T_i}} \frac{\ell_m\left(\widetilde{q_1}\right)}{\widetilde{q_1}} \\
&\qquad < Q_i \left(C\log P_{i-1}\right)^{2^m} \exp\left(-\left(\log P_i\right)^{K-1}\right)\left(C\log P_i\right)^{2^m e},
\end{aligned} \tag{1.30}$$

where Lemma 1.3.3, equations (1.2) and (1.3) are used in the last step. Applying the induction hypotheses from Theorem 1.5.1, we have the following,

$$\begin{aligned}
Q_i &\leq Q_{i-1}|R_i^* \bmod Q_i| \frac{1}{|S_{i-1} \bmod Q_{i-1}|} \exp\left(\left(\log P_i\right)^2\right) \\
&\leq |R_i^* \bmod Q_i| \exp\left(\left(\log P_i\right)^2\right) \exp\left(2\left(\log P_{i-1}\right)^2\right).
\end{aligned}$$

The first inequality holds by statement (2) in the induction hypothesis, while the second inequality holds by statement (1) in the induction hypothesis. Recall, $P_i = e^{P_{i-1}^{\delta}}$. This gives us $\log P_i = P_{i-1}^{\delta} > 2\left(\log P_{i-1}\right)$. Therefore, $\left(\log P_i\right)^2 > 4\left(\log P_{i-1}\right)^2$ or $2\left(\log P_{i-1}\right)^2 < \frac{1}{2}\left(\log P_i\right)^2$. We deduce

$$Q_i < |R_i^* \bmod Q_i| \exp\left(\left(\log P_i\right)^2\right) \exp\left(\frac{1}{2}\left(\log P_i\right)^2\right) = |R_i^* \bmod Q_i| \exp\left(\frac{3}{2}\left(\log P_i\right)^2\right).$$

Applying this bound on Q_i to equation (1.30), we have

$$\begin{aligned}
&\sum_{\widetilde{q_0}|Q_i-1} \sum_{\substack{\widetilde{q_1}\in\mathcal{N}_{i+1} \\ \widetilde{q_1}>T_i}} \ell_m\left(\widetilde{q_0}\right)\ell_m\left(\widetilde{q_1}\right) S\left(\widetilde{q_0},\widetilde{q_1}\right) \\
&\qquad < |R_i^* \bmod Q_i| \frac{\exp\left(\frac{3}{2}\left(\log P_i\right)^2\right)}{\exp\left(\left(\log P_i\right)^{K-1}\right)} \left(C\log P_{i-1}\right)^{2^m} \left(C\log P_i\right)^{2^m e}
\end{aligned} \tag{1.31}$$

Recalling, $m = \sqrt{\log\log P_i} < \log_2 \log P_i$, gives us $2^m < \log P_i$. Thus, we obtain the two inequalities

$$\left(C\log P_{i-1}\right)^{2^m} = \exp\left(2^m \log\left(C\log P_{i-1}\right)\right) < \exp\left(\log P_i \log\left(C\log P_{i-1}\right)\right), \tag{1.32}$$

and

$$(C\log P_i)^{2^m e} = \exp\left(2^m e \log\left(C\log P_i\right)\right) < \exp\left(\log\left(P_i\right) e\log\left(C\log P_i\right)\right). \tag{1.33}$$

Additionally, $K > 3$ implies $K = 2+\epsilon$ where $\epsilon > 0$. Therefore, for M sufficiently large,

$$(\log P_i)^{K-1} - \frac{3}{2}(\log P_i)^2 = (\log P_i)^2\left((\log P_i)^{\epsilon} - \frac{3}{2}\right) > (\log P_i)^2.$$

Thus, we have

$$\exp\left(\frac{3}{2}(\log P_i)^2 - (\log P_i)^{K-1}\right) < \frac{1}{\exp\left((\log P_i)^2\right)}. \tag{1.34}$$

Applying equations (1.32), (1.33), and (1.34) to equation (1.31) we have

$$\sum_{\widetilde{q_0}|Q_i-1}\sum_{\substack{\widetilde{q_1}\in\mathcal{N}_{i+1}\\ \widetilde{q_1}>T_i}} \ell_m\left(\widetilde{q_0}\right)\ell_m\left(\widetilde{q_1}\right)S\left(\widetilde{q_0},\widetilde{q_1}\right)$$
$$< |R_i^* \bmod Q_i|\frac{\exp\left(\log P_i\log\left(C\log P_{i-1}\right)\right)\exp\left(e\log P_i\log\left(C\log P_i\right)\right)}{\exp\left((\log P_i)^2\right)},$$

so that

$$\sum_{\widetilde{q_0}|Q_i-1}\sum_{\substack{\widetilde{q_1}\in\mathcal{N}_{i+1}\\ \widetilde{q_1}>T_i}} \ell_m\left(\widetilde{q_0}\right)\ell_m\left(\widetilde{q_1}\right)S\left(\widetilde{q_0},\widetilde{q_1}\right) < |R_i^* \bmod Q_i| \tag{1.35}$$

holds for M sufficiently large. This gives us the estimate we want for $\widetilde{q_1} > T_i$. Applying (1.29) and (1.35) to (1.26) we deduce (1.22), where possibly the constant C needs to be increased.

In particular, when $m = 1$, using (1.22) we have

$$\frac{1}{|R_i^* \bmod Q_i|}\sum_{r\in R_i^* \bmod Q_i}\sum_{\substack{q\in\mathcal{N}_{i+1}\\ 1<q\le T_{i+1}}}\frac{X_q(r)}{q} = \frac{1}{|R_i^* \bmod Q_i|}\sum_{\substack{q\in\mathcal{N}_{i+1}\\ 1<q\le T_{i+1}}}\frac{1}{q}\sum_{r\in R_i^* \bmod Q_i} X_q(r)$$
$$\le \exp\left(\left(2\log P_{i-1}\right)^2\right)\left(C\log P_i\right)^2\sum_{q\in\mathcal{N}_{i+1}}\frac{1}{q}$$

From (1.1) in Lemma 1.3.3 we have $\sum_{n\in\mathcal{N}_{i+1}}\frac{1}{n} \le C\frac{\log P_{i+1}}{\log P_i}$, which gives us

$$\frac{1}{|R_i^* \bmod Q_i|}\sum_{r\in R_i^* \bmod Q_i}\sum_{\substack{q\in\mathcal{N}_{i+1}\\ 1<q\le T_{i+1}}}\frac{X_q(r)}{q} \le \exp\left(\left(2\log P_{i-1}\right)^2\right)\left(C\log P_i\right)^2\cdot C\frac{\log P_{i+1}}{\log P_i}$$

$$= C^3 \log P_{i+1} \exp\left((2\log P_{i-1})^2\right)(\log P_i).$$

Hence, we have proven equation (1.23). □

Definition 1.6.2 (Jensen's inequality)**.** If φ is a convex function on an interval I, $x_1, x_2, \ldots, x_n \in I$, $c_1, c_2, \ldots, c_n \geq 0$, and $c_1 + c_2 + \ldots + c_n = 1$, then

$$\varphi(c_1x_1 + c_2x_2 + \ldots c_nx_n) \leq c_1\varphi(x_1) + c_2\varphi(x_2) + \ldots c_n\varphi(x_n).$$

Lemma 1.6.3. *Let $\theta > 0$ be any fixed number. For any $\lambda \geq P_i$, and any non-negative constants $(\beta_q)_{q\in\mathcal{N}_{i+1}}$ not all zero, we have*

$$\left|\left\{r \in R_i^* \bmod Q_i : \sum_{q\in\mathcal{N}_{i+1}} \beta_q X_q(r) > \lambda^\theta \sum_{q\in\mathcal{N}_{i+1}} \beta_q\right\}\right| \leq |R_i^* \bmod Q_i| \exp\left(-\frac{\theta}{2}\log\lambda\sqrt{\log\log P_i}\right).$$

Proof. Define

$$A_{\lambda,\theta} = \left\{r \in R_i^* \bmod Q_i : \sum_{q\in\mathcal{N}_{i+1}} \beta_q X_q(r) > \lambda^\theta \sum_{q\in\mathcal{N}_{i+1}} \beta_q\right\}.$$

We must then show

$$|A_{\lambda,\theta}| \leq |R_i^* \bmod Q_i| \exp\left(-\frac{\theta}{2}\log\lambda\sqrt{\log\log P_i}\right).$$

Consider the following function, $\varphi(x) = x^m$. We have $\varphi(x)'' = m(m-1)x^{m-2}$, so $\varphi(x)$ is convex if $m \geq 1$ and $x \geq 0$. Define

$$c_q = \frac{\beta_q}{\sum_{q\in\mathcal{N}_{i+1}} \beta_q}.$$

Notice, $c_q \geq 0$ for all $q \in \mathcal{N}_{i+1}$, by our assumptions on β_q. Also, we have

$$\sum_{q\in\mathcal{N}_{i+1}} c_q = \sum_{q\in\mathcal{N}_{i+1}} \left(\frac{\beta_q}{\sum_{q\in\mathcal{N}_{i+1}} \beta_q}\right) = 1.$$

So, provided $m \geq 1$ and $x \geq 0$, applying Jensen's inequality we have

$$\varphi\left(\sum_{q\in\mathcal{N}_{i+1}}\left(\frac{\beta_q}{\sum\limits_{q\in\mathcal{N}_{i+1}}\beta_q}X_q(r)\right)\right) = \left(\sum_{q\in\mathcal{N}_{i+1}}\left(\frac{\beta_q}{\sum\limits_{q\in\mathcal{N}_{i+1}}\beta_q}X_q(r)\right)\right)^m$$
$$\leq \sum_{q\in\mathcal{N}_{i+1}}\left(\left(\frac{\beta_q}{\sum\limits_{q\in\mathcal{N}_{i+1}}\beta_q}\right)(X_q(r))^m\right).$$

This gives us

$$\sum_{r\in R_i^* \bmod Q_i}\left(\sum_{q\in\mathcal{N}_{i+1}}\left(\frac{\beta_q}{\sum\limits_{q\in\mathcal{N}_{i+1}}\beta_q}\right)X_q(r)\right)^m$$
$$\leq \sum_{r\in R_i^* \bmod Q_i}\left(\sum_{q\in\mathcal{N}_{i+1}}\left(\frac{\beta_q}{\sum\limits_{q\in\mathcal{N}_{i+1}}\beta_q}\right)(X_q(r))^m\right)$$
$$= \sum_{q\in\mathcal{N}_{i+1}}\left(\frac{\beta_q}{\sum\limits_{q\in\mathcal{N}_{i+1}}\beta_q}\right)\sum_{r\in R_i^* \bmod Q_i}(X_q(r))^m$$
$$\leq \left(\max_{q\in\mathcal{N}_{i+1}}\left(\sum_{r\in R_i^* \bmod Q_i}(X_q(r))^m\right)\right)\sum_{q\in\mathcal{N}_{i+1}}\left(\frac{\beta_q}{\sum\limits_{q\in\mathcal{N}_{i+1}}\beta_q}\right)$$
$$= \max_{q\in\mathcal{N}_{i+1}}\left(\sum_{r\in R_i^* \bmod Q_i}(X_q(r))^m\right).$$

Multiplying both sides of the above inequality by $\frac{1}{|R_i^* \bmod Q_i|}\cdot\left(\sum\limits_{q\in\mathcal{N}_{i+1}}\beta_q\right)^m$ we have

$$\frac{1}{|R_i^* \bmod Q_i|}\sum_{r\in R_i^* \bmod Q_i}\left(\sum_{q\in\mathcal{N}_{i+1}}\beta_q X_q(r)\right)^m$$
$$\leq \left(\sum_{q\in\mathcal{N}_{i+1}}\beta_q\right)^m \max_{q\in\mathcal{N}_{i+1}}\left(\frac{1}{|R_i^* \bmod Q_i|}\sum_{r\in R_i^* \bmod Q_i}(X_q(r))^m\right). \tag{1.36}$$

Consider the inequality

$$\frac{1}{|R_i^* \bmod Q_i|}|A_{\lambda,\theta}|\lambda^{\theta m}\left(\sum_{q\in\mathcal{N}_{i+1}}\beta_q\right)^m$$

$$= \frac{1}{|R_i^* \bmod Q_i|} \sum_{r \in A_{\lambda,\theta}} \left(\lambda^\theta \sum_{q \in \mathcal{N}_{i+1}} \beta_q \right)^m$$

$$\leq \frac{1}{|R_i^* \bmod Q_i|} \sum_{r \in A_{\lambda,\theta}} \left(\sum_{q \in \mathcal{N}_{i+1}} \beta_q X_q(r) \right)^m$$

$$\leq \frac{1}{|R_i^* \bmod Q_i|} \sum_{r \in R_i^* \bmod Q_i} \left(\sum_{q \in \mathcal{N}_{i+1}} \beta_q X_q(r) \right)^m$$

$$\leq \left(\sum_{q \in \mathcal{N}_{i+1}} \beta_q \right)^m \max_{q \in \mathcal{N}_{i+1}} \left(\frac{1}{|R_i^* \bmod Q_i|} \sum_{r \in R_i^* \bmod Q_i} (X_q(r))^m \right).$$

The equality holds since $\lambda^{\theta m}$ does not depend on r. The first inequality is true by how we defined $A_{\lambda,\theta}$. The last inequality holds by (1.36). Dividing through by the expression $\left(\sum_{q \in \mathcal{N}_{i+1}} \beta_q \right)^m$ we obtain

$$\frac{1}{|R_i^* \bmod Q_i|} |A_{\lambda,\theta}| \lambda^{\theta m} \leq \max_{q \in \mathcal{N}_{i+1}} \left(\frac{1}{|R_i^* \bmod Q_i|} \sum_{r \in R_i^* \bmod Q_i} (X_q(r))^m \right). \tag{1.37}$$

For $m \leq \sqrt{\log \log P_i}$, we can then apply Lemma 1.6.1 to (1.37), which gives us

$$\frac{1}{|R_i^* \bmod Q_i|} |A_{\lambda,\theta}| \lambda^{\theta m} \leq \exp\left((2 \log P_{i-1})^2 \right) (C \log P_i)^{2^m}.$$

We deduce

$$|A_{\lambda,\theta}| \leq \frac{|R_i^* \bmod Q_i|}{\lambda^{\theta m}} \exp\left((2 \log P_{i-1})^2 \right) (C \log P_i)^{2^m}.$$

Choose $m = \lfloor \sqrt{\log \log P_i} \rfloor$. Observe, $\frac{1}{\lambda^{\theta m}} = \exp(-\theta m \log \lambda)$. Applying this to the above inequality we have

$$|A_{\lambda,\theta}| \leq |R_i^* \bmod Q_i| \exp\left(-\theta \left(\left\lfloor \sqrt{\log \log P_i} \right\rfloor \right) \log \lambda \right) \exp\left((2 \log P_{i-1})^2 \right) (C \log P_i)^{2^m}.$$

When $\sqrt{\log \log P_i} \geq 10$ we have $\lfloor \sqrt{\log \log P_i} \rfloor \geq \frac{9}{10} \sqrt{\log \log P_i}$. We deduce

$$|A_{\lambda,\theta}| \leq |R_i^* \bmod Q_i| \exp\left(-\theta \left(\frac{9}{10} \sqrt{\log \log P_i} \right) \log \lambda \right) \exp\left((2 \log P_{i-1})^2 \right) (C \log P_i)^{2^m}. \tag{1.38}$$

When $\lambda \geq P_i$, we have

$$\frac{\frac{2\theta}{5} \log \lambda \sqrt{\log \log P_i}}{\log P_i} > \frac{2\theta}{5} \sqrt{\log \log P_i}.$$

Notice, as P_i approaches infinity, the right-hand side of this inequality goes to infinity, as well as the left-hand side. Additionally,

$$\frac{(2\log P_{i-1})^2}{\log P_i} = \frac{4(\log P_{i-1})^2}{\log P_i} = \frac{4\left(\log\log P_i^{1/\delta}\right)^2}{\log P_i}$$

goes to zero as P_i approaches infinity. Moreover, when $P_i > e^C$, or equivalently $\log P_i > C$, we obtain

$$\frac{2^m(\log C + \log\log P_i)}{\log P_i} < \frac{2^m(\log\log P_i + \log\log P_i)}{\log P_i} = \frac{2\cdot 2^m \log\log P_i}{\log P_i}.$$

Applying the natural logarithm to both sides of the inequality, as well as dividing by $\log\log P_i$, we find

$$\begin{aligned}\frac{\log\left(\frac{2^m(\log C+\log\log P_i)}{\log P_i}\right)}{\log\log P_i} &< \frac{\log\left(\frac{2^{m+1}\log\log P_i}{\log P_i}\right)}{\log\log P_i} \\ &= \frac{\log 2^{m+1} + \log\log\log P_i - \log\log P_i}{\log\log P_i}.\end{aligned}$$

Notice, as P_i approaches infinity the the right-hand side of the above inequality goes to $-1 < -\frac{1}{2}$. So, for M sufficiently large

$$\frac{\log\left(\frac{2^m(\log C+\log\log P_i)}{\log P_i}\right)}{\log\log P_i} < -\frac{1}{2},$$

which gives us

$$\log\left(\frac{2^m(\log C + \log\log P_i)}{\log P_i}\right) < -\frac{1}{2}\log\log P_i,$$

or

$$\frac{2^m(\log C + \log\log P_i)}{\log P_i} < (\log P_i)^{-1/2}.$$

Then, as P_i approaches infinity, the right-hand side approaches zero, as well as the left-hand side. Using

$$\lim_{P_i\to\infty} \frac{\frac{2\theta}{5}\log\lambda\sqrt{\log\log P_i}}{\log P_i} = \infty, \text{ and } \lim_{P_i\to\infty} \frac{(2\log P_{i-1})^2}{\log P_i} = 0,$$

together with

$$\lim_{P_i\to\infty} \frac{2^m(\log P_i + \log\log P_i)}{\log P_i} = 0,$$

we deduce for M sufficiently large that

$$\begin{aligned}\frac{\frac{2\theta}{5}\log\lambda\sqrt{\log\log P_i}}{\log P_i} &> \frac{\left(2\log P_{i-1}\right)^2}{\log P_i} + \frac{2^m\left(\log P_i + \log\log P_i\right)}{\log P_i} \\ &> \frac{\left(2\log P_{i-1}\right)^2 + 2^m\left(\log C + \log\log P_i\right)}{\log P_i}.\end{aligned}$$

Hence,

$$\frac{2\theta}{5}\log\lambda\sqrt{\log\log P_i} > \left(2\log P_{i-1}\right)^2 + 2^m\left(\log C + \log\log P_i\right).$$

Therefore,

$$\begin{aligned}\exp\left(\frac{2\theta}{5}\log\lambda\sqrt{\log\log P_i}\right) &> \exp\left(\left(2\log P_{i-1}\right)^2 + 2^m\left(\log C + \log\log P_i\right)\right) \\ &= \exp\left(\left(2\log P_{i-1}\right)^2\right)\exp\left(2^m\left(\log\left(C\log P_i\right)\right)\right) \\ &= \exp\left(\left(2\log P_{i-1}\right)^2\right)\left(C\log P_i\right)^{2^m}.\end{aligned}$$

From (1.38) we now obtain

$$\begin{aligned}|A_{\lambda,\theta}| &< |R_i^* \bmod Q_i|\exp\left(-\theta\left(\frac{9}{10}\sqrt{\log\log P_i}\right)\log\lambda\right)\exp\left(\frac{2\theta}{5}\log\lambda\sqrt{\log\log P_i}\right) \\ &= |R_i^* \bmod Q_i|\exp\left(\log\lambda\sqrt{\log\log P_i}\left(-\frac{9\theta}{10}+\frac{2\theta}{5}\right)\right) \\ &= |R_i^* \bmod Q_i|\exp\left(-\frac{\theta}{2}\log\lambda\sqrt{\log\log P_i}\right),\end{aligned}$$

completing the proof. □

Lemma 1.6.4. *There is a constant $c > 0$ such that each of the sets*

$$E_{i,sup} = \left\{r \in R_i^* \bmod Q_i : \exists q \in \mathcal{N}_{i+1}^*, X_q(r) > q^\theta\right\},$$

$$E_{i,GCD} = \left\{r \in R_i^* \bmod Q_i : \exists q \in \mathcal{N}_{i+1}, 1 < q \le T_{i+1}, \sum_{\substack{q' \in \mathcal{N}_{i+1} \\ (q,q')>1}} \frac{X_{q'}(r)}{q'} > P_i^{-1+\theta+(K+1)\delta}\right\},$$

and

$$E_{i,tail} = \left\{r \in R_i^* \bmod Q_i : \sum_{\substack{q \in \mathcal{N}_{i+1} \\ q > T_{i+1}}} \frac{X_q(r)}{q} > \exp\left(-P_i^{(K-1)\delta}\right)P_i^{2e\delta+1}\right\}$$

makes up a proportion of $R_i^* \bmod Q_i$ bounded above by $\exp\left(-c\log P_i\sqrt{\log\log P_i}\right)$.

Proof. Let $q \in \mathcal{N}_{i+1}^*$ be fixed, and let $\lambda = q$. Define $\beta_q = 1$, and $\beta_{q'} = 0$ if $q' \neq q$. We then have

$$\left|\left\{r \in R_i^* \bmod Q_i : \sum_{q' \in \mathcal{N}_{i+1}} \beta_{q'} X_{q'}(r) > \lambda^\theta \sum_{q' \in \mathcal{N}_{i+1}} \beta_{q'}\right\}\right| = \left|\left\{r \in R_i^* \bmod Q_i : X_q(r) > q^\theta\right\}\right|.$$

Note, $q \in \mathcal{N}_{i+1}^*$ implies $\lambda \geq P_i$, and $\beta_q = 1$ implies not all β_q are zero. Thus, the hypothesis of Lemma 1.6.3 are satisfied. Therefore, we have

$$\begin{aligned}\left|\left\{r \in R_i^* \bmod Q_i : X_q(r) > q^\theta\right\}\right| &\leq |R_i^* \bmod Q_i| \exp\left(-\frac{\theta}{2}\log q\sqrt{\log\log P_i}\right) \\ &= |R_i^* \bmod Q_i|\, q^{-\theta\sqrt{\log\log P_i}/2}.\end{aligned}$$

We now let $q \in \mathcal{N}_{i+1}^*$ vary. We deduce

$$\begin{aligned}|E_{i,sup}| &= \left|\left\{r \in R_i^* \bmod Q_i : \exists q \in \mathcal{N}_{i+1}^*, X_q(r) > q^\theta\right\}\right| \\ &\leq \sum_{q \in \mathcal{N}_{i+1}^*} \left|\left\{r \in R_i^* \bmod Q_i : X_q(r) > q^\theta\right\}\right| \\ &\leq |R_i^* \bmod Q_i| \sum_{q > P_i} \frac{1}{q^{\theta\sqrt{\log\log P_i}/2}}.\end{aligned}$$

For $t \geq 2$ and $z \geq 2$, we have

$$\begin{aligned}\sum_{n>z} \frac{1}{n^t} &\leq \int_{z-1}^{\infty} \frac{1}{x^t} \mathrm{dx} \\ &= \frac{x^{-t+1}}{-t+1}\Big|_{x=z-1}^{x=\infty} \\ &= 0 - \frac{(z-1)^{-t+1}}{-t+1} \\ &= \frac{(z-1)^{-t+1}}{t-1} \\ &\leq (z-1)^{-t+1} \\ &\leq \left(\frac{z}{2}\right)^{-t+1}.\end{aligned} \tag{1.39}$$

For large enough M, we then get

$$\begin{aligned}
|E_{i,sup}| &\leq |R_i^* \bmod Q_i|(P_i/2)^{-(\theta/2)\sqrt{\log\log P_i}+1} \\
&\leq |R_i^* \bmod Q_i|(P_i/2)^{-(\theta/4)\sqrt{\log\log P_i}} \\
&= |R_i^* \bmod Q_i| \exp\left(-(\theta/4)\sqrt{\log\log P_i}\,\log(P_i/2)\right),
\end{aligned}$$

which implies the bound stated in the lemma for $E_{i,sup}$.

Define

$$E_{i,mult} = \left\{ r \in R_i^* \bmod Q_i : \exists q \in \mathcal{N}_{i+1}, 1 < q \leq T_{i+1}, \sum_{qq' \in \mathcal{N}_{i+1}} \frac{X_{qq'}(r)}{qq'} > \frac{P_i^\delta}{q^{1-\theta}} \right\}.$$

We show $E_{i,GCD} \subseteq E_{i,mult}$, and then obtain the desired bound on $E_{i,mult}$. Let $r \notin E_{i,mult}$, and fix $q \in \mathcal{N}_{i+1}$ such that $1 < q \leq T_{i+1}$. Observe, for $dq'' = q'$ we have

$$\begin{aligned}
\sum_{\substack{q' \in \mathcal{N}_{i+1} \\ (q,q')>1}} \frac{X_{q'}(r)}{q'} &\leq \sum_{\substack{d \in \mathcal{N}_{i+1} \\ d|q, d>1}} \sum_{dq'' \in \mathcal{N}_{i+1}} \frac{X_{dq''}(r)}{dq''} \\
&\leq \sum_{\substack{d \in \mathcal{N}_{i+1} \\ d|q, d>1}} \frac{P_i^\delta}{d^{1-\theta}},
\end{aligned}$$

where the last inequality holds since $r \notin E_{i,mult}$. Applying Lemma 1.3.4 with $A = 1$, we then have

$$\begin{aligned}
\sum_{\substack{q' \in \mathcal{N}_{i+1} \\ (q,q')>1}} \frac{X_{q'}(r)}{q'} &\leq P_i^\delta \sum_{\substack{d \in \mathcal{N}_{i+1} \\ d|q, d>1}} \frac{1}{d^{1-\theta}} \\
&\leq P_i^\delta \frac{2P_i^{\theta+K\delta-1}}{\log P_i} \\
&\leq P_i^\delta \cdot P_i^{\theta+K\delta-1} \\
&= P_i^{-1+\theta+(K+1)\delta},
\end{aligned}$$

where the last inequality is true since M and, hence, P_i is large. This implies $r \notin E_{i,GCD}$, so $E_{i,GCD} \subseteq E_{i,mult}$.

Now to bound $E_{i,mult}$, we begin with

$$\sum_{qq' \in \mathcal{N}_{i+1}} \frac{1}{qq'} \leq \frac{1}{q} \sum_{q' \in \mathcal{N}_{i+1}} \frac{1}{q'} \leq \frac{1}{q} \cdot C \frac{\log P_{i+1}}{\log P_i},$$

where the last inequality holds by applying (1.1) of Lemma 1.3.3. Then, since $P_{i+1} = e^{P_i^\delta}$, we have

$$\frac{1}{q} \cdot C \frac{\log P_{i+1}}{\log P_i} = \frac{1}{q} \cdot C \frac{P_i^\delta}{\log P_i} \leq \frac{P_i^\delta}{q},$$

where we have used that M is sufficiently large. Thus,

$$\sum_{qq' \in \mathcal{N}_{i+1}} \frac{1}{qq'} \leq \frac{P_i^\delta}{q}. \tag{1.40}$$

Observe

$$\begin{aligned} |E_{i,mult}| &= \left| \left\{ r \in R_i^* \bmod Q_i : \exists q \in \mathcal{N}_{i+1}, 1 < q \leq T_{i+1}, \sum_{qq' \in \mathcal{N}_{i+1}} \frac{X_{qq'}(r)}{qq'} > \frac{P_i^\delta}{q^{1-\theta}} \right\} \right| \\ &\leq \left| \left\{ r \in R_i^* \bmod Q_i : \exists q \in \mathcal{N}_{i+1}, 1 < q \leq T_{i+1}, \sum_{qq' \in \mathcal{N}_{i+1}} \frac{X_{qq'}(r)}{qq'} > q^\theta \sum_{qq' \in \mathcal{N}_{i+1}} \frac{1}{qq'} \right\} \right| \\ &\leq \sum_{\substack{q \in \mathcal{N}_{i+1} \\ 1 < q \leq T_{i+1}}} \left| \left\{ r \in R_i^* \bmod Q_i : \sum_{qq' \in \mathcal{N}_{i+1}} \frac{X_{qq'}(r)}{qq'} > q^\theta \sum_{qq' \in \mathcal{N}_{i+1}} \frac{1}{qq'} \right\} \right|, \end{aligned}$$

by applying (1.40). We apply Lemma 1.6.3 with $\lambda = q$, $\beta_{qq'} = \dfrac{1}{qq'}$ for each $qq' \in \mathcal{N}_{i+1}$, and $\beta_{\widetilde{q}} = 0$ if $q \nmid \widetilde{q}$. We deduce

$$\begin{aligned} &\left| \left\{ r \in R_i^* \bmod Q_i : \sum_{qq' \in \mathcal{N}_{i+1}} \frac{X_{qq'}(r)}{qq'} > q^\theta \sum_{qq' \in \mathcal{N}_{i+1}} \frac{1}{qq'} \right\} \right| \\ &\qquad \leq |R_i^* \bmod Q_i| \exp\left(-\frac{\theta}{2} \log q \sqrt{\log \log P_i} \right). \end{aligned}$$

Therefore,

$$|E_{i,mult}| \leq \sum_{\substack{q \in \mathcal{N}_{i+1} \\ 1 < q \leq T_{i+1}}} |R_i^* \bmod Q_i| \exp\left(-\frac{\theta}{2} \log q \sqrt{\log \log P_i} \right)$$

$$\leq \sum_{q>P_i} |R_i^* \bmod Q_i| \exp\left(-\frac{\theta}{2}\log q\sqrt{\log\log P_i}\right)$$

$$= |R_i^* \bmod Q_i| \sum_{q>P_i} q^{-(\theta/2)\sqrt{\log\log P_i}}$$

$$\leq |R_i^* \bmod Q_i| \exp\left(-(\theta/4)\sqrt{\log\log P_i}\,\log(P_i/2)\right),$$

where the last inequality uses the same argument used for bounding $|E_{i,sup}|$ (see (1.39)). Thus, we have bounded $|E_{i,mult}|$, implying the bound stated for $|E_{i,GCD}|$ in the lemma.

Lastly, to bound $|E_{i,tail}|$, we consider $\sum_{\substack{n\in\mathcal{N}_{i+1}\\ n>T_{i+1}}} \frac{1}{n}$. Applying (1.2) of Lemma 1.3.3, with $m=1$, and recalling $P_{i+1}=e^{p_i^\delta}$, we have

$$\sum_{\substack{n\in\mathcal{N}_{i+1}\\ n>T_{i+1}}} \frac{1}{n} \leq \exp\left(-\left(\log P_{i+1}\right)^{K-1}\right)\left(C\log P_{i+1}\right)^{2e}$$

$$= \exp\left(-P_i^{\delta(K-1)}\right)\left(CP_i^\delta\right)^{2e}$$

$$\leq \exp\left(-P_i^{\delta(K-1)}\right) P_i^{\frac{1}{2}+2e\delta},$$

where the last inequality holds since M sufficiently large implies $C \leq P_i^{1/(4e)}$. Then, for $r \in E_{i,tail}$ we have

$$\sum_{\substack{q\in\mathcal{N}_{i+1}\\ q>T_{i+1}}} \frac{X_q(r)}{q} > \exp\left(-P_i^{\delta(K-1)}\right) P_i^{2e\delta+1} \geq P_i^{\frac{1}{2}} \sum_{\substack{q\in\mathcal{N}_{i+1}\\ q>T_{i+1}}} \frac{1}{q}. \tag{1.41}$$

Recall $\theta < 1/2$. Define $\lambda = P_i^{1/(2\theta)}$. For $q > T_{i+1}$, let $\beta_q = 1/q$, and let $\beta_q = 0$ otherwise. Applying Lemma 1.6.3 we have

$$\left|\left\{r \in R_i^* \bmod Q_i : \sum_{\substack{q\in\mathcal{N}_{i+1}\\ q>T_{i+1}}} \frac{X_q(r)}{q} > P_i^{\frac{1}{2}} \sum_{\substack{q\in\mathcal{N}_{i+1}\\ q>T_{i+1}}} \frac{1}{q}\right\}\right|$$

$$\leq |R_i^* \bmod Q_i| \exp\left(-\frac{\theta}{2}\log\left(P_i^{\frac{1}{2\theta}}\right)\sqrt{\log\log P_i}\right)$$

$$= |R_i^* \bmod Q_i| \exp\left(-\frac{1}{4}\log P_i\,\sqrt{\log\log P_i}\right).$$

Applying (1.41), we obtain

$$|E_{i,tail}| \leq |R_i^* \bmod Q_i| \exp\left(-\frac{1}{4}\log P_i \sqrt{\log\log P_i}\right),$$

which is the desired bound for $|E_{i,tail}|$, completing the proof of the lemma. □

Definition 1.6.5. Set $R_i' := R_i^* \setminus (E_{i,sup} \cup E_{i,GCD} \cup E_{i,tail})$.

Lemma 1.6.6. *Assume that θ, δ, and K satisfy $\theta + \delta(K+1) < \frac{1}{2}$. Then, as M tends to infinity, for all $r \in R_i'$ mod Q_i we have*

$$\log \prod_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} \left(1 - \frac{2X_q(r)}{q}\right) \sim -2 \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} \frac{X_q(r)}{q}. \tag{1.42}$$

Also, for all $r \in R_i'$ mod Q_i and all $q \in \mathcal{N}_{i+1}^*$ where $q \leq T_{i+1}$ we have

$$1 \geq \prod_{\substack{q' \in \mathcal{N}_{i+1}^* \\ q' \leq T_{i+1} \\ (q,q')>1}} \left(1 - \frac{2X_{q'}(r)}{q'}\right) \geq 1 - o(1), \tag{1.43}$$

where $o(1)$ does not depend on i, q or r.

Proof. We begin by proving the following.

Claim 1.6.7. *For $x \in \left(0, \frac{1}{2}\right)$, we have $-x > \log(1-x) > -x - x^2$.*

Proof of Claim. Let $f(x) = x + \log(1-x)$ where $x \in \left[0, \frac{1}{2}\right)$. Then,

$$f'(x) = 1 - \frac{1}{1-x} = \frac{-x}{1-x} < 0 \text{ for } x \in \left(0, \frac{1}{2}\right),$$

and $f(0) = 0$. Thus, $f(x)$ is decreasing on the interval $\left[0, \frac{1}{2}\right)$. Hence, $-x > \log(1-x)$ for $x \in \left(0, \frac{1}{2}\right)$.

Let $g(x) = x + x^2 + \log(1-x)$ where $x \in \left[0, \frac{1}{2}\right)$. Then

$$g'(x) = 1 + 2x - \frac{1}{1-x} = \frac{x(1-2x)}{1-x} > 0 \text{ for } x \in \left(0, \frac{1}{2}\right),$$

and $g(0) = 0$. Thus, $g(x)$ is increasing on the interval $\left[0, \frac{1}{2}\right)$. Therefore, we obtain $\log(1-x) > -x - x^2$ for $x \in \left(0, \frac{1}{2}\right)$. □

Let $r \in R_i'$, which implies $r \notin E_{i,sup}$. Then, for all $q \in \mathcal{N}_{i+1}^*$ we have $X_q(r) \leq q^\theta$. Therefore,

$$\frac{X_q(r)}{q} \leq \frac{q^\theta}{q} = \frac{1}{q^{1-\theta}} \leq \frac{1}{\left(\sqrt{\log M}\right)^{1-\theta}},$$

where the last inequality is true since $q \in \mathcal{N}_{i+1}^*$ implies $q \geq P_i \geq \sqrt{\log M}$. Recall $\theta < 1/2$. Thus, $\dfrac{X_q(r)}{q} < \dfrac{1}{4}$ for large enough M. We deduce that

$$0 < \frac{2X_q(r)}{q} < \frac{1}{2}. \tag{1.44}$$

As M tends to infinity, we have further

$$\frac{X_q(r)}{q} = o(1). \tag{1.45}$$

Claim 1.6.7 implies $\log(1-x) = -x(1+O(x))$ for $x \in \left(0, \frac{1}{2}\right)$. From (1.44), we deduce

$$\begin{aligned}
\log \prod_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} \left(1 - \frac{2X_q(r)}{q}\right) &= \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} \log\left(1 - \frac{2X_q(r)}{q}\right) \\
&= \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} \left(\frac{-2X_q(r)}{q}\left(1 + O\left(\frac{X_q(r)}{q}\right)\right)\right) \\
&= \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} \left(\frac{-2X_q(r)}{q}\left(1 + o(1)\right)\right),
\end{aligned}$$

where the last equality follows from (1.45). Therefore,

$$\log \prod_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} \left(1 - \frac{2X_q(r)}{q}\right) = -2 \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} \left(\frac{X_q(r)}{q}\left(1 + o(1)\right)\right), \tag{1.46}$$

and we have proven statement (1.42).

Fix $r \in R_i'$ and $q \in \mathcal{N}_{i+1}$ with $1 < q \leq T_{i+1}$. Then $r \notin E_{i,GCD}$ so that

$$\sum_{\substack{q' \in \mathcal{N}_{i+1} \\ (q,q')>1}} \frac{X_{q'}(r)}{q'} \leq P_i^{-1+\theta+(K+1)\delta}.$$

Hence,

$$-2\left(1+o(1)\right)\sum_{\substack{q'\in\mathcal{N}_{i+1}\\(q,q')>1}}\frac{X_{q'}(r)}{q'}\geq -2\left(1+o(1)\right)P_i^{-1+\theta+(K+1)\delta}. \tag{1.47}$$

Recall (1.44). The argument for (1.46) gives

$$\log\prod_{\substack{q'\in\mathcal{N}_{i+1}^*\\q'\leq T_{i+1}\\(q,q')>1}}\left(1-\frac{2X_q(r)}{q}\right)=-2\left(1+o(1)\right)\sum_{\substack{q'\in\mathcal{N}_{i+1}^*\\q'\leq T_{i+1}\\(q,q')>1}}\frac{X_{q'}(r)}{q'}.$$

Thus, (1.47) implies

$$\log\prod_{\substack{q'\in\mathcal{N}_{i+1}^*\\q'\leq T_{i+1}\\(q,q')>1}}\left(1-\frac{2X_q(r)}{q}\right)\geq -2\left(1+o(1)\right)P_i^{-1+\theta+(K+1)\delta}.$$

Since $\theta+(K+1)\,\delta<1/2$, we have $-1+\theta+(K+1)\,\delta<-1/2$. We use once again that $P_i\geq P_0\geq\sqrt{\log M}$. For M large, we deduce

$$\begin{aligned}\left|-2\left(1+o(1)\right)P_i^{-1+\theta+(K+1)\delta}\right|&\leq 2\left(1+o(1)\right)\left(\sqrt{\log M}\right)^{-1+\theta+(K+1)\delta}\\&\leq 4\left(\sqrt{\log M}\right)^{-1+\theta+(K+1)\delta}.\end{aligned}$$

As M goes to infinity, the right-hand side will go to zero. Thus,

$$0\geq\log\prod_{\substack{q'\in\mathcal{N}_{i+1}^*\\q'\leq T_{i+1}\\(q,q')>1}}\left(1-\frac{2X_q(r)}{q}\right)\geq o(1).$$

Exponentiating gives (1.43). □

Recall, $R_{i+1,r}=R_{i+1}\cap(r \bmod Q_i)$.

Lemma 1.6.8. *For any $i\geq 0$, let $r\in R_i \bmod Q_i$. Then,*

$$R_{i+1,r}=\bigcap_{q\in\mathcal{N}_{i+1}^*}A_{q,r}^c\cap\left(r \bmod Q_i\right).$$

Set $G_{i+1,r}=\{n \bmod Q_{i+1}: n\equiv r \pmod{Q_i}\}$. For $A\subseteq G_{i+1,r}$, define $P_r(A)=|A|/|G_{i+1,r}|$. Let $q\in\mathcal{N}_{i+1}^*$. Then $A_{q,r}\subseteq G_{i+1,r}$ is independent of any event

$$E_{q',B}=\{x \bmod Q_{i+1}: x\in B \text{ and } x\equiv r \pmod{Q_i}\}$$

with $\gcd(q, q') = 1$ *and with* B *a set of residue classes modulo* q'*. In particular,* $A_{q,r}$ *is independent of the sigma algebra generated by* $\left\{A_{q',r} : q' \in \mathcal{N}_{i+1}^*, \gcd(q, q') = 1\right\}$.

Proof. The set $A_{q,r}$ is everything in $r \bmod Q_i$ which is covered by some congruence modulo qq' where $q'|Q_i$. So, $\bigcup_{q\in\mathcal{N}_{i+1}^*} A_{q,r}$ is everything in $r \bmod Q_i$ which is covered by congruences in M_{i+1}. This means the elements in

$$\left(\bigcup_{q\in\mathcal{N}_{i+1}^*} A_{q,r}\right)^c = \bigcap_{q\in\mathcal{N}_{i+1}^*} A_{q,r}^c$$

and $G_{i+1,r}$ consist of everything in $G_{i+1,r}$ that is not covered by the new congruences in M_{i+1}. Thus,

$$R_{i+1,r} = \bigcap_{q\in\mathcal{N}_{i+1}^*} A_{q,r}^c \cap (r \bmod Q_i)\,.$$

We describe next a general setting where two events, that is two subsets of $G_{i+1,r}$, are independent. Let

$$\mathcal{A} = \{a_1, \ldots, a_k \bmod m_1\} \cap G_{i+1,r} \quad \text{and} \quad \mathcal{B} = \{b_1, \ldots, b_\ell \bmod m_2\} \cap G_{i+1,r}.$$

Suppose that $\gcd(m_1, m_2) = 1$ and that each of m_1 and m_2 divides Q_{i+1}/Q_i. The Chinese Remainder Theorem implies then that the set $\mathcal{A}$ consists of k residue classes modulo m_1Q_i, the set $\mathcal{B}$ consists of ℓ residue classes modulo m_2Q_i, and the set $\mathcal{A}\cap\mathcal{B}$ consists of $k\ell$ residue classes modulo $m_1m_2Q_i$. Observe that $|G_{i+1}, r| = Q_{i+1}/Q_i$. Hence,

$$\mathrm{P}_r(\mathcal{A}) = \frac{kQ_{i+1}/(m_1Q_i)}{Q_{i+1}/Q_i} = \frac{k}{m_1}, \quad \mathrm{P}_r(\mathcal{B}) = \frac{kQ_{i+1}/(m_2Q_i)}{Q_{i+1}/Q_i} = \frac{\ell}{m_2},$$

and

$$\mathrm{P}_r\Big(\mathcal{A}\cap\mathcal{B}\Big) = \frac{k\ell Q_{i+1}/(m_1m_2Q_i)}{Q_{i+1}/Q_i} = \frac{k\ell}{m_1m_2}.$$

Thus,

$$\mathrm{P}_r\left(\mathcal{A}\cap\mathcal{B}\right) = \frac{k\ell}{m_1m_2} = \mathrm{P}_r(\mathcal{A})\,\mathrm{P}_r(\mathcal{B}).$$

Thus, in this case, where $\gcd(m_1, m_2) = 1$ and each of m_1 and m_2 divides Q_{i+1}/Q_i, the sets $\mathcal{A}$ and $\mathcal{B}$ are independent events.

Since $A_{q,r}$ can be expressed in the form of $\mathcal{A}$ above with $m_1 = q$ and $E_{q',B}$ can be expressed in the form of $\mathcal{B}$ above with $m_2 = q'$, where $\gcd(q, q') = 1$ and each of q and q' divides Q_{i+1}/Q_i, we deduce that $A_{q,r}$ and $E_{q',B}$ represent two independent events in G_{i+1}, r.

In order to show $A_{q,r}$ is independent of the sigma algebra generated by the set $S = \left\{A_{q',r} : q' \in \mathcal{N}_{i+1}^*, \gcd(q, q') = 1\right\}$, we want to show that $A_{q,r}$ is independent of events formed by taking complements, unions, and intersections of elements of S. Let A and B are two subsets of S in $G_{i+1,r}$, with A a set of residue classes modulo q' and B a set of residue classes modulo q'', with $q' \in \mathcal{N}_{i+1}$, $q'' \in \mathcal{N}_{i+1}$ and $\gcd(q', q) = \gcd(q'', q) = 1$. Note, being in $G_{i+1,r}$, the elements of A and B are also r modulo Q_i. Then A^c is a set of residue classes modulo q', and the sets $A \cup B$ and $A \cap B$ are sets of residue classes modulo $\operatorname{lcm}(q', q'')$. Thus, every element of the sigma algebra generated by S in $G_{i+1,r}$ consists of a set of residue classes modulo some m with $\gcd(m, q) = 1$ and $m \in \mathcal{N}_{i+1}$. In other words, we can express an arbitrary element A of the sigma algebra generated by S in the form $\mathcal{A}$ above for some m_1 relatively prime to q and with m_1 dividing Q_{i+1}/Q_i. Since $A_{q,r}$ is of the form $\mathcal{B}$ above with $m_2 = q$ and q divides Q_{i+1}/Q_i, we deduce that $A_{q,r}$ and A are independent events in $G_{i+1,r}$, completing the proof. □

1.7 Proof of the Main Theorem

Let us recall the Main Theorem,

Theorem 1.7.1. *For all M that are larger than a fixed constant, we have for all $i \geq 0$,*

$$|R_i \ mod \ Q_i| \geq Q_i \exp\left(-(\log P_i)^2\right).$$

Furthermore, there exists a set $S_{i-1} \subset R_{i-1}$, determined modulo Q_{i-1}, such that S_{i-1} and $R_i^* := S_{i-1} \cap R_i$ satisfy the following properties.

1. *(Large size)*

$$|S_{i-1} \bmod Q_{i-1}| \geq Q_{i-1} \cdot \exp\left(-2\left(\log P_{i-1}\right)^2\right)$$

2. *(Large fibres)*

$$|R_i^* \bmod Q_i| \geq \frac{Q_i}{Q_{i-1}} \cdot |S_{i-1} \bmod Q_{i-1}| \cdot \exp\left(-\left(\log P_i\right)^2\right)$$

3. *(Uniform fibres)*

   $\forall r \in S_{i-1}$ *we have*

$$|R_{i,r} \bmod Q_i| \asymp \frac{|R_i^* \bmod Q_i|}{|S_{i-1} \bmod Q_{i-1}|},$$

   where for $A, B > 0, A \asymp B$ *means* $C_1 B < A < C_2 B$ *for constants* C_1 *and* C_2.

4. *(Uniformity within fibres)*

   $\forall r \in S_{i-1}$ *and all* $q \in \mathcal{N}_i^*$ *such that* $q \leq T_i$,

$$\max_{b \bmod q} \left\{|R_{i,r} \cap (b \bmod q) \bmod Q_i|\right\} \leq \frac{2}{q} |R_{i,r} \bmod Q_i|.$$

In particular, the first two items imply that R_i^* *satisfies*

$$|R_i^* \bmod Q_i| \geq \frac{Q_i}{\exp\left(\frac{3}{2}\left(\log P_i\right)^2\right)},$$

since M *is assumed to be sufficiently large.*

Proof. Let $r \in R_i'$ be fixed. Recall $G_{i+1,r} = \{n \bmod Q_{i+1} : n \equiv r \pmod{Q_i}\}$, and for $A \subseteq G_{i+1,r}$,

$$\mathrm{P}_r(A) = \frac{|A|}{|G_{i+1,r}|} = \frac{Q_i|A|}{Q_{i+1}}.$$

The set $A_{q,r}$ consists of $X_q(r)$ residue classes modulo qQ_i. These residue classes correspond to $X_q(r)Q_{i+1}/(qQ_i)$ residue classes modulo Q_{i+1} and, hence, in $G_{i+1,r}$. Thus, viewing $A_{q,r}$ as residue classes modulo Q_{i+1}, we have

$$\mathrm{P}_r\left(A_{q,r}\right) = \frac{X_q(r)Q_{i+1}/(qQ_i)}{Q_{i+1}/Q_i} = \frac{X_q(r)}{q}.$$

From Lemma 1.6.8 we have

$$R_{i+1,r} = \bigcap_{q \in \mathcal{N}_{i+1}^*} A_{q,r}^c \cap (r \bmod Q_i),$$

which is the set of residues that are r modulo Q_i not covered by any congruence involving moduli dividing Q_{i+1}. The total number of residue classes modulo Q_{i+1} that are r mod Q_i is $\frac{Q_{i+1}}{Q_i}$. Viewing the elements of $R_{i+1,r}$ as residue classes modulo Q_{i+1} that are r mod Q_i, we have $\mathrm{P}_r\left(R_{i+1,r}\right) = \dfrac{|R_{i+1,r}|}{Q_{i+1}/Q_i}$. Using the fact that for any sets A and B, $\mathrm{P}_r(A \cap B) \geq \mathrm{P}_r(A) - \mathrm{P}_r(B^c)$, we deduce

$$\begin{aligned}
\frac{Q_i|R_{i+1,r}|}{Q_{i+1}} &= \mathrm{P}_r(R_{i+1,r}) \\
&= \mathrm{P}_r\left(\bigcap_{q \in \mathcal{N}_{i+1}^*} A_{q,r}^c\right) \\
&= \mathrm{P}_r\left(\left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} A_{q,r}^c\right) \bigcap \left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q > T_{i+1}}} A_{q,r}^c\right)\right) \\
&\geq \mathrm{P}_r\left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} A_{q,r}^c\right) - \mathrm{P}_r\left(\left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q > T_{i+1}}} A_{q,r}^c\right)^c\right) \\
&= \mathrm{P}_r\left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} A_{q,r}^c\right) - \mathrm{P}_r\left(\bigcup_{\substack{q \in \mathcal{N}_{i+1}^* \\ q > T_{i+1}}} A_{q,r}\right) \\
&\geq \mathrm{P}_r\left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} A_{q,r}^c\right) - \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q > T_{i+1}}} \mathrm{P}_r(A_{q,r}) \\
&= \mathrm{P}_r\left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} A_{q,r}^c\right) - \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q > T_{i+1}}} \frac{X_q(r)}{q}.
\end{aligned}$$

Restricting to $r \in R_i'$, which implies $r \notin E_{i,tail}$, we apply Lemma 1.6.4 to obtain

$$\frac{Q_i|R_{i+1,r}|}{Q_{i+1}} \geq \mathrm{P}_r\left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} A_{q,r}^c\right) - \exp\left(-P_i^{(K-1)\delta}\right) P_i^{2e\delta+1}. \tag{1.48}$$

To bound the first term on the right-hand side of inequality (1.48) we use the Lovász Local Lemma. Let $\left\{A_{q,r} : q \in \mathcal{N}_{i+1}^*, q \leq T_{i+1}\right\}$ be the events. We create an

edge (q, q') between $A_{q,r}$ and $A_{q',r}$ if and only if $\gcd(q, q') > 1$. Let E be the set of edges. By Lemma 1.6.8, for all $q \in \mathcal{N}_{i+1}^*$, $q \leq T_{i+1}$, the event $A_{q,r}$ is independent of the sigma algebra generated by

$$\left\{A_{q',r} : q' \in \mathcal{N}_{i+1}^*, q' \leq T_{i+1}, \text{and } \gcd(q, q') = 1\right\} = \left\{A_{q',r} : q' \in \mathcal{N}_{i+1}^*, (q, q') \notin E\right\}.$$

Define $x_q = x_q(i, r) = 2X_q(r)/q$ to be the weights on the graph, for fixed r and i. Since $r \in R_i'$ implies $r \notin E_{i,sup}$, we have $X_q(r) \leq q^\theta$. And, since $\theta < 1/2$, and since $q \in \mathcal{N}_{i+1}^*$ implies for M sufficiently large $q \geq P_i \geq P_0 = \sqrt{\log M} \geq 16$, we have

$$0 \leq x_q \leq \frac{2q^\theta}{q} \leq \frac{2q^{1/2}}{q} = \frac{2}{\sqrt{q}} \leq \frac{1}{2}.$$

Hence, the weights of our graph satisfy the conditions of the Lovász Local Lemma. Furthermore,

$$\begin{aligned} x_q \cdot \prod_{\substack{q' \in \mathcal{N}_{i+1}^* \\ q' \leq T_{i+1} \\ (q,q') \in E}} (1 - x_{q'}) &= \frac{2X_q(r)}{q} \cdot \prod_{\substack{q' \in \mathcal{N}_{i+1}^* \\ q' \leq T_{i+1} \\ (q,q') \in E}} \left(1 - \frac{2X_{q'}(r)}{q'}\right) \\ &= \frac{2X_q(r)}{q}\left(1 - o(1)\right), \end{aligned}$$

where the last equation holds by (1.43) from Lemma 1.6.6. Recall $\mathrm{P}_r(A_{q,r}) = X_q(r)/q$. We obtain

$$x_q \prod_{\substack{q' \in \mathcal{N}_{i+1}^* \\ q' \leq T_{i+1} \\ (q,q') \in E}} (1 - x_{q'}) = 2\mathrm{P}_r(A_{q,r})\left(1 - o(1)\right) \geq \left(2 - o(1)\right)\mathrm{P}_r(A_{q,r}).$$

Hence, for M sufficiently large, we have

$$P_r(A_{q,r}) \leq x_q \cdot \prod_{\substack{q' \in \mathcal{N}_{i+1}^* \\ q' \leq T_{i+1} \\ (q,q') \in E}} (1 - x_{q'}).$$

Thus, the conditions of the Lovász Local Lemma are satisfied. Therefore, we have

$$\mathrm{P}_r\left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} A_{q,r}^c\right) \geq \prod_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \leq T_{i+1}}} (1 - x_q).$$

From (1.42) of Lemma 1.6.6, for M large, we have

$$\log \prod_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} (1-x_q) = \log \prod_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \left(1-\frac{2X_q(r)}{q}\right) \ge -4 \sum_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \frac{X_q(r)}{q}.$$

Therefore,

$$\mathrm{P}_r\left(\bigcap_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} A^c_{q,r}\right) \ge \prod_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} (1-x_q) \ge \exp\left(-4 \sum_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \frac{X_q(r)}{q}\right). \tag{1.49}$$

Note, this inequality holds true for a fixed $r \in R'_i$. Furthermore, Lemma 1.6.4 gave that each of $|E_{i,sup}|$, $|E_{i,GCD}|$ and $|E_{i,tail}|$ is $|R^*_i \bmod Q_i| \cdot o(1)$. Hence, $|R'_i \bmod Q_i| = |R^*_i \bmod Q_i|\,(1-o(1))$. This gives us

$$\begin{aligned}
\frac{1}{|R^*_i \bmod Q_i|} \sum_{r\in R^*_i \bmod Q_i} \sum_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \frac{X_q(r)}{q} &= \frac{1-o(1)}{|R'_i \bmod Q_i|} \sum_{r\in R^*_i \bmod Q_i} \sum_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \frac{X_q(r)}{q} \\
&\ge \frac{1-o(1)}{|R'_i \bmod Q_i|} \sum_{r\in R'_i \bmod Q_i} \sum_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \frac{X_q(r)}{q} \\
&\ge \frac{1/2}{|R'_i \bmod Q_i|} \sum_{r\in R'_i \bmod Q_i} \sum_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \frac{X_q(r)}{q}.
\end{aligned}$$

for M large. On the other hand, Lemma 1.6.1 gives us

$$\frac{1}{|R^*_i \bmod Q_i|} \sum_{r\in R^*_i \bmod Q_i} \sum_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \frac{X_q(r)}{q} \le C^3 \log P_{i+1} \exp\left(\left(2\log P_{i+1}\right)^2\right) \log P_i.$$

Therefore,

$$\frac{1}{|R'_i \bmod Q_i|} \sum_{r\in R'_i \bmod Q_i} \sum_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \frac{X_q(r)}{q} \le 2C^3 \log P_{i+1} \exp\left(\left(2\log P_{i+1}\right)^2\right) \log P_i. \tag{1.50}$$

Let $R''_i \subseteq R'_i$ be the subset of $r \in R'_i$ for which

$$\sum_{\substack{q\in\mathcal{N}^*_{i+1}\\ q\le T_{i+1}}} \frac{X_q(r)}{q} \le 4C^3 \log P_{i+1} \exp\left(\left(2\log P_{i-1}\right)^2\right) (\log P_i).$$

Define $R_i^{'''} = R_i'/R_i^{''}$. Notice

$$\begin{aligned}
&\frac{1}{|R_i' \bmod Q_i|} \sum_{r \in R_i' \bmod Q_i} \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \le T_{i+1}}} \frac{X_q(r)}{q} \\
&\qquad \ge \frac{1}{|R_i' \bmod Q_i|} \sum_{r \in R_i^{'''} \bmod Q_i} \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \le T_{i+1}}} \frac{X_q(r)}{q} \\
&\qquad \ge \frac{|R_i^{'''} \bmod Q_i|}{|R_i' \bmod Q_i|} \left(4C^3 \log P_{i+1} \exp\left((2\log P_{i-1})^2\right) (\log P_i)\right).
\end{aligned}$$

From (1.50), we deduce

$$\begin{aligned}
&2C^3 \log P_{i+1} \exp\left((2\log P_{i+1})^2\right) \log P_i \\
&\qquad \ge \frac{|R_i^{'''} \bmod Q_i|}{|R_i' \bmod Q_i|} \left(4C^3 \log P_{i+1} \exp\left((2\log P_{i-1})^2\right) (\log P_i)\right).
\end{aligned}$$

Hence,

$$\frac{|R_i^{'''} \bmod Q_i|}{|R_i' \bmod Q_i|} \le \frac{1}{2}.$$

We use (1.49). For $r \in R_i^{''} \subseteq R_i'$, we have

$$\begin{aligned}
\mathrm{P}_r \left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \le T_{i+1}}} A_{q,r}^c \right) &\ge \exp\left(-4 \sum_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \le T_{i+1}}} \frac{X_q(r)}{q} \right) \\
&\ge \exp\left(-4 \cdot 4C^3 \log P_{i+1} \exp\left((2\log P_{i-1})^2\right) (\log P_i)\right).
\end{aligned} \tag{1.51}$$

Since $\log P_i = P_{i-1}^{\delta}$, we have with M large that

$$\exp\left((2\log P_{i-1})^2\right) \le \exp\left((\delta/2)\, P_{i-1}^{\delta}\right) = \exp\left((\delta/2) \log P_i\right) = P_i^{\delta/2}.$$

Using $\log P_{i+1} = P_i^{\delta}$ and (1.51), we obtain

$$\mathrm{P}_r \left(\bigcap_{\substack{q \in \mathcal{N}_{i+1}^* \\ q \le T_{i+1}}} A_{q,r}^c \right) \ge \exp\left(-16C^3 P_i^{\delta} P_i^{\delta/2} (\log P_i)\right) = \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right). \tag{1.52}$$

Recall, $K > 3$, so $P_i^{(K-1)\delta} = P_i^{2\delta+\epsilon}$ for some $\epsilon > 0$. Let $\hat{c}$ be an arbitrary constant. Then

$$\frac{\log \hat{c}}{P_i^{(3/2)\delta}} + \frac{(2e\delta+1)\log P_i}{P_i^{(3/2)\delta}} + 16C^3 \log P_i \leq P_i^{(1/2)\delta+\epsilon}, \tag{1.53}$$

since each term on the left-hand side is bounded by $(1/3)\, P_i^{(1/2)\delta}$. Multiplying both sides of (1.53) by $P_i^{(3/2)\delta}$ gives

$$\log \hat{c} + (2e\delta+1)\log P_i + 16C^3 P_i^{(3/2)\delta} \log P_i \leq P_i^{2\delta+\epsilon} = P_i^{(K-1)\delta}$$

or, equivalently,

$$\log \hat{c} + (2e\delta+1)\log P_i - P_i^{(K-1)\delta} \leq -16C^3 P_i^{(3/2)\delta} \log P_i.$$

This implies

$$\hat{c} P_i^{2e\delta+1} \exp\left(-P_i^{(K-1)\delta}\right) \leq \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right).$$

From (1.52),

$$\mathrm{P}_r\left(\bigcap_{\substack{q\in\mathcal{N}_{i+1}^* \\ q\leq T_{i+1}}} A_{q,r}^c\right) \geq \hat{c} P_i^{2e\delta+1} \exp\left(-P_i^{(K-1)\delta}\right) \tag{1.54}$$

Applying (1.48), (1.54), and (1.52), in that order, we have

$$\begin{aligned}
\frac{Q_i |R_{i+1,r}|}{Q_{i+1}} &\geq \mathrm{P}_r\left(\bigcap_{\substack{q\in\mathcal{N}_{i+1}^* \\ q\leq T_{i+1}}} A_{q,r}^c\right) - \exp\left(-P_i^{(K-1)\delta}\right) P_i^{2e\delta+1} \\
&\geq \left(1 - \frac{1}{\hat{c}}\right) \mathrm{P}_r\left(\bigcap_{\substack{q\in\mathcal{N}_{i+1}^* \\ q\leq T_{i+1}}} A_{q,r}^c\right) \\
&\geq \left(1 - \frac{1}{\hat{c}}\right) \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right)
\end{aligned} \tag{1.55}$$

Recall $r \in R_i'$ gives us

$$|R_i^* \bmod Q_i| = (1 + o(1))\, |R_i' \bmod Q_i|$$

$$\leq (2+o(2))\,|R_i^{''} \bmod Q_i|$$

$$= (2+o(1))\,|R_i^{''} \bmod Q_i|.$$

From the inductive hypothesis we have $|R_i^* \bmod Q_i| \geq \dfrac{Q_i}{\exp\left(3/2\,(\log P_i)^2\right)}$. Therefore, for M large,

$$|R_i^{''} \bmod Q_i| \geq \frac{|R_i^* \bmod Q_i|}{(2+o(1))} \geq \frac{Q_i}{3\exp\left(3/2\,(\log P_i)^2\right)}. \tag{1.56}$$

With (1.55) and (1.56) we obtain

$$\begin{aligned}
|R_{i+1} \bmod Q_{i+1}| &\geq \sum_{r\in R_i^{''} \bmod Q_i} |R_{i+1,r}| \\
&\geq |R_i^{''} \bmod Q_i| \cdot \max_{r\in R_i^{''} \bmod Q_i} \{|R_{i+1,r}|\} \\
&\geq |R_i^{''} \bmod Q_i| \frac{Q_{i+1}}{Q_i}\left(1-\frac{1}{\hat{c}}\right)\exp\left(-16C^3P_i^{(3/2)\delta}\log P_i\right) \\
&\geq \frac{Q_{i+1}\left(1-\frac{1}{\hat{c}}\right)}{3\exp\left((3/2)\,(\log P_i)^2\right)}\exp\left(-16C^3P_i^{(3/2)\delta}\log P_i\right) \\
&\geq Q_{i+1}\frac{\exp\left(-16C^3P_i^{(3/2)\delta}\log P_i\right)}{6\cdot\exp\left((3/2)\,(\log P_i)^2\right)},
\end{aligned}$$

where the last inequality holds by taking $\hat{c} \geq 2$. Notice, if we had summed over $r \in R_i$ we would have equality in the first line, but since we are restricting to $r \in R_i^{''}$ we get an inequality. Observe

$$\frac{\exp\left(-16C^3P_i^{(3/2)\delta}\log P_i\right)}{6\cdot\exp\left((3/2)\,(\log P_i)^2\right)} \geq \exp\left(-P_i^{2\delta}\right) = \exp\left(-\left(\log P_{i+1}\right)^2\right). \tag{1.57}$$

Hence,

$$|R_{i+1} \bmod Q_{i+1}| \geq Q_{i+1}\exp\left(-\left(\log\left(P_{i+1}\right)^2\right)\right),$$

which proves the first part of the theorem.

To prove statement (1) of the theorem, we let $j \geq 0$ and consider $r \in R_i''$ mod Q_i for which

$$\begin{aligned} 2^j \left[\left(1 - \frac{1}{\hat{c}}\right) \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right) \right] & \\ \leq \frac{Q_i |R_{i+1,r}|}{Q_{i+1}} & \\ \leq 2^{j+1} \left[\left(1 - \frac{1}{\hat{c}}\right) \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right) \right]. & \end{aligned} \tag{1.58}$$

When $j = 0$ the left-hand side of this inequality is the last expression in (1.55). Thus,

$$2^0 \left[\left(1 - \frac{1}{\hat{c}}\right) \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right) \right] \leq \frac{Q_i |R_{i+1,r}|}{Q_{i+1}}.$$

Since $R_{i+1,r} \subseteq G_{i+1,r}$, we have $|R_{i+1,r}| \leq |G_{i+1,r}| = \dfrac{Q_{i+1}}{Q_i}$. Thus, $\dfrac{Q_i |R_{i+1,r}|}{Q_{i+1}} \leq 1$. Let $k \in \mathbb{Z}$ be maximal such that

$$2^k \left[\left(1 - \frac{1}{\hat{c}}\right) \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right) \right] < 1. \tag{1.59}$$

So

$$\frac{Q_i |R_{i+1,r}|}{Q_{i+1}} < 1 \leq 2^{k+1} \left[\left(1 - \frac{1}{\hat{c}}\right) \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right) \right].$$

Therefore, every $r \in R_i''$ mod Q_i satisfies (1.58) for some $j \in \{0, \ldots, k\}$. By the pigeonhole principle, there is a $0 \leq j \leq k$ such that the number of $r \in R_i''$ mod Q_i satisfying (1.58) is at least $\dfrac{|R_i'' \bmod Q_i|}{k+1}$. Pick such a j, and let S_i denote the set of $r \in R_i''$ mod Q_i that satisfy (1.58). Thus,

$$|S_i \bmod Q_i| \geq \frac{|R_i'' \bmod Q_i|}{k+1}.$$

The above holds for any $\hat{c} > 1$. We choose $\hat{c} = 2$. From (1.59) we obtain

$$2^{k-1} = 2^k \left(1 - \frac{1}{\hat{c}}\right) < \frac{1}{\exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right)} = \exp\left(16C^3 P_i^{(3/2)\delta} \log P_i\right),$$

which implies

$$k - 1 < \frac{16C^3 P_i^{(3/2)\delta} \log P_i}{\log 2},$$

and hence

$$k+1 \ll P_i^{(3/2)\delta} \log P_i.$$

From (1.56) we deduce

$$|S_i \bmod Q_i| \geq \frac{Q_i}{c'' \cdot \exp\left((3/2)\left(\log P_i\right)^2\right)\left(P_i^{(3/2)\delta} \log P_i\right)},$$

for some constant $c'' > 0$. Applying the fact that $P_i^{(3/2)\delta} = \exp\left((3/2)\,\delta \log P_i\right)$ and $\log P_i = \exp\left(\log\log P_i\right)$, to the observation that

$$c'' \cdot \exp\left((3/2)\,\delta \log P_i\right) \exp\left(\log\log P_i\right) \leq \exp\left((1/2)\left(\log P_i\right)^2\right),$$

gives us

$$|S_i \bmod Q_i| \geq \frac{Q_i}{\exp\left((3/2)\left(\log P_i\right)^2\right)\exp\left((1/2)\left(\log P_i\right)^2\right)} = \frac{Q_i}{\exp\left(2\left(\log P_i\right)^2\right)}.$$

Therefore, statement (1) holds with i replaced by $i+1$.

Now to prove statement (2) we choose $\hat{c} = 3$ in equation (1.55). With $r \in S_i \subseteq R_i^{''}$, we have

$$\frac{Q_i |R_{i+1,r}|}{Q_{i+1}} \geq \frac{2}{3} \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right).$$

Applying

$$\exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right) \geq \exp\left(-\left(\frac{3}{2}\left(\log P_i\right)^2\right)\right) \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right)$$

and (1.57), we obtain

$$\begin{aligned} \frac{Q_i |R_{i+1,r}|}{Q_{i+1}} &\geq \frac{2}{3} \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right) \\ &\geq \frac{1}{6} \exp\left(-\left(\frac{3}{2}\left(\log P_i\right)^2\right)\right) \exp\left(-16C^3 P_i^{(3/2)\delta} \log P_i\right) \qquad (1.60) \\ &\geq \exp\left(-\left(\log P_{i+1}\right)^2\right). \end{aligned}$$

We then have

$$|R_{i+1} \cap S_i \bmod Q_{i+1}| = \sum_{r \in S_i \bmod Q_i} |R_{i+1,r}|$$

$$= |S_i \bmod Q_i| \cdot \max_{r \in S_i \bmod Q_i} \{|R_{i+1,r}|\}$$

$$\geq \frac{Q_{i+1}}{Q_i} \exp\left(-(\log P_{i+1})^2\right) |S_i \bmod Q_i|.$$

And, since $R_{i+1} \cap S_i = R^*_{i+1}$, we have

$$|R^*_{i+1} \bmod Q_{i+1}| \geq \frac{Q_{i+1}}{Q_i} \exp\left(-(\log P_{i+1})^2\right) |S_i \bmod Q_i|,$$

which proves statement (2) with i replaced by $i+1$.

Fix $r' \in S_i$. Using (1.58), where j is fixed and r varies, we know that the size of $R_{i+1,r}$ and the size of $R_{i+1,r'}$ differ by at most a factor of 2. This implies the two inequalities

$$|R^*_{i+1} \bmod Q_{i+1}| = \sum_{r \in S_i \bmod Q_i} |R_{i+1,r}|$$

$$\leq \sum_{r \in S_i \bmod Q_i} 2|R_{i+1,r'}|$$

$$= 2|R_{i+1,r'}||S_i \bmod Q_i|$$

and

$$|R^*_{i+1} \bmod Q_{i+1}| = \sum_{r \in S_i \bmod Q_i} |R_{i+1,r}|$$

$$\geq \sum_{r \in S_i \bmod Q_i} \frac{1}{2}|R_{i+1,r'}|$$

$$= \frac{1}{2}|R_{i+1,r'}||S_i \bmod Q_i|.$$

Hence, we have

$$\frac{1}{2}|R_{i+1,r'}| \leq \frac{|R^*_{i+1} \bmod Q_{i+1}|}{|S_i \bmod Q_i|} \leq 2|R_{i+1,r'}|,$$

which proves statement (3).

To prove statement (4), we let $r \in S_i$ and $q \in \mathcal{N}^*_{i+1}$ with $q \leq T_{i+1}$. Let $(b \bmod q)$ maximize $|R_{i+1,r} \cap (b \bmod q) \bmod Q_{i+1}|$. Recall

$$E_{q,B} = \{x \bmod Q_{i+1} : x \in B \bmod q \text{ and } x \equiv r \pmod{Q_i}\}.$$

So

$$E_{q,b} = \{x \bmod Q_{i+1} : x \equiv b \bmod q \text{ and } x \equiv r \pmod{Q_i}\}.$$

Then $|E_{q,b}| = Q_{i+1}/(qQ_i)$ so that

$$P_r\big(E_{q,b}\big) = \frac{Q_{i+1}/(qQ_i)}{Q_{i+1}/Q_i} = \frac{1}{q}.$$

Hence,

$$\begin{aligned} |R_{i+1,r} \cap (b \bmod q) \bmod Q_{i+1}| &= |R_{i+1,r} \cap E_{q,b} \bmod Q_{i+1}| \\ &= \frac{Q_{i+1}}{Q_i} \, \mathrm{P}_r \left(R_{i+1,r} \cap E_{q,b}\right). \end{aligned}$$

Let $p_{max} = \mathrm{P}_r \left(R_{i+1,r} \cap E_{q,b}\right)$. From Lemma 1.6.8, we have that

$$R_{i+1,r} = \bigcap_{q \in \mathcal{N}_{i+1}^*} A_{q,r}^c \cap (r \bmod Q_i)$$

and that $E_{q,b}$ is independent of the sigma algebra generated by the set

$$\left\{A_{q',r} : q' \in \mathcal{N}_{i+1}^* \text{ and } \gcd(q,q') = 1\right\}.$$

We deduce

$$\begin{aligned} p_{max} &= \mathrm{P}_r \left(R_{i+1,r} \cap E_{q,b}\right) \\ &= \mathrm{P}_r \left(E_{q,b} \cap \bigcap_{q' \in \mathcal{N}_{i+1}^*} A_{q',r}^c \right) \\ &\leq \mathrm{P}_r \left(E_{q,b} \cap \bigcap_{\substack{q' \in \mathcal{N}_{i+1}^* \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A_{q',r}^c \right) \\ &= \mathrm{P}_r \left(E_{q,b}\right) \, \mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}_{i+1}^* \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A_{q',r}^c \right). \end{aligned}$$

Thus,

$$p_{max} \leq \frac{1}{q} \, \mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A^c_{q',r} \right) \tag{1.61}$$

In the first part of the proof, we showed that the Lovász Local Lemma applies with $x_q = X_q(r)/q$. Recall that the Lovász Local Lemma states

$$\mathrm{P}\left(\bigcap_{i=1}^{n} A_i^c \right) \geq \mathrm{P}\left(\bigcap_{i=1}^{m} A_i^c \right) \prod_{j=m+1}^{n} (1 - x_j),$$

which gives us

$$\begin{aligned}
\mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1}}} A^c_{q',r} \right) &\geq \mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A^c_{q',r} \right) \prod_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')>1}} (1 - x_{q'}) \\
&= \mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A^c_{q',r} \right) \prod_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')>1}} \left(1 - \frac{2X_{q'}(r)}{q'} \right) \\
&= \mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A^c_{q',r} \right) (1 + o(1)) \,,
\end{aligned}$$

where the last equation holds by applying Lemma 1.6.6. Thus,

$$\mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A^c_{q',r} \right) \geq \mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1}}} A^c_{q',r} \right) \geq \mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A^c_{q',r} \right) (1 + o(1)),$$

which implies

$$\mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A^c_{q',r} \right) = \mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1}}} A^c_{q',r} \right) (1 + o(1)).$$

From (1.61) and (1.55), we have

$$
\begin{aligned}
p_{max} &\leq \frac{1}{q}\ \mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1} \\ \gcd(q,q')=1}} A^c_{q',r} \right) \\
&= \frac{1}{q}\,(1+o(1))\,\mathrm{P}_r \left(\bigcap_{\substack{q' \in \mathcal{N}^*_{i+1} \\ q' \leq T_{i+1}}} A^c_{q',r} \right) \\
&\leq \frac{1}{q}\,(1+o(1))\,\frac{\mathrm{P}_r\left(R_{i+1,r}\right)}{\left(1-\frac{1}{\hat{c}}\right)} \\
&= \frac{(1+o(1))\,\hat{c}}{(\hat{c}-1)} \cdot \frac{\mathrm{P}_r\left(R_{i+1,r}\right)}{q}.
\end{aligned}
$$

Choosing $\hat{c}$ and M sufficiently large gives

$$
\frac{Q_{i+1}}{Q_i}\,p_{max} \leq \frac{Q_{i+1}}{Q_i}\,\frac{2}{q}\,\mathrm{P}_r\left(R_{i+1,r}\right) = \frac{2}{q}\,|R_{i+1,r} \bmod Q_{i+1}|.
$$

Hence, for $|R_{i+1,r} \cap (b \bmod q) \bmod Q_{i+1}|$ maximized by $(b \bmod q)$, we have

$$
|R_{i+1,r} \cap (b \bmod q) \bmod Q_{i+1}| = \frac{Q_{i+1}}{Q_i} \cdot p_{max} \leq \frac{2}{q}\,|R_{i+1,r} \bmod Q_{i+1}|,
$$

which proves statement (4) of the theorem. □

Bibliography

[1] Bob Hough, *The minimum modulus of a covering system,* arXiv:1307.0874, 2013.