[1].

THE THEORY OF RAMIFICATION

THEOPHILUS AGAMA

ABSTRACT. In this paper we introduce and develop the concept of ramification in a given moduli. We study some properties in relation to this concept and it's connection to some important problems in mathematics, particularly the Goldbach conjecture.

1. Introduction and concept

Definition 1.1. Let $n \geq 2$ be an integer and $n \equiv a_1 \pmod{m}$. Then n is said to ramify in $\pmod{m}$ if there exist some $r < m$ with $n \equiv a_2 \pmod{r}$ so that $a_1 + a_2 = m$. We say the modulus m admits a ramifier and we denote the ramifier by $\mathcal{R}(m) = n$.

Remark 1.2. Definition 1.1 has a practical implication. The concept affirms the notion that, given the image of an object on a miror of a certain size, If we can find a miror of a relatively smaller size that produce an image of the same body so that the concatenation of the two covers the size of the larger miror, then the body must indeed be a ramifier. Next we examine some properties of the ramifiers in a given modulus.

2. Properties of the ramifiers

In this section we study some properties of the ramifiers in a fixed modulus. We also count the number of ramifiers in all modulus. We first give a proof that indicates that there must exist a ramifier in any given modulus. The method of proof employs in an ingenious way an infinite descending argument whose consequence is not suitable for that particular regime.

Proposition 2.1. *There exist a ramifier in any given modulus. In particular, for any $m \geq 2$, there exists a ramifier in $\pmod{t}$ for $1 < t \leq m$.*

Proof. Suppose on the contrary that for all $m \geq 2$, then the modulus do not admit a ramifier for $1 < t \leq m$. Then it follows by definition 1.1 that there exist some

[1]

Date: April 10, 2019.
2000 *Mathematics Subject Classification.* Primary 54C40, 14E20; Secondary 46E25, 20C20.
Key words and phrases. Ramification, index, centre.

sequence of positive integers $2 = s_1 < s_2 < \ldots < s_k = m$ such that for all m with $n \equiv a_1 \pmod{m}$

$$m \neq a_1 + r_i$$

where $n \pmod{s_i} = r_i$ for $i = 1, \ldots k-1$. Again there exist some $1 < r_j \leq r_{k-1}$ such that $a_1 + r_j < m$ if and only if $r_j < m - a_1 < m$. Now choose $t_k = m - a_1 < m$, then by assumption it follows that for $n \equiv a_2 \pmod{t_k}$ so that there exist a sequence of positive integers $t_k > v_{k-1} > v_{k-2} > \cdots v_1 > 1$ such that $a_2 + u_i \neq t_k$ for all $i = 1, 2 \ldots k-1$, where $n \pmod{v_i} = u_i$. It follows that there exist some $1 < u_j \leq u_{k-1}$ so that $a_2 + u_j < t_k$ if and only if $u_j < t_k - a_2 < t_k$. By choosing $t_k - a_2 = t_{k-1} < t_k < m$ and using the fact that each $1 < t \leq m$ admits no ramifier, we obtain by induction an infinite descending sequence of positive integers

$$m > t_k > t_{k-1} > t_{k-2} > \cdots > t_{k-i} > \cdots.$$

This proves the proposition. □

Remark 2.1. The next result highlights a sufficient condition for any positive integer to ramify in a given modulus.

Proposition 2.2. *Let $m \geq 2$. Then $\mathcal{R}(m) = n$ if and only if $\mathcal{R}(m) \not\equiv 0 \pmod{m}$.*

Proof. Let $m \geq 2$ and let $\mathcal{R}(m) = n$. Suppose on the contrary that $\mathcal{R}(m) \equiv 0 \pmod{m}$, then it follows that for the sequence $m = r_k > r_{k-1} > \ldots > r_1 > 1$, where $\mathcal{R}(m) \pmod{r_i} = s_i$ with $i = 1, 2, \ldots k-1$, it must certainly be that $s_i + 0 < m$. This contradicts the fact that m admits a ramifier. Conversely, if $\mathcal{R}(m) \equiv 0 \pmod{m}$, then it follows that $\mathcal{R}(m) \neq n$. This completes the proof of the proposition. □

Proposition 2.2, though simple, is somewhat revealing. It enables us to controll at the very least the number of ramifiers for a finite set of integers in a given modulus. That is to say, for any set of the form $\{n \leq x : \mathcal{R}(m) = n\}$, then

$$\begin{aligned}\#\{n \leq x : \mathcal{R}(m) = n\} &= \sum_{\substack{n \leq x \\ \mathcal{R}(m)=n}} 1 \\ &\leq x - \left\lfloor \frac{x}{m} \right\rfloor \\ &= \left(1 - \frac{1}{m}\right)x + O(1).\end{aligned}$$

It follows from this upper bound that the distribution of ramifiers in any finite set of the integers depends greatly on the modulus of ramification. It is clear that the smaller the modulus, the less chance there is to find a ramifier in the set. Conversely, the larger the modulus the high chance there is in picking a ramifier in the set in any random selection. This upper bound, though very weak could serve as a benchmark, for an appeal to Proposition 2.2 indicates that we can do better than this if we knew other subtle properties of the ramifiers in any finite set of the integers. The sequel will be focused on studying such properties.

Theorem 2.2. *Let p be a prime and let $(a,p) = 1$. If a is a quadratic residue modulo p, then the set $\mathcal{M} := \{a, a^2, \ldots, a^{p-1}\}$ contains at least two non-ramifiers modulo p.*

Proof. Let p be a prime and $(a,p) = 1$. It follows that $a^{p-1} \equiv 1 \pmod{p}$. It follows immediately that $\mathcal{R}(p) \neq a^{p-1}$. If we assume that a is a quadratic residue modulo p, then it follows that

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

and it follows that $\mathcal{R}(p) \neq a^{\frac{p-1}{2}}$, thereby ending the proof. □

Remark 2.3. In light of Theorem 2.2, we can certainly improve on the upper bound in the foregone discussion concerning the scale of ramifiers in a given modulus.

Theorem 2.4. *Let m be fixed and let $\mathcal{I} := \{n \leq x : \mathcal{R}(m) = n\}$, then*

$$\#\mathcal{I} \leq \left(1 - \frac{1}{m}\right)x - \frac{\log x}{\log m} + O(1).$$

Proof. In the forgone discussion, the number of ramifiers that led to the upper bound are integers $n \leq x$ satisfying $n \equiv 0 \pmod{m}$. Let $\mathcal{I} := \{n \leq x : \mathcal{R}(m) = n\}$ be the set of ramifiers in modulo m. Then by Theorem 2.2, it follows that the upper bound can slightly be improved to

$$\begin{aligned}\#\mathcal{I} &\leq \left(1 - \frac{1}{m}\right)x - \sum_{\substack{a \leq x \\ a^k \leq x \\ a^k \equiv 1 \pmod{m} \\ (a,m)=1}} 1 + O(1) \\ &= \left(1 - \frac{1}{m}\right)x - \sum_{\substack{a \leq x \\ (a,m)=1}} \sum_{\substack{a^k \equiv 1 \pmod{m} \\ 1 \leq k \leq \lfloor \frac{\log x}{\log a} \rfloor}} 1 + O(1),\end{aligned}$$

and the result follows by taking $a = m + 1$ in the sum. □

Remark 2.5. In the spirit of understanding the Goldbach conjecture we launch a very strict form of the notion of Ramifiers. The Goldbach conjecture can be formulated in this language. It comes in the following sequel.

Definition 2.6. Let $n \geq 2$ be an integer and $n \equiv p_1 \pmod{m}$. Then n is said to ramify strongly in $\pmod{m}$ if there exist some $r < m$ such that $n \equiv p_2 \pmod{r}$, such that $p_1 + p_2 = m$ where p_1, p_2 are all prime. In other words, we say the modulus m admits a strong ramifier.

Conjecture 2.1 (Goldbach). Every even number $n \geq 6$ admits a strong ramifier in $\pmod{n}$.

Theorem 2.7. *There are infinitely many ramifiers in $\pmod{m}$ for some fixed m.*

Proof. It suffices to obtain a lower bound for the quantity $\#\{n \leq x : \mathcal{R}(m) = n\}$. Thus it follows that

$$\begin{aligned}
\#\{n \leq x : \mathcal{R}(m) = n\} &= \sum_{\substack{n \leq x \\ \mathcal{R}(m)=n}} 1 \\
&= \sum_{\substack{n \leq x \\ a_0+b_0=m \\ n \equiv a_0 \pmod{m} \\ n \equiv b_0 \pmod{r_0} \\ r_0<m}} 1 \\
&= \sum_{\substack{n \leq x \\ a_0+b_0=m \\ mr_0|(n-a_0)(n-b_0) \\ r_0<m}} 1 \\
&= \sum_{\substack{n \leq x \\ a_0+b_0=m \\ r_0<m}} \sum_{mr_0|(n-a_0)(n-b_0)} 1 \\
&= \sum_{\substack{a_0+b_0=m \\ r_0<m}} \left\lfloor \frac{(x-a_0)(x-b_0)}{mr_0} \right\rfloor \\
&= \sum_{\substack{a_0+b_0=m \\ r_0<m}} \frac{x^2 - x(a_0+b_0) + a_0b_0}{mr_0} + O_m(1) \\
&\geq \frac{x^2 - xm}{m^2} + O_m(1)
\end{aligned}$$

and the result follows immediately from this estimate. □

The above lower bound for the number of ramifiers in a fixed modulus is somewhat instructive. It puts a threshold on the size of the modulus that cannot admit a ramifier from a finite set of the integers $n \leq x$. Indeed for this lower bound to fail, then it follows that the inequality must be satisfied

$$\frac{x^2 - xm}{m^2} + O_m(1) > x\left(1 - \frac{1}{m}\right) - \frac{\log x}{\log m} + O(1).$$

Using the main term, it follows that

$$m < \frac{x}{\sqrt{x - \log x}}.$$

Thus, the moduli for which the lower bound majorizes the upper bound for the number of ramifiers in a finite set gives the largest scale of a modulus that do not admit a ramifier. It follows that size of any modulus that admits a ramifier in any finite set of the integers $n \leq x$ must satisfy the inequality

$$m \geq \left\lfloor \frac{x}{\sqrt{x - \log x}} \right\rfloor + 1.$$

We examine some immediate consequences of this analysis in relation to the distribution of prime numbers in small intervals. In fact, it is redolent of Bertrand's postulate.

Theorem 2.8. *Let $p \leq x$ be a prime and suppose p admits a ramifier n for some $n \leq x$. Then there must exist at least one prime in the interval*

$$\bigg(\frac{x}{\sqrt{x-\log x}}, x\bigg].$$

Proof. Suppose $p \leq x$ is a prime and that $\mathcal{R}(p)=n$ for some $n \leq x$. Then it follows from our forgone discussion and Theorem 2.7 that

$$p \geq \bigg\lfloor \frac{x}{\sqrt{x-\log x}}\bigg\rfloor +1$$

and the result follows immediately from this inequality. □

Remark 2.9. Next we prove a result that suggests that there are some integers $n \leq x$ that ramifies in more than one modulus $m < x$. We find the following elementary estimate useful:

Lemma 2.10. *The estimate is valid*

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}.$$

Proof. For a proof see [2]. □

Lemma 2.11. *The estimate is valid*

$$\sum_{n\leq x}\frac{1}{n}=\log x+\gamma+O\bigg(\frac{1}{x}\bigg).$$

Proof. For a proof see [1]. □

Theorem 2.12. *The estimate*

$$\sum_{m\leq x}\sum_{\substack{n\leq x\\ \mathcal{R}(m)=n}}1\geq x\log(\sqrt{x-\log x})+O(x)$$

is valid

Proof. We observe that by an application of Lemma 2.10, Lemma 2.11 and Theorem 2.7

$$\begin{aligned}\sum_{\frac{x}{\sqrt{x-\log x}}<m\leq x}\sum_{\substack{n\leq x\\ \mathcal{R}(m)=n}}1 &\geq \sum_{\frac{x}{\sqrt{x-\log x}}<m\leq x}\frac{x^2-xm}{m^2}+O(x)\\ &= x^2\sum_{\frac{x}{\sqrt{x-\log x}}<m\leq x}\frac{1}{m^2}-x\sum_{\frac{x}{\sqrt{x-\log x}}<m\leq x}\frac{1}{m}+O(x)\\ &= x^2\Bigg(\sum_{m>\frac{x}{\sqrt{x-\log x}}}\frac{1}{m^2}-\sum_{m>x}\frac{1}{m^2}\Bigg)-x\sum_{\frac{x}{\sqrt{x-\log x}}<m\leq x}\frac{1}{m}+O(x)\\ &= O(x)+O(1)+x\log(\sqrt{x-\log x})+O(\sqrt{x})\\ &= x\log(\sqrt{x-\log x})+O(x).\end{aligned}$$

□

Corollary 1. There exist at least one integer $n\leq x$ that ramifies in at least two modulus $m\leq x$.

Proof. The result follows from the pigeon-hole principle since

$$\frac{x\log(\sqrt{x-\log x})+O(x)}{x}\geq \log(\sqrt{x-\log x})+O(1).$$

□

3. The index of ramification

In this section we launch the notion of the index of ramification. We expose some relationship between ramifiers and their corresponding indeces.

Definition 3.1. Let $n\geq 2$ be a positive integers that ramifies in modulo $m\geq 2$. Then by the index of ramification in modulo m, denoted $\mathrm{ind}_m(n)$, we mean the value $r_j<m$ so that for $n\equiv a_i \pmod{m}$, then $n\equiv s_j \pmod{r_j}$ such that $a_i+s_j=m$.

Theorem 3.2. *Let* $n\equiv a_i \pmod{m}$ *and suppose* $(n-m,a_i)=1$. *If* $\mathcal{R}(m)=n$, *then* $\mathrm{ind}_m(n)\equiv 0 \pmod{a_i}$ *or* $(\mathrm{ind}_m(n),a_i)=1$.

Proof. Let $n\equiv a_i \pmod{m}$ with $(n-m,a_i)=1$ and suppose for the sake of contradiction that $(\mathrm{ind}_m(n),a_i)=d$ with $1<d<a_i$. Then it follows that $\left(\frac{\mathrm{ind}_m(n)}{d},\frac{a_i}{d}\right)=1$. Since $\mathcal{R}(m)=n$, it follows that there exist some $r_k<m$ such that for $n\equiv s_k \pmod{r_k}$, then it follows that $a_i+s_k=m$. It follows that $d|(m-s_k)$. Since $d|\mathrm{ind}_m(n)$, it follows that $d|(n-s_k)$. Thus it follows that $d|(n-m)$. This contradicts the assumption $(n-m,a_i)=1$, since $d|a_i$ and $1<d<a_i$. □

Remark 3.3. Theorem 3.2 roughly speaking tells us that the image of a body in a miror of somewhat large size could be magnified to cover the size of a certain smaller mirror.

4. **The circle of ramification**

In this section we launch the notion of the circle of ramification in a given modulus. We launch in a more formal way the following terminology:

Definition 4.1. Let $\mathcal{I} := \{n \leq x : \mathcal{R}(m) = n\}$ be any set of ramifiers, then by the circle of ramification relative to $\mathcal{I}$ with center m and radius r we mean $|\mathcal{R}(m) - m| \leq r$, where $r = \max\{|\mathcal{R}(m) - m|\}$.

Remark 4.2. The next result tells us that for any finite set of the integers, we can get controll on the radius of the circle of ramification. In other words, there appears to be lack of degree of freedom in constructing circles of ramification, given any finite set of integers.

Proposition 4.1. *Let $\mathcal{I} := \{n \leq x : \mathcal{R}(m) = n\}$ be any set of ramifiers, then*

$$\max\{|\mathcal{R}(m) - m|\} \leq \frac{x(\sqrt{x - \log x} - 1)}{\sqrt{x - \log x}}.$$

Proof. The result follows by applying Theorem 2.7 and the previous discussion on the least scale of modulus that admits a ramifier. □

Remark 4.3. Proposition 4.1 tells us that the ramifiers in any finite set must not be too far way from the centre of ramification, in the sense that they must be closer to the centre than expected with distance $\leq x^{1-\epsilon}$ for some $\epsilon > 0$.

5. **Ramification character**

It is important to notice that in a given modulus not every integer is a ramifier. In other words there are some numbers that ramify and some that do not ramify in a given modulus. A sequel to this paper will be geared towards launching a criterion for deciding which number is a ramifier for any given modulus. In this section, however, we launch the ramification character and establish some elementary properties in this regard.

Definition 5.1. (Ramification character) Let n be any positive integer. Then we set

$$\kappa_m(n) := \begin{cases} 1 & \text{if} \quad \mathcal{R}(m) = n \\ 0 & \text{otherwise.} \end{cases}$$

Remark 5.2. We begin this section by studying some interesting properties of the ramification character in a given modulus.

Proposition 5.1. *Let m be a fixed positive integer, then the following properties of the ramification character holds:*

(i) $\kappa_m(n + 2m) = \kappa_m(n)$.

(ii) $\kappa_m(n + m!) = \kappa_m(n)$.

(iii) $\kappa_m(1) = 0$.

(iv) $\kappa_m(n) = 0$ *for* $n \equiv 0, 1 \pmod m$.

(v) $\kappa_m(nm!) = \kappa_m(n)\kappa_m(m!)$.

Proof. We prove only (ii), (iii), (iv) and (v). For (ii), since $n+m! \equiv n \pmod{r_i}$ for any sequence $r_0 < r_1 < \ldots r_{k-1} < r_k = m$ the result follows immediately according as n is a ramifier or a non-ramifier. Clearly (iii) and (iv) follows from Proposition 2.2 and Proposition 2.2. Finally (iv) is also easy to establish. □

A natural quest is to, at the very least, seek for various upper and lower bounds for the partial sums of the ramification character in a fixed modulus. That is, we seek estimates for sums of the form

$$\sum_{n\leq x}\kappa_m(n).$$

It is easy to check trivial upper and lower bounds for this sum have been established in Theorem 2.4 and Theorem 2.7, by observing that

$$\sum_{\substack{n\leq x\\ \mathcal{R}(m)=n}} 1 = \sum_{n\leq x}\kappa_m(n).$$

We obtain the following weaker estimate for the partial sums of the ramification character as follows:

Theorem 5.3. *Let m be a fixed positive integer, then the inequality is valid*

$$\frac{x^2-xm}{m^2}+O_m(1)\leq \sum_{n\leq x}\kappa_m(n)\leq \left(1-\frac{1}{m}\right)x-\frac{\log x}{\log m}+O(1)$$

for

$$m\geq \left\lfloor \frac{x}{\sqrt{x-\log x}}\right\rfloor+1.$$

Proof. The result follows by combining Theorem 2.7 and Theorem 2.4. □

6. **Final remarks**

In this paper we have introduced the concept of the ramifiers. We have established some properties and some consequences of this theory. The Goldbach conjecture, which is an important open problem, can be framed in this language as:

Conjecture 6.1 (Goldbach). Every even number $n \geq 6$ admits a strong ramifier in $(\mathrm{mod}\ n)$.

The most striking is the result about the distribution of prime in small intervals given as:

Theorem 6.1. *Let $p \leq x$ be a prime and suppose p admits a ramifier n for some $n \leq x$. Then there must exist at least one prime in the interval*

$$\left(\frac{x}{\sqrt{x - \log x}}, x\right].$$

References

1. Gérald Tenenbaum, *Introduction to analytic and probabilistic number theory*, vol. 163, American Mathematical Soc., 2015.
2. Hildebrand, AJ, *Introduction to Analytic Number Theory Lecture Notes*, Department of Mathematics, University of Illinois, 2005.

Department of Mathematics, African Institute for Mathematical science, Ghana

E-mail address: theophilus@aims.edu.gh/emperordagama@yahoo.com