SOME PROPERTIES OF THE EULER QUOTIENT MATRIX

Ikhalfani Solan

Department of Mathematics and Computer Science, University of the West Indies, Jamaica

ikhalfani.solan@uwimona.edu.jm

Received: 2/15/06, Revised: 10/18/06, Accepted: 11/1/06, Published: 11/22/06

Abstract

Let \( a \) and \( m \) be integers such that \((a, m) = 1\). Let \(q_a = a^{\phi(m) - 1}/m\). We call \( q_a \) the Euler Quotient of \( m \) with base \( a \). This is called the Fermat Quotient when \( m \) is a prime. We consider some properties of the matrix of Euler Quotients reduced modulo \( m \) and show that these quotients are uniformly distributed modulo \( m \).

1. Introduction

Let \( m \) and \( a \) be integers such that \((m, a) = 1\). Let \(q_a = a^{\phi(m) - 1}/m\). We call \( q_a \) the Euler Quotient of \( m \) with base \( a \). This is called the Fermat Quotient when \( m \) is a prime.

The following theorem summarizes some of the logarithmic properties of \( q_a \).

**Theorem 1.1** Let \( a, b \in \mathbb{Z} \) and \( r \in \mathbb{N} \) with \((a, m) = (b, m) = 1\). Then

\[
\begin{align*}
(a) & \quad q_l \equiv 0 \mod m \\
(b) & \quad q_{ab} \equiv q_a + q_b \mod m \\
(c) & \quad q_{ar} \equiv rq_a \mod m
\end{align*}
\]

Additional properties of \( q_a \) are given by the following generalization of a theorem of Wells [4]. It provides conditions when \( q_a \) vanishes modulo \( m \).

**Theorem 1.2** Let \((a, m) = 1\). If \( l \) and \( t \) are integers with \((l, m) = 1\) and \( \alpha \) is a positive integer, then for \( a = l + tm^\alpha \)

\[
q_a \equiv q_l \mod m + \frac{\phi(m)t}{l}m^{\alpha-1} \mod m^\alpha.
\]
2. The Euler Quotient Matrix

Let \( a \) be the \( i^{th} \) integer such that \( 1 \leq a \leq m \) and \( (a,m) = 1 \). The Euler Quotient Matrix, \( M_m \), is the \( m \times \phi(m) \) matrix where the entries in column \( i \) are the least non-negative residues of \( q_k \pmod{m} \) for \( k \leq m^2 \) and \( k \equiv a \pmod{m} \). To be more precise we may call this the order 2 matrix and define the order \( r \) matrix for \( k \leq m^r, r = 1, 2, \ldots \), to be the \( m^r - 1 \times \phi(m) \) matrix \( M_{m^r} \).

Example 2.1 The Euler Quotient Matrices for \( m = 7, 12 \) and 9 are given below.

<table>
<thead>
<tr>
<th>( a= )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

| \( a= \) | 1 | 5 | 7 | 11 |
|---|---|---|---|
| 1 | 0 | 4 | 8 | 8 |
| 2 | 4 | 0 | 0 | 4 |
| 3 | 8 | 8 | 4 | 0 |
| 4 | 0 | 4 | 8 | 8 |
| 5 | 4 | 0 | 0 | 4 |
| 6 | 8 | 8 | 4 | 0 |
| 7 | 0 | 4 | 8 | 8 |
| 8 | 4 | 0 | 0 | 4 |
| 9 | 8 | 8 | 4 | 0 |
| 10 | 0 | 4 | 8 | 8 |
| 11 | 4 | 0 | 0 | 4 |
| 12 | 8 | 8 | 4 | 0 |

<table>
<thead>
<tr>
<th>( a= )</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>5</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>7</td>
<td>5</td>
<td>8</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>7</td>
<td>5</td>
<td>8</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td>5</td>
<td>8</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>

Definition 2.2 Let \( \pi_i \) be the maximum size of the blocks of non-repeated entries in the \( i^{th} \) column. We call \( \pi_i \) the period of column \( i \).

Theorem 2.3 The period of column \( i \) is given by \( \pi_i = \frac{m}{\phi(m)} \) for all \( i \leq \phi(m) \).

Proof. Suppose column \( i \) contains the least non-negative residue of \( q_a \pmod{m} \) such that \( a \equiv l + tm, l < m \) and \( (l,m) = 1 \). Then by Theorem 1.2, taking \( \alpha = 1 \), we have \( q_a \equiv q_l + \phi(m)t \ell^{-1}(\pmod{m}) \). The residues of \( q_a \) and \( q_l \) are equal precisely when \( m \) divides \( \phi(m)t \). This occurs for the first time when \( t = \frac{m}{\phi(m)} \) and subsequently for every integer multiple of \( t \). Thus period of column \( i, \pi_i = \frac{m}{\phi(m)} \).

Definition 2.4 We define the period of \( M_m \) to be the period of each column. That is, period of \( M_m \) is given by \( \pi_m = \frac{m}{\phi(m)} \).

Let \( A_r^m = \{ a \mod{m} : 0 \leq a < m^r \} \). It is of interest to know the size of \( A_r^m \). We list some properties of \( A_r^m \).

(a) When \( m = p \), a prime and \( r = 1 \), Vandiver [5] showed that \( \sqrt{p} \leq |A_1^p| \leq p - (1 + \sqrt{2p-5})/2 \).
(b) When \( r = 2 \) and \( m \) is a prime or a strong psuedoprime \( |A_2^m| = m \).
I don't know of any bounds apart from the trivial bounds for $|A_1^m|$ when $m$ is not prime.

Let $m$ be an integer with $m > 2$. Then we have that

$$\frac{m}{(m, \phi(m))} \leq |A_r^m| \leq \frac{m}{(m, \phi(m))} \frac{\phi(m)}{2}. $$

We note that these bounds are the best possible. For example, when $m$ is a prime, $m = 4$, or $m = 12$, the lower bound is achieved. When $m = 3^\alpha, \alpha \geq 2$, the upper bound is achieved.

In fact we have

$$\frac{m}{(m, \phi(m))} \leq |A_r^m| \leq \frac{m}{(m, \phi(m))} \frac{\phi(m)}{2}$$

whenever $r \geq 2$.

Another area of interest is the vanishing of the quotients modulo $m$.

The following theorem appearing in [1] characterizes the elements of $M_m$ and gives a formula for the number of vanishing quotients modulo $m$ in $M_m$.

**Theorem 2.5** Let $m = p^{\alpha_1} \ldots p^{\alpha_k}$ be the prime factorization of the integer $m \geq 2$ and $q$ the homomorphism from $(\mathbb{Z}/m^2\mathbb{Z})^\times$ into $(\mathbb{Z}/m\mathbb{Z}, +)$ induced by the Euler quotient of $m$. For $1 \leq r \leq k$ put $m_r = p^{\alpha_r}$ and

$$d_r = \begin{cases} (m_r, 2 \prod_{j=1}^k (p_j - 1)), & \text{when } m_r = 2^{\alpha_r}; \alpha_r \geq 2, \\ (m_r, \prod_{j=1}^k (p_j - 1)), & \text{otherwise.} \end{cases} $$

Let $d = \prod_{r=1}^k d_r$. Then the image $q((\mathbb{Z}/m^2\mathbb{Z})^\times)$ equals $\{td + m\mathbb{Z} : 0 \leq t \leq (m/d) - 1\}$; it is therefore isomorphic to $(\mathbb{Z}/(m/d)\mathbb{Z}, +)$ for $m > 2$.

The above theorem immediately leads to the fact that the number of quotients to vanish modulo $m$ in $M_m$ is $d\phi(m)$. A quick glance at the matrices for $m = 7, 12$ and 9 shows that a matrix may have columns containing no vanishing quotients. Using the period of the Euler quotient matrix and the total number of zero entries we obtain the following.

**Theorem 2.6** Let $d$ be as defined in Theorem 2.5 and $m \geq 2$ be an integer. Then the number of columns of $M_m$ containing zeros is given by $\frac{d\phi(m)}{(\phi(m), m)}$.

**Proof.** The proof is just to recognize that the number of zeros in each column with a zero is given by $\frac{m}{\sigma_m} = (\phi(m), m)$. Now, by Theorem 2.5 the total number of zeros in $M_m$ is $d\phi(m)$. Thus, there are exactly $\frac{d\phi(m)}{(\phi(m), m)}$ columns with a least one zero.

The formula for the number of columns without zeros is more interesting. This is given by $\phi(m)(1 - \frac{d}{(\phi(m), m)})$. If one notes that when $m$ is a prime or a strong pseudoprime $d = (\phi(m), m) = 1$, then the term $\frac{d}{(\phi(m), m)}$ can be considered as measure of the primeness of $m$. 


3. Sum of Quotients in the Columns and Rows of $M_m$

In the next two theorems we, respectively, show that the sum of the entries in each column of $M_m$ is congruent to 0 modulo $m$ and that all rows sum to the same constant modulo $m$.

**Theorem 3.1** Let $1 \leq a < m$ with $(a, m) = 1$. If $k < m^2$ and $k \equiv a \pmod{m}$, then

$$\sum_{k \equiv a \pmod{m}} q_k \equiv 0 \pmod{m}.$$  

**Proof.** Let $k = a + im$, $i < m$. Then

$$\sum_{k \equiv a \pmod{m}} q_k = \frac{1}{m} \sum_{i=0}^{m-1} (a + im)^{\phi(m)-1} = \sum_{i=0}^{m-1} q_a + \left( \frac{\phi(m)}{1} \right) \sum_{i=0}^{m-1} i a^{\phi(m)-1} + m\left\{ \left( \frac{\phi(m)}{2} \right) \sum_{i=0}^{m-1} i^2 a^{\phi(m)-2} + \cdots + \left( \frac{\phi(m)}{\phi(m)} \right) \sum_{i=0}^{m-1} i^{\phi(m)-2} \right\}$$

$$= mq_a + \phi(m)m(m-1)a^{\phi(m)-1} \equiv 0 \pmod{m}.$$ 

**Theorem 3.2**

$$\sum_{a=km+1 \atop (a, m) = 1}^{(k+1)m-1} q_a \equiv \sum_{a=1 \atop (a, m) = 1}^{m-1} q_a \pmod{m}, \text{ for each } k \in \{1, 2, \ldots, m-1\}.$$ 

**Proof.** For any $k \in \{1, 2, \ldots, m-1\}$ we have

$$\sum_{a=km+1 \atop (a, m) = 1}^{(k+1)m-1} q_a = \sum_{a=1 \atop (a, m) = 1}^{m-1} \frac{(km + a)^{\phi(m)} - 1}{m}$$

$$= \frac{1}{m} \left\{ \phi(m)m^{\phi(m)} + \left( \frac{\phi(m)}{1} \right) \sum_{a<m \atop (a, m) = 1} a^{\phi(m)-1} + \left( \frac{\phi(m)}{2} \right) \sum_{a<m \atop (a, m) = 1} a^{\phi(m)-2} + \cdots + \left( \frac{\phi(m)}{\phi(m)-1} \right) \sum_{a<m \atop (a, m) = 1} a^{\phi(m)-3} + \sum_{a<m \atop (a, m) = 1} (a^{\phi(m)-1}) \right\}$$

$$= \phi(m)m^{\phi(m)-1} + m^{\phi(m)-2} \left( \frac{\phi(m)}{1} \right) \sum_{a<m \atop (a, m) = 1} a + m^{\phi(m)-3} \left( \frac{\phi(m)}{2} \right) \sum_{a<m \atop (a, m) = 1} a^2 + \cdots + \phi(m) \sum_{a<m \atop (a, m) = 1} a^{\phi(m)-1} + \sum_{a<m \atop (a, m) = 1} q_a$$

$$\equiv \sum_{a<m \atop (a, m) = 1} q_a \pmod{m}.$$  

† From this point on we suppressed, without loss, the use of $k$ in the proof.
4. Equidistribution of the Euler Quotients

A result due to Heath-Brown [3] shows that the Fermat Quotients are uniformly distributed mod $p$ for $1 \leq a < p$. This result generalized nicely to the Euler Quotients. We obtain

**Theorem 4.1** For any integers $a, h$ with $(a, m) = (h, m) = 1$, we have

$$\sum_{M < a < M+N \atop (a,m) = 1} \exp\left(\frac{hqa}{m}\right) \ll N^{1/2}m^{3/8} \text{ uniformly for } M, N \geq 1.$$ 

In particular

$$\sum_{a < m \atop (a,m) = 1} \exp\left(\frac{hqa}{m}\right) \ll m^{7/8} \text{ uniformly.}$$

**Proof.** The proof is similar to that of Heath-Brown [3]. From Theorem 1.1 we have $q_{ab} \equiv q_a + q_b (\text{mod } m)$ whenever $(a, m) = (b, m) = 1$. Thus

$$\chi(a) = \begin{cases} 0, & (a, m) \neq 1 \\ \exp\left(\frac{hqa}{p}\right), & (a, m) = 1. \end{cases}$$

is a non-principal character of order $m$. Hence we have

$$\sum_{M < a < M+N} \exp\left(\frac{hqa}{m}\right) = \sum_{M < a < M+N} \chi(a).$$

Now Burgess [2] proved that for composite modulus $m$

$$\sum_{M < a < M+N} \chi(a) \ll N^{1/2}m^{3/8}.$$ 

Taking $M = 1$ and $N = m$, we obtain

$$\sum_{a < m \atop (a,m) = 1} \exp\left(\frac{hqa}{m}\right) \ll m^{7/8}, \text{ uniformly.}$$

**Acknowledgments**

We would like to thank the referee for the valuable suggestions.
References


