Functional Analysis Meets Number Theory: Matrix-Valued Euler Functions Non-commutative Number Theory? C*-Riemann

Marty Walter

Martin.Walter@Colorado.Edu

JMM-Denver January 16, 2020

Definition of Euler Φ-Function

Definition

Let n be a natural number.
$\Phi[n]$ is the number of integers k in the range $1 \leq k \leq n$ for which the greatest common divisor $gcd(n, k) = 1$.

Definition of Möbius Function

Definition

Let n be a natural number.
$\mu[n]$ is given by: $\mu[1] = 1$, $\mu[n] = 0$ if n is divisible by the square of a prime number, otherwise $\mu[n] = (-1)^k$, where k is the number of prime factors of n.

Matrix-Valued Euler Φ-Functions

Claim: Each natural number n determines a unique $n \times n$ ("*Euler*") matrix modulo conjugation by permutation matrices.

Matrix-Valued Euler Φ-Functions

Claim: Each natural number n determines a unique $n \times n$ ("*Euler*") matrix modulo conjugation by permutation matrices. If $C_n = \{a^0 = a^n = e,\ a^1, \dots,\ a^{n-1}\}$ is a cyclic group with n elements, where $n = \Pi_{i=1}^{r} p_i^{n_i}$, the p_i being pairwise distinct primes for $i = 1, \dots, r$,

Matrix-Valued Euler Φ-Functions

Claim: Each natural number n determines a unique $n \times n$ ("*Euler*") matrix modulo conjugation by permutation matrices. If $C_n = \{a^0 = a^n = e,\ a^1, \ldots,\ a^{n-1}\}$ is a cyclic group with n elements, where $n = \Pi_{i=1}^{r} p_i^{n_i}$, the p_i being pairwise distinct primes for $i = 1, \ldots, r$,
Define the *Euler Φ-function*:

Definition

$\Phi[C_n]{:=}\Sigma\{a^i : gcd[i, n] = 1\}$,

i.e., the formal sum of elements of C_n which generate C_n, where $gcd[x, y]$ stands for greatest common divisor of integers x and y.

Representation π of Φ

If π is a matrix representation of C_n, then $\Phi[C_n]$ can be represented/defined as a matrix as well, viz.,

Definition

$\pi{*}\Phi[C_n]{:=}\Sigma\{\pi[a^i] : gcd[i, n] = 1\}$, a sum of matrices called the π *representation of* Φ.

Euler, Möbius just two different representations

For $0 \leq k \leq n-1$, let χ_k be the homomorphism of $G = C_n$ into $\mathbb{C}$ defined by $\chi_k[a^j] = e^{2\pi Ikj/n}$, $0 \leq j \leq n-1$.
(Note that χ_k is called a *character* of C_n, or an *irreducible unitary representation* of C_n.)

Euler, Möbius just two different representations

For $0 \leq k \leq n-1$, let χ_k be the homomorphism of $G = C_n$ into $\mathbb{C}$ defined by $\chi_k[a^j] = e^{2\pi Ikj/n}$, $0 \leq j \leq n-1$.
(Note that χ_k is called a *character* of C_n, or an *irreducible unitary representation* of C_n.)

We have the following:
(i) $\chi_0 * \Phi[C_n] = \phi[n]$, the classical Euler Φ-function;

Euler, Möbius just two different representations

For $0 \leq k \leq n-1$, let χ_k be the homomorphism of $G = C_n$ into $\mathbb{C}$ defined by $\chi_k[a^j] = e^{2\pi I kj/n}$, $0 \leq j \leq n-1$.
(Note that χ_k is called a *character* of C_n, or an *irreducible unitary representation* of C_n.)

We have the following:
(i) $\chi_0 * \Phi[C_n] = \phi[n]$, the classical Euler Φ-function;
(ii) $\chi_1 * \Phi[C_n] = \mu[n]$, the classical Möbius function;

Euler, Möbius just two different representations

For $0 \leq k \leq n-1$, let χ_k be the homomorphism of $G = C_n$ into $\mathbb{C}$ defined by $\chi_k[a^j] = e^{2\pi I kj/n}$, $0 \leq j \leq n-1$.
(Note that χ_k is called a *character* of C_n, or an *irreducible unitary representation* of C_n.)

We have the following:
(i) $\chi_0 * \Phi[C_n] = \phi[n]$, the classical Euler Φ-function;
(ii) $\chi_1 * \Phi[C_n] = \mu[n]$, the classical Möbius function;
(iii) $\chi_k * \Phi[C_n] = \sum_{d|gcd[k,n]} \mu[\frac{n}{d}]d = \frac{\phi[n]}{\phi[\frac{n}{gcd[k,n]}]}\mu[\frac{n}{gcd[k,n]}]$,

a Ramanujan sum.

Definition of Euler Φ-matrix of C_n

We prove some elementary properties of this Euler Φ-function for cyclic groups, including the formula:

Theorem

$\rho * \Phi[C_n] = \bigotimes_{i=1}^{r} \mathbb{I}[p_i]^{\otimes(n_i-1)} \otimes \Delta[p_i]$,
which we call the "Euler Φ-matrix of C_n,"

where $\mathbb{I}[p]$ is the $p \times p$ matrix of all 1s and
$\Delta[p] = \mathbb{I}[p] - I_p$,
I_p being the $p \times p$ identity matrix,
ρ being a regular representation.

We use this formula to solve to a previously posed problem, viz., each Euler Φ-matrix has a complete set of eigenvectors all the entries of which come from the set $\{-1, 0, 1\}$.

Multiplication Table of a Finite Group: "Standard Form"

Write group G as a $1 \times n$ matrix:

Multiplication Table of a Finite Group: "Standard Form"

Write group G as a $1 \times n$ matrix:

$$G = [g_1, g_2, \ldots, g_n].$$

Let the $n \times 1$ matrix: G^*, be the conjugate transpose of G, where $g_i^* = g_i^{-1}$.
Then the $n \times n$ "standard (positive-symmetric) matrix multiplication table of G" is:

$$M[G] = G^* G = [g_i^{-1} g_j].$$

Permutation Equivalence of Group Multiplication Tables

Given $M[G] = [{g_i}^{-1} g_j]$, $1 \leq i \leq n, 1 \leq j \leq n$.
(Note that the first row of $M[G]$ determines the entire array.)

Permutation Equivalence of Group Multiplication Tables

Given $M[G] = [{g_i}^{-1}g_j]$, $1 \leq i \leq n, 1 \leq j \leq n$.
(Note that the first row of $M[G]$ determines the entire array.)

If $\mathbb{S}_n$ is the permutation group of the set $\{1, \ldots, n\}$, and $\alpha \in \mathbb{S}_n$, then

Permutation Equivalence of Group Multiplication Tables

Given $M[G] = [{g_i}^{-1} g_j]$, $1 \leq i \leq n, 1 \leq j \leq n$.
(Note that the first row of $M[G]$ determines the entire array.)

If $\mathbb{S}_n$ is the permutation group of the set $\{1, \ldots, n\}$, and $\alpha \in \mathbb{S}_n$, then

$$M_\alpha[G] = [{g_{\alpha[i]}}^{-1} g_{\alpha[j]}]$$

is also a form of the multiplication table of G in symmetric form.

Permutation Equivalence of Group Multiplication Tables

Given $M[G] = [{g_i}^{-1} g_j]$, $1 \leq i \leq n, 1 \leq j \leq n$.
(Note that the first row of $M[G]$ determines the entire array.)

If $\mathbb{S}_n$ is the permutation group of the set $\{1, \ldots, n\}$, and $\alpha \in \mathbb{S}_n$, then

$$M_\alpha[G] = [{g_{\alpha[i]}}^{-1} g_{\alpha[j]}]$$

is also a form of the multiplication table of G in symmetric form.
We say that the the collection of all multiplication tables thus arrived at are (pairwise) *permutation equivalent*.

Regular Permutation Length: $N[g] = n - \frac{n}{o(g)}$

Regular Permutation Length: $N[g] = n - \frac{n}{o(g)}$

Given a permutation σ of n distinct objects written as a product of s disjoint cycles, $c_1, \ldots, c_s$, Jacobson associates an integer, $N[\sigma] = (|c_1| - 1) + \cdots + (|c_s| - 1)$, where $|c_i|$ is the number of objects permuted by, or the "cycle length" of, c_i. Note that N is a well-defined function on the permutations of a finite set, and that N of the identity permutation is 0.

Regular Permutation Length: $N[g] = n - \frac{n}{o(g)}$

Given a permutation σ of n distinct objects written as a product of s disjoint cycles, $c_1, \ldots, c_s$, Jacobson associates an integer, $N[\sigma] = (|c_1| - 1) + \cdots + (|c_s| - 1)$, where $|c_i|$ is the number of objects permuted by, or the "cycle length" of, c_i. Note that N is a well-defined function on the permutations of a finite set, and that N of the identity permutation is 0.

If each element, g, of a finite group, G of order n, (abelian or not) is represented by the permutation, $\rho_G[g]$, of the set G, created as that element acts via (left) translation, i.e., $x \in G \longmapsto gx \in G$, (where gx is the product in G of g and x), then we have the integer-valued function, $g \in G \longmapsto N[\rho_G[g]] = \frac{n}{o(g)}[o(g) - 1] = n - \frac{n}{o(g)}$, where $o(g)$ is the order of g, viz., the smallest positive integer k such that $g^k = e$, the identity in G.

Permutation Length Matrix

Here we are making use of a property of the *regular representation*, $\rho_G[g]$; namely that it is a permutation of n objects, and all of its (pairwise) disjoint cycles are of the same length, $o(g)$.

Permutation Length Matrix

Here we are making use of a property of the *regular representation*, $\rho_G[g]$; namely that it is a permutation of n objects, and all of its (pairwise) disjoint cycles are of the same length, $o(g)$. Note: $\rho[x]$ is also a permutation matrix obtained as follows: $x \in G$ occurs exactly once in each row and each column of $M[G] = [g_i^{-1} g_j]$, replace occurence of x in this matrix with a 1, 0 elsewhere, call the resulting permutation matrix $\rho[x]$.

Permutation Length Matrix

Here we are making use of a property of the *regular representation*, $\rho_G[g]$; namely that it is a permutation of n objects, and all of its (pairwise) disjoint cycles are of the same length, $o(g)$. Note: $\rho[x]$ is also a permutation matrix obtained as follows: $x \in G$ occurs exactly once in each row and each column of $M[G] = [g_i^{-1}g_j]$, replace occurence of x in this matrix with a 1, 0 elsewhere, call the resulting permutation matrix $\rho[x]$.

We define the regular permutation length matrix of G to be the following $n \times n$ matrix of natural numbers (zero on the diagonal):

$$\mathbf{N}[G] = [N[g_i^{-1}g_j]].$$

Permutation Length Matrix

Here we are making use of a property of the *regular representation*, $\rho_G[g]$; namely that it is a permutation of n objects, and all of its (pairwise) disjoint cycles are of the same length, $o(g)$. Note: $\rho[x]$ is also a permutation matrix obtained as follows: $x \in G$ occurs exactly once in each row and each column of $M[G] = [g_i^{-1} g_j]$, replace occurence of x in this matrix with a 1, 0 elsewhere, call the resulting permutation matrix $\rho[x]$.

We define the regular permutation length matrix of G to be the following $n \times n$ matrix of natural numbers (zero on the diagonal):

$$\mathbf{N}[G] = [N[g_i^{-1} g_j]].$$

What are the eigenvalues of this matrix?

Permutation Length Matrix

Here we are making use of a property of the *regular representation*, $\rho_G[g]$; namely that it is a permutation of n objects, and all of its (pairwise) disjoint cycles are of the same length, $o(g)$. Note: $\rho[x]$ is also a permutation matrix obtained as follows: $x \in G$ occurs exactly once in each row and each column of $M[G] = [g_i^{-1} g_j]$, replace occurence of x in this matrix with a 1, 0 elsewhere, call the resulting permutation matrix $\rho[x]$.

We define the regular permutation length matrix of G to be the following $n \times n$ matrix of natural numbers (zero on the diagonal):

$$\mathbf{N}[G] = [N[g_i^{-1} g_j]].$$

What are the eigenvalues of this matrix?

What choices of eigenvectors are there?

Is this Matrix Negative Definite?

Eventual Answer: Yes

Is this Matrix Negative Definite?

Eventual Answer: Yes

Why Do I Care?

Definition

A function N: $G \to \mathbb{C}$, is negative definite on group G if and only if the following three conditions are satisfied:

(i) $N[e] \geq 0$, where e is the identity of G,

(ii) $N = N^*$,

(iii) For any natural number m, any $\{g_1, g_2, \ldots, g_m\} \subset G$, and any $\{\rho_1, \rho_2, \ldots, \rho_m\} \subset \mathbb{C}$,

$$\sum_{i=1}^{m} \rho_i = 0, \quad \textit{implies} \sum_{i,j=1}^{m} N[g_i^{-1} g_j] \overline{\rho_i} \rho_j \leq 0.$$

C*-Algebras: One Parameter Semigroup of Completely Positive Maps

Theorem

A function $N : G \to \mathbb{C}$ is negative definite if and only if the following two conditions are satisfied:
(i) $N[e] \geq 0$,
(ii) The function $g \in G \rightarrowtail Exp[-tN[g]]$ is positive definite for all $t > 0$.

The Riemann Hypothesis is near

The Landau function, $\sigma[n] := MAX\{o[g] : g \in \mathbb{S}_n\}$.

The Riemann Hypothesis is near

The Landau function, $\sigma[n] := MAX\{o[g] : g \in \mathbb{S}_n\}$.

Remark

$$ln\, \sigma[n] < (Li^{-1}[n])^{\frac{1}{2}}$$

for sufficiently large n, is equivalent to the Riemann Hypothesis.

The Riemann Hypothesis is near

The Landau function, $\sigma[n] := MAX\{o[g] : g \in \mathbb{S}_n\}$.

Remark

$$ln\, \sigma[n] < (Li^{-1}[n])^{\frac{1}{2}}$$

for sufficiently large n, is equivalent to the Riemann Hypothesis.

Note: $Li[x] = \int_2^x \frac{\mathrm{d}t}{ln\, t}$.

If $G = C_n$: $N[a^i] = n - gcd[n, i]$

If $G = C_n$: $N[a^i] = n - gcd[n, i]$

If $G = C_n = \{a^i : 0 \leq i \leq n-1\}$ then note that $lcm[n, i]gcd[n, i] = ni$, where *lcm* means least common multiple and *gcd*, recall, is greatest common divisor. Now $o(a^i) = \frac{lcm[n,i]}{i}$, since $(a^i)^{\frac{lcm[n,i]}{i}} = e$; and no smaller power has this property. Thus

$$N[a^i] = n - \frac{n}{o(a^i)} = n - \frac{ni}{lcm[n, i]} = n - gcd[n, i].$$

Eigenvalues for N for Cyclic Groups

We thus finally have the closed form formula for each eigenvalue, λ_k, of **N**, $1 \leq k < n$:

$$\lambda_k = -\sum_{d|gcd[n,k]} d\phi[\frac{n}{d}].$$

Note that ϕ is the classical Euler ϕ-function from number theory.
Note that λ_k is the eigenvalue corresponding to $\chi_k = (\chi_1)^k$, the usual group characters of C_n. ($\chi_1[a] = e^{2\pi I/n}$.)
Note that $\lambda_0 = \lambda_n$, the only positive eigenvalue, is the negative sum of all $n-1$ other eigenvalues.

The Formula for Aribitrary Finite Abelian Group A

If A is an abelian group of order $n = \Pi_{k=1}^{r} n_k$,
where $A = C_{n_1} \times C_{n_2} \times \ldots C_{n_r}$, a product of r cyclic groups, C_{n_k}, of order n_k, generated by a_k, $k = 1, \ldots, r$, then

$$N[{a_1}^{i_1}{a_2}^{i_2}\ldots{a_r}^{i_r}] =$$

$$n - gcd[\frac{n}{n_1}gcd[n_1, i_1], \frac{n}{n_2}gcd[n_2, i_2], \ldots, \frac{n}{n_r}gcd[n_r, i_r]\ ].$$

The function N is associated with an $n \times n$ self-adjoint matrix, $\mathbf{N}$, whose eigenvalues are the values of the Fourier transform of N. We calculate these eigenvalues exactly:

The Eigenvalues for $A = C_{n_1} \times C_{n_2} \times \ldots C_{n_r}$

The Eigenvalues for $A = C_{n_1} \times C_{n_2} \times \ldots C_{n_r}$

$$\lambda_{k_1,k_2,..,k_r} =$$

$$-gcd[\tfrac{n}{n_1}, \tfrac{n}{n_2}, \ldots, \tfrac{n}{n_r}] \sum \{\phi[d](\prod_{i=1}^{r} n_i[d]) : d | lcm[n_1, n_2, \ldots, n_r],\ n_i[d] \mid k_i,\ i = 1, 2, \ldots, r\},$$

where lcm means least common multiple, and $n_i[d] = gcd[n_i, \frac{lcm[n_1,\ldots,n_r]}{d}]$ for all i, and where $1 \le k_i \le n_i$, $i = 1, \ldots .r$, and $\lambda_{k_1,k_2,\ldots,k_r} \ne \lambda_{n_1,n_2,\ldots,n_r}$. The negative of the sum of all these eigenvalues is $\lambda_{n_1,n_2,\ldots,n_r}$. Also $\lambda_{n_1,n_2,\ldots,n_r}$ is equal to the sum of the n values of N on A.

A Question Arose

While calculating the eigenvalues/eigenvectors the default algorithm of Mathematica produced eigenvectors with sparse small integer entries. I asked:

Question

How far in this direction can I go? Can I find a complete set of eigenvectors with only 1, -1, and 0 entries?

A Question Arose

While calculating the eigenvalues/eigenvectors the default algorithm of Mathematica produced eigenvectors with sparse small integer entries. I asked:

Question

How far in this direction can I go? Can I find a complete set of eigenvectors with only 1, -1, and 0 entries?

Answer:

A Question Arose

While calculating the eigenvalues/eigenvectors the default algorithm of Mathematica produced eigenvectors with sparse small integer entries. I asked:

Question

How far in this direction can I go? Can I find a complete set of eigenvectors with only 1, -1, and 0 entries?

Answer: Yes!

A Matrix-Valued Euler *Phi*-Function

Definition

If C_n is the cyclic group with n elements, define the *Euler* Φ*-function*: $\Phi[C_n]{:=}\Sigma\{a^i : gcd[i,n] = 1\}$, i.e., the formal sum of the generators of C_n.

Definition

If π is a matrix representation of C_n, then define the π*-representation of* $\Phi[C_n]$ to be $\pi * \Phi[C_n]{:=}\Sigma\{\pi[a^i] : gcd[i,n] = 1\}$, a matrix sum.

Classical Euler Φ "=" Classical Möbius μ??

Remark

In general, there is more than one matrix representation for a given C_n. Thus our definition of Euler Φ-function includes both the classical Euler ϕ-function and the Möbius function. If we take the trivial representation of C_n: $\chi_n : a^i \in C_n \mapsto 1$, for $0 \leq i \leq n-1$, then $\chi_n * \Phi[C_n] = \phi[n]$, Euler's classical function which donotes the number of natural numbers between 0 and n relatively prime to n. If we take instead the faithful representation, χ_1 of C_n, determined by $\chi_1[a] = e^{2\pi I/n}$, we obtain $\chi_1 * \Phi[C_n] = \mu[n]$, the Möbius function of n, which is known (among other things) to equal the sum of the primitive n^{th} roots of unity. Our Euler Φ-function leads to a number of such phenomena.

Our First Lemma

Definition

We will denote by $\mathbb{I}[n]$ the $n \times n$ matrix every entry of which is the natural number 1. We denote the $n \times n$ identity matrix by I_n. We define $\Delta[n] := \mathbb{I}[n] - I_n$, the $n \times n$ matrix of all 1s except for all 0s on the main diagonal.

Lemma

If p is a prime natural number, then $\rho * \Phi[C_p] = \Delta[p]$.

New Set of Eigenvectors

New Set of Eigenvectors

$\Delta[m]$ has an eigenvector with eigenvalue $m-1$, viz., $\vec{e_0}[m] = [1, 1, \ldots, 1]$, 1 in each of the m positions.

New Set of Eigenvectors

$\Delta[m]$ has an eigenvector with eigenvalue $m-1$, viz., $\vec{e_0}[m] = [1, 1, \ldots, 1]$, 1 in each of the m positions.
The matrix $\Delta[m]$ has $m-1$ eigenvectors each with eigenvalue -1, viz., $\vec{e_k}[m] = [0, \ldots, 1, 0, \ldots, -1]$, with a single 1 in the k^{th} position, a single -1 in the m^{th} position, all other positions occupied by 0, $k = 1, \ldots, m-1$.

New Set of Eigenvectors

$\Delta[m]$ has an eigenvector with eigenvalue $m-1$, viz., $\vec{e_0}[m] = [1, 1, \ldots, 1]$, 1 in each of the m positions.
The matrix $\Delta[m]$ has $m-1$ eigenvectors each with eigenvalue -1, viz., $\vec{e_k}[m] = [0, \ldots, 1, 0, \ldots, -1]$, with a single 1 in the k^{th} position, a single -1 in the m^{th} position, all other positions occupied by 0, $k = 1, \ldots, m-1$.
The matrix $\mathbb{I}[m]$ has the *same* set of eigenvectors, viz., $\vec{e_0}[m]$ is an eigenvector with eigenvalue m, and $\vec{e_k}[m]$ is an eigenvector with eigenvalue 0, $k = 1, \ldots, m-1$.

Euler Φ for Prime Power Cyclic Groups

The "Euler Φ function for prime power cyclics proposition."

Proposition

If $n \geq 2$ is a natural number and p is a prime natural number, then (up to permutation equivalence)

$$\rho * \Phi[C_{p^n}] = \mathbb{I}[p]^{\otimes(n-1)} \otimes \Delta[p],$$

where $\mathbb{I}[p]^{\otimes(n-1)}$ is the Kronecker product of $\mathbb{I}[p]$ with itself, $n-1$ factors, i.e., $\mathbb{I}[p^{(n-1)}]$.

Proof

Proof: We exhibit a multiplication table for C_{p^n} that has the desired property. If a generates C_{p^n}, $a^{p^{(n-1)}}$ is an element of order p. Let C_p denote the subgroup it generates. Write the first row of the multiplication table of C_{p^n} as follows: Begin with the first row of the multiplication table of C_p, with $a^{p^n} = a^0 = e$, followed by the integral powers of $a^{p^{(n-1)}}$ in order, viz., $a^{kp^{(n-1)}}, k = 0, \ldots, p-1$. We note that this C_p contains the elements $a^i \in C_{p^n}$ with $gcd[i, p^n] = p^n$ or $p^{(n-1)}$. Next consider $a^{p^{(n-2)}}$ which generates a cyclic subgroup of C_{p^n} of order p^2. There is a decomposition of C_{p^2} into p cosets of subgroup C_p, viz., $\{a^{kp^{(n-2)}} C_p : k = 0, \ldots, p-1\}$. Note that this subgroup C_{p^2} contains the elements $a^i \in C_{p^n}$ with $gcd[i, p^n] = p^n, p^{(n-1)}$, or $p^{(n-2)}$.

Proof: continued

Proceed inductively, letting $a^{p^{(n-r)}}$ generate a cyclic subgroup of order p^r, denoted C_{p^r}, containing the $a^i \in C_{p^n}$, with $gcd[i, p^n] = p^n, p^{(n-1)}, \ldots,$ or $p^{(n-r)}$. There is the coset decomposition of C_{p^r} into p cosets of subgroup $C_{p^{(r-1)}}$, viz., $a^{kp^{(n-r)}} C_{p^{(r-1)}}, k = 0, \ldots, p-1$. The penultimate subgroup in this nest of subgroups, $C_{p^{(n-1)}}$, with order $p^{(n-1)}$, is generated by a^p, and this subgroup contains the elements $a^i \in C_{p^n}$ such that $gcd[i, p^n] = p^n, p^{(n-1)}, \ldots, p^2$, or p. The full group C_{p^n} admits a coset decomposition into p cosets of $C_{p^{(n-1)}}$, viz., $a^k C_{p^{(n-1)}}, k = 0, 1, \ldots, p-1$. The cosets corresponding to $k = 1, \ldots, p-1$ are the elements $a^i \in C_{p^n}$ such that $gcd[i, p^n] = 1$.

Proof: continued

We now observe some desired properties of the symmetric multiplication table of C_{p^n} whose first row is as described above. Each subgroup multiplication table, $M[C_{p^r}]$ is repeated in the form of a $p^r \times p^r$ square, repeated $p^{(n-r)}$ times down the main diagonal of the $p^n \times p^n$ square which is the entire multiplication table. In particular, all of the elements which do not generate all of C_{p^n} occur in the diagonal array $M[C_{p^{(n-1)}}] \otimes I_p$, while the elements a^i with $gcd[i, p^n] = 1$ fill the rest of the table. Replacing these generators with the number 1, and the non-generators with the number 0, we obtain the desired matrix. □

Eigenvectors/Eigenvalues revisited

One can immediately write down a complete set of eigenvectors, p^n of them, that work simultaneoulsly for all $\mathbb{I}[p]^{\otimes(r-1)} \otimes \Delta[p] \otimes {I_p}^{\otimes(n-r)}$, $r = n, \ldots, 1$, by forming all of the Kronecker products of the eigenvectors $\vec{e_k}[p]$ with n factors, viz.

Eigenvectors/Eigenvalues revisited

One can immediately write down a complete set of eigenvectors, p^n of them, that work simultaneoulsy for all $\mathbb{I}[p]^{\otimes(r-1)} \otimes \Delta[p] \otimes {I_p}^{\otimes(n-r)}$, $r = n, \ldots, 1$, by forming all of the Kronecker products of the eigenvectors $\vec{e_k}[p]$ with n factors, viz. $\otimes_{j=1}^{n} \vec{e_{k_j}}[p]$, $0 \leq k_j \leq p-1$.

Eigenvectors/Eigenvalues revisited

One can immediately write down a complete set of eigenvectors, p^n of them, that work simultaneoulsly for all $\mathbb{I}[p]^{\otimes(r-1)} \otimes \Delta[p] \otimes {I_p}^{\otimes(n-r)}$, $r = n, \ldots, 1$, by forming all of the Kronecker products of the eigenvectors $\vec{e_k}[p]$ with n factors, viz. $\otimes_{j=1}^{n} \vec{e_{k_j}}[p]$, $0 \leq k_j \leq p-1$.
Thus $\Delta[p]$ has $p-1$ eigenvalues of -1 and one eigenvalue of $p-1$.

Eigenvectors/Eigenvalues revisited

One can immediately write down a complete set of eigenvectors, p^n of them, that work simultaneoulsy for all $\mathbb{I}[p]^{\otimes(r-1)} \otimes \Delta[p] \otimes {I_p}^{\otimes(n-r)}$, $r = n, \ldots, 1$, by forming all of the Kronecker products of the eigenvectors $\vec{e_k}[p]$ with n factors, viz. $\otimes_{j=1}^{n} \vec{e_{k_j}}[p]$, $0 \leq k_j \leq p-1$.

Thus $\Delta[p]$ has $p-1$ eigenvalues of -1 and one eigenvalue of $p-1$.

The matrix $\mathbb{I}[p]^{\otimes(r-1)}$ has one eigenvalue of $p^{(r-1)}$ and $p^{(r-1)} - 1$ eigenvalues of 0.

Eigenvectors/Eigenvalues continued

Thus the set of eigenvalues of $\rho * \Phi[C_{p^r}] \otimes {I_p}^{(n-r)} =$

Eigenvectors/Eigenvalues continued

Thus the set of eigenvalues of $\rho * \Phi[C_{p^r}] \otimes {I_p}^{(n-r)} = \mathbb{I}[p]^{\otimes(r-1)} \otimes \Delta[p] \otimes {I_p}^{\otimes(n-r)},\ r = 1, \ldots, n$ is equal to the product of the sets of eigenvalues: the set (with multiplicities) of eigenvalues of $\mathbb{I}[p]^{\otimes(r-1)}$ times the set (with multiplicities) of the eigenvalues of $\Delta[p]$ times the set (with multiplicities) of the eigenvalues of ${I_p}^{(n-r)}$.

Eigenvectors/Eigenvalues continued

Thus the set of eigenvalues of $\rho * \Phi[C_{p^r}] \otimes {I_p}^{(n-r)} = \mathbb{I}[p]^{\otimes(r-1)} \otimes \Delta[p] \otimes {I_p}^{\otimes(n-r)},\ r = 1, \ldots, n$ is equal to the product of the sets of eigenvalues: the set (with multiplicities) of eigenvalues of $\mathbb{I}[p]^{\otimes(r-1)}$ times the set (with multiplicities) of the eigenvalues of $\Delta[p]$ times the set (with multiplicities) of the eigenvalues of ${I_p}^{(n-r)}$.

Thus we get the set :

$\{\{(p^{(r-1)}(p-1) = \phi[p^r],\ \text{multiplicity } 1\} \times \{-p^{(r-1)},\ \text{multiplicity } p{-}1\} \times \{0,\ \text{multiplicity } (p^{(r-1)}{-}1)p\}\}$, with this whole set repeated $p^{(n-r)}$ times because of the Kronecker factor of ${I_p}^{\otimes(n-r)}$.

Cyclic Groups of Order n, any Natural Number

Our next goal is to show that our Euler Φ-function is "multiplicative" in the number theoretic sense.
The "Euler Φ function is multiplicative proposition." This next Proposition is well known:

Proposition

If natural number $n = n_1 n_2$, where n_1 and n_2 are relatively prime natural numbers, i.e., gcd$[n_1, n_2[= 1$, then $c \in C_n = C_{n_1} \times C_{n_2}$ is a generator of C_n if and only if there exist generators $a_i \in C_{n_i}$, $i = 1, 2$, such that $c = a_1 a_2$. Thus the Euler function, $\rho * \Phi$, is Kronecker product multiplicative in the number theoretic sense.

Cyclic Groups of Order n, any Natural Number

Our next goal is to show that our Euler Φ-function is "multiplicative" in the number theoretic sense.
The "Euler Φ function is multiplicative proposition." This next Proposition is well known:

Proposition

If natural number $n = n_1 n_2$, where n_1 and n_2 are relatively prime natural numbers, i.e., gcd$[n_1, n_2[= 1$, then $c \in C_n = C_{n_1} \times C_{n_2}$ is a generator of C_n if and only if there exist generators $a_i \in C_{n_i}$, $i = 1, 2$, such that $c = a_1 a_2$. Thus the Euler function, $\rho * \Phi$, is Kronecker product multiplicative in the number theoretic sense.

Proof: Given the groups and notation in Proposition, if $M[C_{n_i}]$, $i = 1, 2$, are symmetric multiplication tables, it is useful to write a multiplication table for C_n as a formal Kronecker product: $M[C_n] = M[C_{n_1}] \otimes M[C_{n_2}]$.

proof cont.

It is then easy to see that $\rho[c] = \rho[a_1] \otimes \rho[a_2]$. Thus if $c_{i_1,i_2} = a_{i_1} a_{i_2}$, $1 \leq i_1 \leq \phi[n_1]$, and $1 \leq i_2 \leq \phi[n_2]$ are all of the generators involved, where ϕ is Euler's orginal ϕ-function, then it is not hard to see that $\Sigma_{i_1,i_2} \rho[c_{i_1,i_2}] = (\Sigma_{i_1} \rho[a_{i_1}]) \otimes (\Sigma_{i_2} \rho[a_{i_2}])$.

Remark

Remark

We have just used special properties of the permutation matrices $\rho[x]$. (For properties of the Kronecker product see Bernstein.) Note that while the Kronecker product is associative and distributes over addition, it is not *commutative. However, although in general $A \otimes B \neq B \otimes A$, they are related, cf., "cannonical shuffle." Now in this special case it is important and easy to see that $M[C_{n_1}] \otimes M[C_{n_2}]$ is permutation equivalent to $M[C_{n_2}] \otimes M[C_{n_1}]$, since the first row of the former corresponds to a decomposition of $C_{n_1} \times C_{n_2}$ into cosets of C_{n_1}, and the latter's first row corresponds to a decomposition of the same group into cosets of C_{n_2}.*

Cyclic Group: General Case

We now have the following formula for the matrix-valued Euler Φ-function of a cyclic group of order n.

Theorem

Given the unique factrorization of natural number $n = \prod_{i=1}^{s} p_i^{n_i}$, where the p_i are pairwise distinct primes for $i = 1, \ldots, s$, then one can express $C_n = C_{p_1^{n_1}} \times C_{p_2^{n_2}} \times \cdots \times C_{p_s^{n_s}}$, the direct product of prime-power cyclic groups. Thus

$$\rho * \Phi[C_n] = \bigotimes_{i=1}^{s} \mathbb{I}[p_i]^{\otimes(n_i - 1)} \otimes \Delta[p_i],$$

(up to permutation equivalence).

Proof: From the structure theorem for finite abelian cyclic groups, C_n can be expressed as the direct product of prime power cyclic groups as described.

proof cont.

If $M[C_{p^{n_i}}]$ is the symmetric multiplication table described in the proof of "Euler Prime Power Proposition," then write the formal Kronecker product: $\otimes_{i=1}^{s} M[C_{p^{n_i}}]$ (which is, $M[C_n]$, up to permutation equivalence). The theorem follows by inductively applying the Euler Prime Power and Kronecker Multiplicative Propositions."

Remark

Remark

It is a routine matter to write down the set of subgroups, $C_{\frac{n}{d}}$ of C_n, which is in bijection with the set of divisors d of n. Then, using a Corollary of the "Prime Power Proposition," one can write down the corresponding $\rho * \Phi[C_{\frac{n}{d}}]$ function for each embedded subgroup. Note that the divisors of n can be linearly ordered, or partially ordered by the divisor relation. Also the maps, $d \leftrightarrow \dfrac{n}{d}$, give two enumerations of the divisors of n. We use whichever is notationally convenient.

An Euler Φ-Function for Finite Abelian Groups

Given a finite abelian group G of order $n = \Pi_{i=1}^{r} p_i^{n_i}$, where the p_i are pairwise distinct primes, it is well known that

$$G = G[p_1] \times G[p_2] \times \cdots \times G[p_r],$$

a direct product, where the $G[p_i]$ are the subgroups of elements whose orders are powers of p_i, $i = 1, 2 \ldots, r$. (In fact, $G[p_i]$ is the Sylow p_i-group of G.)

Let's Look at one Sylow Subgroup

Now each $G[p_i]$ is itself the direct product of cyclic prime-power subgroups; thus

$$G[p_i] = C_{{p_i}^{s_{i_1}}} \times C_{{p_i}^{s_{i_2}}} \times \cdots \times C_{{p_i}^{s_{i_{t_i}}}},$$

Thus we need to extend the "Prime Power Proposition" to a result that "works" for direct products of prime power cyclic groups, of the *same* prime.

General Theorem for One Factor

Proposition

Let p be a prime natural number and let $G = G[p] = C_{p^{s_1}} \times C_{p^{s_2}} \times \cdots \times C_{p^{s_t}}$ be the direct product of cyclic prime-power subgroups with non-increasing integral powers of this prime p. To be specific, suppose that $s_1 = \cdots = s_m > s_{m+1} \geq \cdots \geq s_t$. Then the symmetric multiplication table for G can be written (up to permutation equivalence) in such a way that the Euler Φ-function can be defined for this group and satsifies:

$$\rho * \Phi[G] = \mathbb{I}[p^{-m} \prod_{k=1}^{t} p^{s_k}] \otimes \Delta[p^m].$$

Final Remark

Remark

To obtain this matrix each group element of maximal order, viz., order p^{s_1}, in the group multiplication table is replaced by the number 1. Thus "maximal order" generalizes "gcd =1" in this context.

THANKS FOR ATTENTION!