# SOME NEW EULER FUNCTIONS

Gary L. Mullen

Penn State University

mullen@math.psu.edu

Sept. 29, 2017

Euler's function $\phi(n)$ counts the number of $1 \leq a \leq n$ with $(a, n) = 1$.

Euler's function $\phi(n)$ counts the number of $1 \leq a \leq n$ with $(a, n) = 1$.

Such values of $a$ form a group of order $\phi(n)$.

Euler's function $\phi(n)$ counts the number of $1 \leq a \leq n$ with $(a, n) = 1$.

Such values of $a$ form a group of order $\phi(n)$.

**Theorem**

*If $p$ is a prime and $k \geq 1$ is an integer, then $\phi(p^k) = p^k - p^{k-1}$.*

Euler's function $\phi(n)$ counts the number of $1 \leq a \leq n$ with $(a, n) = 1$.

Such values of $a$ form a group of order $\phi(n)$.

**Theorem**

*If $p$ is a prime and $k \geq 1$ is an integer, then $\phi(p^k) = p^k - p^{k-1}$.*

**Theorem**

*The function $\phi$ is multiplicative so if $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

Euler's function $\phi(n)$ counts the number of $1 \leq a \leq n$ with $(a, n) = 1$.

Such values of $a$ form a group of order $\phi(n)$.

**Theorem**

*If $p$ is a prime and $k \geq 1$ is an integer, then $\phi(p^k) = p^k - p^{k-1}$.*

**Theorem**

*The function $\phi$ is multiplicative so if $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

Hence $\phi(n)$ can be determined for any $n$ if we know the factorization of $n$.

## A Generalization of Euler's Function

**Definition**

*Let* $b \geq 1$ *be an integer. Define the function* $\phi_b(n)$ *to be the number of* $1 \leq a \leq n$ *with*

$$(a, n) = (a - 1, n) = \cdots = (a - b + 1, n) = 1.$$

## A Generalization of Euler's Function

**Definition**

*Let $b \geq 1$ be an integer. Define the function $\phi_b(n)$ to be the number of $1 \leq a \leq n$ with*

$$(a, n) = (a-1, n) = \cdots = (a-b+1, n) = 1.$$

$\phi_1(n) = \phi(n)$

Some properties of the function $\phi_b(n)$.

**Theorem**

*If $p$ is a prime and $k \geq 1$ is an integer, then $\phi_b(p^k) = p^k - bp^{k-1}$.*

Some properties of the function $\phi_b(n)$.

**Theorem**

*If $p$ is a prime and $k \geq 1$ is an integer, then $\phi_b(p^k) = p^k - bp^{k-1}$.*

**Theorem**

*The function $\phi_b$ is multiplicative so if $(m, n) = 1$, then $\phi_b(mn) = \phi_b(m)\phi_b(n)$.*

Some properties of the function $\phi_b(n)$.

**Theorem**

*If $p$ is a prime and $k \geq 1$ is an integer, then $\phi_b(p^k) = p^k - bp^{k-1}$.*

**Theorem**

*The function $\phi_b$ is multiplicative so if $(m, n) = 1$, then $\phi_b(mn) = \phi_b(m)\phi_b(n)$.*

Hence $\phi_b(n)$ can be determined for any $n$ if we know the factorization of $n$.

## An Application to Latin Squares

**Theorem**

*(Keedwell/M, Disc. Math. 2005) If $q \geq 4$ is even, we may form $q - 1$ latin squares of order $q$ which are mutually $(5q - 4)$-orthogonal.*

## An Application to Latin Squares

**Theorem**

*(Keedwell/M, Disc. Math. 2005) If $q \geq 4$ is even, we may form $q-1$ latin squares of order $q$ which are mutually $(5q-4)$-orthogonal.*

Proof uses uniform cyclic neofields

## Theorem

*(Droz, PSU thesis, 2016) If* $q \geq 4$ *is even and* $q-1$ *is a prime, we may form* $q-3$ *latin squares of order* $q$ *which are mutually* $(q^2-2q+2)$*-orthogonal.*

## Theorem

*(Droz, PSU thesis, 2016) If* $q \geq 4$ *is even and* $q - 1$ *is a prime, we may form* $q - 3$ *latin squares of order* $q$ *which are mutually* $(q^2 - 2q + 2)$*-orthogonal.*

Proof uses cyclic uniform neofields

## Theorem

*(Droz, PSU thesis, 2016) If $q \geq 4$ is even and $q - 1$ is a prime, we may form $q - 3$ latin squares of order $q$ which are mutually $(q^2 - 2q + 2)$-orthogonal.*

Proof uses cyclic uniform neofields

## Problem

*If $q \geq 4$ is even, there are $\phi_2(q - 1)$ latin squares which are $(???)$-orthogonal.*

| $q$ | $\phi_2(q-1)$ |
|---|---|
| 4 | 1 |
| 6 | 3 |
| 8 | 5 |
| 10 | 3 |
| 12 | 9 |
| 14 | 11 |
| 16 | 3 |
| 18 | 15 |
| 20 | 17 |
| 22 | 5 |
| 24 | 21 |
| 26 | 15 |
| 28 | 9 |
| 30 | 27 |
| 32 | 29 |
| 34 | 9 |
| 36 | 15 |

# The Polynomial Euler Function

## Definition

*The function* $\Phi_q(N)$ *counts the number of polynomials over* $F_q$ *of degree less than the degree of* $N$ *which are relatively prime to* $N$*.*

# The Polynomial Euler Function

## Definition

*The function $\Phi_q(N)$ counts the number of polynomials over $F_q$ of degree less than the degree of $N$ which are relatively prime to $N$.*

Such polynomials form a group of order $\Phi_q(N)$.

# The Polynomial Euler Function

**Definition**

*The function $\Phi_q(N)$ counts the number of polynomials over $F_q$ of degree less than the degree of $N$ which are relatively prime to $N$.*

Such polynomials form a group of order $\Phi_q(N)$.

**Theorem**

*If $P$ is irreducible of degree $m$ over $F_q$ and $k \geq 1$ is an integer, then* $\Phi(P^k) = q^{mk} - q^{m(k-1)}$.

## The Polynomial Euler Function

### Definition

*The function $\Phi_q(N)$ counts the number of polynomials over $F_q$ of degree less than the degree of $N$ which are relatively prime to $N$.*

Such polynomials form a group of order $\Phi_q(N)$.

### Theorem

*If $P$ is irreducible of degree $m$ over $F_q$ and $k \geq 1$ is an integer, then $\Phi(P^k) = q^{mk} - q^{m(k-1)}$.*

### Theorem

*The function $\Phi_q(N)$ is multiplicative.*

# The Polynomial Euler Function

**Definition**

*The function $\Phi_q(N)$ counts the number of polynomials over $F_q$ of degree less than the degree of $N$ which are relatively prime to $N$.*

Such polynomials form a group of order $\Phi_q(N)$.

**Theorem**

*If $P$ is irreducible of degree $m$ over $F_q$ and $k \geq 1$ is an integer, then $\Phi(P^k) = q^{mk} - q^{m(k-1)}$.*

**Theorem**

*The function $\Phi_q(N)$ is multiplicative.*

Hence the function $\Phi_q(N)$ can be determined for any polynomial $N \in F_q[x]$ if the factorization of $N$ is known.

# The Polynomial Euler Function

**Definition**

*The function $\Phi_q(N)$ counts the number of polynomials over $F_q$ of degree less than the degree of $N$ which are relatively prime to $N$.*

Such polynomials form a group of order $\Phi_q(N)$.

**Theorem**

*If $P$ is irreducible of degree $m$ over $F_q$ and $k \geq 1$ is an integer, then $\Phi(P^k) = q^{mk} - q^{m(k-1)}$.*

**Theorem**

*The function $\Phi_q(N)$ is multiplicative.*

Hence the function $\Phi_q(N)$ can be determined for any polynomial $N \in F_q[x]$ if the factorization of $N$ is known.

## Definition

*If $c$ is non-negative integer, by $G_c$ we mean the unique polynomial in $F_p[x]$ such that $G_c(p) = c$.*

## Definition

*If $c$ is non-negative integer, by $G_c$ we mean the unique polynomial in $F_p[x]$ such that $G_c(p) = c$.*

For example, if $p = 5$ and $c = 193$, then

$$G_{193}(x) = x^3 + 2x^2 + 3x + 3$$

since

$$125 + 2(5^2) + 3(5) + 3 = 193.$$

### Definition

*Let* $N \in F_p[x]$ *and suppose* $n$ *is the smallest degree of any irreducible divisor of* $N$*. For* $b \in \{1, 2, \ldots, p^n - 1\}$*, we define the* **extended polynomial Euler function** $\Phi_b(N)$ *to be the number of polynomials* $A$ *of degree less than the degree of* $N$ *such that gcd*$(A - G_c, N) = 1$ *for all* $c \in \{0, 1, \ldots, b - 1\}$*.*

## Some Properties of the Function $\Phi_b(N)$

**Theorem**

*If $p$ is a prime and $P$ is irreducible of degree $m$ over $F_p$ and $k \geq 1$ is an integer, then $\Phi_b(P^k) = p^{mk} - bp^{m(k-1)}$.*

## Some Properties of the Function $\Phi_b(N)$

### Theorem

*If $p$ is a prime and $P$ is irreducible of degree $m$ over $F_p$ and $k \geq 1$ is an integer, then $\Phi_b(P^k) = p^{mk} - bp^{m(k-1)}$.*

### Theorem

*The function $\Phi_b(N)$ is multiplicative so if $(M, N) = 1$, then $\Phi_b(MN) = \Phi_b(M)\Phi_b(N)$.*

## Some Properties of the Function $\Phi_b(N)$

**Theorem**

*If $p$ is a prime and $P$ is irreducible of degree $m$ over $F_p$ and $k \geq 1$ is an integer, then $\Phi_b(P^k) = p^{mk} - bp^{m(k-1)}$.*

**Theorem**

*The function $\Phi_b(N)$ is multiplicative so if $(M, N) = 1$, then $\Phi_b(MN) = \Phi_b(M)\Phi_b(N)$.*

Hence $\Phi_b(N)$ can be determined for any polynomial $N$ if we know the factorization of $N$.

## Problem

*(1)* $\Phi(x^n - 1) = \Phi_1(x^n - 1)$ *counts the number of normal elements in* $F_{q^n}$ *over* $F_q$.

### Problem

*(1)* $\Phi(x^n - 1) = \Phi_1(x^n - 1)$ *counts the number of normal elements in* $F_{q^n}$ *over* $F_q$.
*(2)* $\Phi_b(x^n - 1)$ *counts the number of normal elements in* $F_{q^n}$ *over* $F_q$ *with property* $b \geq 1$.

## Problem

*(1)* $\Phi(x^n - 1) = \Phi_1(x^n - 1)$ *counts the number of normal elements in* $F_{q^n}$ *over* $F_q$.
*(2)* $\Phi_b(x^n - 1)$ *counts the number of normal elements in* $F_{q^n}$ *over* $F_q$ *with property* $b \geq 1$.
*(3) What is property* $b$*?*

## How to construct a uniform cyclic neofield of even order $q \geq 4$

$$N = \{0, 1, a, a^2, a^3, \ldots, a^{q-2}\}$$

## How to construct a uniform cyclic neofield of even order $q \geq 4$

$$N = \{0, 1, a, a^2, a^3, \ldots, a^{q-2}\}$$

Multiplication is cyclic

## How to construct a uniform cyclic neofield of even order $q \geq 4$

$$N = \{0, 1, a, a^2, a^3, \ldots, a^{q-2}\}$$

Multiplication is cyclic

Let $(u, q-1) = (u-1, q-1) = 1$. Then define

$$1 + a^r = a^{ur}$$

## How to construct a uniform cyclic neofield of even order $q \geq 4$

$$N = \{0, 1, a, a^2, a^3, \ldots, a^{q-2}\}$$

Multiplication is cyclic

Let $(u, q-1) = (u-1, q-1) = 1$. Then define

$$1 + a^r = a^{ur}$$

This gives the additive operation in the neofield.

## How to construct a uniform cyclic neofield of even order $q \geq 4$

$$N = \{0, 1, a, a^2, a^3, \ldots, a^{q-2}\}$$

Multiplication is cyclic

Let $(u, q-1) = (u-1, q-1) = 1$. Then define

$$1 + a^r = a^{ur}$$

This gives the additive operation in the neofield.

FACT: $\phi_2(q-1)$ counts the number of good values of $u$.

## A uniform cyclic neofield of order $q = 6$

Let $(u, q-1) = (u-1, q-1) = (u, 5) = (u-1, 5) = 1$ so we can take $u = 2$ (or $u = 3$ or $u = 4$). Then define $1 + a^r = a^{ur} = a^{2r}, r = 1, 2, 3, 4$

$1 + a = a^2$, $1 + a^2 = a^4$

$1 + a^3 = a^6 = a$, $1 + a^4 = a^8 = a^3$

| $+$ | $0$ | $1$ | $a$ | $a^2$ | $a^3$ | $a^4$ |
|---|---|---|---|---|---|---|
| $0$ | $0$ | $1$ | $a$ | $a^2$ | $a^3$ | $a^4$ |
| $1$ | $1$ | $0$ | $a^2$ | $a^4$ | $a$ | $a^3$ |
| $a$ | $a$ | $a^4$ | $0$ | $a^3$ | $1$ | $a^2$ |
| $a^2$ | $a^2$ | $a^3$ | $1$ | $0$ | $a^4$ | $a$ |
| $a^3$ | $a^3$ | $a^2$ | $a^4$ | $a$ | $0$ | $1$ |
| $a^4$ | $a^4$ | $a$ | $a^3$ | $1$ | $a^2$ | $0$ |

**THANK YOU!!!**