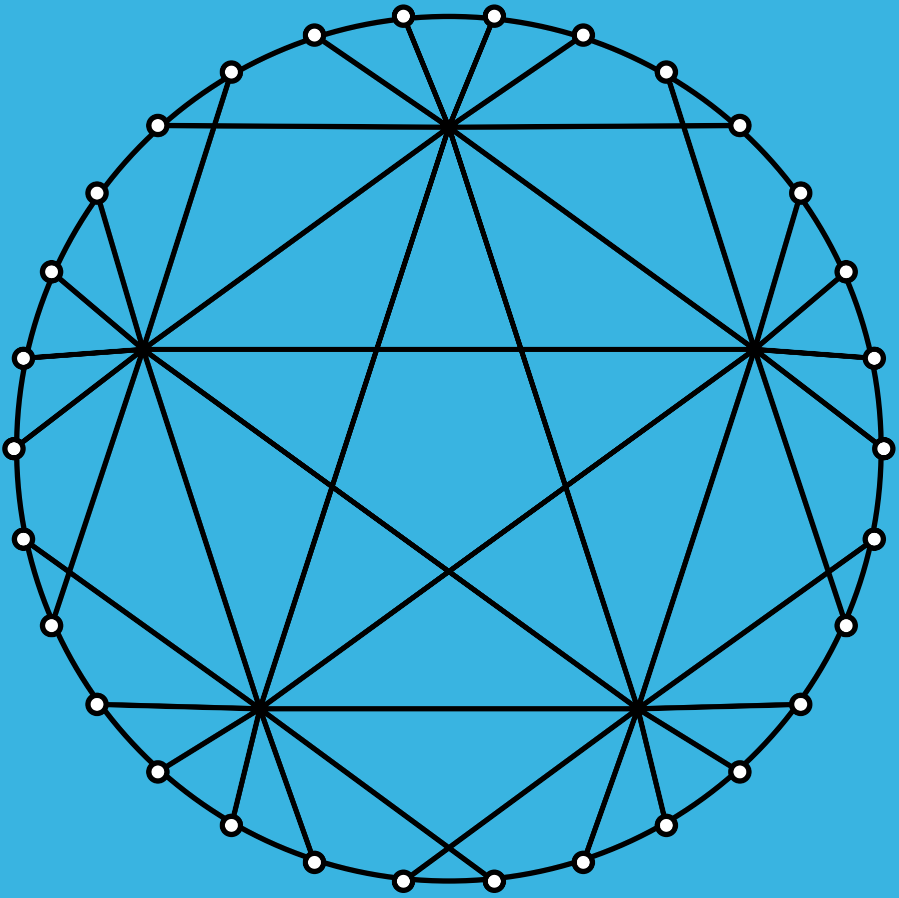
BULLETIN of the INSTITUTE of COMBINATORICS and its APPLICATIONS

Volume 85
February 2019

Editors-in-Chief: Marco Buratti, Donald Kreher, Tran van Trung



Boca Raton, FL, U.S.A.

ISSN 1182 - 1278

BULLETIN OF THE ICA
Volume **85** (2019), Pages 92–111

Two extended Euler functions with applications to latin squares and bases of finite field extensions

Gove Effinger[1] and Gary L. Mullen[2]

[1] *Skidmore College, Saratoga Springs, New York, USA.*
effinger@skidmore.edu
[2] *The Pennsylvania State University, University Park, Pennsylvania, USA.*
mullen@math.psu.edu

Abstract: We discuss two extensions of Euler phi functions, one old and one new. We first describe an extension, due originally to Schemmel, of the Euler ϕ function from elementary number theory. We then present an application of this extended function to the construction of uniform cyclic neofields, which are themselves useful in the construction of sets of latin squares having very uniform orthogonality properties. Next, we extend in an analogous way the polynomial Euler Φ function, which is used in the study of polynomials over finite fields. Finally, we study the relationship of our polynomial Euler function to normal bases in the finite field $\mathbf{F}_{p^n}$ where p is an odd prime.

1 An extended Euler phi function

The *Euler phi function* $\phi(n)$ of elementary number theory counts the number of positive integers less than a positive integer n which are relatively

Key words and phrases: Euler Phi Function, Neofields, Latin Squares, Polynomial Phi Function, Normal Bases of Finite Field Extensions.

AMS (MOS) Subject Classifications: 11A05,11T55,12E20,05B15

Received: 13 May 2018
Accepted: 11 October 2018

prime to n. It is easy to show that if p is a prime number and k is a positive integer, then $\phi(p^k) = p^{k-1}(p-1)$. Moreover, this function is *multiplicative* in the number theory sense, i.e., if n and m are relatively prime, then $\phi(nm) = \phi(n)\phi(m)$. Hence, since ϕ can be computed for prime powers, it can be computed for any positive integer n provided that n can be factored into its prime power representation. We shall use this meaning of "multiplicative" throughout this paper, including applying it to functions on polynomials in Section 3.

A natural extension of this well-known function was first proposed by Schemmel [7] in 1869. Though stated in a different manner, here is his definition:

Definition 1.1. Suppose $n > 1$ and q is the smallest prime dividing n. For $1 \leq b \leq q-1$, we define the *extended Euler phi function* $\phi_b(n)$ to be the number of elements a with $1 \leq a < n$ such that $\gcd(a-c, n) = 1$ for all $c = 0, 1, ..., b-1$. For all b, we define $\phi_b(1) = 1$.

Thus an integer a smaller than n will be counted by $\phi_b(n)$ only if *all* of $a, a-1, \ldots, a-b+1$ are relatively prime to n. It follows then that $\phi_1(n) \geq \phi_2(n) \geq \phi_3(n)$, and so on. Note that when $b = 1$, this is simply the standard Euler phi function. Finally, in the definition we restrict b to be less than q because, as one can check, $\phi_q(n)$ is always 0. Hence if $q = 2$, i.e., if n is even, our extended functions give no new information.

Example 1.1. Suppose $n = 35$ and $b = 3$. We check, for example, that neither 16 nor 17 satisfy the criteria to be counted by $\phi_3(35)$ since $16-1$ is divisible by 5, as is $17-2$. In fact, we see that the numbers which satisfy the criteria are 3, 4, 13, 18, 19, 24, 33, and 34. Hence $\phi_3(35) = 8$.

Schemmel stated, without proof and again in a different manner, the following two propositions. Both of these were proved by Goldschmidt in 1894, see page 147 of Dickson [1]. We shall include the proof of the first here since it is brief but omit the proof of multiplicativity.

Proposition 1.1. *Suppose p is a prime and $k \geq 1$ is a positive integer. Then $\phi_b(p^k) = p^{k-1}(p-b)$.*

Proof. From the set $\{1, 2, ..., p^k\}$ we must eliminate elements which are congruent to $0, 1, \ldots, b-1$ modulo p. Since there are exactly p^{k-1} elements in each of these congruence classes, we must eliminate a total of bp^{k-1} elements. Hence $\phi_b(p^k) = p^k - bp^{k-1} = p^{k-1}(p-b)$. □

Example 1.2. By Proposition 1.1, $\phi_3(25) = 10$. That set of elements is $\{3, 4, 8, 9, 13, 14, 18, 19, 23, 24\}$.

Here then is Schemmel's second proposition, proved, using the Chinese Remainder Theorem as the primary tool, by Goldschmidt as indicated in Dickson:

Proposition 1.2. *The function ϕ_b is multiplicative.*

Example 1.3. In Example 1.1 we saw directly that $\phi_3(35) = 8$. We can now get this result via Proposition 1.1, which tells us that $\phi_3(5) = 2$ and $\phi_3(7) = 4$, and Proposition 1.2, which tells us that $\phi_3(35) = \phi_3(5)\phi_3(7) = 8$.

A well-known (and very nice) result about the standard Euler phi function is that if we add up $\phi(d)$ over all positive divisors d of n, we obtain n as the sum. In a third proposition, Schemmel observed that essentially the same fact holds for the extended functions, *but* the terms of the summation must be weighted by powers of b. Though Goldschmidt provided a proof for a general composite n, we choose to include a version of it here applied to a prime power. In the general case, each term contains multiple powers of b.

Proposition 1.3. *If p is a prime and $k \geq 1$ is an integer, then*

$$\sum_{i=0}^{k} b^{k-i}\phi_b(p^i) = p^k.$$

Proof. Using the fact that for all b, $\phi_b(1) = 1$, we have

$$\begin{aligned}
&\sum_{i=0}^{k} b^{k-i}\phi_b(p^i) \\
= \quad & b^k + \sum_{i=1}^{k} b^{k-i}p^{i-1}(p-b) \\
= \quad & b^k + \sum_{i=1}^{k} b^{k-i}p^{i} - \sum_{i=1}^{k} b^{k-i+1}p^{i-1} \\
= \quad & b^k + \sum_{i=1}^{k} b^{k-i}p^{i} - \sum_{i=0}^{k-1} b^{k-i}p^{i} \\
= \quad & b^k + p^k - b^k = p^k,
\end{aligned}$$

as desired. □

In the final proposition of this section we give an explicit formula for the summation $\sum_{i=0}^{k} \phi_b(p^i)$. This can be generalized to arbitrary composite n because of the following easily proven fact: If $f(n)$ is a multiplicative function on the positive integers, then the function $g(n) = \sum_{d|n} f(d)$ is also multiplicative.

Proposition 1.4. *If p is a prime and $k \geq 1$ is an integer,*

$$\sum_{i=0}^{k} \phi_b(p^i) = \frac{p^k(p-b)+b-1}{p-1}.$$

Proof. By Proposition 1.1, we have

$$\phi_b(1)+\phi_b(p)+\phi_b(p^2)+\cdots+\phi_b(p^k) = 1+(p-b)+(p-b)p+\cdots+(p-b)p^{k-1}$$

$$= 1+(p-b)(1+p+\cdots+p^{k-1}) = 1+(p-b)\frac{p^k-1}{p-1}$$

$$= \frac{(p-1)+p^k(p-b)-(p-b)}{p-1} = \frac{p^k(p-b)+b-1}{p-1},$$

as claimed. □

Note that when $b=1$, we obtain the value p^k, as expected.

Example 1.4. As previously observed, for any given argument n, as b goes up from 1 to $q-1$, $\phi_b(n)$ goes down (because we are counting the elements of a subset of the previous set). In the case $n = p^k$, it is easy to compute that the difference between $\sum_{d|p^k} \phi_b(d)$ and $\sum_{d|p^k} \phi_{b+1}(d)$ is $\frac{p^k-1}{p-1}$. For example, if $n = 125$, $\sum \phi(d) = \sum \phi_1(d) = 125$, $\sum \phi_2(d) = 94$, $\sum \phi_3(d) = 63$, and $\sum \phi_4(d) = 32$, the differences being the constant $(125-1)/(5-1) = 31$. There will be no such simple pattern for n *not* a prime power.

Example 1.5. Using Proposition 1.4 and multiplicativity, we may now compute that $\sum_{d|35} \phi_1(d) = 35$, $\sum_{d|35} \phi_2(d) = 24$, $\sum_{d|35} \phi_3(d) = 15$, and $\sum_{d|35} \phi_4(d) = 8$.

In the following section, we examine an application of the functions $\phi_b(n)$ to the construction of "neofields" (algebraic structures which have almost all of the properties of a finite field) and latin squares derived from those neofields.

2 An application to the construction of neofields and latin squares

We begin this section with the definition of an algebraic structure which has applications in combinatorics in general and latin squares in particular:

Definition 2.1. A set N equipped with two operations $+$ (addition) and $\cdot$ (multiplication) is a *neofield* if

• Addition has a two-sided identity 0 and each element has a two-sided additive inverse;

• For any $a \in N$ the actions $x \to a + x$ and $x \to x + a$ are bijections;

• The non-zero elements of N form a group under multiplication; the multiplicative identity is 1 with $1 \neq 0$;

• Multiplication distributes over addition from both sides.

Hence a neofield differs from a field in that its addition need not be either commutative nor associative, and its multiplication need not be commutative. However, for our purposes here we will only consider a special class of neofields called *uniform cyclic neofields*, as follows.

Let m be an even integer greater than or equal to 4 and let

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

that is, $N \setminus \{0\}$ is a cyclic group generated by a.

In order to define addition in N, let u be a positive integer below $m - 1$ such that $\gcd(u, m-1) = \gcd(u-1, m-1) = 1$. Since m is even, $m - 1$ is odd and so we know from Section 1 that there are $\phi_2(m-1)$ possibilities for u. We now define addition in the neofield N by

$$1 + a^r = a^{ur}, r = 1, 2, \ldots, m-2.$$

As indicated in [2], the set N with these operations forms a *uniform cyclic neofield* of order m. The neofield N is called "uniform" since the addition is defined via the single number u. See also [4] for a detailed treatment of these ideas.

Notation. It will help us below to label a specific uniform cyclic neofield by $N_{m,u}$ where m is its order and u is the uniform exponent multiplier used to define the addition, as above.

Example 2.1. Let us construct two uniform cyclic neofields of order $m = 6$. Since there are $\phi_2(5) = 3$ choices for our u, specifically $u = 2, 3$ or 4, we first let $u = 2$ and construct $N_{6,2}$. Hence, as above, $1 + a^r = a^{ur} = a^{2r}, r = 1, 2, 3, 4$, i.e., we have

$$1 + a = a^2, 1 + a^2 = a^4, 1 + a^3 = a^6 = a, 1 + a^4 = a^8 = a^3.$$

Also, by the second bullet in Definition 2.1 and the fact that $1 + 0 = 1$, we must have that $1 + 1 = 0$. Given these facts, we can make use of the distributive law and the multiplicative cyclicity to do any additions, including that each element of our neofield is its own additive inverse. For example, $a + a^2 = a(1 + a) = a(a^2) = a^3$, whereas $a^2 + a = a^2(1 + a^{-1}) = a^2(1 + a^4) = a^2(a^3) = 1$. Thus the addition table for the uniform cyclic neofield $N_{6,2}$ is:

$+$	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

Next, we set $u = 3$ and construct the addition table for $N_{6,3}$ using the key rule of $1 + a^r = a^{3r}$ for $r = 1, 2, 3, 4$. We obtain

$$1 + a = a^3, 1 + a^2 = a^6 = a, 1 + a^3 = a^9 = a^4, 1 + a^4 = a^{12} = a^2.$$

Proceeding as before, here is the addition table for $N_{6,3}$:

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

We note that the addition operation in neofields need not be commutative or associative. In our two examples, the $u = 3$ addition is commutative, but the $u = 2$ addition is not.

Definition 2.2. A *latin square of order* m is an m by m array in which each of the numbers 0 through $m - 1$ appears once and only once in each row and column. Two latin squares of order m are said to be s*-orthogonal* if when superimposed, s out of the possible m^2 distinct ordered pairs appear. If $s = m^2$, the squares are said to be *orthogonal.*

We can produce $m - 1$ latin squares of order m from any uniform cyclic neofield of order m as follows: Fix k in the range 0 through $m-2$. Label the rows and columns as 0 through $m - 1$. In the $(0, 0)$ cell put 0. In the $(0, j)$ cells (i.e., the rest of Row 0), put a^{j-1}. In the $(i, 0)$ cells (i.e., the rest of Column 0) put $a^k a^{i-1}$. Finally, for all other cells (i, j), put $a^k a^{i-1} + a^{j-1}$. We note that when $k = 0$, we are simply copying the addition table of the neofield.

Notation. We shall refer to the latin square derived from the neofield $N_{m,u}$ using the number k in the above paragraph, as $A_{m,u,k}$.

Example 2.2. We now produce three latin squares of order 6, two from neofield $N_{6,2}$ and one from $N_{6,3}$. More specifically, we shall produce the latin squares $A_{6,2,0}$, $A_{6,3,0}$, and $A_{6,2,3}$. For the first two of these, the fact that $k = 0$ means that we turn the addition tables directly into latin squares. In all cases, in order for our latin squares to consist of the numbers 0 through 5 (not powers of a), we replace a^i with $i + 1$ for $i = 1, 2, 3, 4$.

So here, directly from the $N_{6,2}$ addition table above, is $A_{6,2,0}$:

$$\begin{array}{cccccc}
0 & 1 & 2 & 3 & 4 & 5 \\
1 & 0 & 3 & 5 & 2 & 4 \\
2 & 5 & 0 & 4 & 1 & 3 \\
3 & 4 & 1 & 0 & 5 & 2 \\
4 & 3 & 5 & 2 & 0 & 1 \\
5 & 2 & 4 & 1 & 3 & 0
\end{array}$$

and here, directly from the $N_{6,3}$ addition table above, is $A_{6,3,0}$:

$$\begin{array}{cccccc}
0 & 1 & 2 & 3 & 4 & 5 \\
1 & 0 & 4 & 2 & 5 & 3 \\
2 & 4 & 0 & 5 & 3 & 1 \\
3 & 2 & 5 & 0 & 1 & 4 \\
4 & 5 & 3 & 1 & 0 & 2 \\
5 & 3 & 1 & 4 & 2 & 0
\end{array}$$

For our third latin square $A_{6,2,3}$, we use the procedure described above, with all cells (i, j) not in Row 0 or Column 0 receiving the value $a^3 a^{i-1} + a^{j-1}$, and all cells then translated into numbers 0 through 5. So here is square $A_{6,2,3}$:

$$\begin{array}{cccccc}
0 & 1 & 2 & 3 & 4 & 5 \\
4 & 3 & 5 & 2 & 0 & 1 \\
5 & 2 & 4 & 1 & 3 & 0 \\
1 & 0 & 3 & 5 & 2 & 4 \\
2 & 5 & 0 & 4 & 1 & 3 \\
3 & 4 & 1 & 0 & 5 & 2
\end{array}$$

Having formed our three sample latin squares of order 6, we wish now to investigate the degree to which they are, in pairs, *orthogonal*, as defined in Definition 2.2. We superimpose the three pairings and then count the distinct ordered pairs in those arrays.

We first superimpose the squares $A_{6,2,0}$ and $A_{6,2,3}$ generated by the same neofield, (i.e., "Same u Different k"):

$$\begin{array}{cccccc}
(0,0) & (1,1) & (2,2) & (3,3) & (4,4) & (5,5) \\
(1,4) & (0,3) & (3,5) & (5,2) & (2,0) & (4,1) \\
(2,5) & (5,2) & (0,4) & (4,1) & (1,3) & (3,0) \\
(3,1) & (4,0) & (1,3) & (0,5) & (5,2) & (2,4) \\
(4,2) & (3,5) & (5,0) & (2,4) & (0,1) & (1,3) \\
(5,3) & (2,4) & (4,1) & (1,0) & (3,5) & (0,2)
\end{array}$$

Second, we superimpose the squares $A_{6,2,0}$ and $A_{6,3,0}$ generated from different neofields but both directly from the addition tables (i.e., "Different u Same k"):

$$\begin{array}{cccccc}
(0,0) & (1,1) & (2,2) & (3,3) & (4,4) & (5,5) \\
(1,1) & (0,0) & (3,4) & (5,2) & (2,5) & (4,3) \\
(2,2) & (5,4) & (0,0) & (4,5) & (1,3) & (3,1) \\
(3,3) & (4,2) & (1,5) & (0,0) & (5,1) & (2,4) \\
(4,4) & (3,5) & (5,3) & (2,1) & (0,0) & (1,2) \\
(5,5) & (2,3) & (4,1) & (1,4) & (3,2) & (0,0)
\end{array}.$$

Finally, we superimpose the squares $A_{6,3,0}$ and $A_{6,2,3}$ which differ both in their generating neofield *and* their row multiplier a^k (i.e., "Different u Different k"):

$$\begin{array}{cccccc}
(0,0) & (1,1) & (2,2) & (3,3) & (4,4) & (5,5) \\
(1,4) & (0,3) & (4,5) & (2,2) & (5,0) & (3,1) \\
(2,5) & (4,2) & (0,4) & (5,1) & (3,3) & (1,0) \\
(3,1) & (2,0) & (5,3) & (0,5) & (1,2) & (4,4) \\
(4,2) & (5,5) & (3,0) & (1,4) & (0,1) & (2,3) \\
(5,3) & (3,4) & (1,1) & (4,0) & (2,5) & (0,2)
\end{array}.$$

The reader is now invited to comb through these three arrays and count the number of distinct ordered pairs which appear and, if they do appear, how many times for each. We summarize below what will have been discovered:

Same u Different k	**Different u Same k**	**Different u Different k**
21 pairs appear once.	20 pairs appear once.	16 pairs appear once.
5 pairs appear 3 times.	5 pairs appear twice.	10 pairs appear twice.
	1 pair appears 6 times.	

Of course, these results are from only three out the $5\phi_2(5) = 15$ possible latin squares which can be generated by uniform cyclic neofields of order

6, so we do not know to what extent this data is anomalous. However, it turns out that this data does indeed point to counts which are consistent across all even orders m, with one caveat (see below). We now summarize what we know and what has been proven in [2] and [4] in our main result of this section.

Theorem 2.1. *For every $m \geq 4$ an even integer, there are $\phi_2(m-1)$ distinct uniform cyclic neofields of order m. Each of these neofields in turn can generate $m-1$ latin squares of order m, which we have denoted by $A_{m,u,k}$, where u identifies the generating neofield and k denotes the "row multiplier" used to generate the addition table. Concerning orthogonality of pairs of squares, there are then three general cases to consider:* (1) *A_{m,u,k_1} with A_{m,u,k_2} $(k_1 \neq k_2)$, (2) $A_{m,u_1,k}$ with $A_{m,u_2,k}$ $(u_1 \neq u_2)$, and* (3) *A_{m,u_1,k_1} with A_{m,u_2,k_2}* ($u_1 \neq u_2$ and $k_1 \neq k_2$)*.* In the latter two cases, we add the requirement that $m-1$ be a prime number*. Then the following counts always hold true:*

Same u **Different** k	**Different** u **Same** k	**Different** u **Different** k
$4m{-}3$ *pairs once.*	$(m{-}2)(m{-}1)$ *pairs once.*	$(m{-}2)^2$ *pairs once.*
$m{-}1$ *pairs 3 times.*	$m{-}1$ *pairs twice.*	$2m{-}2$ *pairs twice.*
	1 pair m times.	

Hence we conclude that the latin squares A_{m,u,k_1} and A_{m,u,k_2} are $(5m-4)$-orthogonal, and if $m-1$ is prime, $A_{m,u_1,k}$ and $A_{m,u_2,k}$ are (m^2-2m+2)-orthogonal, as are A_{m,u_1,k_1} and A_{m,u_2,k_2}.

At this time it is not known what the level of orthogonality is for pairs of latin squares generated by different neofields when $m-1$ is *not* prime. The reader may wish to study this problem, the smallest case obviously being $m = 10$.

Finally, we make a brief transition to the next section by bringing in the finite field $\mathbf{F}_q$ of order q. Please note that whereas q played the role of the smallest prime dividing n in Section 1, from here on in this paper it will represent a power of a prime number p.

Suppose we generate $q-1$ distinct latin squares via the arithmetic of the finite field $\mathbf{F}_q$ using the linear polynomial $ai + j$ to fill in each (i, j) cell (with a a fixed nonzero element of $\mathbf{F}_q$ for each square). Then in fact it is known that *every pair of squares in this set are orthogonal.* So for example, if we denote latin squares of this type by $B_{q,a}$, then here are $B_{5,1}$, $B_{5,3}$, and their superimposition:

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

$(0,0)$	$(1,1)$	$(2,2)$	$(3,3)$	$(4,4)$
$(1,3)$	$(2,4)$	$(3,0)$	$(4,1)$	$(0,2)$
$(2,1)$	$(3,2)$	$(4,3)$	$(0,4)$	$(1,0)$
$(3,4)$	$(4,0)$	$(0,1)$	$(1,2)$	$(2,3)$
$(4,2)$	$(0,3)$	$(1,4)$	$(2,0)$	$(3,1)$

The reader can check that all possible ordered pairs appear exactly once.

Hence we see in general that sets of latin squares generated by a given finite field display greater orthogonality than those generated by a given neofield. For example, any two squares generated by $N_{8,2}$ are, by Theorem 2.1, 36-orthogonal, whereas any two squares generated by $\mathbf{F}_8$ are 64-orthogonal. In fact, *it is an unproved conjecture that a set of $n-1$ latin squares of order n can be all pairwise orthogonal if and only if n is a prime power.* See, for example, [6] for a discussion of these ideas.

3 An extension of the polynomial Euler function

If q is a prime power, let $\mathbf{F}_q$ denote the finite field of order q and let $\mathbf{F}_q[x]$ denote the ring of all polynomials in the indeterminate x over $\mathbf{F}_q$. It is a fact that this ring has a great deal in common with the ring $\mathbb{Z}$ of integers. For example, monic (i.e., leading coefficient 1) irreducible polynomials in $\mathbf{F}_q[x]$ play the role of prime numbers in $\mathbb{Z}$, and both rings have unique factorization. Moreover, the density of monic irreducibles in $\mathbf{F}_q[x]$ closely matches the density of primes in $\mathbb{Z}$. Thus many number theoretic results in $\mathbb{Z}$ can be explored and possibly verified in $\mathbf{F}_q[x]$ as well. For a discussion of many of the parallels between these two domains, see, for example, [3].

Hence it is no surprise that the standard integer Euler phi function ϕ defined in Section 1 has an analogue Φ in the ring of polynomials over a finite field, defined as follows:

Definition 3.1. Suppose $f \in \mathbf{F}_q[x]$ is of degree $m > 0$. Then *the polynomial Euler function* $\Phi(f)$ counts the number of polynomials over $\mathbf{F}_q$ of degree less than m which are relatively prime to f. If $\deg(f) = 0$, we define $\Phi(f) = 1$.

One can show (see, for example, [5], Lemma 3.69) that the value of $\Phi(P^k)$, where $P \in \mathbf{F}_q[x]$ is irreducible of degree m and $k \geq 1$, is $q^{(k-1)m}(q^m - 1)$. Recalling from the beginning of Section 1 that $\phi(p^k) = p^{k-1}(p-1)$, this result simply replaces p with q^m. Moreover, the function Φ is multiplicative, so we can compute the value of Φ for arbitrary polynomials in $\mathbf{F}_q[x]$ provided that we can factor them into the product of powers of irreducible polynomials.

We would now like to extend the polynomial Euler function Φ in a way analogous to the way the integer Euler function ϕ was extended in Section 1 to the function ϕ_b. In order to simplify our statements and arguments here, we assume for now that we are working over $\mathbf{F}_p$, a finite field of *prime* (as opposed to prime power) order p. Later we will discuss generalizing our ideas to arbitrary finite fields. We first provide a natural order to list the polynomials over the field $\mathbf{F}_p$.

Definition 3.2. If c is a non-negative integer, then c possesses a unique base p representation. Using this fact, by G_c we mean the unique polynomial in $\mathbf{F}_p[x]$ such that $G_c(p) = c$. For example, if $p = 5$ and $c = 193$, then $G_{193} = x^3 + 2x^2 + 3x + 3$ since $5^3 + 2(5^2) + 3(5) + 3 = 193$.

We are now ready to define an extended polynomial Euler function Φ_b for $\mathbf{F}_p[x]$ where p is prime.

Definition 3.3. Suppose $f \in \mathbf{F}_p[x]$ is of positive degree and assume that n is the smallest degree of any irreducible divisor of f. For $b \in \{1, 2, ..., p^n - 1\}$, define the *extended polynomial Euler function* $\Phi_b(f)$ to be the number of polynomials A of degree less than the degree of f such that $\gcd(A - G_c, f) = 1$ for all $c \in \{0, 1, ..., b-1\}$. If $\deg(f) = 0$, we define $\Phi_b(f) = 1$ for all b.

Proposition 3.1. *Let P be an irreducible polynomial of degree m over $\mathbf{F}_p$ and let k be a positive integer. Then $\Phi_b(P^k) = p^{(k-1)m}(p^m - b)$.*

Proof. Though a bit more involved, the argument here runs directly parallel to the argument proving Proposition 1.1. Starting with the p^{km} polynomials A of degree less than km, we must remove those which have any of the properties that $A = QP$, $A - C_1 = QP$,..., $A - C_{b-1} = QP$. That is, we remove all polynomials A which fall in the sets $A = QP$, $A = QP + C_1$,..., $A = QP + C_{b-1}$, where the polynomials Q range over all polynomials of degree less than $m(k-1)$, of which there are $p^{m(k-1)}$ polynomials. Finally, we claim that the b sets above are pair-wise disjoint, for if $Q_1P + C_{a_1} = Q_2P + C_{a_2}$, we have $P(Q_1 - Q_2) = C_{a_2} - C_{a_1}$. However, if Q_1 and Q_2 differ, then the degree of the left-hand side is greater than or equal to m, but the degree of the right-hand side is less than m since $b \leq p^m - 1$.

It follows then that $Q_1 = Q_2$, thus forcing $C_{a_1} = C_{a_2}$. Hence the sets are all pair-wise disjoint, and we arrive then at bp^{km-m} polynomials A which need to be discarded, and our count becomes $p^{km} - bp^{(k-1)m} = p^{(k-1)m}(p^m - b)$, completing the proof. □

Note the similarity of this proposition's formula to that of Proposition 1.1. Also note that if $b = 1$, this formula corresponds to the formula for $\Phi(P^k)$ previously stated just after Definition 3.1.

Example 3.1. Let $P = x^3 + x^2 + 3x + 1$, which is irreducible over $\mathbf{F}_5$. According to Proposition 3.1, we have $\Phi_3(P^2) = 5^3(5^3 - 3) = 15,250$, and $\Phi_{18}(P^2) = 5^3(5^3 - 18) = 13,375$. These values can be confirmed by simply counting polynomials using, for example, *Mathematica.*

It remains to show that the function Φ_b is multiplicative, for then it can be computed for arbitrary polynomials of degree at least 1 over $\mathbf{F}_p$ via Proposition 3.1. The argument proving multiplicativity of Φ_b, as expected, runs entirely parallel to the argument made originally by Goldshcmidt on the function ϕ_b, but here using as the primary tool the Chinese Remainder Theorem as applied to polynomials over a finite field, as done in the previously cited [5]. Hence we again omit the proof.

Proposition 3.2. *The function Φ_b is a multiplicative function on $\mathbf{F}_p[x]$.*

Example 3.2. Suppose P is as in Example 3.1 above and let $Q = x^3 + 4x^2 + x + 1$, which is also irreducible over $\mathbf{F}_5$. Then *Mathematica* confirms that $\Phi_{18}(PQ) = \Phi_{18}(P)\Phi_{18}(Q) = (125 - 18)^2 = 11,449$.

Continuing with the parallels between $\mathbb{Z}$ and $\mathbf{F}_p[x]$, we now state the analogues of Propositions 1.3 and 1.4 on summing over divisors. In both cases the proofs run exactly parallel to the proofs of those results, so we leave them to the reader. We of course need Definition 3.3 and Proposition 3.1.

Proposition 3.3. *Suppose P is a monic irreducible polynomial of degree m over $\mathbf{F}_p$ and $k \geq 1$. Then*

$$\sum_{i=0}^{k} b^{k-i}\Phi_b(P^i) = p^{mk} = p^{\deg(P^k)}.$$

Proposition 3.4. *Suppose P is a monic irreducible polynomial of degree m over $\mathbf{F}_p$ and $k \geq 1$ then*

$$\sum_{i=0}^{k} \Phi_b(P^i) = \frac{p^{mk}(p^m - b) + b - 1}{p^m - 1}.$$

Exactly as in Section 1, multiplicativity of the summation function tells us that we can compute the summation in Proposition 3.4 for an arbitrary monic polynomial F over $\mathbf{F}_p$. We also note that by setting $b = 1$ in Proposition 3.4 we obtain $p^{mk} = p^{\deg(P^k)}$, so for an arbitrary monic f we will obtain $p^{\deg(F)}$, as expected.

As mentioned earlier in this section, the definition and propositions about Φ_b can easily be extended to arbitrary finite fields $\mathbf{F}_q$ where $q = p^k$ for some prime p. To do this, the elements of $\mathbf{F}_q$ can be viewed as the p^k polynomials of degree less than k in, say, a variable θ. This then provides a natural ordering of the elements of $\mathbf{F}_q$, and we can proceed as above. However, we must caution that though this *ordering* of the elements of $\mathbf{F}_q$ is canonical, the *arithmetic* for manipulating them is *not* canonical. To do the arithmetic, we must select and fix a monic irreducible polynomial P of degree k over $\mathbf{F}_p$, and then do polynomial arithmetic mod P on our elements.

Example 3.3. We consider the finite field $\mathbf{F}_9$. Its elements can be put in the natural order $\{0, 1, 2, \theta, \theta+1, \theta+2, 2\theta, 2\theta+1, 2\theta+2\}$ with all arithmetic being done, say, modulo the irreducible $P = \theta^2 + 1$ over $\mathbf{F}_3$. Hence the element 0 is represented by the number 0, the element $\theta + 2$ by the number 5, and so on. Now suppose we have the polynomial $f(x) = x^2 + (\theta+2)x + 1$, then $f(9) = 9^2 + 5(9) + 1 = 127$, and so in the notation of this section, $G_{127} = f(x)$.

With this agreement, all the results of this section generalize from $\mathbf{F}_p[x]$ to $\mathbf{F}_q[x]$.

We now study how the function Φ_b is related to normal bases of the extension field $\mathbf{F}_{p^n}$ over the base field $\mathbf{F}_p$.

4 An application to normal bases

An element α of $\mathbf{F}_{p^n}$ is called *normal* if the elements $\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}\}$ form a basis (called a *normal basis*) for $\mathbf{F}_{p^n}$ over $\mathbf{F}_p$. The elements of this basis are called the *p-conjugates* of α, and we note that by definition, all these p-conjugates are themselves normal. It is known (see, for example, Theorem 3.73 of [5]) that the number of normal elements of $\mathbf{F}_{p^n}$ is given by $\Phi(t^n - 1)$, which is why normal bases are of interest to us in this paper.

Definition 4.1. If an element α in $\mathbf{F}_{p^n}$ has the property that $\alpha, \alpha - 1, \alpha - 2, \ldots, \alpha - (b-1)$ are all normal, we say that α has *normal depth b*.

Our generalized Φ_b function from Section 3 now comes into play, because $\Phi_b(t^n - 1)$ will count the number of elements in $\mathbf{F}_{p^n}$ of normal depth b. As in Section 2, where we focused on the function ϕ_2, here we focus on elements α which have normal depth 2, the number of which will be counted by the function $\Phi_2(t^n - 1)$.

Notation. We shall denote by N the set of elements of $\mathbf{F}_{p^n}$ which are normal, i.e., which are counted by $\Phi(t^n - 1)$, and by N_2 the subset of N whose elements are of normal depth 2, i.e., are counted by $\Phi_2(t^n - 1)$. In general, we shall denote elements of $\mathbf{F}_{p^n}$ either as polynomials $a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$, where each a_i is in $\mathbf{F}_p$, or as the vector of coefficients $(a_{n-1}, \ldots, a_1, a_0)$.

A key advantage of working with normal bases is the following: *the p-conjugates of any element can be identified by simply rotating its coefficients.* For a full discussion of the procedure for forming normal bases, please see [5], Section 3.4 on linearized polynomials. Here we simply give an example. Suppose $n = 3$, $p = 5$ and $\alpha = t^2 + 4t + 2$, which is in fact a normal element of $\mathbf{F}_{125}$. We replace α by its *associated linearized polynomial* $t^{25} + 4t^5 + 2t$ (i.e., this is "linearized" since each exponent is a power of 5). But now its first 5-conjugate is $(t^{25} + 4t^5 + 2t)^5 = t^{125} + 4t^{25} + 2t^5 = 4t^{25} + 2t^5 + t$ since in our field $t^{125} = t$. Thus we see that the coefficients have been rotated one place to the left. Finally, we rewrite this 5-conjugate in its "conventional" form, i.e., $4t^2 + 2t + 1$. In the same way, α's other 5-conjugate is $2t^2 + t + 4$.

The main question we now explore is: To what extent do the p-conjugates of an element α of normal depth 2 themselves have normal depth 2? Put another way, to what extent are normal bases preserved under this "depth" operation.

Definition 4.2. We call an element α which is of normal depth 2 (i.e., is an element of N_2) *lonely* if at least one of its p-conjugates fails to have normal depth 2 (i.e., is not present in N_2).

In the following chart, we show for the elements of $\mathbf{F}_{p^n}$ the factorization of $t^n - 1$ over $\mathbf{F}_p$, the value of $\Phi_2(t^n - 1)$, the number of normal bases contained within N_2, and the number of lonely elements in N_2. Note that of necessity, we always have n(Normal bases) + Lonely elements = $\Phi_2(t^n - 1)$.

n	p	Factorization	$\Phi_2(t^n-1)$	Normal	Lonely
		of t^n-1		bases	elements
2	3	$(t-1)(t+1)$	1	0	1
	5	$(t-1)(t+1)$	9	3	3
	7	$(t-1)(t+1)$	25	10	5
	11	$(t-1)(t+1)$	81	36	9
	13	$(t-1)(t+1)$	121	55	11
	17	$(t-1)(t+1)$	225	105	15
3	3	$(t-1)^3$	9	3	0
	5	$(t-1)(t^2+t+1)$	69	21	6
	7	$(t-1)(t+3)(t+5)$	125	15	80
	11	$(t-1)(t^2+t+1)$	1071	351	18
	13	$(t-1)(t+4)(t+10)$	1331	297	440
	17	$(t-1)(t^2+t+1)$	4305	1425	30
	19	$(t-1)(t+8)(t+12)$	4913	1275	1088
4	3	$(t-1)(t+1)(t^2+1)$	7	0	7
	5	$(t-1)(t+1)(t+2)(t+3)$	81	0	81
	7	$(t-1)(t+1)(t^2+1)$	1175	220	295
	11	$(t-1)(t+1)(t^2+1)$	9639	2088	1287
	13	$(t-1)(t+1)(t+5)(t+8)$	14,641	1760	7601
5	3	$(t-1)(t^4+t^3+t^2+t+1)$	79	15	4
	5	$(t-1)^5$	1875	375	0
	7	$(t-1)(t^4+t^3+t^2+t+1)$	11,995	2395	20
6	3	$(t-1)^3(t+1)^3$	81	0	81
	5	$(t-1)(t+1)(t^2+t+1)(t^2-t+1)$	4761	378	2493

The reader can look for patterns here, which may be elusive, but a couple of patterns should jump out. First, when $n=p=3$ and $n=p=5$, there are no lonely elements. Second, whenever $t^{n-1}+t^{n-2}+\cdots+t+1$ is irreducible, the number of lonely elements is $(n-1)(p-2)$. We now show that these two patterns hold true in general.

Proposition 4.1. *For all odd primes p, if $n=p$, then N_2 contains no lonely elements.*

Proof. Because $n=p$ and because $t^p-1=(t-1)^p$, we see that $\alpha=(a_{p-1}t^{p-1}+a_{p-2}t^{p-2}+\cdots+a_1t+a_0)$ is of normal depth 2 if and only if both it and $\alpha-1$ are not divisible by $t-1$. It is easy to show (using long division) that an element is relatively prime to $t-1$ if and only if the sum of its coefficients is not congruent to 0 mod p. Hence α will be of normal depth 2 (i.e., in N_2) if the sum of its coefficients modulo p is neither 1 nor 0. But the coefficients of all of α's p-conjugates also have that same sum (as they have only been rotated), so they too are of normal depth 2. We conclude that N_2 contains no lonely elements. □

On the other hand, we can say the following:

Proposition 4.2. *The value $\Phi_2(t^n-1)$ is odd for all odd primes p. Hence if n is even, N_2 will contain an odd number of lonely elements. In particular, if n is even, there will always be at least one lonely element.*

Proof. For all odd primes p, regardless of how t^n-1 factors over $\mathbf{F}_p$, all factors of $\Phi_2(t^n-1)$ are of the form p^i or $(p^j-2)^k$ for some i, j and k. Since every factor is odd, $\Phi_2(t^n-1)$ is odd. If n is even, then the number of elements of N_2 which form normal bases within N_2 must be even. Hence the number of lonely elements must be odd, and in particular greater than 0. □

We now turn to the second pattern in the chart by first looking at an example.

Example 4.1. Suppose $n=3$ and $p=5$. Note from the chart that t^2+t+1 is irreducible over $\mathbf{F}_5$ and that $\Phi_2(t^3-1)=(5-2)(25-2)=69$, i.e., there are 69 elements α in $\mathbf{F}_{125}$ which have the property that both α and $\alpha-1$ are relatively prime to both $t-1$ and t^2+t+1. We list below these elements, arranged first by the sum of their coefficients modulo 5 and within that together with their 3-conjugates (which, recall, are simply rotations of the coefficients), with those sets separated by semi-colons:

Sum = 2:

$\{(2,3,2),(3,2,2);(0,0,2),(0,2,0),(2,0,0);(0,1,1),(1,0,1),(1,1,0);$
$(0,3,4),(3,4,0),(4,0,3);(0,4,3),(4,3,0),(3,0,4);(1,2,4),(2,4,1),(4,1,2);$
$(1,3,3),(3,3,1),(3,1,3);(1,4,2),(4,2,1),(2,1,4)\}$

Sum = 3:

$\{(0,4,4),(4,0,4);(0,0,3),(0,3,0),(3,0,0);(0,1,2),(1,2,0),(2,0,1);$
$(0,2,1),(2,1,0),(1,0,2);(1,3,4),(3,4,1),(4,1,3);(1,4,3),(4,3,1),(3,1,4);$
$(2,2,4),(2,4,2),(4,2,2);(2,3,3),(3,3,2),(3,2,3)\}$

Sum = 4:

$\{(1,2,1),(2,1,1);(0,0,4),(0,4,0),(4,0,0);(0,1,3),(1,3,0),(3,0,1);$
$(0,3,1),(3,1,0),(1,0,3);(0,2,2),(2,2,0),(2,0,2);(1,4,4),(4,4,1),(4,1,4);$
$(2,3,4),(3,4,2),(4,2,3);(2,4,3),(4,3,2),(3,2,4)\}$

Note that, as predicted by our chart, 21 normal bases are present, but the first pair of elements for each sum is missing a 3-conjugate, and so there are

6 lonely elements. The 3 elements which are missing are $(2,2,3)$, $(4,4,0)$ and $(1,1,2)$.

We can now state and prove the general result:

Proposition 4.3. *If the polynomial $t^{n-1}+t^{n-2}+\cdots+t+1$ is irreducible over $\mathbf{F}_p$ for an odd prime p, then N_2 contains exactly $(n-1)(p-2)$ lonely elements, and so the number of normal bases inside N_2 is $(p-2)(p^{n-1}-n-1)/n$.*

Proof. We assume that $t^{n-1}+t^{n-2}+\cdots+t+1$ is irreducible over $\mathbf{F}_p$. Suppose $\alpha=(a_{n-1},a_{n-2},\ldots,a_1,a_0)$ is an element of $\mathbf{F}_{p^n}$ which has the property that both α and $\alpha-1$ are relatively prime to $t-1$, and let us denote the set of all such elements as S_{t-1}. As we already observed in the proof of Proposition 4.1, an element is relatively prime to $t-1$ if and only if the sum of its coefficients is not congruent to 0 mod p. Hence α has the property that $\sum_{i=0}^{n-1} a_i \mod p \neq 0$ and 1. It follows that the number of elements in S_{t-1} is $p^{n-1}(p-2)$. We also observe that if α is in S_{t-1} *then so are all of its p-conjugates* (since we merely rotate the coefficients, maintaining their sum).

Now, $\Phi_2(t^n-1)=(p-2)(p^{n-1}-2)$, and so the number of elements which are in S_{t-1} but not in N_2 is $p^{n-1}(p-2)-(p-2)(p^{n-1}-2)=2(p-2)$. These are elements β in S_{t-1} for which either β or $\beta-1$ is divisible by $t^{n-1}+t^{n-2}+\cdots+t+1$. Thus β is of the form $(a,a,\ldots,a,a)$ or $(a,a,\ldots,a,a+1)$. For the former form, if $na\equiv 0 \mod p$, a must be 0 since $n \mod p$ cannot be 0 (if $n=kp$ then $t^{kp}-1=(t^k-1)^p$). If $na\equiv 1 \mod p$, then $a=(n \mod p)^{-1}$. Neither of these elements $(0,0,\ldots,0)$ and $((n \mod p)^{-1},(n \mod p)^{-1},\ldots,(n \mod p)^{-1})$ is in S_{t-1}, but the other $p-2$ elements of this form *are* in S_{t-1} but not in N_2. We also observe that all of the p-conjugates of each of these elements are identical to the element itself, so removing it creates no lonely elements in N_2. Moving to the latter form $(a,a,\ldots,a,a+1)$, by a similar argument we see that though $(0,0,\ldots,0,1)$ and $(-(n \mod p)^{-1},-(n \mod p)^{-1},\ldots,-(n \mod p)^{-1}+1)$ are not in S_{t-1}, the other $p-2$ elements of this form are in S_{t-1} but not in N_2. This then accounts for our $2(p-2)$ elements β cited above. However, in this latter case, as opposed to the former, each of these $p-2$ elements has $n-1$ p-conjugates, all of which are in N_2 since if γ, say, is any one of them, neither γ nor $\gamma-1$ is divisible by $t^{n-1}+t^{n-2}+\cdots+t+1$. Hence we have identified the predicted $(n-1)(p-2)$ lonely elements in N_2.

Finally then, since $\Phi_2(t^n-1)=(p-2)(p^{n-1}-2)$, the number of normal bases in N_2 is

$$\frac{(p-2)(p^{n-1}-2)-(n-1)(p-2)}{n}=\frac{(p-2)(p^{n-1}-n-1)}{n}. \quad \square$$

Let us single out the special cases $n = 2$ and $n = 3$ in the following two corollaries:

Corollary 4.1. *For $n = 2$ and all odd primes p, N_2 contains $p - 2$ lonely elements and hence $(p - 2)(p - 3)/2$ normal bases.*

Proof. The polynomial $t+1$ is always irreducible, so Proposition 4.3 applies. □

Corollary 4.2. *For $n = 3$ and all primes p of the form $3k + 2$ for some $k > 0$, N_2 contains $2(p - 2)$ lonely elements and hence $(p - 2)^2(p + 2)/3$ normal bases.*

Proof. The roots of $t^2 + t + 1$ are $(-1 \pm \sqrt{-3})/2$. Using an argument attributed to Gauss, one can show that if p is of the form $3k+2$, then -3 is a non-quadratic residue mod p, so t^2+t+1 is irreducible (see, for example, [8], Chapter 24.) We now apply Proposition 4.3. □

There are no doubt numerous other patterns to be discovered and discussed here. For example, here are three possible lines of inquiry:

1. In the case $n = 3$, we have established general patterns when $p = 3$ and p of the form $3k + 2$. What about p of the form $3k + 1$?

2. Why are there *no* normal bases within N_2 in the cases of $n = 4$, $p = 3$ or 5, and $n = 6$, $p = 3$?

3. In a different direction: What happens with normal bases for elements of normal depth 3, or 4, or b?

The possibilities go on, but we choose to finish at this point in hopes that the reader will explore further.

Acknowledgment. The authors wish to sincerely thank Sophie Huczynska, Senior Lecturer at University of Saint Andrews, Saint Andrews, Scotland, for contributing various helpful ideas to this paper. We also wish to thank the two referees for their careful reading and constructive comments on the previous draft.

References

[1] L.E. Dickson, *History of the Theory of Numbers. Vol. I: Divisibility and Primality*, Chelsea Publishing Co., New York 1966.

[2] D. Droz, *Orthogonal Sets of Latin Squares and Class-r Hypercubes Generated by Finite Algebraic Systems*, Ph.D. Thesis, Penn State University, May 2016.

[3] G. Effinger, K. Hicks, and G.L. Mullen, Integers and polynomials: comparing the close cousins $\mathbb{Z}$ and $\mathbf{F}_q[x]$, *Math. Intelligencer*, **27** (2005), vol 2, 26–34.

[4] A.D. Keedwell and G.L. Mullen, Sets of partially orthogonal latin squares and projective planes, *Discrete Math.*, **288** (2004), 49–60.

[5] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications*, Vol. 20, Sec. ed., Cambridge University Press, Cambridge, 1997.

[6] G.L. Mullen, A candidate for the “next Fermat problem”, *Math. Intelligencer*, **17** (1995), 18–22.

[7] V. Schemmel, Über relative Primzahlen, *Journal für die reine und angewandte Mathematik*, **70** (1869), 191–192.

[8] J.H. Silverman, *A Friendly Introduction to Number Theory*, Prentice Hall, 2006.