JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **31**, No. 3, August 2018
http://dx.doi.org/10.14403/jcms.2018.31.1.309

GALOIS POLYNOMIALS FROM QUOTIENT GROUPS

Ki-Suk Lee*, Ji-eun Lee**, Gerold Brändli***, and Tim Beyne****

Abstract. Galois polynomials are defined as a generalization of the cyclotomic polynomials. The definition of Galois polynomials (and cyclotomic polynomials) is based on the multiplicative group of integers modulo n, i.e. $\mathbb{Z}_n^*$. In this paper, we define Galois polynomials which are based on the quotient group $\mathbb{Z}_n^*/H$.

1. Introduction

Galois polynomials based on quotient groups have been studied before [6], especially the question of their irreducibility or reducibility. Here we place them in a broader context.

Let n be a nonnegative integer and w be the n-th primitive root of unity, that is $w = e^{\frac{2\pi i}{n}}$. The cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial with integer coefficients satisfying that $\Phi_n(w) = 0$ and is irreducible over the field of the rational numbers. It is well known that

$$\Phi_n(x) = \prod_{k \in \mathbb{Z}_n^*} (x - w^k),$$

where $\mathbb{Z}_n^*$ is the multiplicative group of integers modulo n. These denotations are used throughout this paper.

Definition 1.1. Let H be a subgroup of $\mathbb{Z}_n^*$ and $\mathbb{Z}_n^*/H = \{r_1H, r_2H, \cdots, r_lH\}$ be its corresponding quotient group. Since it is itself a group, one r_i must be 1, one could say $r_1 = 1$ without loosing generality. For each $k = 1, \cdots, l$, define $a_k = \sum_{h \in H} w^{r_k h}$. We define the Galois polynomials,

$$\Phi_{n,H}(x) = (x - a_1)(x - a_2) \cdots (x - a_l).$$

Received January 30, 2018; Accepted July 23, 2018.
2010 Mathematics Subject Classification: Primary 12D05, 12E05, 12F05, 12F10.
Key words and phrases: n-th cyclotomic polynomial, Galois irreducible polynomial, semi-cyclotomic polynomial.

*Correspondence should be addressed to Ki-Suk Lee, ksleeknue@gmail.com.

It is known that $\Phi_{n,H}(x)$ is a monic polynomial with integer coefficients.

Let N be a subgroup of $\mathbb{Z}_n^*$ and H be a subgroup of $\mathbb{Z}_n^*/N$. We define the Galois polynomial from a quotient group $\Psi_{n,H}(x)$ as follows. Let's denote $N = \{n_1, n_2, \cdots, n_r\}$, $\mathbb{Z}_n^*/N = \{r_1N, r_2N, \cdots, r_tN\}$, $H = \{h_1, h_2, \cdots, h_m\}$ and $(\mathbb{Z}_n^*/N)/H = \{k_1H \times N, k_2H \times N, \cdots, k_sH \times N\}$. Then

$$k_vH \times N = k_v\{h_1, h_2, \cdots, h_m\}\{n_1, n_2, \cdots, n_r\}.$$

Definition 1.2. Let $a_v = \sum_{j=1}^{m}\sum_{l=1}^{r} w^{k_v h_j n_l}$, where $w = e^{\frac{2\pi i}{n}}$ and $v = 1, 2, \cdots, s$. Then the Galois polynomial from a quotient group is defined as

$$\Psi_{n,H}(x) = (x - a_1)(x - a_2)\cdots(x - a_s).$$

In this paper, we define two kinds of reduced modular Galois polynomials $\Psi_{n,H}^{re}(x)$ having real roots by using $\mathbb{Z}_n^*/\langle n-1\rangle$, and if $n = 4m$ two kinds: $\Psi_{n,H}^{re}(x)$ and additionally $\Psi_{n,H}^{im}(x)$ having pure imaginary roots. They are constructed in two ways from

$$\mathbb{Z}_n^*/\big(\langle n-1\rangle\langle \tfrac{n}{2}-1\rangle\big).$$

$\langle n-1\rangle$ is the multiplicative group modulo n generated by $n-1$.

If $H = N \times M$ is a subgroup of $\mathbb{Z}_n^*$, then M is a subgroup of $\mathbb{Z}_n^*/N$ and their corresponding Galois polynomials are identical. So Galois polynomials from quotient groups have integer coefficients as other Galois polynomials,[6, Theorem2.3].

2. Galois polynomials from $\mathbb{Z}_n^*/\langle n-1\rangle$

Given a positive integer n, then the integers in the range $1, \ldots, n-1$ that are coprime to n form a group with multiplication modulo n. It is denoted by $\mathbb{Z}_n^*$ and is called the multiplicative group of integers modulo n.

It is well known that $\mathbb{Z}_n^*$ has a primitive root, equivalently, $\mathbb{Z}_n^*$ is cyclic, if and only if $n \in \{2, 4, p^k, 2p^k\}$, where p is an odd prime.

Definition 2.1. A helpful function in this paper is

$$j(n) = \frac{\varphi(n)}{\lambda(n)},$$

the quotient of Euler's totient function $\varphi(n)$ and the Carmichael function $\lambda(n)$. $\varphi(n)$ is the order and $\lambda(n)$ the exponent of $\mathbb{Z}_n^*$.

Definition 2.2. To simplify the writing we introduce the denotation

$$\mathbb{Z}_n^{*/2} = \mathbb{Z}_n^*/\langle n-1\rangle.$$

One could, therefore, also say $\mathbb{Z}_n^*$ is cyclic, if and only if $j(n) = 1$. Because w^k and w^{-k} are mirror points in the unit circle, there is a way [8] of halving the number of elements in $\mathbb{Z}_n^*$ by the following special modulus.

Definition 2.3. If the representatives of the residue classes in $\mathbb{Z}_n^*$ mod n are selected in the interval $]0, n[$, the following reduced modulus returns values in the interval $]0, n/2[$.

$$a \bmod^* n = \min\big(a \bmod n, (n-a) \bmod n\big),$$

where $a \in \mathbb{N}$.

Note, mod* halves the number of elements of $\mathbb{Z}_n^*$.
$\langle 3\rangle \bmod 7 = \{3, 2, 6, 4, 5, 1\}$, where $6 = n - 1$
$\langle 3\rangle \bmod^* 7 = \{3, 2, 1\}$.

Let $n \in \{2^k (k>2),\ 4p_1^{k_1},\ p_1^{k_1}p_2^{k_2},\ 2p_1^{k_1}p_2^{k_2}\}$, where $p_1^{k_1}$ and $p_2^{k_2}$ are distinct odd prime powers satisfying $\big(\varphi(p_1^{k_1}), \varphi(p_2^{k_2})\big) = 2$, then $j(n) = 2$. The order of the group is halved, the exponent remains. It is said in [4] that the group $\mathbb{Z}_n^*$ has semi-primitive roots.

The reduced modulus (mod* n) may also be applied to $n \in \{2,\ 4,\ p^k,\ 2p^k\}$, where $j(n) = 1$, by halving order and exponent of $\mathbb{Z}_n^*$. See the example above for $n = 7$.

To study the Galois polynomials from $\mathbb{Z}_n^{*/2}$ the following function is useful.

Theorem 2.4. *The function s_k is given by the following explicit formula*

$$s_k = 2^{1-k} \sum_{j=0}^{\lfloor k/2\rfloor} (-1)^j \binom{k}{2j} s^{k-2j}(4-s^2)^j,$$

where $s_k = w^k + w^{-k} = 2\cos\left(\frac{2\pi}{n}k\right)$ and $s = s_1$.

Proof. We expand $(a \pm b)^k$ and collect the terms according to the parity of the exponents of b

$$\begin{aligned}(a \pm b)^k &= \sum_{j=0}^{k} \binom{k}{j} a^{k-j} b^j \\ &= \sum_{j=0}^{\lfloor k/2\rfloor} \binom{k}{2j} a^{k-2j} b^{2j} \pm \sum_{j=0}^{\lceil k/2-1\rceil} \binom{k}{2j+1} a^{k-2j-1} b^{2j+1}.\end{aligned}$$

By adding the expressions of above, we get

$$(a+b)^k + (a-b)^k = 2 \sum_{j=0}^{\lfloor k/2 \rfloor} \binom{k}{2j} a^{k-2j} b^{2j}.$$

Substituting $a = w + w^{-1}$ and $b = w - w^{-1}$ completes the proof. □

The functions s_k may also be calculated by the following recurrence relations

$$s_k = s \cdot s_{k-1} - s_{k-2}$$

or

$$s_k = s_j \cdot s_{k-j} - s_{k-2j}$$

with the starting points $s_0 = 2$, $s_1 = s$, $s_2 = s^2 - 2$, $s_3 = s^3 - 3s$.

Let $\langle n-1 \rangle = \{1, n-1\}$ be a subgroup of $\mathbb{Z}_n^*$ and consider the quotient group $\mathbb{Z}_n^{*/2}$. Let H' be a subgroup of $\mathbb{Z}_n^{*/2}$ and $\{r_1 H', r_2 H', \cdots, r_l H'\}$ be its quotient group. For each $k = 1, 2, \cdots, l$, we define $b_k = \sum_{h \in H'} s_{r_k h}$, where $s_{r_k h}$ is defined as above and get the first kind of a Galois polynomial from a quotient group $\Psi^{re}_{n,H'}(x) = (x - b_1)(x - b_2) \cdots (x - b_l)$. Since b_i's are sums of s_k's, $\Psi_{n,H'}(x)$ has only real roots.

Once the $s_k^\prime s$ have been defined one can calculate the Galois polynomials by the following formula

$$\Psi^{re}_n(x) = \prod_{k \in \mathbb{Z}_n^{*/2}} (x - s_k).$$

Example 2.5. *When* $n = 21$,

$$\Phi_{21,\langle -1 \rangle} = x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1 = \Psi^{re}_{21}$$
$$\Phi_{21,\langle -1 \rangle \langle 8 \rangle} = x^3 - x^2 - 2x + 1 = \Psi^{re}_{21,\langle 8 \rangle}$$
$$\Phi_{21,\langle -1 \rangle \langle 4 \rangle} = x^2 - x - 5 = \Psi^{re}_{21,\langle 4 \rangle}$$

Note, in the reduced group $\mathbb{Z}_n^{*/2}$ one writes $\langle 4 \rangle = \{4, 5, 1\}$ instead of $\{4, 16, 1\}$. Remember, 16 and 5 are mirror points in the unit circle and have identical cosine functions.

Theorem 2.6. *Let* $\mathbb{Q}(s)$ *be the simple extension field of* $\mathbb{Q}$ *containing* $s = w + w^{-1}$. *Then the Galois group* $Gal_{\mathbb{Q}}\mathbb{Q}(s)$ *is isomorphic to* $\mathbb{Z}_n^*/\langle -1 \rangle$.

Proof. Let σ_k be the map in $Gal_{\mathbb{Q}}\mathbb{Q}(s)$ which sends w to w^k, where $k \in \mathbb{Z}_n^*$ and $w = e^{\frac{2\pi i}{n}}$. Define $\Sigma : \mathbb{Z}_n^*/\langle -1 \rangle \to Gal_{\mathbb{Q}}\mathbb{Q}(s)$ as $\Sigma(k) =$

$\sigma_k \mid_{\mathbb{Q}(s)}$, i.e., the restriction of σ_k to $\mathbb{Q}(s)$. Since $\sigma_k \mid_{\mathbb{Q}(s)} = \sigma_{-k} \mid_{\mathbb{Q}(s)}$, Σ is a well-defined map. Then

$$\begin{cases} \sigma_k(s_t) = \sigma_k(w^t + w^{-t}) = w^{kt} + w^{-kt} \\ \sigma_{-k}(s_t) = \sigma_{-k}(w^t + w^{-t}) = w^{-kt} + w^{kt}. \end{cases}$$

Since $\Sigma(k)$ sends s to s_k and s_k's are all different, Σ is a bijective map. Also Σ is a homomorphism, i.e., $\Sigma(k_1k_2)(s) = s_{k_1k_2} = (\Sigma_{k_1} \circ \Sigma_{k_2})(s)$. □

3. Galois polynomials from $\mathbb{Z}_n^*/\big(\langle n-1\rangle\langle \frac{n}{2}+1\rangle\big)$

Given a number $n = 4m$, where m is a nonnegative integer. Then the multiplicative group of integers modulo n has an additional subgroup of order 2, namely $\langle \frac{n}{2}+1\rangle$. $\langle n-1\rangle\langle \frac{n}{2}+1\rangle$ is the Klein four-group and could be expressed also by $\langle n-1\rangle\langle \frac{n}{2}-1\rangle$.

We have now four symmetric points on the unit circle $w^k, w^{n/2-k}$, $w^{n/2+k}$ and w^{n-k} and can reduce the number of elements in $\mathbb{Z}_n^*$ to a quarter.

Definition 3.1. To simplify the writing we introduce the denotation

$$\mathbb{Z}_n^{*/4} = \mathbb{Z}_n^*/\big(\langle n-1\rangle\langle \tfrac{n}{2}+1\rangle\big).$$

Definition 3.2. If $n = 4m$, then the following special modulus returns representatives in the interval $]0, \frac{n}{4}[$.

$$a \bmod^* \tfrac{n}{2} = \min\big(a \bmod \tfrac{n}{2}, (n-a) \bmod \tfrac{n}{2}\big),$$

where $a \in \mathbb{N}$.

Theorem 3.3. *Let $n = 4m$ ($m \in \mathbb{N}$) and $\mathbb{Z}_n^{*/4}$ be the multiplicative group of integers mod* $\frac{n}{2}$. Then the group $\mathbb{Z}_n^{*/4}$ is cyclic, if and only if $n \in \{2^k(k>3),\ 4p^k,\ 8p^k,\ 4p_1^{k_1}p_2^{k_2}\}$, where $p_1^{k_1}$ and $p_2^{k_2}$ are different odd prime powers satisfying $(\varphi(p_1^{k_1}), \varphi(p_2^{k_2})) = 2$.*

Proof. If n is divisible by 4 and $n \in \{2^k(k>3),\ 4p^k\}$ with $j(n) = 2$ or $n \in \{8p^k,\ 4p_1^{k_1}p_2^{k_2}\}$ with $j(n) = 4$, then $\mathbb{Z}_n^{*/4}$ is cyclic, because the order is quartered $|\mathbb{Z}_n^{*/4}| = |\mathbb{Z}_n^*|/4$ for all n, and for $n \in \{2^k(k>3),\ 4p^k\}$ the exponent $\lambda(n)$ is halved. □

Example 3.4. *When $n = 84$,*

$\mathbb{Z}_n^{*/4} = \{1, 5, 11, 13, 17, 19\}$,
$\langle 11\rangle = \{11, 11^2, 11^3, \cdots, 11^6\}$ (mod* $\frac{n}{2}$) $= \{11, 5, 13, 17, 19, 1\}$.

The "primitive" roots of $\mathbb{Z}_n^{*/4}$ *are 11 and 19.*

Let $w^k = e^{\frac{2\pi ik}{n}}$ be a point on the unit circle. Then the group $\langle n-1\rangle$ applied to k mirrors the points at the x-axis, the addition of the two points yields $w^k + w^{n-k} = 2\ cos(\frac{2\pi k}{n})$. The group $\langle \frac{n}{2}-1\rangle$ mirrors the points at the y-axis, the addition yields $w^k + w^{\frac{n}{2}-k} = 2i\ sin(\frac{2\pi k}{n})$. The combination of the two groups, namely $\langle \frac{n}{2}+1\rangle$, mirrors the points at the origin, the addition yields $w^k + w^{\frac{n}{2}+k} = 0$.

Still given $n = 4m$ and using the definition of s_k above, we have two special cases:

Case $\mathbb{Z}_n^*/\langle n-1\rangle$: The Galois polynomial has typical pairs of factors $(x-s_k)(x+s_k) = x^2 - s_k^2$ and has only real roots

$$\Psi_n^{re}(x) = \prod_{k\in\mathbb{Z}_n^{*/4}} (x^2 - s_k^2).$$

Case $\mathbb{Z}_n^*/\langle \frac{n}{2}-1\rangle$: The Galois polynomial has typical pairs of factors $\big(x - 2i\ sin(\frac{2\pi k}{n})\big)\ \big(x + 2i\ sin(\frac{2\pi k}{n})\big) = x^2 + 4sin(\frac{2\pi k}{n})^2 = x^2 + 4 - s_k^2$ and has only pure imaginary roots.

$$\Psi_n^{im}(x) = \prod_{k\in\mathbb{Z}_n^{*/4}} (x^2 + 4 - s_k^2).$$

Example 3.5. *When* $n = 20$,
Case $\mathbb{Z}_n^*/\langle n-1\rangle$*:*

$$\Phi_{20,\langle n-1\rangle} = x^4 - 5x^2 + 5 = \Psi_{20}^{re},$$
$$\Phi_{20,\langle n-1\rangle\langle 3\rangle} = x^2 - 5 = \Psi_{20,\langle 3\rangle}^{re}.$$

Case $\mathbb{Z}_n^*/\langle \frac{n}{2}-1\rangle$*:*

$$\Phi_{20,\langle n/2-1\rangle} = x^4 + 3x^2 + 1 = \Psi_{20}^{im},$$
$$\Phi_{20,\langle n/2-1\rangle\langle 3\rangle} = x^2 + 3 = \Psi_{20,\langle 3\rangle}^{im}.$$

4. Galois polynomials from $\mathbb{Z}_n^*/\big(\langle n-1\rangle\langle \frac{n}{4}+1\rangle\big)$

Given a number $n = 8m$, where m is a positive integer. Then the multiplicative group of integers modulo n can be halved a third time. The group $\langle \frac{n}{4}+1\rangle$ comprises $\langle \frac{n}{2}+1\rangle$ as a subgroup.

We have now eight symmetric points on the unit circle and can reduce the number of elements in $\mathbb{Z}_n^*$ to an eighth.

Definition 4.1. To simplify the writing we introduce the denotation

$$\mathbb{Z}_n^{*/8} = \mathbb{Z}_n^*/\big(\langle n-1\rangle\langle \tfrac{n}{4}+1\rangle\big).$$

Definition 4.2. If $n = 8m$, then the following special modulus returns representatives in the interval $[0, \frac{n}{8}]$.

$$a \bmod^* \tfrac{n}{4} = \min\big(a \bmod \tfrac{n}{4}, (n-a) \bmod \tfrac{n}{4}\big),$$

where $a \in \mathbb{N}$.

Theorem 4.3. *Let $n = 8m$ ($m \in \mathbb{N}$) and $\mathbb{Z}_n^{*/8}$ be the multiplicative group of integers mod* $\frac{n}{4}$. Then the group $\mathbb{Z}_n^{*/8}$ is cyclic, if $n \in \{2^k (k>3),\ 8p^k,\ 16p^k,\ 8p_1^{k_1}p_2^{k_2}\}$, where $p_1^{k_1}$ and $p_2^{k_2}$ are different odd prime powers satisfying $(\varphi(p_1^{k_1}), \varphi(p_2^{k_2})) = 2$.*

Proof. If n is divisible by 8 and $n \in \{2^k(k>3),\ 8p^k\}$ with $j(n) = 2$ or $n \in \{16p^k,\ 8p_1^{k_1}p_2^{k_2}\}$ with $j(n) = 4$, then $\mathbb{Z}_n^{*/8}$ is cyclic, because the order is divided by eight $|\mathbb{Z}_n^{*/8}| = |\mathbb{Z}_n^*|/8$ for all n, and for $n \in \{2^k(k>3),\ 8p^k\}$ the exponent $\lambda(n)$ is halved. $\square$

Example 4.4. *When $n = 168$,*

$\mathbb{Z}_n^{*/8} = \{1, 5, 11, 13, 17, 19\}$,
$\langle 11\rangle = \{11, 11^2, 11^3, \cdots, 11^6\}\ (\bmod^*\ \frac{n}{4}) = \{11, 5, 13, 17, 19, 1\}$.

Still given $n = 8m$ and using the definition of s_k above, we have two special cases:
Case $\mathbb{Z}_n^*/\langle n-1\rangle$, Galois polynomial with real roots:

$$\Psi_n^{re}(x) = \prod_{k \in \mathbb{Z}_n^{*/8}} (x^4 - 4x^2 + 4s_k^2 - s_k^4).$$

Case $\mathbb{Z}_n^*/\langle \frac{n}{2}-1\rangle$, Galois polynomial with pure imaginary roots:

$$\Psi_n^{im}(x) = \prod_{k \in \mathbb{Z}_n^{*/8}} (x^4 + 4x^2 + 4s_k^2 - s_k^4).$$

Example 4.5. *When $n = 104 = 8 \cdot 13$, one gets $\langle 7\rangle$ mod* $\frac{n}{4} = \{7, 3, 5, 9, 11, 1\}$.*
The Galois polynomials Ψ_n^{re} and Ψ_n^{im} have – disregarding the signs – the same coefficients. The minus signs are for Ψ_n^{re}.

$\Psi_{104,\langle 7\rangle}^{re/im}(x) = x^4 \mp 4x^2 + 11$,
$\Psi_{104,\langle 3\rangle}^{re/im}(x) = x^8 \mp 8x^6 + 27x^4 \mp 44x^2 + 27$,
$\Psi_{104,\langle 5\rangle}^{re/im}(x) = x^{12} \mp 12x^{10} + 59x^8 \mp 152x^6 + 212x^4 \mp 144x^2 + 31$,

$$\Psi^{re/im}_{104,\langle 1\rangle}(x) = x^{24} \mp 24x^{22} + 251x^{20} \mp 1500x^{18} + \ldots + 1.$$

5. Galois polynomials from $\mathbb{Z}_n^*/\big(\langle n-1\rangle\langle \frac{n}{q}-1\rangle\big)$

Given a number $n = q^2m$, where q is an odd prime and m a positive integer. Then the multiplicative group of integers modulo n has an additional subgroup of order q, namely $\langle \frac{n}{q} - 1\rangle$, beside the standard subgroup $\langle n-1\rangle$ of order 2.

We have now $2q$ symmetric points on the unit circle and can reduce the number of elements in $\mathbb{Z}_n^*$ by the factor $2q$.

Definition 5.1. To simplify the writing we introduce the denotation

$$\mathbb{Z}_n^{*/2q} = \mathbb{Z}_n^*/\big(\langle n-1\rangle\langle \tfrac{n}{q}-1\rangle\big).$$

Definition 5.2. If $n = q^2m$, then the following special modulus returns representatives in the interval $[0, \frac{n}{2q}]$.

$$a \bmod^* \tfrac{n}{q} = \min\big(a \bmod \tfrac{n}{q}, (n-a) \bmod \tfrac{n}{q}\big),$$

where $a \in \mathbb{N}$.

Theorem 5.3. *The Galois polynomials from $\mathbb{Z}_n^{*/2q}$ are all reducible over $\mathbb{Q}$.*

Proof. The roots a_k of the Galois polynomial

$$\Psi_n = \prod_{k\in\mathbb{Z}_n^{*/2q}} (x - a_k).$$

are

$$a_k = s_k + s_{f-k} + s_{f+k} + s_{2f-k} + s_{2f+k} + \ldots + s_{tf-k} + s_{tf+k},$$

where s_k are defined as before and $f = \frac{2n}{q}$ and $t = \frac{q-1}{2}$.

Because of the symmetric positions on the unit circle of the elements of the group $\langle \frac{n}{q} - 1\rangle$, we have $a_k = 0$ and therefore $\Psi_n = x^h$ with $h = |\mathbb{Z}_n^{*/2q}|$. □

Examples are $n = 45$ or $n = 75$. One could extend this section even to $n = 105$, where n and $\varphi(n)$ are divisible by 3 resulting in reducible Galois polynomials.

6. Cyclic Semiprimes

In studying the applications of mod* the term cyclic semiprime [8] was created. Note, all products of twin primes or pairs of Sophie Germain primes are cyclic semiprimes.

Definition 6.1. Let $n = p_1^{k_1} p_2^{k_2}$ with $(\varphi(p_1^{k_1}), \varphi(p_2^{k_2})) = 2$, where p_i are distinct odd primes and k_i positive integers. Then n is called a cyclic semiprime.

If n is a cyclic semiprime, $\mathbb{Z}_n^*/\langle -1 \rangle$ is cyclic. In this case, Galois polynomials over $\mathbb{Z}_n^{*/2}$ can be calculated more easily.

Remark 6.2. If n is an odd cyclic semiprime, then $2n$ is it as well. The focus below is on n.

The odd cyclic semiprimes <100> are 15, 21, 33, 35, 39, 45, 51, 55, 57, 69, 75, 77, 87, 93, 95 and 99. Note, although the numbers 63, 65, 85 and 91 are composed of two primes, they are not cyclic semiprimes.

Theorem 6.3. *There are infinitely many cyclic semiprimes.*

Proof. There are even infinitely many cyclic semiprimes with a fixed first factor $p_1^{k_1}$. Let $\{q_1, q_2, \ldots, q_l\}$ be the set of all prime factors of $\varphi(p_1^{k_1})/2$. Powers of q_i need not to be considered. There is a chance of $\frac{q_i-2}{q_i-1}$ for odd q_i and of $\frac{1}{2}$ for $q_i = 2$ that $\varphi(p_2^{k_2})/2$ is not divisible by q_i and a combined chance of

$$c = \prod_{i=1}^{l} \frac{q_i - 2}{q_i - 1} \quad \text{or} \qquad (6.1)$$

$$c = \frac{1}{2} \cdot \prod_{i=2}^{l} \frac{q_i - 2}{q_i - 1}$$

if $q_1 = 2$, that $\varphi(p_2^{k_2})/2$ is not divisible by any q_i. We will show below that $c \approx 1/2$.

The denominator $q_i - 1$ follows from the fact, that in randomly selected integers every ${q_i}^{th}$ number is divisible by q_i. The numerator $q_i - 2$ takes additional in account that $(q_i - 1)/2$ is not an allowed divisior of $\varphi(p_2^{k_2})/2$, because p_2 would be a multiple of q_i.
Because c is a nonzero constant for any $p_1^{k_1}$ and because there exist infinitely many primes p_2, the theorem follows. □

Examples: All numbers of the form $n = 3p$ $(p > 3)$ with $c = 1$ are cyclic semiprimes.
Numbers $n \in \{5p, 9p, 21p, 61p\}$ would have the chance $c = \{\frac{1}{2}, \frac{1}{2}, \frac{1}{4}, \frac{3}{16}\}$, respectively.

Theoretically, one could expect a value of

$$c_{theo} = \left(\frac{1}{2}\right)^{\frac{1}{2}} \prod_{i=2}^{\infty} \left(\frac{p_i - 2}{p_i - 1}\right)^{\frac{1}{p_i}} \approx 0.499075\dots \ ,$$

where p_i is the i^{th} prime.

It is difficult to verify this result heuristically. One procedure is to prepare a list of all odd $p^k < m$ up to a maximum m, then to determine the frequency of $\big(\varphi(p_1^{k_1}), \varphi(p_2^{k_2})\big) = 2$ in all pairs $p_1 \neq p_2$. We did this up to $m = 10^4$ testing more than 10^8 pairs and found that the results begin at $c_{heur} \approx 5.0$, do not converge, but rather fluctuate down to $c_{heur} \approx 4.96$. A converging procedure was not found.

The constant c estimates the probability that a number $n = p_1^{k_1} p_2^{k_2}$ is a cyclic semiprime. It is similar – but not analogue – to Artin's well known constant for primes.

References

[1] J. R. Bastida and R. Lyndon, *Field Extensions and Galois Theory*, Encyclopedia of Mathematics and Its Application, Addison-Wesley Publishing Company, 1984.
[2] T. W. Hungerford, *Abstract Algebra : An Introduction*, Brooks/Cole, Cengage Learning, 2012.
[3] S. Lang, *Algebra, 2nd ed.* Addison-Wesley Publising Company, USA, 1984.
[4] K. S. Lee, M. Kwon, and G. C. Shin, *Multiplicative groups of integers with semi-primitive roots modulo n*, Commun. Korean Math. Soc, **28** (2013), no.1, 71-77.
[5] K. S. Lee, J. E. Lee, and J. H. Kim, *semi-cyclotomic polynomials*, Honam Mathematical Journal, **37** (2015), no.4, 469-472.
[6] M. Kwon, J. E. Lee, and K. S. Lee, *Galois irreducible polynomials*, Commun. Korean Math. Soc, **32** (2017), no.1, 1-6.
[7] K. S. Lee and J. E. Lee, *Classification of Galois Polynomials*, Honam Mathematical Journal, **39** (2017), no.2, 259-265.
[8] Gerold Brändli and Tim Beyne, *Modified Congruence Modulo n with Half The Amount of Residues*, preprint, https://arxiv.org/abs/1504.02757.
[9] P. Ribenboim, *Algebraic Numbers*, John Wiley and Sons Inc. 1972.
[10] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford: Oxford University Press, UK, 1980.

*

Department of Mathematics Education
Korea National University of Education
Cheongjusi, Chungbuk 363-791, Republic of Korea
E-mail: ksleeknue@gmail.com

**

Department of Mathematics Education
Korea National University of Education
Cheongjusi, Chungbuk 363-791, Republic of Korea
E-mail: dlwldms818@gmail.com

***

Schanzmättelistrasse 27, 5000 Aarau, Switzerland
E-mail: braendli@hispeed.ch

****

Rotspoelstraat 15, 3001 Heverlee-Leuven, Belgium
E-mail: tim.beyne@student.kuleuven.be