IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 5, 2018, accepted July 5, 2018, date of publication July 9, 2018, date of current version July 30, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2854373

A Coefficient Test for Quintic Permutation Polynomials Over Integer Rings

LUCIAN TRIFINA AND DANIELA TARNICERIU
Department of Telecommunications and Information Technologies, Faculty of Electronics, Telecommunications and Information Technology,
Gheorghe Asachi Technical University of Iasi, 700506 Iasi, Romania

Corresponding author: Lucian Trifina (luciant@etti.tuiasi.ro)

ABSTRACT For selecting appropriate permutation polynomials (PPs) in practical applications, it is necessary to know the coefficients of the polynomial since a brute-force exhaustive search is impractical when the number of PPs is large. Previous results give the conditions on the coefficients of a polynomial of degree up to four so that it is a PP modulo a given positive integer. For polynomials of degree higher than four, we only know the conditions so that they are PPs modulo a power of two. In [13] all PPs of degree no more than six are generated using an algorithm based on normalized PPs, two previous important theorems about PPs and the Chinese remainder theorem. In this paper, we propose a coefficient test for quintic permutation polynomials (5-PPs) over integer rings which, unlike the algorithm from [13], allows to decide directly whether a polynomial of degree five or less is PP. Using the proposed coefficient test, the coefficients of PPs modulo a given positive integer can be obtained in a desired order, which is tractable in computer processing.

INDEX TERMS Coefficient test, integer rings, permutation polynomials, quintic polynomial.

I. INTRODUCTION

Permutation polynomials (PPs) are used in cryptography, sequences' generation or as interleavers in turbo codes [1]–[3].

For selecting PPs in practical applications, it is necessary to know the coefficients of the polynomial. For example, when PPs are used as interleavers for turbo codes, the coefficients have to be carefully chosen for a good error rate performance. Thus, we use a certain criterion (for example the distance spectrum) to select the coefficients of the PP for a good PP interleaver. This selection may require testing a lot of PP interleavers. When the interleaver length is big, the number of PPs is large and a brute-force exhaustive search is impractical. Therefore, we require the conditions on the polynomials' coefficients so that they are PPs. Previous known results concerning the conditions on a polynomial's coefficients to be a PP are:

1) the conditions for a polynomial of any degree to be a PP modulo 2^w, with w a positive integer [4],
2) the conditions for a polynomial of second degree to be a quadratic permutation polynomial (QPP) [3], [5],
3) the conditions for a polynomial of third degree to be a cubic permutation polynomial (CPP) [6], [7], and
4) the conditions for a polynomial of fourth degree to be a quartic permutation polynomial (denoted 4-PP) [8].

In this paper, we extend the conditions from [6], [8] for quintic polynomials' coefficients so that they are PPs (denoted 5-PPs). Let N be a positive integer. The 5-PPs in this paper are evaluated modulo N. In the paper we use an exhaustive approach in which we considered all the prime numbers from the decomposition of the positive integer. We consider that this approach facilitates the understanding and the use of permutation polynomials in various applications. The analysis was performed for values of N whose prime decompositions contain up to eight different prime numbers, namely 2, 3, 5, 7, 13, primes $p = 1 \pmod 5$, $p = 2, 3 \pmod 5$, and $p = 4 \pmod 5$. This analysis is done separately, for each prime number to power of one or to powers greater than one. The cases concerning the prime numbers 2 and 3 were previously addressed in [4] and [9], [10], respectively. The case $p = 5$ was addressed in [10], but the author used Corollary 2.9 from [11], and thus, he did not consider the situation when the coefficient of the third degree term is equal to 0 modulo 5. We point out that the coefficients' conditions from Lemma 4 in [9] are only sufficient and not necessary for a polynomial of any degree to be a PP modulo p^n, with $n > 1$, as it was shown in [12]. Using this Lemma in Corollary 2 from [9] does not provide all CPPs.

We mention that reference [13] presents an algorithm that generates all PPs over $\mathbb{Z}_N$, of degree no more than six.

The algorithm is based on normalized PPs, Theorems 1 and 2 from Section II about PPs, and the Chinese remainder theorem. The authors of [13] also give the conditions for the coefficients of a normalized permutation polynomial of sixth degree, but only for the prime numbers equal to 2, 3 and 5 from the prime decomposition of N. These conditions for the prime numbers 2, 3 or 5 can be particularized for a quintic permutation polynomial. However, in [13] the conditions on the coefficients for any permutation polynomial were not given. Unlike [13], using the conditions on coefficients derived in this paper, we can decide directly whether a polynomial of degree five or less is PP.

II. RESULTS ON PERMUTATION POLYNOMIALS OVER INTEGER RINGS

A PP of degree d is of the form:

$$\pi(x) = q_0 + q_1 x + q_2 x^2 + \cdots + q_d x^d \pmod{N}, \qquad (1)$$

where N is a positive integer and the coefficients q_k, $k = 1, \cdots, d$, are chosen so that $\pi(x)$ from (1), with $x = 0, 1, \cdots, N-1$, is a permutation of the set of integers modulo N, $\mathbb{Z}_N = \{0, 1, \cdots, N-1\}$. As the free term q_0 only determines a cyclic shift of the permutation elements, we will consider $q_0 = 0$.

Let $\mathcal{P} = \{2, 3, 5, \cdots\}$ be the set of prime numbers. In the following, the notation $p \mid N$ means that p divides N, the notation $p \nmid N$ means that p does not divide N and $\pi'(x)$ denotes the formal derivative of the polynomial $\pi(x)$. We recall two theorems that are useful for getting the results in Section III. The first theorem is from [3], [6]. The second theorem is a Nöbauer's result [14], but it is also given in [3], [6], [15]. In [15] it is mentioned that the result of this theorem is a direct consequence of Theorem 123 from [16]. Below, we give the two theorems.

Theorem 1: For any $N = \prod_{\substack{p\in\mathcal{P},\\ p|N}} p^{n_{N,p}}$, $\pi(x)$ is a PP modulo N iff $\pi(x)$ is also a PP modulo $p^{n_{N,p}}$, $\forall p$ such that $n_{N,p} \geq 1$.

Theorem 2: $\pi(x)$ is a PP modulo p^n, with $n > 1$, iff $\pi(x)$ is a PP modulo p and $\pi'(x) \neq 0 \pmod{p}$, for every integer x.

In this paper, we present a direct test on the coefficients q_1, q_2, q_3, q_4, and q_5 of a quintic polynomial, so that it is 5-PP.

III. A COEFFICIENT TEST FOR QUINTIC PPS

In this section we use the same three-step algorithm as in [6] (given below) to check if a quintic polynomial $\pi(x)$ is 5-PP, but under the conditions from Table 1.

1) Factor N as $N = \prod_{\substack{p\in\mathcal{P},\\ p|N}} p^{n_{N,p}}$.
2) For each p and the corresponding $n_{N,p}$ from the previous step, test if the conditions in Table 1 are satisfied.
3) $\pi(x)$ is a 5-PP iff all tests in step 2) are satisfied.

The cases $p = 2$, $p = 3$, $p = 5$, $p = 7$, and $p = 13$ are addressed in Subsections III-A, III-B, III-C, III-D and III-E, respectively, and the cases $p = 1 \pmod{5}$, $p = 2, 3 \pmod{5}$, with $p > 13$, and $p = 4 \pmod{5}$, in Subsections III-F, III-G and III-H, respectively. Table 1 shows the coefficient conditions for a 5-PP modulo p^n.

A. $p = 2$

For $p = 2$, a simple test on the coefficients is given in [4] for any degree of the polynomial. For the fifth degree, the conditions are given in Table 1.

B. $p = 2$

1) $p = 3$ AND $n = 1$

Theorem 3: $\pi(x) = q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + q_5 x^5 \pmod{3}$ is a PP iff $(q_1 + q_3 + q_5) \neq 0 \pmod{3}$ and $(q_2 + q_4) = 0 \pmod{3}$.

Proof: As $\pi(0) = 0$, it requires that

$$\pi(1) = q_1 + q_2 + q_3 + q_4 + q_5 \neq 0 \pmod{3}, \qquad (2)$$

$$\pi(2) = 2q_1 + q_2 + 2q_3 + q_4 + 2q_5 \neq 0 \pmod{3}, \qquad (3)$$

and

$$\pi(1) \neq \pi(2) \pmod{3}. \qquad (4)$$

Replacing (2) and (3) in (4), we have that

$$(q_1 + q_3 + q_5) \neq 0 \pmod{3}. \qquad (5)$$

If $(q_1 + q_3 + q_5) = 1 \pmod{3}$, then, from (2) it follows that $(q_2 + q_4) = 0 \pmod{3}$ or $(q_2 + q_4) = 1 \pmod{3}$, and from (3) it follows that $(q_2 + q_4) = 0 \pmod{3}$ or $(q_2 + q_4) = 2 \pmod{3}$. Therefore, $(q_2 + q_4) = 0 \pmod{3}$. The case $(q_1 + q_3 + q_5) = 2 \pmod{3}$ is approached similarly and leads to the same result. ■

2) $p = 3$ AND $n > 1$

Theorem 4: $\pi(x) = q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + q_5 x^5 \pmod{3^n}$, with $n > 1$, is a PP iff $q_1 \neq 0 \pmod{3}$, $(q_1 + q_3 + q_5) \neq 0 \pmod{3}$, $(q_2 + q_4) = 0 \pmod{3}$, $(q_1 + q_2 + 2 \cdot q_5) \neq 0 \pmod{3}$ and $(q_1 + q_4 + 2 \cdot q_5) \neq 0 \pmod{3}$.

Proof: To prove the necessity, we assume that $\pi(x)$ is a PP $\pmod{3^n}$, with $n > 1$. Then, according to Theorem 2, $\pi(x)$ is a PP $\pmod{3}$ and

$$\begin{aligned}\pi'(x) &= q_1 + 2q_2 x + 3q_3 x^2 + 4q_4 x^3 + 5q_5 x^4 \pmod{3}\\ &= q_1 + 2q_2 x + q_4 x^3 + 2q_5 x^4 \neq 0 \pmod{3}\end{aligned} \qquad (6)$$

As $\pi(x)$ is a PP $\pmod{3}$, from Theorem 3, we have that $(q_1 + q_3 + q_5) \neq 0 \pmod{3}$ and $(q_2 + q_4) = 0 \pmod{3}$. Replacing $x = 0$ in (6), we have that $\pi'(0) = q_1 \neq 0 \pmod{3}$. Replacing $x = 1$ in (6), we have that $\pi'(1) = q_1 + 2q_2 + q_4 + 2q_5 \neq 0 \pmod{3}$. Because $(q_2 + q_4) = 0 \pmod{3}$, it follows that

$$\pi'(1) = q_1 + q_2 + 2 \cdot q_5 \neq 0 \pmod{3} \qquad (7)$$

Replacing $x = 2$ in (6), we have that $\pi'(2) = q_1 + q_2 + 2q_4 + 2q_5 \neq 0 \pmod{3}$ and, because $(q_2 + q_4) = 0 \pmod{3}$, it follows that

$$\pi'(2) = q_1 + q_4 + 2 \cdot q_5 \neq 0 \pmod{3} \qquad (8)$$

TABLE 1. A coefficient test for 5-PPs modulo *p*.

Prime number p	Power of p, $n_{N,p}$	Conditions on the coefficients
$p=2$	$n_{N,2}=1$	$(q_1+q_2+q_3+q_4+q_5)=1 \pmod 2$
	$n_{N,2}>1$	$q_1=1 \pmod 2$, $(q_2+q_4)=0 \pmod 2$ and $(q_3+q_5)=0 \pmod 2$
$p=3$	$n_{N,3}=1$	$(q_1+q_3+q_5)\neq 0 \pmod 3$ and $(q_2+q_4)=0 \pmod 3$
	$n_{N,3}>1$	$q_1\neq 0 \pmod 3$, $(q_1+q_3+q_5)\neq 0 \pmod 3$, $(q_2+q_4)=0 \pmod 3$, $(q_1+q_2+2q_5)\neq 0 \pmod 3$ and $(q_1+q_4+2q_5)\neq 0 \pmod 3$
$p=5$	$n_{N,5}=1$	(1) $q_4=q_2=0 \pmod 5$ and $(q_1+q_5)\neq 0 \pmod 5$, when $q_3=0 \pmod 5$, or (2) $q_4=0 \pmod 5$ and $(q_2)^2=3(q_1+q_5)q_3 \pmod 5$, when $q_3\neq 0 \pmod 5$.
	$n_{N,5}>1$	(1) $q_4=q_3=q_2=0 \pmod 5$, $q_1\neq 0 \pmod 5$ and $(q_1+q_5)\neq 0 \pmod 5$, or (2) $q_4=0 \pmod 5$, $(q_2)^2=3(q_1+q_5)q_3 \pmod 5$ and (2.1) $(q_3+q_5)=0 \pmod 5$, or (2.2) $(q_3-q_5)=0 \pmod 5$, when $q_5\neq 0 \pmod 5$, or (3) $q_4=q_3=q_2=0 \pmod 5$ and $q_1\neq 0 \pmod 5$, when $q_5=0 \pmod 5$.
$p=7$	$n_{N,7}=1$	(1) $4q_2(q_5)^2=2(q_4)^3 \pmod 7$ and $6q_1(q_5)^3=(q_4)^4 \pmod 7$, or (2) $4q_2(q_5)^2=2(q_4)^3\pm(q_5)^3 \pmod 7$ and $6q_1(q_5)^3=(q_4)^4\pm 2q_4(q_5)^3 \pmod 7$, when $q_5\neq 0 \pmod 7$ and $5q_3q_5=2(q_4)^2 \pmod 7$, or (3) $4q_2(q_5)^2=2(q_4)^3+\alpha q_4(q_5)^2 \pmod 7$ and $6q_1(q_5)^3=(q_4)^4+\alpha(q_4)^2(q_5)^2+4\alpha^2(q_5)^4 \pmod 7$, where $\alpha=(q_3q_5+(q_4)^2)\cdot\left((q_5)^2\right)^{-1} \pmod 7$, when $q_5\neq 0 \pmod 7$ and $5q_3q_5\neq 2(q_4)^2 \pmod 7$, or (4) $4q_2(q_5)^2=2(q_4)^3+\alpha q_4(q_5)^2\pm 4(q_5)^3 \pmod 7$ and $6q_1(q_5)^3=(q_4)^4+\alpha(q_4)^2(q_5)^2\pm q_4(q_5)^3+4\alpha^2(q_5)^4 \pmod 7$, where $\alpha=(q_3q_5+(q_4)^2)\cdot\left((q_5)^2\right)^{-1} \pmod 7$, when $\alpha\in\{3,5,6\}$, $q_5\neq 0 \pmod 7$ and $5q_3q_5\neq 2(q_4)^2 \pmod 7$, or (5) $3(q_3)^2=q_2q_4 \pmod 7$ and $2q_1(q_4)^2=(q_3)^3+(q_4)^3$, or (6) $3(q_3)^2=q_2q_4 \pmod 7$ and $2q_1(q_4)^2=(q_3)^3+6(q_4)^3 \pmod 7$, when $q_5=0 \pmod 7$ and $q_4\neq 0 \pmod 7$, or (7) $q_3=q_2=0 \pmod 7$ and $q_1\neq 0 \pmod 7$, when $q_5=q_4=0 \pmod 7$.

TABLE 1. ***Continued.*** **A coefficient test for 5-PPs modulo *p*.**

Prime number p	Power of p, $n_{N,p}$	Conditions on the coefficients
	$n_{N,7} > 1$	(1) $5q_3q_5 \neq 2(q_4)^2 \pmod 7$, $4q_2(q_5)^2 = 2(q_4)^3 + \alpha q_4(q_5)^2 \pmod 7$ and $6q_1(q_5)^3 = (q_4)^4 + \alpha(q_4)^2(q_5)^2 + 4\alpha^2(q_5)^4 \pmod 7$, where $\alpha = (q_3q_5 + (q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod 7$, when $q_5 \neq 0 \pmod 7$, or (2) $q_4 = q_3 = q_2 = 0 \pmod 7$ and $q_1 \neq 0 \pmod 7$, when $q_5 = 0 \pmod 7$.
$p = 13$	$n_{N,13} = 1$	(1) $12q_2(q_5)^2 = 2(q_4)^3 \pmod{13}$ and $8q_1(q_5)^3 = (q_4)^4 \pmod{13}$, when $q_5 \neq 0 \pmod{13}$ and $5q_3q_5 = 2(q_4)^2 \pmod{13}$, or (2) $12q_2(q_5)^2 = 2(q_4)^3 + 2\alpha q_4(q_5)^2 \pmod{13}$ and $8q_1(q_5)^3 = (q_4)^4 + 2\alpha(q_4)^2(q_5)^2 + 12\alpha^2(q_5)^4 \pmod{13}$, where $\alpha = (q_3q_5 + 10(q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod{13}$, when $q_5 \neq 0 \pmod{13}$ and $5q_3q_5 \neq 2(q_4)^2 \pmod{13}$, or (3) $12q_2(q_5)^2 = 2(q_4)^3 + 2\alpha q_4(q_5)^2 \pmod{13}$ and $8q_1(q_5)^3 = (q_4)^4 + 2\alpha(q_4)^2(q_5)^2 + 11\alpha^2(q_5)^4 \pmod{13}$, where $\alpha = (q_3q_5 + 10(q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod{13}$, when $\alpha \in \{2, 5, 6, 7, 8, 11\}$, $q_5 \neq 0 \pmod{13}$ and $5q_3q_5 \neq 2(q_4)^2 \pmod{13}$, or (4) $q_4 = q_3 = q_2 = 0 \pmod{13}$ and $q_1 \neq 0 \pmod{13}$, when $q_5 = 0 \pmod{13}$.
	$n_{N,13} > 1$	(1) $5q_3q_5 \neq 2(q_4)^2 \pmod{13}$, $12q_2(q_5)^2 = 2(q_4)^3 + 2\alpha q_4(q_5)^2 \pmod{13}$ and $8q_1(q_5)^3 = (q_4)^4 + 2\alpha(q_4)^2(q_5)^2 + 12\alpha^2(q_5)^4 \pmod{13}$, where $\alpha = (q_3q_5 + 10(q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod{13}$, when $q_5 \neq 0 \pmod{13}$, or (2) $q_4 = q_3 = q_2 = 0 \pmod{13}$ and $q_1 \neq 0 \pmod{13}$, when $q_5 = 0 \pmod{13}$.
$p = 1 \pmod 5$	$n_{N,p} = 1$	(1) $q_5 = q_4 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$, when $3 \nmid (p-1)$ and $q_3 = 0 \pmod p$, or (2) $q_5 = q_4 = 0 \pmod p$ and $(q_2)^2 = 3q_1q_3 \pmod p$, when $3 \nmid (p-1)$ and $q_3 \neq 0 \pmod p$, or (3) $q_5 = q_4 = q_3 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$, when $3 \mid (p-1)$.
	$n_{N,p} > 1$	$q_5 = q_4 = q_3 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$
$p = 2, 3 \pmod 5$	$n_{N,p} = 1$	(1) $25q_2(q_5)^2 = 2(q_4)^3 \pmod p$ and $125q_1(q_5)^3 = (q_4)^4 \pmod p$, when $q_5 \neq 0 \pmod p$ and $5q_3q_5 = 2(q_4)^2 \pmod p$, or (2) $25q_2(q_5)^2 = 2(q_4)^3 + 15\alpha q_4(q_5)^2 \pmod p$ and $125q_1(q_5)^3 = (q_4)^4 + 15\alpha(q_4)^2(q_5)^2 + 25\alpha^2(q_5)^4 \pmod p$, where $\alpha = (5q_3q_5 + (p-2) \cdot (q_4)^2) \cdot \left(5(q_5)^2\right)^{-1} \pmod p$, when $q_5 \neq 0 \pmod p$ and $5q_3q_5 \neq 2(q_4)^2 \pmod p$, or

TABLE 1. ***Continued.*** **A coefficient test for 5-PPs modulo *p*.**

Prime number p	Power of p, $n_{N,p}$	Conditions on the coefficients
		(3) $q_4 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$, when $3 \nmid (p-1)$ and $q_5 = q_3 = 0 \pmod p$, or (4) $q_4 = 0 \pmod p$ and $(q_2)^2 = 3q_1q_3 \pmod p$, when $3 \nmid (p-1)$, $q_5 = 0 \pmod p$ and $q_3 \neq 0 \pmod p$, or (5) $q_4 = q_3 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$, when $3 \mid (p-1)$ and $q_5 = 0 \pmod p$.
	$n_{N,p} > 1$	(1) $5q_3q_5 \neq 2(q_4)^2 \pmod p$, $25q_2(q_5)^2 = 2(q_4)^3 + 15\alpha q_4(q_5)^2 \pmod p$ and $125q_1(q_5)^3 = (q_4)^4 + 15\alpha(q_4)^2(q_5)^2 + 25\alpha^2(q_5)^4 \pmod p$, where $\alpha = (5q_3q_5 + (p-2)\cdot(q_4)^2)\cdot\left(5(q_5)^2\right)^{-1} \pmod p$, when $q_5 \neq 0 \pmod p$, or (2) $q_4 = q_3 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$, when $q_5 = 0 \pmod p$.
$p = 4 \pmod 5$	$n_{N,p} = 1$	(1) $5q_3q_5 = 2(q_4)^2 \pmod p$, $25q_2(q_5)^2 = 2(q_4)^3 \pmod p$ and $125q_1(q_5)^3 = (q_4)^4 \pmod p$, when $q_5 \neq 0 \pmod p$, or (2) $q_4 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$, when $3 \nmid (p-1)$ and $q_5 = q_3 = 0 \pmod p$, or (3) $q_4 = 0 \pmod p$ and $(q_2)^2 = 3q_1q_3 \pmod p$, when $3 \nmid (p-1)$, $q_5 = 0 \pmod p$ and $q_3 \neq 0 \pmod p$, or (4) $q_4 = q_3 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$, when $3 \mid (p-1)$ and $q_5 = 0 \pmod p$.
	$n_{N,p} > 1$	$q_5 = q_4 = q_3 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$.

To prove the sufficiency, we assume that $q_1 \neq 0 \pmod 3$, $(q_1 + q_3 + q_5) \neq 0 \pmod 3$, $(q_2 + q_4) = 0 \pmod 3$, $(q_1 + q_2 + 2\cdot q_5) \neq 0 \pmod 3$ and $(q_1 + q_4 + 2\cdot q_5) \neq 0 \pmod 3$. Then, from Theorem 3, it follows that $\pi(x)$ is a PP $\pmod 3$. For $x = 0$, from (6) we have that $\pi'(0) = q_1 \neq 0 \pmod 3$. For $x = 1$ and $x = 2$, and taking into account the equality $(q_2 + q_4) = 0 \pmod 3$, from (6), we have that $\pi'(1) = q_1 + q_2 + 2\cdot q_5 \neq 0 \pmod 3$ and $\pi'(2) = q_1 + q_4 + 2\cdot q_5 \neq 0 \pmod 3$, respectively. Then, according to Theorem 2, it results that $\pi(x)$ is a PP $\pmod{3^n}$. ■

For the next cases we need the following propositions. They follow from [17], [18].

Proposition 1: A polynomial $\pi(x)$ is a PP modulo p, with $p \nmid d$, iff $a\pi(x+b)+c$ is PP for all $a \neq 0, b, c \in \mathbb{Z}_p$.

Proposition 2: A polynomial $\pi(x)$ is a PP modulo p, with $p \mid d$, iff $a\pi(x)+c$ is PP for all $a \neq 0$, $c \in \mathbb{Z}_p$.

Definition 1: Let $\bar{\pi}(x) = \sum_{k=1}^{d} q_k x^k \pmod{p^n}$. The polynomial $\bar{\pi}(x)$ is a normalized PP if $q_d = 1$, $\bar{\pi}(0) = 0$, and $q_{d-1} = 0$ when $p \nmid d$.

C. p = 5

1) *p* = 5 AND *n* = 1

Proposition 3: ([17]) The only normalized quintic PPs $\pmod 5$ are $\bar{\pi}(x) = x^5 \pmod 5$, $\bar{\pi}(x) = x^5 - \alpha x \pmod 5$ (α not a fourth power) and $\bar{\pi}(x) = x^5 - 2\alpha x^3 + \alpha^2 x \pmod 5$ (α not a square).

Theorem 5: $\pi(x) = q_1x + q_2x^2 + q_3x^3 + q_4x^4 + q_5x^5 \pmod 5$ is PP iff:

1) $q_4 = q_2 = 0 \pmod 5$ and $(q_1 + q_5) \neq 0 \pmod 5$, when $q_3 = 0 \pmod 5$,
or iff:
2) $q_4 = 0 \pmod 5$ and $(q_2)^2 = 3(q_1 + q_5)q_3 \pmod 5$, when $q_3 \neq 0 \pmod 5$.

Proof: From Propositions 2 and 3, we have that, when $q_5 \neq 0 \pmod 5$, all 5-PPs can be obtained with the formula $a\bar{\pi}(x) + c$, where $\bar{\pi}(x) = x^5 \pmod 5$ or $\bar{\pi}(x) = x^5 - \alpha x \pmod 5$ (α not a fourth power) or $\bar{\pi}(x) = x^5 - 2\alpha x^3 + \alpha^2 x \pmod 5$ (α not a square). We note that if α is not a fourth power modulo 5, then $\alpha \in \{2, 3, 4\}$ and, if α is not a square modulo 5, then $\alpha \in \{2, 3\}$.

When $\bar{\pi}(x) = x^5 \pmod 5$, it follows that $q_5 \neq 0 \pmod 5$, $q_4 = 0 \pmod 5$, $q_3 = 0 \pmod 5$, $q_2 = 0 \pmod 5$ and $q_1 = 0 \pmod 5$.

When $\bar{\pi}(x) = x^5 - \alpha x \pmod 5$ ($\alpha \in \{2, 3, 4\}$), it follows that $q_5 \neq 0 \pmod 5$, $q_4 = 0 \pmod 5$, $q_3 = 0 \pmod 5$, $q_2 = 0 \pmod 5$ and $q_1 + \alpha q_5 = 0 \pmod 5$ for only one $\alpha \in \{2, 3, 4\}$.

When $\bar{\pi}(x) = x^5 - 2\alpha x^3 + \alpha^2 x \pmod 5$ ($\alpha \in \{2, 3\}$), we have that $q_5 \neq 0 \pmod 5$, $q_4 = 0 \pmod 5$, $q_3 = -2\alpha q_5 \pmod 5$, $q_2 = 0 \pmod 5$ and $q_1 = \alpha^2\ q_5 = 4\ q_5 \pmod 5$. For $\alpha \in \{2, 3\}$, the equality $q_3 = -2\alpha q_5 \pmod 5$ is equivalent to $q_3 + q_5 = 0 \pmod 5$ or $q_3 - q_5 = 0 \pmod 5$, and the equality $q_1 = 4\ q_5 \pmod 5$ is equivalent to $(q_1 + q_5) = 0 \pmod 5$.

Because there are four null quintic polynomials modulo 5, namely $x^5 + 4\,x \pmod 5$, $2x^5 + 3x \pmod 5$, $3x^5 + 2\,x \pmod 5$ and $4x^5 + x \pmod 5$, we have that a quintic polynomial $\pi(x) = q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + q_5 x^5 \pmod 5$ is equivalent to the polynomial $\pi(x) + q_5 x + (5 - q_5)x^5 \pmod 5$, $\forall q_5 \in \mathbb{Z}_5^*$. There are two normalized PPs modulo 5 of degree less than five [17], i.e. $\bar{\pi}(x) = x \pmod 5$ and $\bar{\pi}(x) = x^3 \pmod 5$. Therefore, a 5-PP can also result when $\pi(x) + q_5 x + (5 - q_5)x^5 \pmod 5 = a(x + b) + c$, or $\pi(x) + q_5 x + (5 - q_5)x^5 \pmod 5 = a(x + b)^3 + c$, with $a \neq 0$, b, $c \in \mathbb{Z}_5$.

Considering the analysis for CPPs [6] or for 4-PPs [8], for the normalized PP $\bar{\pi}(x) = x \pmod 5$, we have that $q_5 \neq 0 \pmod 5$, $q_4 = 0 \pmod 5$, $q_3 = 0 \pmod 5$, $q_2 = 0 \pmod 5$ and $q_1 + q_5 \neq 0 \pmod 5$.

We note that for the normalized PPs $\bar{\pi}(x) = x^5 \pmod 5$, $\bar{\pi}(x) = x^5 - \alpha x \pmod 5$ ($\alpha \in \{2, 3, 4\}$) and $\bar{\pi}(x) = x \pmod 5$, the common conditions on the coefficients q_5, q_4, q_3, q_2 are $q_5 \neq 0 \pmod 5$, $q_4 = 0 \pmod 5$, $q_3 = 0 \pmod 5$ and $q_2 = 0 \pmod 5$. The condition for the coefficient q_1 is just $q_1 + q_5 \neq 0 \pmod 5$, because it includes the conditions for all the normalized PPs above. Indeed, for $q_1 = 0 \pmod 5$, we have that $q_1 + q_5 \neq 0 \pmod 5$, $\forall q_5 \neq 0 \pmod 5$, and the condition $q_1 + \alpha q_5 = 0 \pmod 5$ for any $\alpha \in \{2, 3, 4\}$ and for only one $q_5 \neq 0 \pmod 5$ is equivalent to $q_1 \in \{\mathbb{Z}_5^* - (-q_5)\}$ and, therefore, $q_1 + q_5 \neq 0 \pmod 5$. Thus, for the three normalized PPs, the conditions in 1) result for $q_5 \neq 0 \pmod 5$.

For the normalized PP $\bar{\pi}(x) = x^3 \pmod 5$, we have that $q_5 \neq 0 \pmod 5$, $q_4 = 0 \pmod 5$, $q_3 \neq 0 \pmod 5$ and $(q_2)^2 = 3(q_1 + q_5)q_3 \pmod 5$. We note that for the normalized PP $\bar{\pi}(x) = x^5 - 2\alpha x^3 + \alpha^2 x \pmod 5$ ($\alpha \in \{2, 3\}$), the conditions on the coefficients are included in those for the normalized PP $\bar{\pi}(x) = x^3 \pmod 5$, because for $q_2 = 0 \pmod 5$ and $q_1 + q_5 = 0 \pmod 5$, we have that $(q_2)^2 = 3(q_1 + q_5)q_3 \pmod 5$. Thus, for the two normalized PPs, conditions 2) result for $q_5 \neq 0 \pmod 5$.

When $q_5 = 0 \pmod 5$, we can use the test on the coefficients of a 4-PP from [8], for the case $3 \nmid (p - 1)$ and $n = 1$. This is given by conditions 1) or 2) for $q_5 = 0 \pmod 5$. ■

2) $p = 5$ AND $n > 1$

Theorem 6: $\pi(x) = q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + q_5 x^5 \pmod{5^n}$, with $n > 1$, is PP iff:

1) $q_4 = q_3 = q_2 = 0 \pmod 5$, $q_1 \neq 0 \pmod 5$ and $(q_1 + q_5) \neq 0 \pmod 5$,
   or iff:
2) $q_4 = 0 \pmod 5$, $(q_2)^2 = 3(q_1 + q_5)q_3 \pmod 5$ and
   (2.1) $q_3 + q_5 = 0 \pmod 5$,
   or
   (2.2) $q_3 - q_5 = 0 \pmod 5$,
   when $q_5 \neq 0 \pmod 5$,
   or iff:
3) $q_4 = q_3 = q_2 = 0 \pmod 5$ and $q_1 \neq 0 \pmod 5$, when $q_5 = 0\,(\mathrm{mod}\ 5)$.

Proof: To prove the necessity, we assume that $\pi(x)$ is a PP $\pmod{5^n}$, with $n > 1$. Then, from Theorem 2, it follows that $\pi(x)$ is PP $\pmod 5$ and

$$\begin{aligned} \pi'(x) &= q_1 + 2q_2 x + 3q_3 x^2 + 4q_4 x^3 + 5q_5 x^4 \pmod 5 \\ &= q_1 + 2q_2 x + 3q_3 x^2 + 4q_4 x^3 \neq 0 \pmod 5 \end{aligned} \tag{9}$$

Because $\pi(x)$ is PP $\pmod 5$, $q_4 = 0 \pmod 5$ and, consequently

$$\pi'(x) = q_1 + 2q_2 x + 3q_3 x^2 \neq 0 \pmod 5. \tag{10}$$

As in the proof of Theorem 5, from Propositions 2 and 3, when $q_5 \neq 0 \pmod 5$, we have that all 5-PPs can be obtained with the formula $a\bar{\pi}(x) + c$, with $a \neq 0, c \in \mathbb{Z}_5$, where $\bar{\pi}(x) = x^5 \pmod 5$ or $\bar{\pi}(x) = x^5 - \alpha x \pmod 5$ ($\alpha \in \{2, 3, 4\}$) or $\bar{\pi}(x) = x^5 - 2\alpha x^3 + \alpha^2 x \pmod 5$ ($\alpha \in \{2, 3\}$). Thus, we have that $\pi'(x) = a\bar{\pi}'(x) = q_5\bar{\pi}'(x)$. In the following we will consider each normalized PP.

When $\bar{\pi}(x) = x^5 \pmod 5$, it follows that $\pi'(x) = q_5\bar{\pi}'(x) = 5\,q_5\,x^4 \pmod 5 = 0 \pmod 5$. Therefore, the value $q_1 = 0 \pmod 5$, under conditions 1) from Theorem 5, is invalid for this case.

When $\bar{\pi}(x) = x^5 - \alpha x \pmod 5$ ($\alpha \in \{2, 3, 4\}$), we have that $\pi'(x) = q_5\bar{\pi}'(x) = q_5(5x^4 - \alpha) \pmod 5 = -\alpha q_5 \pmod 5 \neq 0 \pmod 5$, $\forall q_5 \neq 0 \pmod 5$ for $\alpha \in \{2, 3, 4\}$.

When $\bar{\pi}(x) = x^5 - 2\alpha x^3 + \alpha^2 x \pmod 5$ ($\alpha \in \{2, 3\}$), we have that $\pi'(x) = q_5\bar{\pi}'(x) = q_5(5x^4 - 2\alpha \cdot 3\,x^2 + \alpha^2) \pmod 5 = 4\,q_5(\alpha x^2 + 1) \pmod 5$. It is easy to verify that the equation $(\alpha x^2 + 1) = 0 \pmod 5$ has no solution for $\alpha = 2$ or $\alpha = 3$. Because in this case $\pi'(x) \neq 0$, $\forall x \in \mathbb{Z}_5$, conditions 2) from Theorem 5, for $q_5 \neq 0 \pmod 5$, are still valid when $q_3 + q_5 = 0 \pmod 5$ or $q_3 - q_5 = 0 \pmod 5$, resulting in conditions 2) from Theorem 6.

For the two normalized PPs modulo 5 of degree less than 5, when $q_5 \neq 0 \pmod 5$, all 5-PPs can be obtained with the formula $\pi(x) + q_5 x + (5 - q_5)x^5 \pmod 5 = a\bar{\pi}(x+b) + c$, with $a \neq 0, b, c \in \mathbb{Z}_5$. Thus, we have that $\pi'(x) = (a\bar{\pi}'(x + b) - q_5) \pmod 5$.

When $\bar{\pi}(x) = x \pmod 5$, $a = q_1 + q_5$ and we have that $\pi'(x) = q_1 \pmod 5$. Therefore, beside conditions 1) from Theorem 5, when $q_5 \neq 0 \pmod 5$ we have to additionally impose $q_1 \neq 0 \pmod 5$, resulting in conditions 1) from Theorem 6.

When $\bar{\pi}(x) = x^3 \pmod 5$, then $a = q_3$ and we have that $\pi'(x) = q_3\bar{\pi}'(x + b) - q_5 = 3\ q_3(x + b)^2 - q_5$. As $q_3 \neq 0 \pmod 5$ then from [6], it follows that $b = \frac{q_2}{3q_3}$. The equation $3\ q_3(x + b)^2 - q_5 = 0 \pmod 5$ is equivalent to $(x + b)^2 = \frac{q_5}{3q_3} \pmod 5$. For this equation to have no solution, $\frac{q_5}{3q_3}$ can not be a square modulo 5, that is $\frac{q_5}{3q_3} = 2 \pmod 5$ or $\frac{q_5}{3q_3} = 3 \pmod 5$. These equalities are equivalent to $q_3 - q_5 = 0 \pmod 5$ or $q_3 + q_5 = 0 \pmod 5$, respectively. Therefore, besides equalities (2) from Theorem 5, when $q_5 \neq 0 \pmod 5$, we have to impose the equalities $q_3 + q_5 = 0 \pmod 5$ or $q_3 - q_5 = 0 \pmod 5$, resulting in conditions 2) of Theorem 6.

When $q_5 = 0 \pmod 5$, we can apply the coefficient test on a 4-PP from [8], when $3 \nmid (p - 1)$ and $n > 1$. This is given by conditions 3) from Theorem 6.

To prove the sufficiency, we assume that the conditions on the coefficients from the theorem statement are fulfiled. From these conditions, we have that $\pi(x)$ is PP $\pmod 5$. According to Theorem 2, we still need to show that $\pi'(x) \neq 0 \pmod 5$, $\forall x \in \mathbb{Z}_5$, where $\pi'(x)$ is that from (10).

In cases (1) and (3), as $q_3 = q_2 = 0 \pmod 5$, we have that $\pi'(x) = q_1 \neq 0 \pmod 5$, $\forall x \in \mathbb{Z}_5$.

Case 2) follows from the equivalence of equations $\pi'(x) = 0 \pmod 5$ and $(x + b)^2 = \frac{q_5}{3q_3} \pmod 5$, with $b = \frac{q_2}{3q_3}$. Therefore, for conditions (2.1) or (2.2) the equation has no solution modulo 5. Thus, $\pi'(x) \neq 0 \pmod 5$, $\forall x \in \mathbb{Z}_5$, also in this case. ■

We remark that in the algorithm from [13], all PPs of degree no more than six are generated using Theorems 1 and 2 and the Chinese remainder theorem. PPs modulo p are generated using Propositions 1 and 2, where $\pi(x)$ is either an explicit normalized PP for $p > 5$ or $\pi(x)$ is generated by the coefficients' conditions for $p = 2$, $p = 3$ or $p = 5$. However, the generation of all PPs by the coefficients' conditions is simpler and easier for implementation.

TABLE 2. Quintic normalized PPs modulo p for $p > 5$.

Normalized PP	p
$\bar{\pi}(x) = x^5$	$p \neq 1 \pmod 5$
$\bar{\pi}(x) = x^5 \pm 2x^2$	$p = 7$
$\bar{\pi}(x) = x^5 + \alpha x^3 \pm x^2 + 3\alpha^2 x$, α not a square	$p = 7$
$\bar{\pi}(x) = x^5 + \alpha x^3 + 5^{-1}\alpha^2 x$, α arbitrary	$p = 2, 3 \pmod 5$
$\bar{\pi}(x) = x^5 + \alpha x^3 + 3\alpha^2 x$, α not a square	$p = 13$

Because for $p > 5$ there are seven normalized quintic PPs [17] (given in Table 2), we give a unified approach for the conditions on the coefficients of a 5-PP, when the normalized PP has the form:

$$\bar{\pi}(x) = x^5 + a_3x^3 + a_2x^2 + a_1x \tag{11}$$

Lemma 1: Let $\pi(x) = q_1x + q_2x^2 + q_3x^3 + q_4x^4 + q_5x^5 \pmod p$, where $q_5 \neq 0 \pmod p$. Then, $\pi(x)$ can be factorized as $\pi(x) = a\big((x + b)^5 + a_3(x + b)^3 + a_2(x + b)^2 + a_1(x + b)\big) + c \pmod p$ iff the following three conditions are fulfilled:

1) $5\ q_3\ q_5 = 2(q_4)^2 + 5\ a_3(q_5)^2 \pmod p$,
2) $25\ q_2(q_5)^2 = 2(q_4)^3 + 15\ a_3\ q_4(q_5)^2 + 25\ a_2(q_5)^3 \pmod p$,
3) $125\ q_1(q_5)^3 = (q_4)^4 + 15\ a_3(q_4)^2(q_5)^2 + 50\ a_2\ q_4(q_5)^3 + 125\ a_1(q_5)^4 \pmod p$.

Proof: We consider that $\pi(x) = a\big((x + b)^5 + a_3(x + b)^3 + a_2(x + b)^2 + a_1(x + b)\big) + c \pmod p$. Then, we can write

$$\begin{aligned}\pi(x) = {} & ax^5 + 5abx^4 + a(10b^2 + a_3)x^3 \\ & + a(10b^3 + 3a_3b + a_2)x^2 \\ & + a(5b^4 + 3a_3b^2 + 2a_2b + a_1)x \\ & + a(b^5 + a_3b^5 + a_2b^2 + a_1b)x + c \pmod p\end{aligned} \tag{12}$$

By identifying the coefficients of degree 5, 4, 3, 2, 1 and 0, we have that

$$a = q_5, \tag{13}$$

$$b = \frac{q_4}{5q_5} \pmod p, \tag{14}$$

$$q_3 = 10q_5\left(\frac{q_4}{5q_5}\right)^2 + a_3q_5 \pmod p, \tag{15}$$

$$q_2 = 10q_5\left(\frac{q_4}{5q_5}\right)^3 + a_3q_5\frac{q_4}{5q_5} + a_2q_5 \pmod p, \tag{16}$$

$$\begin{aligned}q_1 = {} & 5q_5\left(\frac{q_4}{5q_5}\right)^4 + 3a_3q_5\left(\frac{q_4}{5q_5}\right)^2 \\ & + 2a_2q_5\frac{q_4}{5q_5} + a_1q_5 \pmod p,\end{aligned} \tag{17}$$

$$\begin{aligned}c = {} & -q_5\left(\left(\frac{q_4}{5q_5}\right)^5 + a_3\left(\frac{q_4}{5q_5}\right)^3\right. \\ & \left. + a_2\left(\frac{q_4}{5q_5}\right)^2 + a_1\frac{q_4}{5q_5}\right) \pmod p,\end{aligned} \tag{18}$$

(15), (16) and (17) are equivalent to:

$$5q_3q_5 = 2(q_4)^2 + 5a_3(q_5)^2 \pmod p, \tag{19}$$

$$5q_2(q_5)^2 = 2(q_4)^3 + 15a_3q_4(q_5)^2 + 25a_2(q_5)^3 \pmod p, \tag{20}$$

and

$$\begin{aligned}125q_1(q_5)^3 = {} & (q_4)^4 + 15a_3(q_4)^2(q_5)^2 \\ & + 50a_2q_4(q_5)^3 + 125a_1(q_5)^4 \pmod p,\end{aligned} \tag{21}$$

respectively.

Then, we have that

$$\begin{aligned}\pi(x) = {} & q_5\left(\left(x+\frac{q_4}{5q_5}\right)^5 + a_3\left(x+\frac{q_4}{5q_5}\right)^3\right.\\ & \left.+a_2\left(x+\frac{q_4}{5q_5}\right)^2 + a_1\left(x+\frac{q_4}{5q_5}\right)\right)\\ & -q_5\left(\left(\frac{q_4}{5q_5}\right)^5 + a_3\left(\frac{q_4}{5q_5}\right)^3 + a_2\left(\frac{q_4}{5q_5}\right)^2\right.\\ & \left.+a_1\frac{q_4}{5q_5}\right) \pmod{p} = q_5x^5 + q_4x^4\\ & +\left(10q_5\left(\frac{q_4}{5q_5}\right)^2 + a_3q_5\right)x^3\\ & +\left(10q_5\left(\frac{q_4}{5q_5}\right)^3 + 3a_3q_5\frac{q_4}{5q_5} + a_2q_5\right)x^2\\ & +\left(5q_5\left(\frac{q_4}{5q_5}\right)^4 + 3a_3q_5\left(\frac{q_4}{5q_5}\right)^2\right.\\ & \left.+2a_2q_5\frac{q_4}{5q_5} + a_1q_5\right)x \pmod{p} \qquad (22)\end{aligned}$$

Therefore, conditions (19), (20) and (21) have to be met, that is, the three conditions of the lemma statement.

The reciprocal is proved by the reverse way. ■

To facilitate the handling of cases for PPs modulo p^n, with $p > 5$ and $n > 1$, we remark that when a quintic PP has a corresponding normalized quintic PP, $\bar{\pi}(x)$, according to Proposition 1, it is of the form $\pi(x) = a\bar{\pi}(x+b)+c$, with $a \neq 0, b, c \in \mathbb{Z}_p$. According to Theorem 2, it requires that $\pi'(x) = a\bar{\pi}'(x+b) \neq 0 \pmod{p}$, $\forall x \in \mathbb{Z}_p$. Therefore, if x is a solution for the equation $\bar{\pi}'(x) = 0 \pmod{p}$, then $x - b$ is a solution for the equation $\pi'(x) = 0 \pmod{p}$. The next lemma addresses the solving of equation $\bar{\pi}'(x) = 0 \pmod{p}$, for each normalized PP from Table 2.

We note that if α is not a square modulo 7, then $\alpha \in \{3, 5, 6\}$, and if α is not a square modulo 13, then $\alpha \in \{2, 5, 6, 7, 8, 11\}$.

Lemma 2: Let $\bar{\pi}(x)$ be a normalized PP from Table 2. The equation $\bar{\pi}'(x) = 0 \pmod{p}$ always has solutions modulo p, except for $\bar{\pi}(x) = x^5 + \alpha x^3 + 5^{-1}\alpha^2\,x$, with $\alpha \in \mathbb{Z}_p^*$ and $p = 2, 3 \pmod{5}$.

Proof: For $\bar{\pi}(x) = x^5 \pmod{p}$, with $p \neq 1 \pmod{5}$, we have that $\bar{\pi}'(x) = 5x^4 = 0 \pmod{p}$, with solution $x = 0$.

For $\bar{\pi}(x) = x^5 \pm 2x^2 \pmod{7}$, we have that $\bar{\pi}'(x) = 5x^4 \pm 4x = 0 \pmod{7}$, with solution $x = 0$.

For $\bar{\pi}(x) = x^5 + \alpha x^3 \pm x^2 + 3\alpha^2\,x \pmod{7}$, with $\alpha \in \{3, 5, 6\}$, we have that $\bar{\pi}'(x) = 5x^4 + 3\alpha x^2 \pm 2x + 3\alpha^2 = 0 \pmod{7}$. It can be easily verified that for $\alpha = 3$, the solutions are $x = 2$ and $x = 5$, for $\alpha = 5$, the solutions are $x = 3$ and $x = 4$, and for $\alpha = 6$, the solutions are $x = 1$ and $x = 6$.

For $\bar{\pi}(x) = x^5 + \alpha x^3 + 3\alpha^2\,x \pmod{13}$, with $\alpha \in \{2, 5, 6, 7, 8, 11\}$, we have that $\bar{\pi}'(x) = 5x^4 + 3\alpha x^2 + 3\alpha^2 = 0 \pmod{13}$. It can be easily verified that for $\alpha = 2$, the solutions are $x = 6$ and $x = 7$, for $\alpha = 5$, the solutions are $x = 5$ and $x = 8$, for $\alpha = 6$, the solutions are $x = 2$ and $x = 11$, for $\alpha = 7$, the solutions are $x = 3$ and $x = 10$, for $\alpha = 8$, the solutions are $x = 1$ and $x = 12$, and for $\alpha = 11$, the solutions are $x = 4$ and $x = 9$.

For $\bar{\pi}(x) = x^5 + \alpha x^3 + 5^{-1}\alpha^2\,x \pmod{p}$, with $p = 2, 3 \pmod{5}$ and arbitrary α, we have that $\bar{\pi}'(x) = 5x^4 + 3\alpha x^2 + 5^{-1}\alpha^2 = 0 \pmod{p}$. We use the substitution $x^2 = y$ and one of the following equation results: $5y^2 + 3\alpha y + 5^{-1}\alpha^2 = 0 \pmod{p}$ or $25y^2 + 15\alpha y + \alpha^2 = 0 \pmod{p}$ or $(5y)^2 + 2 \cdot 5y \cdot 2^{-1} \cdot 3\alpha + (2^{-1} \cdot 3\alpha)^2 + \alpha^2 - (2^{-1} \cdot 3\alpha)^2 = 0 \pmod{p}$ or $(5y + 2^{-1} \cdot 3\alpha)^2 + \alpha^2 - (2^{-1} \cdot 3\alpha)^2 = 0 \pmod{p}$ or $(10y + 3\alpha)^2 + 4\alpha^2 - (3\alpha)^2 = 0 \pmod{p}$ or $(10y + 3\alpha)^2 = 5\alpha^2 \pmod{p}$. The last equation has solutions modulo p for $\alpha \neq 0 \pmod{p}$ if $5\alpha^2$ is a quadratic residue modulo p. As α^2 is a quadratic residue, according to Theorem 85 from [16], $5\alpha^2$ is a quadratic residue, only if 5 is a quadratic residue. But, according to Theorem 97 in [16], 5 is a quadratic non-residue for $p = 2, 3 \pmod{5}$. Therefore, the equation $(10y + 3\alpha)^2 = 5\alpha^2 \pmod{p}$ has no solution for $p = 2, 3 \pmod{5}$ and $\alpha \neq 0 \pmod{p}$. ■

D. $p = 7$

1) $p = 7$ AND $n = 1$

Theorem 7: $\pi(x) = q_1x + q_2x^2 + q_3x^3 + q_4x^4 + q_5x^5 \pmod{7}$ is PP iff:

1) $4\ q_2(q_5)^2 = 2(q_4)^3 \pmod{7}$ and $6\ q_1(q_5)^3 = (q_4)^4 \pmod{7}$,
or iff:
2) $4\ q_2(q_5)^2 = 2(q_4)^3 \pm (q_5)^3 \pmod{7}$ and $6\ q_1(q_5)^3 = (q_4)^4 \pm 2\ q_4(q_5)^3 \pmod{7}$,
when $q_5 \neq 0 \pmod{7}$ and $5\ q_3\ q_5 = 2(q_4)^2 \pmod{7}$,
or iff:
3) $4\,q_2(q_5)^2 = 2(q_4)^3 + \alpha q_4(q_5)^2 \pmod{7}$ and $6\,q_1(q_5)^3 = (q_4)^4 + \alpha(q_4)^2(q_5)^2 + 4\alpha^2(q_5)^4 \pmod{7}$, where $\alpha = (q_3\ q_5 + (q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod{7}$,
when $q_5 \neq 0 \pmod{7}$ and $5\ q_3\ q_5 \neq 2(q_4)^2 \pmod{7}$,
or iff:
4) $4\ q_2(q_5)^2 = 2(q_4)^3 + \alpha q_4(q_5)^2 \pm 4(q_5)^3 \pmod{7}$ and $6\ q_1(q_5)^3 = (q_4)^4 + \alpha(q_4)^2(q_5)^2 \pm q_4(q_5)^3 + 4\alpha^2(q_5)^4 \pmod{7}$, where $\alpha = (q_3\ q_5 + (q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod{7}$,
when $\alpha \in \{3, 5, 6\}$, $q_5 \neq 0 \pmod{7}$ and $5\ q_3\ q_5 \neq 2(q_4)^2 \pmod{7}$,
5) $3(q_3)^2 = q_2\ q_4 \pmod{7}$ and $2\ q_1(q_4)^2 = (q_3)^3 + (q_4)^3$,
or iff:
6) $3(q_3)^2 = q_2\ q_4 \pmod{7}$ and $2\ q_1(q_4)^2 = (q_3)^3 + 6(q_4)^3 \pmod{7}$,
when $q_5 = 0 \pmod{7}$ and $q_4 \neq 0 \pmod{7}$,
or iff:
7) $q_3 = q_2 = 0 \pmod{7}$ and $q_1 \neq 0 \pmod{7}$, when $q_5 = q_4 = 0 \pmod{7}$.

Proof: If $q_5 \neq 0 \pmod{7}$, considering Proposition 1, Lemma 1 and the normalized PPs modulo 7 from Table 2, the next conditions result.

1) $5\ q_3\ q_5 = 2(q_4)^2 \pmod 7$, $4\ q_2(q_5)^2 = 2(q_4)^3 \pm (q_5)^3 \pmod 7$ and $6\ q_1(q_5)^3 = (q_4)^4 \pm 2\ q_4(q_5)^3 \pmod 7$,

or

2) $5\ q_3\ q_5 = 2(q_4)^2 + 5\alpha(q_5)^2 \pmod 7$, $4\ q_2(q_5)^2 = 2(q_4)^3 + \alpha q_4(q_5)^2 \pm 4(q_5)^3 \pmod 7$ and $6\ q_1(q_5)^3 = (q_4)^4 + \alpha(q_4)^2(q_5)^2 \pm q_4(q_5)^3 + 4\alpha^2(q_5)^4 \pmod 7$, for only one $\alpha \in \{3, 5, 6\}$,

or

3) $5\ q_3\ q_5 = 2(q_4)^2 + 5\alpha(q_5)^2 \pmod 7$, $4\ q_2(q_5)^2 = 2(q_4)^3 + \alpha q_4(q_5)^2 \pmod 7$ and $6\ q_1(q_5)^3 = (q_4)^4 + \alpha(q_4)^2(q_5)^2 + 4\alpha^2(q_5)^4 \pmod 7$, for only one $\alpha \in \mathbb{Z}_7$.

Because the conditions 2) and 3) above need up to three and seven sets of checking conditions, respectively, it is more efficient to compute the value of α from the first congruence equation in these sets of conditions. This congruence equation is equivalent to:

$$\alpha(q_5)^2 = q_3 q_5 + (q_4)^2 \pmod 7 \tag{23}$$

Because $q_5 \neq 0 \pmod 7$, we have that $(q_5)^2 \neq 0 \pmod 7$. Then, the congruence equation (23) has only one solution [16], which is $\alpha = 0 \pmod 7$ if $5\ q_3\ q_5 = 2(q_4)^2 \pmod 7$, and $\alpha \neq 0 \pmod 7$ if $5\ q_3\ q_5 \neq 2(q_4)^2 \pmod 7$. To find the solution, we need to compute the inverse modulo 7 of $(q_5)^2$. An algorithm for finding the arithmetic inverse of an integer modulo other integer is given in Table 2 from [19]. The six values of the inverses modulo 7 for $\{1, 2, 3, 4, 5, 6\}$ are $\{1, 4, 5, 2, 3, 6\}$, respectively, in this order. These values can be stored in an array before proceeding to find 5-PPs modulo a number which contains 7 as a prime factor. Thus, if $q_5 \neq 0 \pmod 7$, the conditions 1) or 2) and 3) or 4) from the theorem result.

If $q_5 = 0 \pmod 7$, we can apply the test coefficient for 4-PPs from [8], resulting the conditions 5) or 6) or 7) from Theorem 7. ■

2) $p = 7$ AND $n > 1$

Theorem 8: $\pi(x) = q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + q_5 x^5 \pmod{7^n}$, with $n > 1$, is PP iff:

1) $5\ q_3\ q_5 \neq 2(q_4)^2 \pmod 7$, $4\ q_2(q_5)^2 = 2(q_4)^3 + \alpha q_4(q_5)^2 \pmod 7$ and $6\ q_1(q_5)^3 = (q_4)^4 + \alpha(q_4)^2 (q_5)^2 + 4\alpha^2(q_5)^4 \pmod 7$, where $\alpha = (q_3\ q_5 + (q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod 7$,

when $q_5 \neq 0 \pmod 7$,

or iff:

2) $q_4 = q_3 = q_2 = 0 \pmod 7$ and $q_1 \neq 0 \pmod 7$, when $q_5 = 0 \pmod 7$.

Proof: If $q_5 \neq 0 \pmod 7$, according to Theorem 2 and Lemma 2, $\pi(x)$ is PP iff the normalized PP leading to $\pi(x) \pmod 7$ is $\bar{\pi}(x) = x^5 + \alpha x^3 + 5^{-1}\alpha^2\ x \pmod 7$, with $\alpha \in \mathbb{Z}_7^*$. Because $\alpha \neq 0 \pmod 7$, we need $5\ q_3\ q_5 \neq 2(q_4)^2 \pmod 7$. Then, the conditions on the coefficients are those from 3) in Theorem 7.

If $q_5 = 0 \pmod 7$, we can apply the conditions on the coefficients for 4-PPs $\pmod{7^n}$ with $n > 1$ from [8]. These are those in 2) from Theorem 8. ■

E. $p = 13$

1) $p = 13$ AND $n = 1$

Theorem 9: $\pi(x) = q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + q_5 x^5 \pmod{13}$ is PP iff:

1) $12\ q_2(q_5)^2 = 2(q_4)^3 \pmod{13}$ and $8\ q_1(q_5)^3 = (q_4)^4 \pmod{13}$,

when $q_5 \neq 0 \pmod{13}$ and $5\ q_3\ q_5 = 2(q_4)^2 \pmod{13}$,

or iff:

2) $12\ q_2(q_5)^2 = 2(q_4)^3 + 2\alpha q_4(q_5)^2 \pmod{13}$ and $8\ q_1(q_5)^3 = (q_4)^4 + 2\alpha(q_4)^2(q_5)^2 + 12\alpha^2(q_5)^4 \pmod{13}$, where $\alpha = (q_3\ q_5 + 10(q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod{13}$,

when $q_5 \neq 0 \pmod{13}$ and $5\ q_3\ q_5 \neq 2(q_4)^2 \pmod{13}$,

or iff:

3) $12\ q_2(q_5)^2 = 2(q_4)^3 + 2\alpha q_4(q_5)^2 \pmod{13}$ and $8\ q_1(q_5)^3 = (q_4)^4 + 2\alpha(q_4)^2(q_5)^2 + 11\alpha^2(q_5)^4 \pmod{13}$, where $\alpha = (q_3\ q_5 + 10(q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod{13}$,

when $\alpha \in \{2, 5, 6, 7, 8, 11\}$, $q_5 \neq 0 \pmod{13}$ and $5\ q_3\ q_5 \neq 2(q_4)^2 \pmod{13}$,

or iff:

4) $q_4 = q_3 = q_2 = 0 \pmod{13}$ and $q_1 \neq 0 \pmod{13}$, when $q_5 = 0 \pmod{13}$.

Proof: If $q_5 \neq 0 \pmod{13}$, considering Proposition 1, Lemma 1 and the normalized PPs modulo 13 from Table 2, the next conditions result:

1) $5\ q_3\ q_5 = 2(q_4)^2 + 5\alpha(q_5)^2 \pmod{13}$, $12\ q_2(q_5)^2 = 2(q_4)^3 + 2\alpha q_4(q_5)^2 \pmod{13}$ and $8\ q_1(q_5)^3 = (q_4)^4 + 2\alpha(q_4)^2(q_5)^2 + 12\alpha^2(q_5)^4 \pmod{13}$, for only one $\alpha \in \mathbb{Z}_{13}$,

or

2) $5\ q_3\ q_5 = 2(q_4)^2 + 5\alpha(q_5)^2 \pmod{13}$, $12\ q_2(q_5)^2 = 2(q_4)^3 + 2\alpha q_4(q_5)^2 \pmod{13}$ and $8\ q_1(q_5)^3 = (q_4)^4 + 2\alpha(q_4)^2(q_5)^2 + 11\alpha^2(q_5)^4 \pmod{13}$, for only one $\alpha \in \{2, 5, 6, 7, 8, 11\}$.

Because the conditions above need up to 13 and six sets of checking conditions, respectively, it is more efficient to compute the value of α from the first congruence equation in these sets of conditions. This congruence equation is equivalent to:

$$\alpha(q_5)^2 = q_3 q_5 + 10(q_4)^2 \pmod{13} \tag{24}$$

Because $q_5 \neq 0 \pmod{13}$, we have that $(q_5)^2 \neq 0 \pmod{13}$. Then, the congruence equation (24) has only one solution [16], which is $\alpha = 0 \pmod{13}$, if $5\ q_3\ q_5 = 2(q_4)^2 \pmod{13}$, and $\alpha \neq 0 \pmod{13}$, if $5\ q_3\ q_5 \neq 2(q_4)^2 \pmod{13}$. The 12 values of the inverses modulo 13 for $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ are $\{1, 7, 9, 10, 8, 11, 2, 5, 3, 4, 6, 12\}$, in this order, and they can be stored in an array before to proceed for finding 5-PPs modulo a number which contains 13 as prime factor. Thus, if $q_5 \neq 0 \pmod{13}$, the conditions 1) or 2) or 3) in the theorem result.

If $q_5 = 0 \pmod{13}$, we can apply the test for 4-PPs from [8]. This is given by conditions 4) from Theorem 9. ■

2) $p = 13$ AND $n > 1$

Theorem 10: $\pi(x) = q_1x + q_2x^2 + q_3x^3 + q_4x^4 + q_5x^5 \pmod{13^n}$, with $n > 1$, is PP iff:

1) $5\, q_3\, q_5 \neq 2(q_4)^2 \pmod{13}$, $12\, q_2(q_5)^2 = 2(q_4)^3 + 2\alpha q_4(q_5)^2 \pmod{13}$ and $8\, q_1(q_5)^3 = (q_4)^4 + 2\alpha(q_4)^2(q_5)^2 + 12\alpha^2(q_5)^4 \pmod{13}$, where $\alpha = (q_3\, q_5 + 10(q_4)^2) \cdot \left((q_5)^2\right)^{-1} \pmod{13}$,
when $q_5 \neq 0 \pmod{13}$,
or iff:
2) $q_4 = q_3 = q_2 = 0 \pmod{13}$ and $q_1 \neq 0 \pmod{13}$,
when $q_5 = 0 \pmod{13}$.

Proof: If $q_5 \neq 0 \pmod{13}$, according to Theorem 2 and Lemma 2, $\pi(x)$ is PP iff the normalized PP leading to $\pi(x) \pmod{13}$ is $\bar{\pi}(x) = x^5 + \alpha x^3 + 5^{-1}\alpha^2\, x \pmod{13}$, with $\alpha \in \mathbb{Z}^*_{13}$. Because $\alpha \neq 0 \pmod{13}$, we need $5\, q_3\, q_5 \neq 2(q_4)^2 \pmod{13}$. Then, the conditions on the coefficients are those from 2) in Theorem 9.

If $q_5 = 0 \pmod{13}$, we can apply the conditions on the coefficients for 4-PPs $\pmod{13^n}$ with $n > 1$ from [8]. These are those in 2) from Theorem 10. ■

F. $p = 1 \pmod 5$

1) $p = 1 \pmod 5$ AND $n = 1$

Theorem 11: $\pi(x) = q_1x + q_2x^2 + q_3x^3 + q_4x^4 + q_5x^5 \pmod{p}$, with $p = 1 \pmod 5$, is PP iff:

1) $q_5 = q_4 = q_2 = 0 \pmod{p}$ and $q_1 \neq 0 \pmod{p}$,
when $3 \nmid (p-1)$ and $q_3 = 0 \pmod{p}$,
or iff:
2) $q_5 = q_4 = 0 \pmod{p}$ and $(q_2)^2 = 3\, q_1\, q_3 \pmod{p}$,
when $3 \nmid (p-1)$ and $q_3 \neq 0 \pmod{p}$,
or iff:
3) $q_5 = q_4 = q_3 = q_2 = 0 \pmod{p}$ and $q_1 \neq 0 \pmod{p}$,
when $3 \mid (p-1)$.

Proof: Because in this case there are no normalized PPs of fifth or fourth degree, we can apply the coefficient test for CPPs from [6], [7]. ■

2) $p = 1 \pmod 5$ AND $n > 1$

Theorem 12: $\pi(x) = q_1x + q_2x^2 + q_3x^3 + q_4x^4 + q_5x^5 \pmod{p^n}$, with $p = 1 \pmod 5$ and $n > 1$, is PP iff $q_5 = q_4 = q_3 = q_2 = 0 \pmod{p}$ and $q_1 \neq 0 \pmod{p}$.

Proof: Because in this case there are no normalized PPs of fifth or fourth degree, we can apply the coefficient test for CPPs from [6]. ■

G. $p = 2, 3 \pmod 5$ WITH $p > 13$

1) $p = 2, 3 \pmod 5$ WITH $p > 13$ AND $n = 1$

Theorem 13: $\pi(x) = q_1x + q_2x^2 + q_3x^3 + q_4x^4 + q_5x^5 \pmod{p}$, with $p = 2, 3 \pmod 5$ and $p > 13$, is PP iff:

1) $25\, q_2(q_5)^2 = 2(q_4)^3 \pmod{p}$ and $125\, q_1(q_5)^3 = (q_4)^4 \pmod{p}$,
when $q_5 \neq 0 \pmod{p}$ and $5\, q_3\, q_5 = 2(q_4)^2 \pmod{p}$,
or iff:
2) $25\, q_2(q_5)^2 = 2(q_4)^3 + 15\alpha q_4(q_5)^2 \pmod{p}$ and $125\, q_1(q_5)^3 = (q_4)^4 + 15\alpha(q_4)^2(q_5)^2 + 25\alpha^2(q_5)^4 \pmod{p}$,
where $\alpha = (5\, q_3\, q_5 + (p-2)\cdot(q_4)^2)\cdot\left(5(q_5)^2\right)^{-1} \pmod{p}$,
when $q_5 \neq 0 \pmod{p}$ and $5\, q_3\, q_5 \neq 2(q_4)^2 \pmod{p}$,
or iff:
3) $q_4 = q_2 = 0 \pmod{p}$ and $q_1 \neq 0 \pmod{p}$,
when $3 \nmid (p-1)$ and $q_5 = q_3 = 0 \pmod{p}$,
or iff:
4) $q_4 = 0 \pmod{p}$ and $(q_2)^2 = 3\, q_1\, q_3 \pmod{p}$,
when $3 \nmid (p-1)$, $q_5 = 0 \pmod{p}$ and $q_3 \neq 0 \pmod{p}$,
or iff:
5) $q_4 = q_3 = q_2 = 0 \pmod{p}$ and $q_1 \neq 0 \pmod{p}$,
when $3 \mid (p-1)$ and $q_5 = 0 \pmod{p}$.

Proof: If $q_5 \neq 0 \pmod{p}$, by considering Proposition 1, Lemma 1 and the normalized PPs modulo p from Table 2, when $p = 2, 3 \pmod 5$ and $p > 13$, that is $\bar{\pi}(x) = x^5 \pmod{p}$ and $\bar{\pi}(x) = x^5 + \alpha x^3 + 5^{-1}\alpha^2\, x \pmod{p}$, with $\alpha \in \mathbb{Z}^*_p$, the next conditions result:
$5\, q_3\, q_5 = 2(q_4)^2 + 5\alpha(q_5)^2 \pmod{p}$, $25\, q_2(q_5)^2 = 2(q_4)^3 + 15\alpha q_4(q_5)^2 \pmod{p}$ and
$125\, q_1(q_5)^3 = (q_4)^4 + 15\alpha(q_4)^2(q_5)^2 + 25\alpha^2(q_5)^4 \pmod{p}$, for only one $\alpha \in \mathbb{Z}_p$.

Because the conditions above need up to p sets of checking conditions, it is more efficient to compute the value of α from the first congruence equation from this set of conditions. This congruence equation is equivalent to:

$$\alpha \cdot 5(q_5)^2 = 5q_3q_5 + (p-2)\cdot(q_4)^2 \pmod{p} \qquad (25)$$

Because $q_5 \neq 0 \pmod{p}$, we have that $(q_5)^2 \neq 0 \pmod{p}$. Then, the congruence equation (25) has only one solution [16], which is $\alpha = 0 \pmod{p}$ if $5\, q_3\, q_5 = 2(q_4)^2 \pmod{p}$, and $\alpha \neq 0 \pmod{p}$ if $5\, q_3\, q_5 \neq 2(q_4)^2 \pmod{p}$. Thus, if $q_5 \neq 0 \pmod{p}$, the conditions 1) or 2) in the theorem result.

If $q_5 = 0 \pmod{p}$, we can apply the test for 4-PPs from [8]. This is given by conditions 3) or 4) or 5) from Theorem 13. ■

2) $p = 2, 3 \pmod 5$ WITH $p > 13$ AND $n > 1$

Theorem 14: $\pi(x) = q_1x + q_2x^2 + q_3x^3 + q_4x^4 + q_5x^5 \pmod{p^n}$, with $p = 2, 3 \pmod 5$, $p > 13$ and $n > 1$, is PP iff:

1) $5\, q_3\, q_5 \neq 2(q_4)^2 \pmod{p}$, $25\, q_2(q_5)^2 = 2(q_4)^3 + 15\alpha q_4(q_5)^2 \pmod{p}$ and $125\, q_1(q_5)^3 = (q_4)^4 + 15\alpha(q_4)^2(q_5)^2 + 25\alpha^2(q_5)^4 \pmod{p}$, where $\alpha = (5\, q_3\, q_5 + (p-2)\cdot(q_4)^2)\cdot\left(5(q_5)^2\right)^{-1} \pmod{p}$, when $q_5 \neq 0 \pmod{p}$,
or iff:
2) $q_4 = q_3 = q_2 = 0 \pmod{p}$ and $q_1 \neq 0 \pmod{p}$, when $q_5 = 0 \pmod{p}$.

Proof: If $q_5 \neq 0 \pmod{p}$, according to Theorem 2 and Lemma 2, $\pi(x)$ is PP iff the normalized PP leading to $\pi(x) \pmod{p}$ is $\bar{\pi}(x) = x^5 + \alpha x^3 + 5^{-1}\alpha^2\, x \pmod{p}$, with $\alpha \in \mathbb{Z}^*_p$. Because $\alpha \neq 0 \pmod{p}$, we need $5\, q_3\, q_5 \neq 2(q_4)^2 \pmod{p}$. Then, the conditions for the coefficients are those in 2) from Theorem 13.

If $q_5 = 0 \pmod p$, we can apply the conditions on coefficients for 4-PPs $\pmod{p^n}$ with $n > 1$ from [8]. These are those in 2) from Theorem 14. ■

H. $p = 4 \pmod 5$

1) $p = 4 \pmod 5$ and $n = 1$

Theorem 15: $\pi(x) = q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + q_5 x^5 \pmod p$, with $p = 4 \pmod 5$, is PP iff:

1) $5\ q_3\ q_5 = 2(q_4)^2 \pmod p$, $25\ q_2 (q_5)^2 = 2(q_4)^3 \pmod p$ and $125\ q_1 (q_5)^3 = (q_4)^4 \pmod p$, when $q_5 \neq 0 \pmod p$,
or iff:
2) $q_4 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$, when $3 \nmid (p-1)$ and $q_5 = q_3 = 0 \pmod p$,
or iff:
3) $q_4 = 0 \pmod p$ and $(q_2)^2 = 3\ q_1\ q_3 \pmod p$, when $3 \nmid (p-1)$, $q_5 = 0 \pmod p$ and $q_3 \neq 0 \pmod p$,
or iff:
4) $q_4 = q_3 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$, when $3 \mid (p-1)$ and $q_5 = 0 \pmod p$.

Proof: If $q_5 \neq 0 \pmod p$, the conditions in the theorem result by considering Proposition 1, Lemma 1 and the normalized PP modulo p, when $p = 4 \pmod 5$, from Table 2, that is $\bar{\pi}(x) = x^5 \pmod p$.

If $q_5 = 0 \pmod p$, we can apply the test for 4-PPs from [8]. ■

2) $p = 4 \pmod 5$ and $n > 1$

Theorem 16: $\pi(x) = q_1 x + q_2 x^2 + q_3 x^3 + q_4 x^4 + q_5 x^5 \pmod{p^n}$, with $p = 4 \pmod 5$ and $n > 1$, is PP iff $q_5 = q_4 = q_3 = q_2 = 0 \pmod p$ and $q_1 \neq 0 \pmod p$.

Proof: Because in this case the only normalized quintic PP is $\bar{\pi}(x) = x^5 \pmod p$ and the equation $\bar{\pi}'(x) = 0 \pmod p$ always has solutions, we have that $q_5 = 0 \pmod p$ and thus, we can apply the coefficient test for 4-PPs from [8]. ■

IV. COMPLEXITY ANALYSIS

The algorithm in the beginning of Section III is based on Theorems 1 and 2. Using only these two theorems, for every prime number p dividing N, we need to check if $\pi(x)$ is PP modulo p and, if $n_{N,p} > 1$, we need to check if $\pi'(x) \neq 0 \pmod p$ for every $x \in \mathbb{Z}_p$. Using the brute-force method, named the direct test for only prime number, for a 5-PP we can compute $\pi(x) \pmod p$ for a given x in an efficient way, as follows:

$$\pi(x) = \Big(q_1 + \big(q_2 + (q_3 + (q_4 + q_5 \cdot x) \cdot x) \cdot x\big) \cdot x\Big) \cdot x \pmod p \qquad (26)$$

Thus, to compute a value of $\pi(x) \pmod p$, we need to perform five multiplications, four additions and a modulo p operation. If $\pi(x) \pmod p$ is a 5-PP and if we set $\pi(0) = 0 \pmod p$ and $\pi(1) = (q_1 + q_2 + q_3 + q_4 + q_5) \pmod p$, for all $x \in \mathbb{Z}_p$ we need to perform $5 \cdot (p-2) = 5 \cdot p - 10$ multiplications, $4 \cdot (p-2) + 4 = 4 \cdot p - 4$ additions, $p - 1$ modulo p operations, $1 + 2 + 3 + \cdots + p - 1 = p \cdot (p-1)/2$ comparisons, and to store p values. If $\pi(x) \pmod p$ is not a 5-PP, the number of operations could be lower.

To compute the value $\pi'(x) \pmod p$, similarly to (26), we have that:

$$\pi'(x) = \Big(q_1 + \big(2 \cdot q_2 + (3 \cdot q_3 + (4 \cdot q_4 + 5 \cdot q_5 \cdot x) \cdot x) \cdot x\big) \cdot x\Big) \pmod p \qquad (27)$$

Thus, to compute a value of $\pi'(x) \pmod p$, we need to perform eight multiplications, four additions and a modulo p operation. If we store the values $2 \cdot q_2$, $3 \cdot q_3$, $4 \cdot q_4$ and $5 \cdot q_5$, we only need to perform four multiplications, four additions and a modulo p operation. Thus, if $\pi(x) \pmod{p^{n_{N,p}}}$ with $n_{N,p} > 1$ is a 5-PP and if we set $\pi'(0) = q_1 \pmod p$ and $\pi'(1) = (q_1 + 2 \cdot q_2 + 3 \cdot q_3 + 4 \cdot q_4 + 5 \cdot q_5) \pmod p$, in order to check that $\pi'(x) \neq 0 \pmod p$, for all $x \in \mathbb{Z}_p$ we need to perform $4 \cdot (p-2) + 4 = 4 \cdot p - 4$ multiplications, $4 \cdot (p-2) + 4 = 4 \cdot p - 4$ additions, p modulo p operations and p comparisons, and to store 4 values. If $\pi(x) \pmod{p^{n_{N,p}}}$ is not a 5-PP, the number of operations could be lower. Overall, if $\pi(x) \pmod{p^{n_{N,p}}}$ with $n_{N,p} > 1$ is a 5-PP, we require $9 \cdot p - 14$ multiplications, $8 \cdot p - 8$ additions, $2 \cdot p - 1$ modulo p operations, $p + p \cdot (p-1)/2$ comparisons, and to store $p + 4$ values.

Looking at the conditions in Table 1, we see that the most complex operations are for $p = 7$, $p = 13$ and $p = 2, 3 \pmod 5$, with $p > 13$. These cases require the computation of the inverses modulo p for computing the value of α. As it was mentioned in the proof of Theorem 7, these inverses modulo p can be computed off-line and then stored in an array, before proceeding to find the 5-PPs for a specific application.

The analysis below is done for the case when $\pi(x) \pmod 7$ is a 5-PP. Similar analyzes can be carried out for the cases when $\pi(x) \pmod{13}$ or $\pi(x) \pmod p$, with $p = 2, 3 \pmod 5$ and $p > 13$, is a 5-PP.

Considering the above analysis done for checking 5-PPs using the direct test, we need to perform 25 multiplications, 24 additions, 6 modulo 7 operations, 21 comparisons, and to store 7 values, when $\pi(x) \pmod 7$ is a 5-PP.

In the following, we determine and explain the minimum and maximum number of operations and the storage requirements for checking 5-PPs $\pmod 7$ using the test from Table 1.

For $p = 7$, to test if $q_5 \neq 0 \pmod 7$, we require a modulo 7 operation and a comparison. In our implementation, we firstly compute and store the following eight values $q4\_to\_2 = q_4 \cdot q_4$, $q5\_to\_2 = q_5 \cdot q_5$, $q4\_to\_3 = q4\_to\_2 \cdot q_4$, $q5\_to\_3 = q5\_to\_2 \cdot q_5$, $q4\_to\_4 = q4\_to\_2 \cdot q4\_to\_2$, $right\_term1 = (q3 \cdot q5 + q4\_to\_2) \pmod 7$, $left\_term2 = (4 \cdot q_2 \cdot q5\_to\_2) \pmod 7$ and $left\_term3 = (6 \cdot q_1 \cdot q5\_to\_3) \pmod 7$. To compute these values, we require 10 multiplications, one addition, and three modulo 7 operations. The condition $right\_term1 = 0$ is equivalent to $5\ q_3\ q_5 = 2(q_4)^2 \pmod 7$.

TABLE 3. The number of operations to check whether a quintic polynomial is a 5-PP modulo $p^{n_{N,p}}$. The notation ($a \div b$), with a and b non-negative integers ($a < b$), means that the number of operations can take values from a up to b.

Prime number p	Power of p, $n_{N,p}$	Method and supplementary conditions $(\bmod p)$	Multiplications (5-PP / not 5-PP)	Additions/ Substractions (5-PP / not 5-PP)	Modulo operations (5-PP / not 5-PP)	Comparisons (5-PP / not 5-PP)	Stored values (5-PP / not 5-PP)
$p=2$	$n_{N,2}=1$	the direct test	0	4	1	1	2
$p=2$	$n_{N,2}=1$	Table 1	0	4	1	1	0
$p=2$	$n_{N,2}>1$	Theorem 2 and the direct test	$4/(0 \div 4)$	$8/(4 \div 8)$	$3/(1 \div 3)$	$3/(1 \div 3)$	$6/(2 \div 6)$
$p=2$	$n_{N,2}>1$	Table 1	0	$2/(0 \div 2)$	$3/(1 \div 3)$	$3/(1 \div 3)$	0
$p=3$	$n_{N,3}=1$	the direct test	$5/(0 \div 5)$	$8/(4 \div 8)$	$2/(1 \div 2)$	$3/(1 \div 3)$	$3/(2 \div 3)$
$p=3$	$n_{N,3}=1$	Table 1	0	$3/(1 \div 3)$	$2/(1 \div 2)$	$2/(1 \div 2)$	0
$p=3$	$n_{N,3}>1$	Theorem 2 and the direct test	$13/(0 \div 13)$	$16/(4 \div 16)$	$5/(1 \div 5)$	$6/(2 \div 6)$	$7/(2 \div 7)$
$p=3$	$n_{N,3}>1$	Table 1	$2/(0 \div 2)$	$7/(0 \div 7)$	$5/(1 \div 5)$	$5/(1 \div 5)$	0
$p=5$	$n_{N,5}=1$	the direct test	$15/(0 \div 15)$	$16/(4 \div 16)$	$4/(1 \div 4)$	$10/(1 \div 10)$	$5/(2 \div 5)$
$p=5$	$n_{N,5}=1$	Table 1, $q_3=0$	0	$1/(0 \div 1)$	$4/(1 \div 4)$	$4/(1 \div 4)$	0
		Table 1, $q_3 \neq 0$	$3/(0 \div 3)$	$1/(0 \div 1)$	$4/(1 \div 4)$	$3/(1 \div 3)$	0
$p=5$	$n_{N,5}>1$	Theorem 2 and the direct test	$31/(0 \div 31)$	$32/(4 \div 32)$	$9/(1 \div 9)$	$15/(1 \div 15)$	$9/(2 \div 9)$
$p=5$	$n_{N,5}>1$	Table 1, $q_5 \neq 0$, $q_3=0$	0	$1/(0 \div 1)$	$6/(1 \div 6)$	$6/(1 \div 6)$	0
		Table 1, $q_5 \neq 0$, $q_3 \neq 0$	$3/(0 \div 4)$	$2/(0 \div 3)$	$6/(1 \div 7)$	$5/(1 \div 6)$	0
		Table 1, $q_5=0$	0	0	$5/(1 \div 5)$	$5/(1 \div 5)$	0
$p=7$	$n_{N,7}=1$	the direct test	$25/(0 \div 25)$	$24/(4 \div 24)$	$6/(1 \div 6)$	$21/(1 \div 21)$	$6/(2 \div 6)$
$p=7$	$n_{N,7}=1$	Table 1, $q_5 \neq 0$, $5q_3q_5 = 2(q_4)^2$	$11/(14 \div 18)$	$1/(3 \div 5)$	$6/(7 \div 10)$	$4/(5 \div 8)$	8
		Table 1, $q_5 \neq 0$, $5q_3q_5 \neq 2(q_4)^2$	$18/(18 \div 23)$	$4/(4 \div 8)$	$8/(7 \div 12)$	$4/(6 \div 11)$	17

TABLE 3. ***Continued.*** **The number of operations to check whether a quintic polynomial is a 5-PP modulo $p^{n_{N,p}}$. The notation ($a \div b$), with a and b non-negative integers ($a < b$), means that the number of operations can take values from a up to b.**

Prime number p	Power of p, $n_{N,p}$	Method and supplementary conditions (mod p)	Multiplications (5-PP / not 5-PP)	Additions/ Substractions (5-PP / not 5-PP)	Modulo operations (5-PP / not 5-PP)	Comparisons (5-PP / not 5-PP)	Stored values (5-PP / not 5-PP)
$p = 4 \pmod 5$	$n_{N,p} = 1$	Table 1, $q_5 \neq 0$	14/(4 $\div$14)	0	7/(3 $\div$7)	4/(2 $\div$4)	2/(1 $\div$2)
		Table 1, $q_5 = 0$, $(p-1) = 0 \pmod 3$	0	0	6/(2 $\div$6)	6/(2 $\div$6)	0
		Table 1, $q_5 = 0$, $(p-1) \neq 0 \pmod 3$, $q_3 \neq 0$	3/(0 $\div$3)	0	6/(2 $\div$6)	5/(2 $\div$5)	0
		Table 1, $q_5 = 0$, $(p-1) \neq 0 \pmod 3$, $q_3 = 0$	0	0	6/(2 $\div$6)	6/(2 $\div$6)	0
$p = 2, 3 \pmod 5$	$n_{N,p} = 1$	Table 1, $q_5 \neq 0$, $5q_3q_5 = 2(q_4)^2$	14/(10 $\div$14)	2	6/(4 $\div$6)	4/3($\div$4)	3
		Table 1, $q_5 \neq 0$, $5q_3q_5 \neq 2(q_4)^2$	22/(13 $\div$22)	6/(4 $\div$6)	8/(6 $\div$8)	4/(3 $\div$4)	$p+3$
		Table 1, $q_5 = 0$, $(p-1) = 0 \pmod 3$	0	0	6/(2 $\div$6)	6/(2 $\div$6)	0
		Table 1, $q_5 = 0$, $(p-1) \neq 0 \pmod 3$, $q_3 \neq 0$	3/(0 $\div$3)	0	6/(2 $\div$6)	5/(2 $\div$5)	0
		Table 1, $(p-1) \neq 0 \pmod 3$, $q_3 = 0$	0	0	6/(2 $\div$6)	6/(2 $\div$6)	0
$p = 11$ or $p > 13$	$n_{N,p} > 1$	Theorem 2 and the direct test	$(9p-14)$ / $\big(0\div (9p-14)\big)$	$(8p-8)$ / $\big(4\div (8p-8)\big)$	$(2p-1)$ / $\big(1\div (2p-1)\big)$	$(p + p(p-1)/2)$ / $\big(1\div (p + p(p-1)/2)\big)$	$(p+4)$ / $\big(2\div (p+4)\big)$
$p = 1 \pmod 5$	$n_{N,p} > 1$	Table 1	0	0	5/(1 $\div$5)	5/(1 $\div$5)	0
$p = 4 \pmod 5$	$n_{N,p} > 1$	Table 1	0	0	5/(2 $\div$5)	5/(2 $\div$5)	0

TABLE 3. ***Continued.*** **The number of operations to check whether a quintic polynomial is a 5-PP modulo $p^{n_{N,p}}$. The notation ($a \div b$), with a and b non-negative integers ($a < b$), means that the number of operations can take values from a up to b.**

Prime number p	Power of p, $n_{N,p}$	Method and supplementary conditions $(\bmod\ p)$	Multiplications (5-PP / not 5-PP)	Additions/ Substractions (5-PP / not 5-PP)	Modulo operations (5-PP / not 5-PP)	Comparisons (5-PP / not 5-PP)	Stored values (5-PP / not 5-PP)
$p = 2, 3 \pmod 5$ and $p > 13$	$n_{N,p} > 1$	Table 1, $q_5 \neq 0$	22/(4 ÷22)	6/(2 ÷6)	9/(2 ÷9)	4/(2 ÷4)	$(p+3)$/ $\big((p+1)\div (p+3)\big)$
		Table 1, $q_5 = 0$	0	0	5/(2 ÷5)	5/(2 ÷5)	0

TABLE 4. **Comparison of times needed to find all the true different 5-PPs modulo different prime numbers using the test from Table 1 and the direct test.**

$p^{n_{N,p}}$	$p \pmod 5$ $(n_{N,p})$	Time using the test from Table 1				Time using the direct test				Time ratio
		hours	min.	sec.	milisec.	hours	min.	sec.	milisec.	
11	1 (1)	0	0	0	7	0	0	0	20	2.86
41		0	0	3	899	0	0	32	707	8.39
101		0	4	11	40	1	16	46	964	18.35
151		0	30	15	676	12	56	31	455	25.66
19	4 (1)	0	0	0	177	0	0	0	406	2.29
59		0	0	51	239	0	4	25	390	5.18
109		0	13	22	391	1	54	14	908	8.54
149		1	4	51	296	11	58	29	153	11.08
17	2 (1)	0	0	0	143	0	0	0	218	1.53
47		0	0	23	521	0	1	11	858	3.06
107		0	16	15	7	1	42	43	414	6.32
157		1	52	1	118	16	17	30	380	8.73
23	3 (1)	0	0	0	669	0	0	1	219	1.82
53		0	0	43	712	0	2	23	731	3.29
103		0	14	12	101	1	22	14	178	5.79
163		2	22	57	682	20	13	35	746	8.49
7	-	0	0	0	8	0	0	0	3	0.38
13	-	0	0	0	34	0	0	0	47	1.38

If $right\_term1 = 0$ (one comparison), we need to check conditions (1) and, possibly, (2). When $\pi(x) \pmod 7$ is a 5-PP, under conditions (1), the computation requirements are: one multiplication for $2 \cdot q4\_to\_3$, 2 modulo 7 operations, and 2 comparisons (these are to check if $left\_term2 = 0$ and $left\_term3 = 0$). If conditions (1) and (2) with sign "+" are not met, but conditions (2) with sign "−" are met, the computation requirements for the right terms of these sets of conditions and for comparisons with the corresponding left terms are: $1+3+4 = 8$ multiplications, $2+2 = 4$ additions, $2+2+2 = 6$ modulo 7 operations, and $2+2+2 = 6$ comparisons. Overall, if $q_5 \neq 0 \pmod 7$ and $5\ q_3\ q_5 = 2(q_4)^2 \pmod 7$, when $\pi(x) \pmod 7$ is a 5-PP, we need to perform at least 11 multiplications, one addition, 6 modulo 7 operations, 4 comparisons, and to store 8 values and at most 18 multiplications, 5 additions, 10 modulo 7 operations, 8 comparisons, and to store 8 values.

If $right\_term1 > 0$ (one comparison), we need to compute and to store the value of $\alpha = \big(right\_term1 \cdot \big(q5\_to\_2 \pmod 7\big)^{-1}\big) \pmod 7$ and to check conditions (3) and, possibly, (4). In our implementation, we firstly compute and store the values $right\_term2 = 2 \cdot q4\_to\_3 + \alpha \cdot q_4 \cdot$

TABLE 5. Comparison of times needed to find 100000 true different 5-PPs modulo different squared prime numbers using the test from Table 1 and using Theorem 2 togheter with the direct test (The start value of coefficient q_5 is set to p and if $p \pmod 5 = 2$ or $p \pmod 5 = 3$ the value of q_5 is set to $p + 1$, when 50000 true different 5-PPs are found).

$p^{n_{N,p}}$	$p \pmod 5$ $(n_{N,p})$	Time using the test from Table 1			Time using Theorem 2 togheter with the direct test			Time ratio
		min.	sec.	milisec.	min.	sec.	milisec.	
11^2 (121)	1 (2)	0	4	714	0	11	571	2.46
41^2 (1681)		0	4	445	0	32	265	7.26
101^2 (10201)		0	0	432	0	16	556	38.32
151^2 (22801)		0	0	639	0	47	127	73.75
19^2 (361)	4 (2)	0	2	62	0	4	844	2.35
59^2 (3481)		0	0	369	0	4	533	12.29
109^2 (11881)		0	0	638	0	20	797	32.60
149^2 (22201)		0	0	801	0	44	617	55.70
17^2 (289)	2 (2)	0	1	850	0	3	760	2.03
47^2 (2209)		0	8	598	0	26	926	3.13
107^2 (11449)		0	48	723	5	19	957	6.57
157^2 (24649)		1	56	818	19	19	336	9.92
23^2 (529)	3 (2)	0	3	280	0	7	939	2.42
53^2 (2809)		0	11	48	0	38	43	3.44
103^2 (10609)		0	44	863	4	44	403	6.34
163^2 (26569)		2	9	169	22	18	94	10.36
5^2 (25)	- (2)	0	0	113	0	0	203	1.80
5^3 (125)	- (3)	0	0	228	0	0	488	2.14
5^4 (625)	- (4)	0	0	77	0	0	119	1.55
7^2 (49)	- (2)	0	0	423	0	0	537	1.27
7^3 (343)	- (3)	0	0	208	0	0	324	1.56
7^4 (2401)	- (4)	0	0	34	0	0	60	1.77
13^2 (169)	- (2)	0	5	928	0	18	587	3.14
13^3 (2197)	- (3)	0	0	59	0	0	172	2.92
13^4 (28561)	- (4)	0	0	51	0	0	146	2.86

$q5\_to\_2$ and $right\_term3 = q4\_to\_4 + (q4\_to\_2 + 4 \cdot \alpha \cdot q5\_to\_2) \cdot \alpha \cdot q5\_to\_2$. To compute these two values and that of α, we require 8 multiplications, 3 additions, 2 modulo 7 operations and to store the six values of the inverses modulo 7. To check conditions (3), we require 2 modulo 7 operations and 2 comparisons. When conditions (3) are not met, to check conditions (4), we firstly need to check if $\alpha \in \{3, 5, 6\}$, that is, one up to three comparisons, and then 2 or 5 multiplications, 2 or 4 additions, 2 or 4 modulo 7 operations and 2 or 4 comparisons. Thus, if $q_5 \neq 0 \pmod 7$ and $5\, q_3\, q_5 \neq 2(q_4)^2 \pmod 7$, when $\pi(x) \pmod 7$ is a 5-PP, we need in total at least 18 multiplications, 4 additions, 8 modulo 7 operations, 4 comparisons and to store 17 values, and at most 23 multiplications, 8 additions, 12 modulo 7 operations, 11 comparisons and to store 17 values.

If $q_5 = 0 \pmod 7$, we firstly need to check whether $q_4 = 0 \pmod 7$. If $q_4 \neq 0 \pmod 7$, we firstly check the condition $3(q_3)^2 = q_2\, q_4 \pmod 7$. This check requires 3 multiplications, 2 modulo 7 operations, and one comparison. If the equalilty holds, we store the next three values $left\_term = (2 \cdot q_1 \cdot q_4 \cdot q_4) \pmod 7$, $q3\_to\_3 = q_3 \cdot q_3 \cdot q_3$ and $q4\_to\_3 = q_4 \cdot q_4 \cdot q_4$, which require 7 multiplications and one modulo 7 operation. Then, we check the second condition from (5) and (6). Overall, we need to perform at least 10 multiplications, one addition, 6 modulo 7 operations, 4 comparisons, and to store 3 values and at most

11 multiplications, 2 additions, 7 modulo 7 operations, 5 comparisons and to store 3 values. If $q_4 = 0 \pmod 7$, in total we need to perform 5 modulo 7 operations, and 5 comparisons.

Finally, we mention that when $\pi(x) \pmod 7$ is not a 5-PP, if $q_5 \neq 0 \pmod 7$ and if $5\, q_3\, q_5 = 2(q_4)^2 \pmod 7$, the least number of operations occurs when the first conditions from all three sets of conditions (1) and (2) are not met. This means 14 multiplications, 3 additions, 7 modulo 7 operations, 5 comparisons and storing of 8 values. If $q_5 \neq 0 \pmod 7$ and if $5\, q_3\, q_5 \neq 2(q_4)^2 \pmod 7$, the least number of operations is performed when the first condition from the set (3) is not met and when $\alpha \notin \{3, 5, 6\}$. This means 18 multiplications, 4 additions, 7 modulo 7 operations, 6 comparisons and storing of 17 values. If $q_5 = 0 \pmod 7$ and $q_4 \neq 0 \pmod 7$, we require at least 3 multiplications, 4 modulo 7 operations and 3 comparisons, and if $q_5 = 0 \pmod 7$ and $q_4 = 0 \pmod 7$, we require at least 3 modulo 7 operations and 3 comparisons. The maximum number of operations for checking that $\pi(x) \pmod 7$ is not a 5-PP is the same as when it is a 5-PP.

The analysis for $\pi(x) \pmod{7^{n_{N,7}}}$, with $n_{N,7} > 1$, follows taking into account that the conditions are those for $n_{N,7} = 1$ in the cases (3) or (7).

Table 3 summarizes the above results for $p = 7$ and for other prime numbers. From this table, we see that in the worst cases for all prime numbers, the number of multiplications, additions and comparisons is much smaller than using the direct test. The number of modulo operations is also smaller than using the direct test, except for $p = 7$. The number of stored values is not so important because, in general, to find a good 5-PP for a possible application, we perform these checking operations off-line, on a computer with sufficient memory resources. The time needed for checking operations is an important issue. The greater the prime number p is, the smaller the number of operations with the test in Table 1 is compared to using the direct test for the power of one or using Theorem 2 togheter with the direct test for powers greater than one. Thus, for large prime numbers in the decomposition of N, the test in Table 1 is much efficient than using Theorem 1 togheter with the direct test or using Theorems 1 and 2 togheter with the direct test.

To justify the efficiency of the coefficient test from Table 1 compared to the direct test or using Theorem 2 togheter with the direct test (except for $p = 7$), in Table 4, we give the times for finding all the true different 5-PPs modulo different prime numbers. Table 5 presents the times for finding 100000 true different 5-PPs modulo different squared prime numbers. This limit for the number of true different 5-PPs is chosen to reduce the testing time because the number of true different 5-PPs is huge in these cases. To further reduce the testing time, the start value of the coefficient q_5 is set to p, because for $p \pmod 5 = 1$ or $p \pmod 5 = 4$ the condition for the coefficient q_5 of a 5-PP is $q_5 = 0 \pmod 5$. Because for $p \pmod 5 = 2$ or $p \pmod 5 = 3$ there are also true different 5-PPs for $q_5 \neq 0 \pmod 5$ the value of q_5 is set to $p + 1$, when 50000 true different 5-PPs are found. The times are given for four different prime numbers p or p^2 for each $p \pmod 5 = 1$, $p \pmod 5 = 4$, $p \pmod 5 = 2$ or $p \pmod 5 = 3$ and, finally, for $p = 7$ and $p = 13$, or for the first three powers of 5, 7 or 13, greater than one. The time for the prime number 5 is not given because the testing time is very small for both methods. The four types of prime numbers and the prime numbers 5, 7 and 13, and their powers, are separated by double lines in Tables 4 and 5. From the ratio of times obtained through the two methods in these tables, we see that the coefficient test from Table 1 is the most efficient one for the prime numbers p with $p \pmod 5 = 1$, then for $p \pmod 5 = 4$, and then for $p \pmod 5 = 2$ or $p \pmod 5 = 3$. For $p = 7$, we see that the direct test is more efficient compared to that given in Table 1. Generally, the same remark applies for interleaver lengths containing 7 as a prime factor. Thus, in these cases, for $p = 7$ we can use the direct test instead of the test in Table 1. For $p = 13$ and for powers of the prime numbers 5, 7 and 13, the test from Table 1 is slightly better in terms of required time compared to the direct test or using Theorem 2 togheter with the direct test.

V. CONCLUSION

In this paper, we derived necessary and sufficient conditions on the coefficients of a quintic polynomial to verify if it is a PP over integer rings. As expected, these conditions are more complicated compared to those for lower degrees PPs. For higher degrees, we expect that conditions become even more complicated, but we note that in order to obtain we require normalized PPs of the involved degree. Nevertheless, the test we have proposed is more efficient than brute-force test for finding quintic PPs. We checked that it is also more efficient than checking 5-PPs using Theorem 1 togheter with the direct test, except for the prime number $p = 7$, or using Theorems 1 and 2 togheter with the direct test. The proposed test is useful for finding 5-PPs for different applications, such as cryptography, sequences' generation or interleavers for turbo codes.

Finally, we give some merits of this paper:

- We determined the necessary and sufficient conditions on the coefficients of a quintic polynomial, for any prime number or a power of it from the decomposition of N, so that it is 5-PP modulo N. These conditions are usefull to find 5-PPs for a specific application and our paper is targeted to this necessity.
- For a set of coefficients of a polynomial of degree no more than five, we can directly decide whether they determine a PP.
- Using the proposed method, the coefficients can be obtained in a desired order, which is tractable in computer processing.

REFERENCES

[1] S. D. Cohen, "Permutation group theory and permutation polynomials," in *Algebras and Combinatorics*. Singapore: Springer, 1999, pp. 133–146.

[2] R. Lidl and H. Niederreiter, *Introduction to Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[3] J. Sun and O. Y. Takeshita, "Interleavers for turbo codes using permutation polynomials over integer rings," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 101–119, Jan. 2005.

[4] R. L. Rivest, "Permutation polynomials modulo 2^w" *Finite Fields Appl.*, vol. 7, no. 2, pp. 287–292, 2001.

[5] O. Y. Takeshita, "Permutation polynomial interleavers: An algebraic-geometric perspective," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2116–2132, Jun. 2007.

[6] Y.-L. Chen, J. Ryu, and O. Y. Takeshita, "A simple coefficient test for cubic permutation polynomials over integer rings," *IEEE Commun. Lett.*, vol. 10, no. 7, pp. 549–551, Jul. 2006.

[7] H. Zhao and P. Fan, "A note on 'a simple coefficient test for cubic permutation polynomials over integer rings,"' *IEEE Commun. Lett.*, vol. 11, no. 12, p. 991, Dec. 2007.

[8] L. Trifina and D. Tarniceriu, "A coefficient test for fourth degree permutation polynomials over integer rings," *AEU-Int. J. Electron. Commun.*, vol. 70, no. 11, pp. 1565–1568, Nov. 2016.

[9] L. Zhang, Y. Xu, X. Ma, H. Luo, and X. Gan, "Study on interleaver design for turbo codes using permutation polynomials over integer rings," in *Proc. IEEE 64th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2006, pp. 1–5.

[10] R. P. Singh and S. Maity. (2009). *Permutation Polynomials Modulo p^n*. Accessed: Sep. 20, 2016. [Online]. Available: https://eprint.iacr.org/2009/393.pdf

[11] R. A. Mollin and C. Small, "On permutation polynomials over finite fields," *Int. J. Math. Math. Sci.*, vol. 10, no. 3, pp. 535–543, 1987.

[12] H. Zhao and P. Fan, "Simple method for generating *m*th-order permutation polynomials over integer rings," *Electron. Lett.*, vol. 43, no. 8, pp. 449–451, Apr. 2007.

[13] G. Weng and C. Dong, "A note on permutation polynomials over $\mathbb{Z}_n$," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4388–4390, Sep. 2008.

[14] W. Nöbauer, "Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen," *Monatshefte Math.*, vol. 69, no. 3, pp. 230–238, 1965.

[15] G. Mullen and H. Stevens, "Polynomial functions (mod *m*)," *Acta Math. Hungarica*, vol. 44, nos. 3–4, pp. 237–241, 1984.

[16] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed. London, U.K.: Oxford Univ. Press, 1975.

[17] L. E. Dickson, "The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group," *Ann. Math.*, vol. 11, nos. 1–6, pp. 65–120, 1896–1897.

[18] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*. New York, NY, USA: Dover, 1901. Accessed: Sep. 22, 2016. [Online]. Available: https://ia801406.us.archive.org/22/items/lineargroupswith00dickuoft/lineargroupswith00dickuoft.pdf

[19] J. Ryu and O. Y. Takeshita, "On quadratic inverses for quadratic permutation polynomials over integer rings," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1254–1260, Mar. 2006.

LUCIAN TRIFINA was born in Falticeni, Romania, in 1976. He received the B.Sc. degree in electronics and telecommunications engineering and the M.Sc. degree in modern techniques for signal processing from the Gheorghe Asachi Technical University of Iasi, Romania, in 2002 and 2003, respectively, and the Ph.D. degree with the thesis on turbo codes-theoretical and practical aspects in 2007. He is currently with Gheorghe Asachi Technical University of Iasi, Faculty of Electronics, Telecommunications and Information Technology, Department of Telecommunications and Information Technologies as an Assistant Professor. His research interests include coding theory with emphasis on turbo codes and space-time turbo codes.

DANIELA TARNICERIU was born in Iasi, Romania, in 1960. She received the M.Sc. degree in electrical engineering and the Ph.D. degree in electronics and telecommunications from the Gheorghe Asachi Technical University of Iasi, Romania, in 1983 and 1997, respectively. In 1991, she joined the Department of Communications, Faculty of Electronics and Telecommunications, Iasi, and received the title of Professor in 2000. From 2005 to 2008, she was the Vice-Dean of the Faculty and from 2008 to 2016, she was the Head of the Department of Telecommunications. Since 2016, she has been the Dean of the Faculty. Her current research interests include digital signal processing and coding theory with emphasis on turbo coding and wireless systems.