Permutation Polynomials over Finite Fields defined by functional equations

Neranga Fernando
Joint work with Dr. Xiang-dong Hou

Department of Mathematics and Statistics
University of South Florida

AMS Spring Southeastern Section Meeting , Tampa , Florida

March 10,2012

Outline

1. Introduction
2. Desirable Triples
3. Families of Desirable Triples
4. An update of the table of Desirable Triples $(n, e; q)$ with $q = 3$ and $e \leq 6$

$q = p^k, n \geq 0.$

There exists a unique polynomial $g_{n,q} \in \mathbb{F}_p[x]$ such that

$$\sum_{a \in \mathbb{F}_q} (x+a)^n = g_{n,q}(x^q - x)$$

Question : When is $g_{n,q}$ a permutation polynomial(PP) of $\mathbb{F}_{q^e}$?

If $g_{n,q}$ is a PP , we call triple $(n, e; q)$ **desirable**.

$$g_{0,q} = \dots = g_{q-2,q} = 0,$$
$$g_{q-1,q} = -1,$$

$$g_{n,q} = xg_{n-q,q} + g_{n-q+1,q} \quad , \quad n \geq q$$

Above recurrence relation can be used to define $g_{n,q}$ for $n < 0$:

$$g_{n,q} = \frac{1}{x}(g_{n+q,q} - g_{n+1,q}).$$

For $n < 0$, there exists a $g_{n,q} \in \mathbb{F}_p[x, x^{-1}]$ such that

$$\sum_{a \in \mathbb{F}_q} (x+a)^n = g_{n,q}(x^q - x)$$

Recurrence relation holds for all $n \in \mathbb{Z}$.

The nth Reversed Dickson Polynomial $D_n(1, x) \in \mathbb{Z}[x]$ is defined by

$$D_n(1, x(1-x)) = x^n + (1-x)^n$$

When $q = 2$,

$$g_{n,2}(x(1-x)) = x^n + (1-x)^n \quad \in \quad \mathbb{F}_2[x]$$

$g_{n,2} = D_n(1, x) \quad \in \quad \mathbb{F}_2[x]$.

Desirable Triples

Equivalence

1. $g_{pn,q} = g_{n,q}^{p}$.

Desirable Triples

Equivalence

1. $g_{pn,q} = g_{n,q}^{p}$.
2. If $n_1, n_2 > 0$ are integers such that $n_1 \equiv n_2 \pmod{q^{pe} - 1}$, then $g_{n_1,q} \equiv g_{n_2,q} \pmod{x^{q^e} - x}$.

1. $g_{pn,q} = g_{n,q}^p$.
2. If $n_1, n_2 > 0$ are integers such that $n_1 \equiv n_2 \pmod{q^{pe} - 1}$, then $g_{n_1,q} \equiv g_{n_2,q} \pmod{x^{q^e} - x}$.
3. If $m, n > 0$ belong to the same p-cyclotomic coset modulo q^{pe} - 1, we say that two triples $(m, e; q)$ and $(n, e; q)$ are *equivalent* and write $(m, e; q) \sim (n, e; q)$.

   If $(m, e; q) \sim (n, e; q)$,

   $g_{m,q}$ is a PP if and only if $g_{n,q}$ is a PP.

If $(n, e; 2)$ is desirable , $\gcd(n, 2^{2e} - 1) = 3$.

If $(n, e; q)$ is desirable , $\gcd(n, q - 1) = 1$.

If $(n, e; q)$ is desirable where $q > 2$ or $e > 1$, the p-cyclotomic coset of n modulo $q^{pe} - 1$ has cardinality $pek(q = p^k)$.

Generating function

A Quick Reminder :

$g_{0,q} = \ldots = g_{q-2,q} = 0,$

$g_{q-1,q} = -1,$

$$g_{n,q} = xg_{n-q,q} + g_{n-q+1,q} \quad , \quad n \geq q$$

$$\sum_{n\geq 0} g_{n,q} t^n = \frac{-t^{q-1}}{1 - t^{q-1} - xt^q}$$

Theorem

$$\sum_{n\geq 0} g_{n,q} t^n \equiv \frac{-(xt)^{q-1}}{1-(xt)^{q-1}-(xt)^q} + (1-x^{q-1})\frac{-t^{q-1}}{1-t^{q-1}} \pmod{x^q - x}$$

$$g_{n,q} \equiv a_n x^n + \begin{cases} x^{q-1}-1 & : \text{if } n>0\,,\ n\equiv 0 \pmod{q-1} \pmod{x^q-x} \\ 0 & : \text{otherwise} \pmod{x^q-x} \end{cases}$$

where $\displaystyle \sum_{n\geq 0} a_n t^n = \frac{-t^{q-1}}{1-t^{q-1}-t^q}$

Proof of the Theorem

$$\sum_{n\geq 0} g_{n,q} t^n = \frac{-t^{q-1}}{1-t^{q-1}-xt^q}$$

$$\frac{-t^{q-1}}{1-t^{q-1}-xt^q} \equiv \frac{-(xt)^{q-1}}{1-(xt)^{q-1}-(xt)^q} + (1-x^{q-1})\frac{-t^{q-1}}{1-t^{q-1}} \pmod{x^{q-1}-1}$$

and

$$\frac{-t^{q-1}}{1-t^{q-1}-xt^q} \equiv \frac{-(xt)^{q-1}}{1-(xt)^{q-1}-(xt)^q} + (1-x^{q-1})\frac{-t^{q-1}}{1-t^{q-1}} \pmod{x}$$

The case e = 1

$(n, 1; q)$ is desirable if and only if $\gcd(n, q-1) = 1$ and $a_n \neq 0$.

Proof : By the Theorem , we have

$$g_{n,q} \equiv a_n x^n + \begin{cases} x^{q-1} - 1 & : \textit{if } n > 0,\ n \equiv 0\ (\textit{mod } q-1) \pmod{x^q - x} \\ 0 & : \textit{otherwise} \pmod{x^q - x} \end{cases}$$

$(\Rightarrow)$

Since $g_{n,q}$ is PP , by a previous fact, $\gcd(n, q-1) = 1$.

So $g_{n,q}(x) \equiv a_n x^n \pmod{x^q - x}$ which implies $a_n \neq 0$.

$(\Leftarrow)$

$\gcd(n, q-1) = 1$ and $a_n \neq 0 \Rightarrow g_{n,q}(x) \equiv a_n x^n \pmod{x^q - x} \Rightarrow g_{n,q}$ is PP.

Open question : Determine n s.t. $a_n \neq 0$.

Some Desirable Triples

[Hou 2011]

1. $(q^{pe} - 2, e; q)$ when $q > 2$.

Some Desirable Triples

[Hou 2011]

1. $(q^{pe} - 2, e; q)$ when $q > 2$.
2. When $q = 3^k$, $(q^{2e} - q^e - 1, e; q)$ is desirable.

Some Desirable Triples

[Hou 2011]

1. $(q^{pe} - 2, e; q)$ when $q > 2$.
2. When $q = 3^k$, $(q^{2e} - q^e - 1, e; q)$ is desirable.
3. $(3^{2e+1} - 2.3^e - 2, e; 3)$ is desirable.

A useful Lemma - (A)

Let $n = \alpha_0 q^0 + \ldots + \alpha_t q^t$, $0 \leq \alpha_i \leq q-1$ and $w_q(n)$ be the base q weight of n ,

$$g_{n,q} = \begin{cases} 0 & : \text{if} \quad w_q(n) < q-1 \\ -1 & : \text{if} \quad w_q(n) = q-1 \\ \alpha_0 x^{q^0} + (\alpha_0+\alpha_1)x^{q^1} + \ldots + (\alpha_0 + \ldots + \alpha_{t-1})x^{q^{t-1}} + \delta & : \text{if} \quad w_q(n) = q \end{cases}$$

where

$$\delta = \begin{cases} 1 & : \text{if} \ \ q = 2 \\ 0 & : \text{if} \ \ q > 2 \end{cases}$$

Proposition

Let $n = \alpha_0 q^0 + \ldots + \alpha_t q^t$, $0 \leq \alpha_i \leq q-1$, with $w_q(n) = q$.

Then $(n, e; q)$ is *desirable* if and only if

$$\gcd(\alpha_0 + (\alpha_0 + \alpha_1)x + \ldots + (\alpha_0 + \ldots + \alpha_{t-1})x^{t-1}, x^e - 1) = 1.$$

We are going to write $n = \alpha(p^{0e} + p^{1e} + \ldots + p^{(p-1)e}) + \beta$, where $\alpha, \beta \in \mathbb{Z}$ and impose conditions on α and β so that $(n, e; p)$ is *desirable*.

Another Useful Lemma - (B)

Let $n = \alpha(p^{0e} + p^{1e} + \ldots + p^{(p-1)e}) + \beta$, where $\alpha, \beta \in \mathbb{Z}$. Then for $x \in \mathbb{F}_{p^e}$,

$$g_{n,p}(x) = \begin{cases} g_{\alpha p+\beta,p}(x) & : \text{if } \ \mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x) = 0 \\ x^{\alpha} g_{\beta,p}(x) & : \text{if } \ \mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x) \neq 0 \end{cases}$$

Proposition

In the previous Lemma , $(n, e; p)$ is *desirable* if the following two conditions are satisfied.

(i) Both $g_{\alpha p+\beta,p} + \delta$ and $x^{\alpha} g_{\beta,p}$ are $\mathbb{F}_p$- linear on $\mathbb{F}_{p^e}$ and are $1-1$ on $\mathrm{Tr}^{-1}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(0) = \{x \in \mathbb{F}_{p^e} : \mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x) = 0\}$,

(ii) $g_{\beta,p}(1) \neq e\delta$

A Desirable Family - 1

[Hou 2011]

Let $n = 8(3^0 + 3^e + 3^{2e}) + 7$. $(\alpha = 8, \beta = 7)$

$$g_{n,3} = \begin{cases} g_{8\cdot 3+7,3}(x) = g_{31,3}(x) = x^{3^0} - x^{3^1} - x^{3^2} & : \text{if } \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) = 0 \\ x^8 g_{7,3}(x) = x^9 & : \text{if } \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) \neq 0 \end{cases}$$

$g_{n,3}$ is a PP of $\mathbb{F}_{3^e}$ if and only if $g_{31,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$.

$-g_{31,3}(x^3 - x) = x + x^3 + x^{3^3}$.

$g_{31,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ if and only if $\gcd(1 + x + x^3, x^e - 1) = x - 1$.

$(n, e; 3)$ is *desirable* if and only if $\gcd(1 + x + x^3, x^e - 1) = x - 1$.

A Desirable Family - 2

Let $n = 26(3^0 + 3^e + 3^{2e}) + 7$. $\quad (\alpha = 26, \beta = 7)$

$$g_{n,3} = \begin{cases} g_{26\cdot 3+7,3}(x) = g_{85,3}(x) = x^{3^0} - x^{3^1} - x^{3^2} - x^{3^3} & : \text{if} \quad \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) = 0 \\ x^{26} g_{7,3}(x) = x^{27} & : \text{if} \quad \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) \neq 0 \end{cases}$$

$g_{n,3}$ is a PP of $\mathbb{F}_{3^e}$ if and only if $g_{85,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$.

$-g_{85,3}(x^3 - x) = x^{3^0} + x^{3^1} + x^{3^4}$.

$g_{85,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ if and only if $\gcd(1 + x + x^4, x^e - 1) = x - 1$.

$(n, e; 3)$ is *desirable* if and only if $\gcd(1 + x + x^4, x^e - 1) = x - 1$.

A Desirable Family - 3

Let $n = 163(3^0 + 3^e + 3^{2e}) - 162$. $(\alpha = 163, \beta = -162)$

$$g_{n,3} = \begin{cases} g_{163\cdot 3-162,3}(x) = g_{327,3}(x) = x^{3^1} + x^{3^2} + x^{3^3} - x^{3^4} & : \text{if} \quad \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) = 0 \\ x^{163} g_{-162,3}(x) = x & : \text{if} \quad \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) \neq 0 \end{cases}$$

$g_{n,3}$ is a PP of $\mathbb{F}_{3^e}$ if and only if $g_{327,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$.

$-g_{327,3}(x^3 - x) = x^{3^1} + x^{3^4} + x^{3^5}$.

$g_{327,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ if and only if $\gcd(x + x^4 + x^5, x^e - 1) = x - 1$.

$(n, e; 3)$ is *desirable* if and only if $\gcd(x + x^4 + x^5, x^e - 1) = x - 1$.

A Desirable Family - 4

[Hou 2011]

Let $n = 4(3^0 + 3^e + 3^{2e}) - 7$. $\quad (\alpha = 4, \beta = -7)$

Then $(n, e; 3)$ is *desirable*.

$$g_{n,3} = \begin{cases} g_{4\cdot 3-7,3}(x) = g_{5,3}(x) = -x & : \text{if } \ \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) = 0 \\ x^4 g_{-7,3}(x) = -x + x^{-1} - x^{-3} & : \text{if } \ \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) \neq 0 \end{cases}$$

$-x + x^{-1} - x^{-3}$ is 1-1 on $\mathbb{F}_{3^e} \setminus \mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$.

(Proved in the Paper " Permutation Polynomials of the form $(x^p - x + \delta)^s + L(x)$" by J. Yuan, C. Ding , H. Wang , J. Pieprzyk , 2008)

Table

$*$ - [Hou 2011] $\bullet$ - New Results

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
1	5	2 1	$\bullet *$
1	7	1 2	$\bullet *$
1	17	2 2 1	$\bullet *$
2	5	2 1	$*$
2	7	1 2	$*$
2	31	1 1 0 1	$*$
2	37	1 0 1 1	$*$
2	71	2 2 1 2	$*$
2	95	2 1 1 0 1	$*$
2	101	2 0 2 0 1	$*$
2	103	1 1 2 0 1	$*$
2	119	2 0 1 1 1	$*$
2	151	1 2 1 2 1	$*$
2	197	2 2 0 1 2	$*$
2	485	2 2 2 2 2 1	$*$

Table

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
3	5	2 1	$*$
3	7	1 2	$*$
3	11	2 0 1	$*$
3	19	1 0 2	$*$
3	31	1 1 0 1	$*$
3	37	1 0 1 1	$*$
3	83	2 0 0 0 1	$*$
3	85	1 1 0 0 1	$*$
3	101	2 0 2 0 1	
3	109	1 0 0 1 1	$*$
3	163	1 0 0 0 2	$*$
3	253	1 0 1 0 0 1	$*$
3	271	1 0 0 1 0 1	$*$
3	407	2 0 0 0 2 1	
3	475	1 2 1 2 2 1	
3	605	2 0 1 1 1 2	
3	619	1 2 2 1 1 2	
3	671	2 1 2 0 2 2	
3	701	2 2 2 1 2 2	$*$
3	761	2 1 0 1 0 0 1	$*$
3	769	1 1 1 1 0 0 1	$*$
3	775	1 0 2 1 0 0 1	$*$
3	779	2 1 2 1 0 0 1	
3	785	2 0 0 2 0 0 1	$*$
3	787	1 1 0 2 0 0 1	$*$
3	827	2 2 1 0 1 0 1	

Table

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
3	839	2 0 0 1 1 0 1	$*$
3	847	1 0 1 1 1 0 1	$*$
3	925	1 2 0 1 2 0 1	$*$
3	1003	1 1 0 1 0 1 1	$*$
3	1007	2 2 0 1 0 1 1	$*$
3	1009	1 0 1 1 0 1 1	$*$
3	1097	2 2 1 1 1 1 1	
3	1175	2 1 1 1 2 1 1	
3	1247	2 1 0 1 0 2 1	
3	1423	1 0 2 1 2 2 1	
3	1519	1 2 0 2 0 0 2	$*$
3	1739	2 0 1 1 0 1 2	
3	1753	1 2 2 1 0 1 2	
3	1915	1 2 2 1 2 1 2	
3	2021	2 1 2 2 0 2 2	$*$
3	2117	2 0 1 0 2 2 2	
3	2131	1 2 2 0 2 2 2	$*$
3	2537	2 2 2 0 1 1 0 1	
3	2723	2 1 2 1 0 2 0 1	
3	2819	2 0 1 2 1 2 0 1	
3	2897	2 2 0 2 2 2 0 1	
3	3137	2 1 0 2 2 0 1 1	
3	3317	2 1 2 2 1 1 1 1	
3	3361	1 1 1 1 2 1 1 1	
3	3517	1 2 0 1 1 2 1 1	
3	3551	2 1 1 2 1 2 1 1	

Table

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
3	3559	1 1 2 2 1 2 1 1	
3	3833	2 2 2 0 2 0 2 1	
3	4019	2 1 2 1 1 1 2 1	
3	4253	2 1 1 1 1 2 2 1	
3	4261	1 1 2 1 1 2 2 1	
3	5093	2 2 1 2 2 2 0 2	
3	5507	2 2 2 2 1 1 1 2	
3	5557	1 1 2 1 2 1 1 2	
3	5665	1 1 2 2 0 2 1 2	
3	5719	1 1 2 1 1 2 1 2	
3	13121	2 2 2 2 2 2 2 2 1	$*$
4	5	2 1	$*$
4	7	1 2	$*$
4	31	1 1 0 1	$*$
4	37	1 0 1 1	$*$
4	85	1 1 0 0 1	$*$
4	109	1 0 0 1 1	$*$
4	173	2 0 1 0 2	$*$
4	245	2 0 0 0 0 1	$*$
4	253	1 0 1 0 0 1	$*$
4	271	1 0 0 1 0 1	$*$
4	487	1 0 0 0 0 2	$*$
4	733	1 1 0 0 0 0 1	$*$
4	973	1 0 0 0 0 1 1	$*$
4	1477	1 0 2 0 0 0 2	$*$
4	2215	1 0 0 1 0 0 0 1	$*$

Table

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
4	2269	1 0 0 0 1 0 0 1	$*$
4	6479	2 2 2 2 1 2 2 2	$*$
4	6647	2 1 0 0 1 0 0 0 1	$*$
4	6653	2 0 1 0 1 0 0 0 1	$*$
4	6655	1 1 1 0 1 0 0 0 1	$*$
4	6661	1 0 2 0 1 0 0 0 1	$*$
4	6671	2 0 0 1 1 0 0 0 1	$*$
4	6679	1 0 1 1 1 0 0 0 1	$*$
4	6725	2 0 0 0 2 0 0 0 1	$*$
4	6727	1 1 0 0 2 0 0 0 1	$*$
4	6733	1 0 1 0 2 0 0 0 1	$*$
4	6751	1 0 0 1 2 0 0 0 1	$*$
4	6887	2 0 0 0 1 1 0 0 1	$*$
4	6895	1 0 1 0 1 1 0 0 1	$*$
4	7135	1 2 0 0 1 2 0 0 1	$*$
4	7373	2 0 0 0 1 0 1 0 1	$*$
4	7375	1 1 0 0 1 0 1 0 1	$*$
4	7381	1 0 1 0 1 0 1 0 1	$*$
4	7399	1 0 0 1 1 0 1 0 1	$*$
4	8119	1 0 2 0 1 0 2 0 1	$*$
4	8831	2 0 0 0 1 0 0 1 1	$*$
4	8839	1 0 1 0 1 0 0 1 1	$*$
4	8855	2 2 2 0 1 0 0 1 1	$*$
4	11071	1 0 0 2 1 0 0 2 1	$*$
4	17717	2 1 0 2 2 0 0 2 2	$*$

Table

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
4	19519	1 2 2 2 0 2 2 2 2	$*$
4	26725	1 1 2 2 2 1 0 0 1 1	
4	28669	1 1 2 2 2 0 0 1 1 1	
4	29525	2 1 1 1 1 1 1 1 1 1	
4	36997	1 2 0 2 0 2 2 1 2 1	
4	43933	1 1 0 1 2 0 0 2 0 2	
4	53149	1 1 1 0 2 2 0 0 2 2	$*$
4	57575	2 0 1 2 2 2 0 2 2 2	$\bullet$
4	84965	2 1 2 2 1 1 2 2 0 1 1	$*$
4	88655	2 1 1 1 2 1 1 1 1 1 1	
4	90815	2 1 1 0 2 1 1 2 1 1 1	
4	91525	1 1 2 2 1 1 2 2 1 1 1	
4	107765	2 2 0 1 1 2 0 1 1 2 1	
4	133079	2 1 2 2 1 1 2 0 2 0 2	
4	148415	2 1 2 0 2 1 2 1 1 1 2	
4	167173	1 2 1 2 2 0 1 1 1 2 2	
4	265805	2 2 1 1 2 1 1 1 1 1 1 1	
4	267935	2 1 1 2 1 1 1 2 1 1 1 1	
4	272375	2 2 2 1 2 1 1 1 2 1 1 1	$*$
4	272615	2 1 2 1 2 2 1 1 2 1 1 1	
4	273095	2 2 1 1 2 1 2 1 2 1 1 1	
4	354293	2 2 2 2 2 2 2 2 2 2 2 1	$*$

Table

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
5	515	2 0 0 1 0 2	
5	569	2 0 0 0 1 2	
5	2675	2 0 0 0 0 2 0 1	
5	4393	1 0 2 0 0 0 0 2	
5	13177	1 0 0 2 0 0 0 0 2	
5	20171	2 0 0 0 0 2 0 0 0 1	
5	58805	2 2 2 2 2 1 2 2 2 2	*
5	59297	2 1 0 0 0 1 0 0 0 0 1	
5	59303	2 0 1 0 0 1 0 0 0 0 1	
5	59305	1 1 1 0 0 1 0 0 0 0 1	*
5	59311	1 0 2 0 0 1 0 0 0 0 1	*
5	59321	2 0 0 1 0 1 0 0 0 0 1	
5	59323	1 1 0 1 0 1 0 0 0 0 1	
5	59329	1 0 1 1 0 1 0 0 0 0 1	
5	59347	1 0 0 2 0 1 0 0 0 0 1	
5	59375	2 0 0 0 1 1 0 0 0 0 1	*
5	59377	1 1 0 0 1 1 0 0 0 0 1	
5	59383	1 0 1 0 1 1 0 0 0 0 1	
5	59401	1 0 0 1 1 1 0 0 0 0 1	
5	59455	1 0 0 0 2 1 0 0 0 0 1	
5	59537	2 0 0 0 0 2 0 0 0 0 1	*
5	59539	1 1 0 0 0 2 0 0 0 0 1	*
5	59545	1 0 1 0 0 2 0 0 0 0 1	
5	59563	1 0 0 1 0 2 0 0 0 0 1	
5	59617	1 0 0 0 1 2 0 0 0 0 1	*
5	60023	2 0 0 0 0 1 1 0 0 0 1	*

Table

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
5	60031	1 0 1 0 0 1 1 0 0 0 1	$*$
5	60049	1 0 0 1 0 1 1 0 0 0 1	
5	60103	1 0 0 0 1 1 1 0 0 0 1	
5	60757	1 2 0 0 0 1 2 0 0 0 1	$*$
5	61481	2 0 0 0 0 1 0 1 0 0 1	$*$
5	61483	1 1 0 0 0 1 0 1 0 0 1	$*$
5	61489	1 0 1 0 0 1 0 1 0 0 1	$*$
5	61507	1 0 0 1 0 1 0 1 0 0 1	$*$
5	61561	1 0 0 0 1 1 0 1 0 0 1	$*$
5	63685	1 0 2 0 0 1 0 2 0 0 1	$*$
5	65855	2 0 0 0 0 1 0 0 1 0 1	$*$
5	65857	1 1 0 0 0 1 0 0 1 0 1	$*$
5	65863	1 0 1 0 0 1 0 0 1 0 1	$*$
5	65881	1 0 0 1 0 1 0 0 1 0 1	$*$
5	65935	1 0 0 0 1 1 0 0 1 0 1	$*$
5	72469	1 0 0 2 0 1 0 0 2 0 1	$*$
5	78977	2 0 0 0 0 1 0 0 0 1 1	$*$
5	78979	1 1 0 0 0 1 0 0 0 1 1	
5	78985	1 0 1 0 0 1 0 0 0 1 1	$*$
5	79003	1 0 0 1 0 1 0 0 0 1 1	$*$
5	79055	2 2 2 2 0 1 0 0 0 1 1	$*$
5	79057	1 0 0 0 1 1 0 0 0 1 1	
5	98821	1 0 0 0 2 1 0 0 0 2 1	$\bullet$
5	118591	1 2 0 0 0 2 0 0 0 0 2	
5	158117	2 1 0 0 2 2 0 0 0 2 2	$*$
5	176659	1 2 2 2 2 0 2 2 2 2 2	$*$

Table

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
5	474349	1 1 1 0 0 2 2 0 0 0 2 2	$*$
5	513875	2 0 1 0 2 2 2 0 0 2 2 2	•
5	766661	2 1 2 2 2 1 1 2 2 2 0 1 1	$*$
5	1121443	1 2 2 2 2 0 2 2 2 2 0 0 2	$*$
5	1541623	1 1 0 1 0 2 2 2 0 0 2 2 2	
5	9565937	2 2 2 2 2 2 2 2 2 2 2 2 2 2 1	$*$
6	530711	2 2 2 2 2 2 1 2 2 2 2 2	
6	532175	2 1 0 0 0 0 1 0 0 0 0 0 1	
6	532183	1 1 1 0 0 0 1 0 0 0 0 0 1	$*$
6	532189	1 0 2 0 0 0 1 0 0 0 0 0 1	$*$
6	532199	2 0 0 1 0 0 1 0 0 0 0 0 1	
6	532253	2 0 0 0 1 0 1 0 0 0 0 0 1	
6	532261	1 0 1 0 1 0 1 0 0 0 0 0 1	
6	532279	1 0 0 1 1 0 1 0 0 0 0 0 1	
6	532423	1 0 1 0 0 1 1 0 0 0 0 0 1	
6	532495	1 0 0 0 1 1 1 0 0 0 0 0 1	
6	532901	2 0 0 0 0 0 2 0 0 0 0 0 1	$*$
6	532903	1 1 0 0 0 0 2 0 0 0 0 0 1	
6	532927	1 0 0 1 0 0 2 0 0 0 0 0 1	
6	532981	1 0 0 0 1 0 2 0 0 0 0 0 1	
6	534359	2 0 0 0 0 0 1 1 0 0 0 0 1	$*$
6	534367	1 0 1 0 0 0 1 1 0 0 0 0 1	$*$
6	536551	1 2 0 0 0 0 1 2 0 0 0 0 1	$*$
6	538735	1 1 0 0 0 0 1 0 1 0 0 0 1	$*$
6	538741	1 0 1 0 0 0 1 0 1 0 0 0 1	$*$
6	538813	1 0 0 0 1 0 1 0 1 0 0 0 1	$*$

Table

Table : Desirable pairs $(n, e; 3)$, $e \leq 6$

e	n	3-adic digits of n	reference
6	538975	1 0 0 0 0 1 1 0 1 0 0 0 1	$*$
6	551855	2 0 0 0 0 0 1 0 0 1 0 0 1	$*$
6	551935	1 0 0 0 1 0 1 0 0 1 0 0 1	$*$
6	571591	1 0 0 2 0 0 1 0 0 2 0 0 1	$*$
6	591221	2 0 0 0 0 0 1 0 0 0 1 0 1	$*$
6	591229	1 0 1 0 0 0 1 0 0 0 1 0 1	$*$
6	591247	1 0 0 1 0 0 1 0 0 0 1 0 1	$*$
6	591463	1 0 0 0 0 1 1 0 0 0 1 0 1	$*$
6	650431	1 0 0 0 2 0 1 0 0 0 2 0 1	$\bullet$
6	709327	1 0 1 0 0 0 1 0 0 0 0 1 1	$*$
6	709399	1 0 0 0 1 0 1 0 0 0 0 1 1	$*$
6	709559	2 2 2 2 2 0 1 0 0 0 0 1 1	$*$
6	1419125	2 1 0 0 0 2 2 0 0 0 0 2 2	$*$
6	1592863	1 2 2 2 2 2 0 2 2 2 2 2 2	$*$
6	4612151	2 0 1 0 0 2 2 2 0 0 0 2 2 2	$\bullet$
6	6905813	2 1 2 2 2 2 1 1 2 2 2 2 0 1 1	$*$
6	10095919	1 2 2 2 2 2 0 2 2 2 2 2 0 0 2	$*$
6	19657477	1 0 2 2 2 2 0 0 2 2 2 2 0 0 1 1	
6	258280325	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 1	$*$

References

(1) X. H., *A new Approach to Permutation Polynomials over finite fields*, Finite Fields Appl. (2011).

(2) X. H., G.L. Mullen, J.A. Sellers, J.L. Yucas , *Reversed Dickson Polynomials over Finite Fields*, Finite Fields Appl. **15** (2009), 748-773.

(3) X. H., *Two classes of Permutation Polynomials over Finite Fields*, J. Combin. Theory A , **118** (2011), 448-454.

(4) X. H. and T. Ly, *Necessary conditions for reversed Dickson polynomials to be permutational*, Finite Fields Appl. **16** (2010) 436-448.

(5) J. Yuan, C. Ding , H. Wang , J. Pieprzyk , *Permutation Polynomials of the form* $(x^p - x + \delta)^s + L(x)$, Finite Fields Appl. **14** (2008), 482 - 493.

Thank You!