Elem. Math. 68 (2013) 53 – 55
0013-6018/13/020053-3
DOI 10.4171/EM/220

Elemente der Mathematik

A new class of permutation polynomials of $\mathbb{F}_q$

Mohamed Ayad and Omar Kihel

Mohamed Ayad received his Ph.D. from Université de Caen in 1992. He taught in Algerian and French universities. Since 1994 he is Maître de Conférences at Université du Littoral (Calais, France). His main fields of research are number theory, arithmetic geometry, finite fields, and algorithmic algebra.

Omar Kihel received his Ph.D. from Université Laval (Canada) in 1996. He then had a postdoctoral position at CICMA (McGill University and Concordia University) and another postdoctoral position at Université Laval. Professor Omar Kihel joined Brock University (Ontario, Canada) in July 2002. His areas of research are algebraic number theory, elliptic curves and finite fields.

Let $\mathbb{F}_q$ be the finite field of characteristic p containing $q = p^r$ elements. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial of $\mathbb{F}_q$ if the induced map $f : \mathbb{F}_q \to \mathbb{F}_q$ is one to one. The study of permutation polynomials goes back to Hermite [2] for $\mathbb{F}_p$ and to Dickson [1] for $\mathbb{F}_q$. One of the open problems proposed by Lidl and Mullen [3], is to find new classes of permutation polynomials of $\mathbb{F}_q$. We refer to [4] or [5] for the basic results on permutation polynomials. Wan and Lidl [7], gave conditions on a polynomial of the form $x^r f(x^{(q-1)/d})$ to be a permutation polynomial. The conditions are not explicitely given in terms of q and r, and may be difficult to verify in general. In the present note, without using the characterization of Wan and Lidl [7], but using only an elementary method, we exhibit a new class of permutation polynomials. We prove the following:

Theorem 1 *Let $q = p^r$, where p is a prime number and r is a positive integer. Let u be a positive integer and let*

$$f(x) = x^u\left(x^{\frac{q-1}{2}} + x^{\frac{q-1}{4}} + 1\right). \tag{1}$$

Unter einem Permutationspolynom des kommutativen Ringes R mit Einselement versteht man ein Polynom $p \in R[x]$, für welches die durch $\pi\alpha := p(\alpha)$ definierte Abbildung von R nach R eine Permutation der Ringelemente ist. Permutationspolynome sind beliebte Studienobjekte der Zahlentheorie, der Algebra und der Kombinatorik. Am besten untersucht ist wohl der Fall, wenn R ein endlicher Körper ist. Die Autoren der vorliegenden Arbeit steuern zu dieser Theorie eine neue, einfache Klasse von Permutationspolynomen bei.

Assume that the following conditions hold:

(i) $gcd(u, q-1) = 1$.
(ii) $q \equiv 1 \pmod 8$.
(iii) $3^{\frac{q-1}{4}} \equiv 1 \pmod p$.

Then $f(x)$ *is a permutation polynomial of* $\mathbb{F}_q$.

Proof. We will prove that under the above conditions, the polynomial f induces a one-to-one application on $\mathbb{F}_q$. Suppose that $f(a) = f(b)$ for some elements a and b of $\mathbb{F}_q$. If one of them, say a, is 0, then $b^u\big(b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1\big) = 0$. Suppose that $b \neq 0$, then $b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1 = 0$. Set $c = b^{\frac{q-1}{4}}$, then $c^2 + c + 1 = 0$ and c is a cubic root of unity. Condition (iii) implies $c \neq 1$. We have $c = c^4 = b^{q-1} = 1$, which is a contradiction. It follows that $b = 0 = a$.

From now on we may suppose that $ab \neq 0$. It is clear that $a^{\frac{q-1}{2}} = \pm 1$ and $b^{\frac{q-1}{2}} = \pm 1$. By symmetry, we have to consider only the following three cases:

Case 1: If $a^{\frac{q-1}{2}} = b^{\frac{q-1}{2}} = 1$. If $a^{\frac{q-1}{4}} = b^{\frac{q-1}{4}} = 1$, then $a^u = b^u$, hence $(\frac{a}{b})^u = 1$. Therefore $a = b$ by (i). To complete Case 1, we may suppose that $a^{\frac{q-1}{4}} = 1$ and $b^{\frac{q-1}{4}} = -1$. From equation (1) we have $3a^u = b^u$ or $(\frac{b}{a})^u = 3$. We deduce that $\left(\frac{b^{\frac{q-1}{4}}}{a^{\frac{q-1}{4}}}\right) = 3^{\frac{q-1}{4}}$, hence $(-1)^u = 1$ by (iii). By (i), u is odd and we reached a contradiction.

Case 2: If $a^{\frac{q-1}{2}} = b^{\frac{q-1}{2}} = -1$. From equation (1) we get: $a^{u+\frac{q-1}{4}} = b^{u+\frac{q-1}{4}}$, hence $(b/a)^{u+\frac{q-1}{4}} = 1$. The order δ of b/a in $\mathbb{F}_q$ divides $q-1$ and $u + \frac{q-1}{4}$. Let l be a prime factor of δ. Because u is odd and by (ii), we may exclude the case $l = 2$. It follows that l is odd and $l \mid \frac{q-1}{4}$, therefore $l \mid u$, which contradicts (i).

Case 3: If $a^{\frac{q-1}{2}} = -b^{\frac{q-1}{2}} = 1$. Here we have $a^{\frac{q-1}{4}} = \pm 1$ and $b^{\frac{q-1}{4}} = \zeta$, where ζ is a primitive quartic root of unity.

- If $a^{\frac{q-1}{4}} = -1$ and $b^{\frac{q-1}{4}} = \zeta$, then by equation (1), we have $a^u = \zeta b^u$. We deduce that $(a/b)^u = \zeta$, therefore $(a/b)^{4u} = 1$. Using (i), we conclude that $(a/b)^4 = 1$. If $a/b = -1$, then $a^{\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}} b^{\frac{q-1}{2}} = b^{\frac{q-1}{2}}$, which is a contradiction. Suppose next that $a/b = \pm\zeta$, then $a^{\frac{q-1}{2}} = (\pm\zeta)^{\frac{q-1}{2}} b^{\frac{q-1}{2}}$. Hence $1 = (\zeta^4)^{\frac{q-1}{8}}(-1) = -1$, which is a contradiction. We conclude that $a = b$.
- Suppose now that $a^{\frac{q-1}{4}} = 1$ and $b^{\frac{q-1}{4}} = \zeta$, then by equation (1) we have $3a^u = \zeta b^u$. By condition (iii), the characteristic of the field is $\neq 3$, hence we may write this equation in the form: $(a/b)^u = \zeta/3$. It follows that $\left(\frac{a^{\frac{q-1}{2}}}{b^{\frac{q-1}{2}}}\right)^u = \frac{\zeta^{\frac{q-1}{2}}}{3^{\frac{q-1}{2}}}$, hence $3^{\frac{q-1}{2}} = -1$, contradicting (iii). □

Remark 1 The minimal example for Theorem 1 is when $p = 7$ and $q = 7^2$.

Example 1 Let p be a prime number such that $p \equiv 1 \pmod 8$ and $p \equiv 1 \pmod 3$ and let $q = p^r$ where r is positive and even. It is clear that condition (ii) of Theorem 1 is satisfied. Euler criteria gives that $3^{\frac{p-1}{2}} = \left(\frac{3}{p}\right) = 1$ (see [6]). It follows that $3^{\frac{p-1}{4}} = \pm 1$, hence $3^{\frac{q-1}{4}} = (3^{\frac{p-1}{4}})^{(1+p+\ldots+p^{r-1})} = 1$ and condition (iii) of Theorem 1 is fulfilled. By Dirichlet's theorem (see [6]), there exist infinitely many prime numbers $p \equiv 1 \pmod 8$ and $p \equiv 1 \pmod 3$. The smallest such prime is 73. Any polynomial $f(x)$ of the form (1) such that u satisfies condition (i) of Theorem 1 induces a permutation of $\mathbb{F}_q$. We may put $u = 1$ for example.

Acknowledgement

The second author was supported in part by NSERC.

References

[1] Dickson, L.E.: The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Ann. of Math.* 11 (1896/97) 16, 161–183.

[2] Hermite, C.: Sur les fonctions de sept lettres. *C.R. Acad. Sci. Paris* 57 (1863) 750–757.

[3] Lidl, R.; Mullen, G.L.: When does a polynomial over a finite field permute the elements of the field? *Amer. Math. Monthly* 95 (1988) 243–246.

[4] Lidl, R.; Niederreiter, H.: *Finite fields* (*Encyclopedia of Mathematics and its Applications*). Cambridge Univ. Press, 2008.

[5] Small, C.: *Arithmetic of finite fields*. Marcel Dekker, Inc., 1991.

[6] Strayer, J.K.: *Elementary Number Theory*. PWS Publishing Company, Boston 1994.

[7] Wan, D.Q.; Lidl, R.: Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure. *Monatsh. Math.* 112 (1991) 2, 149–163.

Mohamed Ayad
Laboratoire de Mathématiques Pures et Appliquées
Université du Littoral
F-62228 Calais, France
e-mail: `ayad@lmpa.univ-littoral.fr`

Omar Kihel
Department of Mathematics
Brock University
Ontario, Canada L2S 3A1
e-mail: `okihel@brocku.ca`