Publ. Math. Debrecen
55 / 1-2 (1999), 101–111

On a conditional Cauchy functional equation involving cubes of finite fields II: The case of odd characteristic $p \equiv 2 \pmod 3$

By J-L. GARCÍA-ROIG (Barcelona)
and EMMA MARTÍN-GUTIÉRREZ (La Coruña)

Abstract. We show that the conditional Cauchy functional equation $f(x^3+y^3) = f(x^3)+f(y^3)$, where f is a map from a finite field of odd characteristic $p \equiv 2 \pmod 3$ into itself, is equivalent to the unconditional Cauchy functional equation $f(x+y) = f(x)+f(y)$.

Introduction

In this paper we solve the conditional Cauchy functional equation

$$f(x^3+y^3) = f(x^3)+f(y^3) \tag{1}$$

where f is a map from a finite field $\mathbb{F}_q$ ($q = p^n$, p prime) into itself, and the characteristic p is odd and congruent with 2 mod 3.

The case $p \equiv 1 \pmod 3$ was treated in our earlier paper [G-M]. In contrast to our previous results in the present case there appear no exceptions, so that (1) is eventually equivalent to the usual Cauchy functional equation.

The case p odd, $p \equiv 2 \pmod 3$ is split into two subcases: $q = p^n$, n even, and $q = p^n$, n odd. The odd case turns out to be immediate but the even case is considerably more difficult to settle and the technicalities needed may look probably more entangled than those of our previous paper.

Mathematics Subject Classification: 39B52.
Key words and phrases: functional equation, Cauchy functional equation, finite field.

1. The functional equation $f(x^3+y^3)=f(x^3)+f(y^3)$ for maps $f:\mathbb{F}_q\to\mathbb{F}_q$, with $q=p^n$ and odd $p\equiv 2 \pmod 3$

The case n odd can be readily dealt with.

Lemma 1. *Let p be odd and congruent to 2 modulo 3, and let $q=p^n$ be a power of p. Then the map $x\mapsto x^3$ from $\mathbb{F}_q$ into itself is bijective if and only if n is odd.*

Proof. By applying the law of quadratic reciprocity (see [S], Ch. I §3), we have

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right)=\left(\frac{p}{3}\right)=-1,$$

so that $\sqrt{-3}\notin\mathbb{F}_p$ and consequently, $\sqrt{-3}\in\mathbb{F}_{p^n}$ if and only if n is even. This entails that the quadratic form X^2+XY+Y^2 is irreducible over $\mathbb{F}_{p^n}$ if and only if n is odd. From

$$X^3-Y^3=(X-Y)(X^2+XY+Y^2),$$

we see that $x\mapsto x^3$ is injective if and only if n is odd. But injective here is equivalent to bijective, since the fields involved are finite. □

Corollary. *For n odd, the functional equation (1) is equivalent to the Cauchy functional equation.*

We next treat the case $q=p^n$, n even, and we proceed as in the case $p\equiv 1 \pmod 3$, but the number of technical details here seems to be larger.

Recall (cf. [G-M]) that any map $f:\mathbb{F}_q\to\mathbb{F}_q$ is induced by a polynomial $P(T)$, with coefficients in $\mathbb{F}_q$, which may be assumed to be reduced (via $T^q\equiv T$):

$$P(T)=a_0+a_1T+a_2T^2+\cdots+a_{q-1}T^{q-1}. \tag{2}$$

If the functional equation (1) is to be satisfied, then the reductions of the polynomials $P(X^3+Y^3)$ and $P(X^3)+P(Y^3)$ must coincide and, consequently, all "mixed" terms aX^rY^s, with $r,s>0$, occurring in $P(X^3+Y^3)$ have to vanish (after expansion and reduction).

But now we can proceed exactly as in [G-M]: just observe that as n is even, $p\equiv 2 \pmod 3$ implies $q\equiv 1 \pmod 3$ and thus we can split the

Figure 1

arithmetic triangle mod p up to its $(q-1)$st row into 3 parts of equal width $k = \frac{q-1}{3}$ (see Figure 1).

The reasoning of [G-M] can then be applied and we eventually have to deal with the system of linear equations

$$E_r^j = 0, \quad \text{with } k < j \leq 2k \quad \text{and} \quad 0 < r \leq k \tag{3}$$

(this entails that somewhat more redundant equations occur than in [G-M], but we do so in order to simplify further considerations), where E_r^j stands for

$$\binom{j-k}{r} a_{j-k} + \left[\binom{j}{r} + \binom{j}{r+k}\right] a_j + \left[\binom{j+k}{r} + \binom{j+k}{r+k} + \binom{j+k}{r+2k}\right] a_{j+k} = 0,$$

if $\binom{j}{r}$ lies outside the triangle ABC (see the figure), and for

$$\binom{j}{r} a_j + \left[\binom{j+k}{r} + \binom{j+k}{r+k}\right] a_{j+k} = 0,$$

if $\binom{j}{r}$ lies either inside the triangle ABC or on its sides AC or BC.

2. The arithmetic triangle modulo p in connection with (3), for $p \equiv 2 \pmod 3$ and even powers of p

Throughout this section we will assume that p is an odd prime congruent to 2 modulo 3 and that $q = p^n$, with n even.

In order to compute binomial coefficients $\binom{j}{r}$ modulo p, we will use the formula (see [H] or [L]):

$$\binom{j}{r} \equiv \binom{j_{n-1}}{r_{n-1}}\binom{j_{n-2}}{r_{n-2}}\cdots\binom{j_0}{r_0} \pmod p \tag{4}$$

where $j = \sum_{i=0}^{n-1} j_i p^i$ and $r = \sum_{i=0}^{n-1} r_i p^i$, $0 \le j_i,\ r_i < p$, and where we assume $\binom{j_i}{r_i} = 0$ for $j_i < r_i$.

With the same proof as in case $p \equiv 1 \pmod 3$ (see [G-M], Prop. 1) we have:

Proposition 2. *Let $(a_2, a_3, \dots, a_{3k}) \in \mathbb{F}_q^{3k-1}$ be any solution of the system* (3). *If $a_{k+1} = \cdots = a_{3k} = 0$ then, for $2 \le t \le k$, we have:*

$$a_t = 0, \qquad \text{if } t \ne p^m,$$

$$a_t \text{ is arbitrary}, \quad \text{if } t = p^m.$$

We will show that the hypothesis of Proposition 2 always holds (as in [G-M]). In what follows ω will stand for the positive integer $\frac{p-2}{3}$ and we will always abbreviate the p-adic expansions $a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1}p^{n-1}$ (where $0 \le a_i < p$, all i), as we usually do in the decimal (or binary) system, by

$$(a_{n-1}, \dots, a_2, a_1, a_0).$$

Of course, in our case the number of digits appearing above will be even (counting zeros if necessary).

Contrary to our earlier result (see Lemma 2 of [G-M]), and with our previous notations (recall that $k = \frac{q-1}{3}$), we have

Lemma 3. $\binom{2k}{k} \equiv 0 \pmod p$.

Proof. In the present case we have

$$k = (\omega, 2\omega+1, \omega, 2\omega+1, \dots, \omega, 2\omega+1),$$

$$2k = (2\omega+1, \omega, 2\omega+1, \omega, \dots, 2\omega+1, \omega),$$

and the result follows from (4). □

In fact, not only the vertex C is zero modulo p, for we can state:

Lemma 4. *For $j = (2\omega+1)p^{n-1}$, we have*

$$\binom{j}{j-k} \equiv \binom{j}{j-k+1} \equiv \cdots \equiv \binom{j}{k} \equiv 0 \pmod{p}.$$

PROOF. Immediate from (4) since the p-adic expansion of j is $(2\omega+1, 0, \ldots, 0, 0)$, while the second digit (starting from the left) of all integers between $j-k$ and k is strictly positive. □

In view of the additive property for binomial coefficients, the preceding lemma entails that in triangle ABC, from row $(2\omega+1)p^{n-1}$ onwards, all entries are zero modulo p. This situation is thus completely different from the case $p \equiv 1 \pmod 3$.

However, as in case $p \equiv 1 \pmod 3$, the vertex $E = \binom{3k}{k}$ is not congruent to zero modulo p, so that (as in [G-M], Lemma 3) we have:

Lemma 5. *For each j, with $k < j \leq 2k$, there exists at least one r, with $j-k \leq r \leq k$, such that*

$$\binom{j+k}{r} + \binom{j+k}{j-r} \not\equiv 0 \pmod{p}$$

As a consequence of the two preceding lemmas, we have:

Proposition 6. *Let $(a_2, a_3, \ldots, a_{3k})$ be a solution of the linear system (3). Then,*

(i) *if, for some j with $k < j < (2\omega+1)p^{n-1}$, we have $a_{j+k} = 0$, then $a_j = 0$.*

(ii) *if, for some j with $k < j \leq 2k$, we have $a_j = 0$, then $a_{j+k} = 0$.*

PROOF. As the p-adic expansion of $(2\omega+1)p^{n-1} - 1$ is $(2\omega, 3\omega+1, 3\omega+1, \ldots, 3\omega+1)$, row $(2\omega+1)p^{n-1}-1$ of the arithmetic triangle contains no zeros modulo p. Consequently, in each row j of triangle ABC with $k < j < (2\omega+1)p^{n-1}$, there will be at least a $\binom{j}{r} \not\equiv 0 \pmod p$, whose corresponding equation $E_r^j = 0$ yields (i). Considering now $E_r^j = 0$ for the r appearing in Lemma 5, we get (ii). □

We will distinguish the cases $n > 2$ and $n = 2$. The next four lemmas treat the case $n > 2$.

Lemma 7. *Let $q = p^n$ with $n > 2$, and let $(a_2, \dots, a_{3k})$ be a solution of the system* (3). *Then*

$$a_k = a_{2k} = a_{3k} = 0.$$

PROOF. Equation $E_k^{2k} = 0$ yields $a_{3k} = 0$, by observing Lemma 3 and the fact that $\binom{3k}{k} \not\equiv 0 \pmod{p}$. Now, equation $E_{2\omega}^{2k} = 0$ yields $a_k = 0$ and finally, from $E_1^{2k} = 0$, we get $a_{2k} = 0$. □

Lemma 8. *Let $q = p^n$ with $n > 2$, and let $(a_2, \dots, a_{3k})$ be a solution of the system* (3). *Then, for $(2\omega+1)p^{n-1} \le j < 2k$, we have $a_j = a_{j+k} = 0$.*

PROOF. Lemmas 4 and 5 allow us to consider an equation yielding $a_{j+k} = 0$ immediately (here it seems easier to proceed in this way rather than invoking Proposition 6 (ii)). On the other hand, as, in terms of p-adic expansions, we are in the case

$$(2\omega + 1, 0, \dots, 0, 0) \le j < (2\omega + 1, \omega, \dots, 2\omega + 1, \omega),$$

we see that $j = (2\omega + 1, j_{n-2}, j_{n-3}, \dots)$ with $0 \le j_{n-2} \le \omega$, and we will distinguish two cases:

(i) $j_{n-2} < \omega$

Equation $E_r^j = 0$, with $r = \omega p^{n-2}$, yields $a_{j-k} = 0$, and now from equation $E_s^j = 0$, with $s = p^{n-1}$, we get $a_j = 0$.

(ii) $j_{n-2} = \omega$

Here there are two possibilities for $j - k$:

(a) $j - k = (\omega, 2\omega + 1, j'_{n-3}, \dots)$, with $j'_{n-3} = j_{n-3} - \omega$ or $j'_{n-3} = j_{n-3} - \omega - 1$,

or

(b) $j - k = (\omega, 2\omega, j'_{n-3}, \dots)$, with $j'_{n-3} = j_{n-3} + 2\omega + 1$ or $j'_{n-3} = j_{n-3} + 2\omega + 2$.

For (a), we get $a_j = 0$ from $E_r^j = 0$, with $r = j_{n-3}p^{n-3}$, since $j'_{n-3} < j_{n-3}$ entails $\binom{j-k}{r} \equiv 0 \pmod{p}$. This argument is no longer valid for (b), in which case, $E_s^j = 0$, with $s = (j_{n-3} + 1)p^{n-3}$, yields $a_{j-k} = 0$ and then, from the equation E_r^j considered for (a), we also get $a_j = 0$. □

Lemma 9. *Let $k < j < (2\omega+1)p^{n-1}$, with (even) $n > 2$. Then we can choose r_{n-1} and r_{n-2} in $r = (r_{n-1}, r_{n-2}, \dots, r_1, r_0)$ so that, independently of the values of $r_{n-3}, \dots, r_0$, the first two factors on the left of the right hand side of formula* (4) *are nonzero* $\bmod p$ *for both $\binom{j}{r}$ and $\binom{j+k}{r}$, and the binomial coefficient $\binom{j}{r}$ lies inside the triangle ABC (of Figure 1).*

PROOF. By hypothesis,

$$(\omega, 2\omega+1, \dots, \omega, 2\omega+1) < j = (j_{n-1}, \dots, j_0) < (2\omega+1, 0, \dots, 0, 0),$$

so that $\omega \le j_{n-1} < 2\omega + 1$.

If $j_{n-1} < 2\omega$ then the leading digit (on the left) of $j - k$ (which is either $j_{n-1} - \omega$ or $j_{n-1} - \omega - 1$) is $< \omega$ and thus $r = (\omega, 0, \dots, r_1, r_0)$ satisfies our requirements.

If $j_{n-1} = 2\omega$, then the leading digit of $j - k$ is either ω or $\omega - 1$. In the latter case the above reasoning holds, but in the former we must have $j_{n-2} \ge 2\omega + 1$, and here we consider two possibilities:

(a) $2\omega + 1 \le j_{n-2} < 3\omega + 1$

In this case the second digit (on the left) of $j - k$: $j_{n-2} - (2\omega + 1)$ or $j_{n-2} - (2\omega + 1) - 1$, is $< \omega$ and we can take $r = (\omega, \omega, \dots, r_1, r_0)$.

(b) $j_{n-2} = 3\omega + 1$

In this situation $j-k$ starts (on the left) with either (ω, ω) or $(\omega, \omega-1)$, and $r = (\omega, \omega + 1, \dots, r_1, r_0)$ satisfies the lemma. □

Remark. This technical lemma will allow us to prove the following one by using the second type of equations (3) which involve just two unknowns instead of three. Obviously this trick cannot be applied in the preceding cases.

Lemma 10. *Let $q = p^n$ with $n > 2$, and let $(a_2, \dots, a_{3k})$ be a solution of system* (3)*. Then, for $k < j < (2\omega + 1)p^{n-1}$ we have $a_j = a_{j+k} = 0$.*

PROOF. By Proposition 6 it suffices to prove that either $a_j = 0$ or $a_{j+k} = 0$. Furthermore we will assume r_{n-1} and r_{n-2} chosen satisfying the requirements of Lemma 9, and all other digits (if any) occurring in the dots of our expressions will be assumed to be zero. We now proceed to the proof by paying attention to the first digit j_0 on the right of j, and consider several cases:

(I) $j_0 > \omega + 1$

Take $r = (r_{n-1}, r_{n-2}, \ldots, 0, j_0)$ to get $a_j = 0$ if $\binom{j+k}{r+k} \equiv 0 \pmod{p}$. Otherwise, consider the system $E_r^j = E_{r-1}^j = 0$.

(II) $j_0 = \omega + 1$

Take $r = (r_{n-1}, r_{n-2}, \ldots, 0, j_0 - 1)$ to get $a_j = 0$.

(III) $j_0 < \omega$

Take $r = (r_{n-1}, r_{n-2}, \ldots, 0, j_0 + 1)$ to get $a_{j+k} = 0$.

(IV) $j_0 = \omega$

In this case we cannot annihilate $\binom{j+k}{r}$ or $\binom{j+k}{r+k}$ if we only pay attention to j_0. We have to consider j_1 and distinguish several subcases:

(IV.a) $j_1 > 2\omega + 1$

Take $r = (r_{n-1}, r_{n-2}, \ldots, \omega, 0)$ to get $a_j = 0$.

(IV.b) $j_1 < 2\omega + 1$

Take $r = (r_{n-1}, r_{n-2}, \ldots, j_1 + 1, 0)$ to get $a_{j+k} = 0$.

(IV.c) $j_1 = 2\omega + 1$

Here again we cannot annhilate $\binom{j+k}{r}$ or $\binom{j+k}{r+k}$ and we have to pay attention (if it exists) to the second couple of digits starting from the right. But in this case observe that the first couple (on the right) of digits of $j + k$ is $(3\omega + 1, 3\omega + 1)$ so that we do not carry any units in computing the second couple for the sum of j and k, and, moreover, the first couple of factors (on the right) of (4) for $\binom{j+k}{*}$ cannot vanish. This assures that the reasoning used for the first couple of digits on the right of $j + k$ may also be applied to the second, and so on, until we reach the case

$$j = (j_{n-1}, j_{n-2}, 2\omega + 1, \omega, \ldots, 2\omega + 1, \omega).$$

For this j, the inequalities $k < j < (2\omega + 1)p^{n-1}$ imply that if $j_{n-2} \geq 2\omega + 1$, then $\omega \leq j_{n-1} < 2\omega + 1$, and if $j_{n-2} < 2\omega + 1$, then $\omega < j_{n-1} < 2\omega + 1$.

When $j_{n-2} < 2\omega + 1$, then by adding the equations $E_r^j = 0$ and E_{r+1}^j for $r = (\omega, 0, \ldots, 0, 0)$, we obtain $a_j = 0$. Finally, if $j_{n-2} \geq 2\omega + 1$, the previous argument also shows that $a_j = 0$ if we now take $r = (j_{n-1} - \omega, j_{n-2} - (2\omega + 1), \omega + 1, 0, \ldots, 0, 0)$. □

This settles the case $n > 2$, but there still remains to see what happens for $n = 2$.

Proposition 11. *Let $q = p^2$ and let $(a_2, \ldots, a_{3k})$ be a solution of (3). Then $a_j = a_{j+k} = 0$, for $k < j \leq 2k$.*

PROOF. The case $j = 2k$ is settled by proceeding as in Lemma 7 to get $a_{3k} = 0$. But $a_k = a_{2k} = 0$ is obtained from the system of equations $E^{2k}_{2\omega} = E^{2k}_{2\omega+1} = 0$.

For the case $(2\omega+1)p \leq j < 2k$, the argument of Lemma 8 holds with the simplification that case (ii) of its proof does not take place here.

Thus we are left with the case $k < j < (2\omega + 1)p$.

Again by Proposition 6 it suffices to show that either a_j or a_{j+k} is zero. We distinguish two subcases:

(a) $j_1 = \omega$ (in which case, $j_0 > 2\omega + 1$)

(b) $\omega < j_1 < 2\omega + 1$ (here j_0 is arbitrary: $0 \leq j_0 \leq 3\omega + 1$).

In case (a) the system of linear equations $E^j_r = E^j_{r+1} = 0$ with $r = (\omega, 0)$ has nonvanishing determinant and consequently $a_j = a_{j+k} = 0$.

Case (b) is subtler to treat and we have considered 3 possibilities:

(b.1) $\omega < j_1 < 2\omega + 1$, $j_0 = 3\omega + 1$

In this case, in the equation $E^j_{j-k} + E^j_{j-k+1} = 0$ the coefficient of a_j vanishes $\mod p$. Thus if the coefficient of a_{j+k} does not vanish we are done. This certainly happens if $j_1 = 2\omega$ and $\omega = 1$ (i.e., $p = 5$). In the remaining cases, if in the preceding equation the coefficient of a_{j+k} vanishes, then equation $E^j_{j-k+1} + E^j_{j-k+2} = 0$ has vanishing coefficient for a_j but not for a_{j+k}, and thus, $a_{j+k} = 0$.

(b.2) $\omega < j_1 < 2\omega + 1$, $2\omega + 1 \leq j_0 < 3\omega + 1$

In this case, from $\binom{a}{b} \equiv \binom{a}{b-1} \frac{a-b+1}{b} \pmod p$ for $b \not\equiv 0 \pmod p$, we can check that the system $E^j_{j-k} = E^j_{j-k+1} = 0$ has nonvanishing determinant $\mod p$ and thus $a_j = a_{j+k} = 0$.

(b.3) $\omega < j_1 < 2\omega + 1$, $j_0 < 2\omega + 1$

Equation $E_r^j = 0$ with $r = (\omega, \omega)$ yields $a_j = 0$ for $\omega < j_0 < 2\omega + 1$, and $a_{j+k} = 0$, for $j_0 < \omega$. In the case $j_0 = \omega$ it suffices to consider $E_{r-1}^j + E_r^j = 0$ to get $a_j = 0$. □

3. The solutions of (1) for odd $p \equiv 2 \pmod 3$

Theorem 12. *The solutions $f : \mathbb{F}_q \to \mathbb{F}_q$ of the functional equation (1) for $q = p^n$, n even, and p odd $\equiv 2 \pmod 3$ are exactly the maps*

$$f(x) = a_1 x + a_p x^p + a_{p^2} x^{p^2} + \cdots + a_{p^{n-1}} x^{p^{n-1}}$$

where $a_1, a_p, a_{p^2}, \ldots, a_{p^{n-1}}$ are arbitrary elements in $\mathbb{F}_q$.

Proof. We treat the case n even, since the case n odd is a direct consequence of the Corollary to Lemma 1, and we can assume that f is induced by a polynomial of type (2). Then, if f satisfies (1), by applying Propositions 2 and 11 we see that f is induced by a polynomial of type

$$P(T) = a_0 + a_1 T + a_p T^p + a_{p^2} T^{p^2} + \cdots + a_{p^{n-1}} T^{p^{n-1}}.$$

Equating now $P(X^3 + Y^3)$ and $P(X^3) + P(Y^3)$ we get $a_0 = 2a_0$ and consequently $a_0 = 0$. Now, as any map of type $a_1 x + a_p x^p + a_{p^2} x^{p^2} + \cdots + a_{p^{n-1}} x^{p^{n-1}}$ clearly satisfies (1), we are done. □

Corollary. *For the cases considered in Theorem 12, functional equation (1) is equivalent to the Cauchy functional equation.*

Acknowledgement. We thank the referee for his remarks concerning the final version of the paper.

References

[G-M] J. L. García-Roig and E. Martín, On a conditional Cauchy functional equation involving cubes of finite fields I: The case of characteristic $p \equiv 1 \pmod 3$, *Publ. Math. Debrecen* **52**/3–4 (1998), 385–396.

[H] A. M. Hinz, Pascal's Triangle and the Tower of Hanoi, *Amer. Math. Monthly* (6), **99** (June–July, 1992), 538–544.

[L] E. Lucas, Théorie des Fonctions Numériques Simplement Périodiques, *Amer. J. Math.* **1** (1878), 184–240, 289–321.

[S] J. P. Serre, A Course in Arithmetic, G.T.M. 7., 2nd ed., *Springer-Verlag*, 1978.

J.L. García–Roig
Secció Matemàtiques i Inf., ETSAB
Universitat Politècnica Catalunya
Diagonal 649
08028 Barcelona
Spain

Emma Martín–Gutiérrez
E.T.S. de Arquitectura de La Coruña
Campus de Zapateira S/N
Universidade da Coruña
15192 La Coruña
Spain

(Received October 30, 1997; revised March 26, 1998)