Publ. Math. Debrecen
52 / 3-4 (1998), 385–396

On a conditional Cauchy functional equation involving cubes of finite fields I: the case of characteristic $p \equiv 1 \pmod 3$

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

Dedicated to Professor Zoltán Daróczy on his 60th birthday

Abstract. We solve the conditional Cauchy functional equation $f(x^3+y^3) = f(x^3)+f(y^3)$, for maps from a finite field of characteristic $p \equiv 1 \pmod 3$ into itself.

Introduction

The aim of this paper is to solve the conditional Cauchy functional equation

$$(1) \qquad f(x^3+y^3) = f(x^3)+f(y^3)$$

where f stands for a map from the finite field $\mathbb{F}_q$ of q elements into itself, and $q = p^n$ is a power prime, with $p \equiv 1 \pmod 3$. *A priori* we hope to get as solutions the additive mappings $f(x) = \sum_{\nu=0}^{n-1} a_\nu x^{p^\nu}$ (see [3], Ch. VI §12) as is the case with the similar but simpler functional equation $f(x^2+y^2) = f(x^2)+f(y^2)$ solved in [1]. However, in our situation, it turns out that there appear three exceptional cases where there are more solutions, and which we completely solve. In this paper we stick to the case $p \equiv 1 \pmod 3$, because of the so many technical difficulties arisen

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

concerning a huge system of linear equations (thus, quite elementary in nature), which require a subtle choosing of suitable equations in order to overcome the various cases involved. These technical difficulties behave in quite a different manner for the case $p \equiv 2 \pmod 3$, to be dealt with in another paper.

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 $p \equiv 1 \pmod 3$.

To begin with, observe that $p \equiv 1 \pmod 3$ entails that the map $x \mapsto x^3$ from $\mathbb{F}_q$ into itself is not injective (in fact it is 3 to 1, except for zero). This is becuase $\mathbb{F}_q$ contains the 3 distinct cubic roots of unity (which in fact lie actually in the prime field $\mathbb{F}_p$) since $T^3 - 1 = (T-1)(T^2+T+1)$ and the discriminant -3 of T^2+T+1 is a square in $\mathbb{F}_p$ because the Legendre symbol $\left(\frac{-3}{p}\right) = +1$, as is easily seen by making use of the quadratic reciprocity law (see [6], Ch. I §3). This observation tells us that (1) is not, *a priori*, equivalent to the Cauchy functional equation.

Now, we recall that any map $f : \mathbb{F}_q \to \mathbb{F}_q$ is induced by a polynomial (see [3] p. 214, although it is readily seen as an immediate consequence of Lagrange interpolation formula). As the polynomials T^q and T induce the same map on $\mathbb{F}_q$ (see [3], p. 177, p. 245), we can assume that any solution f of (1) is induced by a (reduced) polynomial of $\mathbb{F}_q[T]$:

$$P(T) = a_0 + a_1 T + a_2 T^2 + \cdots + a_{q-1} T^{q-1}. \tag{2}$$

Obviously functional equation (1) entails that the reductions via $T^q \equiv T$ of the polynomials $P(X^3 + Y^3)$ and $P(X^3) + P(Y^3)$ must coincide. As the latter polynomial contains no "mixed" terms (i.e. monomials aX^rY^s, with $a \neq 0$ and both r and s positive) the same must happen to the reduction of the former polynomial.

In order to study how these mixed terms reduce, we consider the arithmetic triangle modulo p corresponding to the binomial coefficients occurring in the binomial power expansions for exponents up to q. Observe that by assuming $p \equiv 1 \pmod 3$, necessarily $q = p^n \equiv 1 \pmod 3$, so that the arithmetic triangle built up to its $(q-1)$st row may be split into three horizontal strips of equal width $k := \frac{q-1}{3}$. By tracing from the vertices of

Figure 1.

these strips parallel lines to the other sides of the triangle, there appear 3 "inverted" triangles (see Figure 1).

After expanding $P(X^3+Y^3)$ we easily see that either 3 or 6 terms contribute to the same (mixed) reduction according as to whether or not these terms (respectively) are associated with the inverted triangles together with their boundaries (except, of course, lines AB and DD' in the figure). After this observation, assuming f is induced by (2), the vanishing of mixed terms after expansion and subsequent reduction of $P(X^3+Y^3)$ can easily be expressed by the linear equations (in $\mathbb{F}_q$):

$$E^j_r = 0, \quad \text{for } k < j \leq 2k, \text{ and } 0 < r \leq [j/2], \tag{3}$$

which the coefficients of $P(T)$ have to satisfy, where $[j/2]$ denotes the integral part of $\frac{j}{2}$ and E^j_r stands for either

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

or

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

depending, as said earlier, on whether or not $\binom{j}{r}$ lies in the upper inverted triangle (including its lower boundary). [It will be irrelevant for us the fact that (3) contains some redundant equations.]

2. The arithmetic triangle modulo p in connection with (3), for $p \equiv 1 \pmod 3$

In this section we will always assume $p \equiv 1 \pmod 3$.

Recall that $\binom{j}{r}$ mod p can easily be computed from the p-adic expansions of both j and r, namely we have (see [5], Section XXI, or [2]):

$$\binom{j}{r} \equiv \prod_{i=0}^{n-1} \binom{j_i}{r_i} \pmod p, \tag{4}$$

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 $j_i < r_i$.

In the same vein as in [1] for the case of squares, we prove

Proposition 1. *If a solution $(a_2, a_3, \ldots, a_{3k}) \in (\mathbb{F}_q)^{3k-1}$ of system (3) satisfies $a_{k+1} = \cdots = a_{3k} = 0$ then, for $2 \le t \le k$, a_t is arbitrary, if $t = p^m$, and zero, otherwise.*

Proof. Equations (3) have the shape

$$\binom{t}{r} a_t = 0, \quad t = 2, \ldots, k,\ 0 < r < t.$$

When $t = p^m$, trivially $\binom{p^m}{r} \equiv 0 \pmod p$, so that a_t is arbitrary. Otherwise we may write $t = p^m \cdot s$, with $s > 1$ and $p \nmid s$, but now it follows easily from (4) that $\binom{p^m s}{p^m} \equiv s \pmod p$, so that $a_t = 0$. □

We will show in this section that the hypothesis of the previous Proposition always holds but first we need a couple of lemmas.

Lemma 2. *$\binom{\lambda k}{k} \not\equiv 0 \pmod p$, for $\lambda \in \{2, 3\}$.*

Proof. Setting $\omega := \frac{p-1}{3}$, we have $k = \sum_{i=0}^{n-1} \omega p^i$, $2k = \sum_{i=0}^{n-1} 2\omega p^i$ and $3k = \sum_{i=0}^{n-1} 3\omega p^i$. The result follows from (4). □

Lemma 3. *For each j, with $k < j \le 2k$, there exists at least an r, with $j - k \le r \le k$, such that*

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

Proof. Trivial, by using the additive property

$$\binom{r}{s} + \binom{r}{s+1} = \binom{r+1}{s+1}$$

and bearing in mind that vertex $E = \binom{3k}{k}$ is not congruent to 0 modulo p by Lemma 2.

From the lemmas we have:

Proposition 4. *Let $(a_2, a_3, \dots, a_{3k})$ be a solution of system (3). Then:*

(i) *If for some j, with $k < j \le 2k$, $a_{j+k} = 0$, then $a_j = 0$.*
(ii) *If for some j, with $k < j \le 2k$, $a_j = 0$, then $a_{j+k} = 0$.*

Proof. By Lemma 2, vertex C of triangle ABC (see Figure 1) is not congruent to zero, so that, by the additive property, in each row j of this little triangle there must exist a binomial coefficient $\binom{j}{s} \not\equiv 0 \pmod{p}$; the corresponding equation $E^j_s = 0$ yields (i), and for (ii), it suffices to consider the equation $E^j_r = 0$ corresponding to the r appearing in Lemma 3. □

As the number of equations appearing in (3) is quite large, it seems that the quickest way to prove that, for each j (with $k < j \le 2k$), either $a_j = 0$ or $a_{j+k} = 0$, is by choosing a point inside triangle ABC (whose corresponding equation involves only the unknowns a_j and a_{j+k}) in such a way that exactly one coefficient is zero. But this is not always possible (for instance, when $j = 2k$, both coefficients are nonzero). In these cases we will look for a couple of equations with nonzero determinant so as to get just the trivial solution $a_j = a_{j+k} = 0$.

We next distinguish between the case $n > 1$ and $n = 1$ and will start with the former.

Proposition 5. *Let $q = p^n$, with $n > 1$, and let $(a_2, a_3, \dots, a_{3k})$ be a solution of (3). Then for each j, with $k < j \le 2k$, we have either $a_j = 0$ or $a_{j+k} = 0$.*

Proof. When $j = 2k$, it suffices to consider equations $E^{2k}_{\omega} = 0$, $E^{2k}_{\omega+1} = 0$ and $E^{2k}_{\omega+2} = 0$ (where $\omega := \frac{p-1}{3}$); by adding the first two equations and then the last two, we get a system involving only a_k and a_{2k} with nonvanishing determinant and, consequently, $a_k = a_{2k} = 0$. Now it is easy to see that $a_{3k} = 0$.

For $k < j < 2k$ consider the p-adic expansion of $j : \sum_{i=0}^{n-1} j_i p^i$. We shall distinguish 4 cases:

(I) For $0 \leq i \leq n-1$, we have $\omega \leq j_i \leq 2\omega$.
(II) For $0 \leq i \leq n-1$, we have $j_i \leq 2\omega$ but there exists some $j_l < \omega$.
(III) For $0 \leq i \leq n-1$, we have $\omega \leq j_i$ but there exists some $j_m > 2\omega$.
(IV) There exists some $j_l < \omega$ and some $j_m > 2\omega$.

In case (I) we shall also distinguish two subcases:

(I.1) $k < j < 2k - \omega$
(I.2) $2k - \omega \leq j < 2k$.

It is quite easy to show that equation $E^j_{j-k+\omega+1} = 0$ yields $a_{j+k} = 0$ in case (I.1), when $j_0 < 2\omega$; and when $j_0 = 2\omega$ the problem is solved by considering the system of equations $E^j_{j-k+\omega-1} = 0$ and $E^j_{j-k+\omega} = 0$ and proceeding as follows:

If the coefficient, say σ, of a_{j+k} in the second equation vanishes, then $a_j = 0$ since its coefficient (in the 2nd equation) does not vanish. So assume in what follows that $\sigma \not\equiv 0 \pmod{p}$, and observe that the sum of the coefficients of a_{j+k} in the previous two equations vanishes. Then the determinant of the system becomes

$$\begin{vmatrix} \binom{j}{j-k+\omega-1} & -\sigma \\ \binom{j}{j-k+\omega} & \sigma \end{vmatrix} \equiv \sigma \binom{j}{j-k+\omega} (2\omega+1) \not\equiv 0 \pmod{p},$$

so that $a_j = a_{j+k} = 0$.

In case (I.2), $j = 2k - t$, $0 < t \leq \omega$, and we get $a_j = 0$, if in equation $E^j_{j-k} = 0$ the coefficient $\binom{3k-t}{k-t} + \binom{3k-t}{2k-t}$ of a_{j+k} vanishes; otherwise we consider the system of equations: $E^j_{j-k} = 0$ and $E^j_{j-2k+p} = 0$, and proceed as follows:

It is easily seen that the respective coefficients of a_{j-k}, a_j and a_{j+k} in equation $E^j_{j-2k+p} = 0$ are

$$0, \quad \binom{2k-t}{k+p-t} \quad \text{and} \quad \binom{3k-t}{k+p-t} + \binom{3k-t}{2k+p-t},$$

so that $E^j_{j-2k+p} = 0$ will be seen as involving only a_j and a_{j+k}.

By means of

$$(5)\qquad \binom{a}{b+1} \equiv \binom{a}{b}\frac{a-b}{b+1} \pmod p \quad (\text{with } b+1 \not\equiv 0 \pmod p),$$

we have

$$\begin{aligned}\binom{2k-t}{k+p-t} &\equiv \binom{2\omega}{\omega}\cdots\binom{2\omega}{\omega}\binom{2\omega}{\omega+1}\binom{2\omega-t}{\omega-t} \pmod p\\ &\equiv \binom{2\omega}{\omega}\cdots\binom{2\omega}{\omega}\binom{2\omega}{\omega}\binom{2\omega-t}{\omega-t}\cdot\frac{\omega}{\omega+1} \pmod p\\ &\equiv \binom{2k-t}{k-t}\cdot\frac{\omega}{\omega+1} \pmod p\end{aligned}$$

and, in a similar way, we see that

$$\binom{3k-t}{k+p-t} \equiv -\binom{3k-t}{k-t} \text{ and } \binom{3k-t}{2k+p-t} \equiv -\binom{3k-t}{2k-t} \pmod p,$$

so that the determinant of the system $E^j_{j-k} = 0$ and $E^j_{j-2k+p} = 0$ of linear equations in a_j and a_{j+k} is

$$\begin{aligned}&\begin{vmatrix} \binom{2k-t}{k-t} & \binom{3k-t}{k-t} + \binom{3k-t}{2k-t} \\ \binom{2k-t}{k+p-t} & \binom{3k-t}{k+p-t} + \binom{3k-t}{2k+p-t} \end{vmatrix}\\ &\equiv \binom{2k-t}{k-t}\left[\binom{3k-t}{k-t} + \binom{3k-t}{2k-t}\right]\cdot\begin{vmatrix} 1 & 1 \\ \frac{\omega}{\omega+1} & -1 \end{vmatrix}\\ &\equiv -\binom{2k-t}{k-t}\left[\binom{3k-t}{k-t} + \binom{3k-t}{2k-t}\right]\cdot\frac{2\omega+1}{\omega+1} \not\equiv 0 \pmod p\end{aligned}$$

and, consequently, $a_j = a_{j+k} = 0$.

For the next two cases, equation $E^j_k = 0$ yields $a_{j+k} = 0$ in case (II) and $a_j = 0$ in (III).

Finally, in case (IV) we choose $r = \sum_{i=0}^{n-1} r_i p^i$ such that:

$$r_i = \begin{cases} j_i & \text{if } j_i < \omega \\ \omega & \text{if } j_i \geq \omega \\ 0 & \text{otherwise} \end{cases}$$

and consider the system of equations $E^j_r = E^j_{r+1} = 0$. Paying attention to the lth place in the p-adic expansions, where l is the least nonnegative integer such that $j_l < \omega$, we see that $\binom{j}{r+k} \equiv \binom{j+k}{r+2k} \equiv \binom{j}{r+1+k} \equiv \binom{j+k}{r+1+2k} \equiv 0$ (mod p), and doing the same for the least m such that $j_m > 2\omega$, we obtain $\binom{j+k}{r} \equiv \binom{j+k}{r+k} \equiv \binom{j+k}{r+1} \equiv \binom{j+k}{r+1+k} \equiv 0$ (mod p), so that the preceding system reduces to

$$\left.\begin{aligned} \binom{j-k}{r} a_{j-k} + \binom{j}{r} a_j = 0 \\ \binom{j-k}{r+1} a_{j-k} + \binom{j}{r+1} a_j = 0 \end{aligned}\right\}$$

with $\binom{j}{r} \not\equiv 0$ (mod p). Now, if $\binom{j-k}{r} \equiv 0$ (mod p), then $a_j = 0$ and we are done. Otherwise, i.e. if $\binom{j-k}{r} \not\equiv 0$ (mod p), by means of (5), we see that the determinant of the above system is

$$\binom{j-k}{r}\binom{j}{r} \begin{vmatrix} 1 & 1 \\ \frac{j-k-r}{r+1} & \frac{j-r}{r+1} \end{vmatrix} \equiv \binom{j-k}{r}\binom{j}{r} \frac{k}{r+1} \not\equiv 0 \text{ (mod } p),$$

and the proof is complete. □

When $n = 1$ (and consequently $q = p$), we obtain the same result as that in Proposition 5, but with 3 exceptional cases, as a consequence of the following lemmas.

Lemma 6. *If* $(a_2, a_3, \dots, a_{3k})$ *is a solution of* (3) *when* $q = p$, *then we have* $a_j = a_{j+k} = 0$, *for each* j *such that* $k < j < 2k - 1$.

Proof. Consider the equations $E^j_{t-1} = 0$ and $E^j_t = 0$, with $t = \left[\frac{j}{2}\right]$, and use (5). Although the cases j odd and j even have to be dealt with separately, we eventually get a nonvanishing determinant and consequently $a_j = a_{j+k} = 0$. □

Lemma 7. *Any solution* $(a_2, a_3, \dots, a_{3k})$ *of* (3), *for* $q = p > 13$, *satisfies* $a_k = a_{2k} = a_{3k} = 0$.

Proof. As $q > 13$ entails $k = \frac{p-1}{3} > 4$, we see that the numbers $\binom{2k}{i}$, for $1 \leq i \leq 4$, lie outside triangle ABC. By considering first the equations associated to these four numbers, adding then the 3 pairs of consecutive equations, and taking into account that the q-th row consists of zeros, if we discard both ends (which are ones), we get the following system of equations:

$$E_i^{2k} + E_{i+1}^{2k} = \binom{k+1}{i+1} a_k + \left[\binom{2k+1}{i+1} + \binom{2k+1}{i+1+k}\right] a_{2k} = 0, \; i = 1, 2, 3.$$

Now it is a trivial matter to check that the determinant of the first two equations above does not vanish when $\binom{2k+1}{2} - \binom{2k+1}{3+k} \not\equiv 0 \pmod{p}$. Otherwise the last two equations have nonzero determinant. Thus in either case we get $a_k = a_{2k} = 0$. Now, from $E_1^{2k} = 0$, we see that $a_{3k} = 0$. □

Lemma 8. *Any solution* $(a_2, a_3, \dots, a_{3k})$ *of* (3), *for* $q = p > 19$ *satisfies* $a_{k-1} = a_{2k-1} = a_{3k-1} = 0$.

Proof. In this situation $k > 6$, since $p > 19$, and thus the numbers $\binom{2k-1}{i}$, for $1 \le i \le 5$, lie outside triangle ABC. Consider the system of equations

$$\gamma_i := E_i^{2k-1} + E_{i+1}^{2k-1} = 0, \text{ for } i = 1, 2, 3, 4.$$

As the $3k$-th row of the arithmetic triangle modulo p is

$$1, \quad -1, \quad 1, \quad -1, \quad , \dots , \quad -1, \quad 1$$

and k is necessarily even, the coefficient of a_{3k-1} in the above 4 equations is $+3$, when i is odd, and -3, when i is even. Thus the system

$$\left.\begin{aligned} \gamma_1 + \gamma_2 = 0 \\ \gamma_2 + \gamma_3 = 0 \end{aligned}\right\}$$

involves just the unknowns a_{k-1} and a_{2k-1}, and has nonzero determinant if $\binom{2k+1}{3} - \binom{2k+1}{4+k} \not\equiv 0 \pmod{p}$; otherwise, the determinant of

$$\left.\begin{aligned} \gamma_2 + \gamma_3 = 0 \\ \gamma_3 + \gamma_4 = 0 \end{aligned}\right\}$$

is nonzero. Consequently $a_{k-1} = a_{2k-1} = 0$, and coming back to $\gamma_1 = 0$, we also get $a_{3k-1} = 0$. □

From these lemmas we can state

Proposition 9. *Any solution* $(a_2, a_3, \dots, a_{3k})$ *of* (3), *for* $q = p > 19$, *satisfies* $a_j = a_{j+k} = 0$, *for* $k < j \le 2k$.

Finally we cover the cases $q = p = 7, 13, 19$.

Proposition 10. *For $q = p = 7, 13, 19$, the solutions $(a_2, a_3, \ldots, a_{p-1})$ of (3) are given by*

(i) *Case $p = 7$: $a_4 = 4a_2$, $a_5 = 4a_3$ and $a_6 = 2a_2$, with both a_2 and a_3 arbitrary;*

(ii) *Case $p = 13$: $a_7 = 11a_3$ and $a_{11} = 5a_3$, with a_3 arbitrary, and the remaining a's being zero;*

(iii) *Case $p = 19$: $a_{11} = 9a_5$ and $a_{17} = 3a_5$, with a_5 arbitrary, and the remaining a's being zero.*

Proof. (i) By just solving (3), which in this case reads

$$\left.\begin{aligned} 2a_2 + a_4 + 4a_6 = 0 \\ 3a_3 + a_5 = 0 \\ 6a_4 + 2a_6 = 0 \end{aligned}\right\}$$

(ii) By Lemma 6, $a_2 = a_5 = a_6 = a_9 = a_{10} = 0$, and then (3) reduces to

$$\left.\begin{aligned} 3a_3 + 2a_7 + 8a_{11} = 0 \\ 9a_7 + a_{11} = 0 \\ 4a_4 + 12a_8 + 10a_{12} = 0 \\ 6a_4 + 4a_8 + 3a_{12} = 0 \\ 5a_8 + 2a_{12} = 0 \end{aligned}\right\}$$

(iii) By Proposition 1 and Lemmas 6 and 7, there remains to see what happens for $j = 2k - 1$: all a's are zero except for a_5, a_{11} and a_{17}, which are required to satisfy the system (of rank 2)

$$\left.\begin{aligned} 5a_5 + 18a_{11} + 14a_{17} = 0 \\ 10a_5 + 11a_{11} + 8a_{17} = 0 \\ 6a_{11} + a_{17} = 0 \end{aligned}\right\}. \qquad \square$$

3. Solutions of (1) in case $p \equiv 1 \pmod 3$

Theorem 11. *If $p \equiv 1 \pmod 3$, for $q = p^n$, other than 7, 13 or 19, functional equation (1) has q^n solutions $f : \mathbb{F}_q \to \mathbb{F}_q$, namely the maps*

$$f(x) = a_1x + a_px^p + a_{p^2}x^{p^2} + \cdots + a_{p^{n-1}}x^{p^{n-1}}, \text{ with } a_{p^i} \in \mathbb{F}_q.$$

Proof. By Propositions 1, 4 and 5, $P(T)$ has to be of the shape

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

Now, by equating $P(X^3+Y^3)$ and $P(X^3)+P(Y^3)$ we get the supplementary condition $a_0 = 2a_0$, whence $a_0 = 0$. The rest is obvious. □

Corollary. *For the cases considered in Theorem 11, functional equation* (1) *is equivalent to the Cauchy functional equation.*

Proof. $f : \mathbb{F}_q \to \mathbb{F}_q$ satisfies the Cauchy functional equation if and only if f is $\mathbb{F}_p$-linear. But $\mathbb{F}_q$ has rank n over $\mathbb{F}_p$, so that exactly q^n maps satisfy Cauchy. The rest is trivial. □

The reasoning in the remaining cases, i.e. $q = 7, 13, 19$, follows the same pattern as in Theorem 11 but the shape of $P(T)$ is now given by Proposition 10. The result is the following.

Theorem 12. *For $p = 7, 13, 19$, there are (respectively) $7^3, 13^2, 19^2$ solutions $f : \mathbb{F}_p \to \mathbb{F}_p$ of functional equation* (1)*, which are given (respectively) by*

$$\begin{aligned}
f(x) &= a_1x + a_2x^2 + a_3x^3 + 4a_2x^4 + 4a_3x^5 + 2a_2x^6, && \textit{with } a_1, a_2, a_3 \in \mathbb{F}_7,\\
f(x) &= a_1x + a_3x^3 + 11a_3x^7 + 5a_3x^{11}, && \textit{with } a_1, a_3 \in \mathbb{F}_{13},\\
f(x) &= a_1x + a_5x^5 + 9a_5x^{11} + 3a_5x^{17}, && \textit{with } a_1, a_5 \in \mathbb{F}_{19}.
\end{aligned}$$

Remark 1. The cases of higher powers of 7, 13 and 19 are covered by Theorem 11.

Remark 2. The solutions in Theorem 12 are, in fact, easily checked to satisfy (1). The 3 exceptional cases appearing in (1) are in contrast with the fact that, except for $\mathbb{F}_7$, in all fields $\mathbb{F}_{p^n}$, $p \equiv 1 \pmod 3$, each element is a sum of 2 cubes (cf. [4], p. 327). By the way, a direct computation for $p = 7$ shows that any solution of (1) is determined by $f(1)$ and the values of f on 3 and 4 (the only two elements which are not sums of two cubes).

Remark 3. If $q = 3^n$, the functional equation (1), for $f : \mathbb{F}_q \to \mathbb{F}_q$, is just the Cauchy functional equation (since $x \mapsto x^3$ is the Frobenius automorphism). On the lines of the proof of the above Corollary we see that in this case the solutions of the Cauchy functional equation are also given as in Theorem 11.

Acknowledgement. The authors thank the referee for his/her helpful suggestions.

References

[1] J. L. Garcia-Roig and J. Salillas, On a Pythagorean Functional Equation involving Finite Fields, (to appear in *Results of Math.*) (1996).

[2] A. M. Hinz, Pascal's Triangle and the Tower of Hanoi, *Amer. Math. Monthly* **99** no. 6 (June–July, 1992), 538–544.

[3] S. Lang, Algebra, 3rd edn, *Addison-Wesley*, 1993.

[4] R. Lidl and H. Niederreiter, Finite fields, vol. 20, *Encycl. of Math. and Its Appl., Addison-Wesley*, 1983.

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

[6] J.P. Serre, A Course in Arithmetic, G.T.M. 7. 2nd edn, *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 December 31, 1996; revised January 18, 1998)