BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 52, No. 3, 2004

NUMBER THEORY

On Equations $y^2 = x^n + k$ in a Finite Field

by

A. SCHINZEL and M. SKAŁBA

Presented by Andrzej SCHINZEL

Summary. Solutions of the equations $y^2 = x^n + k$ $(n = 3, 4)$ in a finite field are given almost explicitly in terms of k.

Let F be a finite field. It follows easily from Hasse's theorem on the number of points on an elliptic curve over F that each of the curves

$$y^2 = x^n + k \quad (n = 3, 4;\ k \in F) \tag{1}$$

has a point (x, y) in F^2, except for $n = 4$, $F = \mathbb{F}_5$, $k = 2$. The aim of the present paper is to indicate such a point almost explicitly in terms of k. Note that if $\operatorname{char} K = 2$, then (1) is satisfied by $y = (x^n + k)^{\operatorname{card} F/2}$, and if $\operatorname{char} K = 3$, $n = 3$ then (1) is satisfied by $x = (y^2 - k)^{\operatorname{card} F/3}$. We shall prove

THEOREM 1. *Let* $\operatorname{char} F > 3$ *and* $k \in F$. *Set*

$$y_1 = \begin{cases} 12 & \text{if } k + 72 = 0, \\ \frac{k}{12} + 3 & \text{if } k^2 - 72k + 72^2 = 0, \end{cases}$$

and if $k^3 + 72^3 \neq 0$, *set*

$$y_1 = -2^{-9}3^{-5}k^3 + 2^{-6}3^{-3}k^2 - 2^{-3}k - 3,$$

$$y_2 = 2^{-8}3^{-6}k^3 - 2^{-5}3^{-3}k^2 + 2^{-2}3^{-1}k + 2,$$

$$y_3 = \frac{k^6 - 288k^5 + 46656k^4 - 3732480k^3}{2^8 3^5 (k+72)^3} + \frac{134369280k^2 - 11609505792k + 139314069504}{2^8 3^5 (k+72)^3},$$

2000 *Mathematics Subject Classification*: 11G20, 11A15, 11D25.
Key words and phrases: finite fields, elliptic curves.

$$y_4 = \frac{k^9 - 504k^8 + 124416k^7 - 17915904k^6 + 1558683648k^5}{2^{10}3^5(k^2-72k+72^2)^3} + \frac{-69657034752k^4 + 5851190919168k^3}{2^{10}3^5(k^2-72k+72^2)^3} + \frac{20061226008576k^2 + 2166612408926208k + 51998697814228992}{2^{10}3^5(k^2-72k+72^2)^3}.$$

Then for at least one $j \le 4$ the equation $y_j^2 = x^3 + k$ is solvable in $x \in F$.

THEOREM 2. *Let* $\operatorname{char} F \neq 2$ *and* $k \in F^*$. *If* $k - 2 = 0$ *and* $\operatorname{char} F \neq 5$, *set*

$$u_1 = \frac{-5}{8}, \quad u_2 = 2, \quad u_3 = 5;$$

if $\operatorname{char} F = 5$ *and* $\alpha \in F \setminus \mathbb{F}_5$, *set*

$$u_1 = \frac{4\alpha}{1+\alpha^2}, \quad u_2 = \frac{2-2\alpha^2}{1+\alpha^2}, \quad u_3 = \frac{4\alpha(2-2\alpha^2)}{(1+\alpha^2)^2};$$

if $k^2 - 4k - 4 = 0$ *and* $k^3 - 8 \neq 0$, *set*

$$u_1 = \frac{-k^6 - 16k^3 + 64}{16k^4}, \quad u_2 = \frac{1}{k}, \quad u_3 = \frac{-k^6 - 16k^3 + 64}{k(k^3-8)^2};$$

if $k^2 - 4k - 4 = k^3 - 8 = 0$, *set*

$$u_1 = u_2 = u_3 = -1;$$

and if $(k-2)(k^2-4k-4) \neq 0$, *set*

$$u_1 = \frac{k^2-4k-4}{16}, \quad u_2 = \frac{k}{4}, \quad u_3 = \frac{k(k^2-4k-4)}{4(k-2)^2}.$$

Then $u_j \in F^*$ $(1 \le j \le 3)$ and for at least one $j \le 3$ the equation

$$\left(\frac{4u_j^2 + k}{4u_j}\right)^2 = x^4 + k$$

is solvable in $x \in F$.

The proof of Theorem 1 is based on the following

LEMMA 1. *Let A, B, C, D be in F and*

$$z_1 = A, \quad z_2 = B, \quad z_3 = ABC^3, \quad z_4 = AB^2D^3.$$

Then for at least one $j \le 4$ the equation $x^3 = z_j$ is solvable in $x \in F$.

Proof. If $ABCD = 0$ the assertion is clear and if $ABCD \neq 0$ it follows from the fact that the multiplicative group of F is cyclic and for all a, b in $\mathbb{Z}$ at least one of the numbers $a, b, a+b, a+2b$ is divisible by 3.

Proof of Theorem 1. If $k + 72 = 0$ or $k^2 - 72k + 72^2 = 0$ we have $y_1^2 - k = 6^3$ or $(-3)^3$, respectively. If $k^3 + 72^3 \neq 0$ we put in Lemma 1

$$A = y_1^2 - k, \quad B = y_2^2 - k, \quad C = 2^6 3^4 (k+72)^{-2}, \quad D = 2^{10} 3^8 (k^2 - 72k + 72^2)$$

and verify that

$$y_3 = \frac{y_1 y_2 + k}{y_1 + y_2}, \qquad y_3^2 - k = ABC^3,$$

$$y_4 = \frac{y_1 y_2^2 + k y_1 + 2k y_2}{y_2^2 + 2 y_1 y_2 + k}, \quad y_4^2 - k = AB^2 D^3.$$

The proof of Theorem 2 is based on the following

LEMMA 2. *Let u_j be as in Theorem 2. Then $u_j \in F^*$ and*

$$\sqrt{4u_j^3 - k u_j} \in F \quad \textit{for at least one } j \leq 3. \tag{2}$$

Proof. If $k - 2 = 0$ and $\operatorname{char} K \neq 5$, then $u_1 u_2 u_3 \neq 0$ and (2) holds because

$$(4u_1^3 - k u_1)(4u_2^3 - k u_2) = (4u_3^3 - k u_3)(1/8)^2.$$

If $k - 2 = 0$ and $\operatorname{char} K = 5$, $\alpha \in F \setminus \mathbb{F}_5$, then clearly $u_1 u_2 u_3 \neq 0$ and (2) holds as

$$(4u_1^3 - k u_1)(4u_2^3 - k u_2) = (4u_3^3 - k u_3) 2^2.$$

If $k^2 - 4k - 4 = 0$ and $k^3 - 8 \neq 0$, then $u_1 u_2 u_3 \neq 0$, since otherwise $k^6 + 16k^3 - 64 = 0$, while $\operatorname{char} F \neq 2$ implies

$$(k^2 - 4k - 4, k^6 + 16k^3 - 64) = 1.$$

Also (2) holds in view of the identity

$$(4u_1^3 - k u_1)(4u_2^3 - k u_2) = (4u_3^3 - k u_3) \left(\frac{k^3 - 8}{2k^2} \right)^6 (1/4)^2.$$

If $k^2 - 4k - 4 = k^3 - 8 = 0$, then $\operatorname{char} F = 7$, $k = 1$, $u_1 u_2 u_3 \neq 0$ and

$$4u_1^3 - k u_1 = 2^2.$$

If $(k - 2)(k^2 - 4k - 4) \neq 0$, then clearly $u_1 u_2 u_3 \neq 0$ and (2) holds since

$$(4u_1^3 - k u_1)(4u_2^3 - k u_2) = (4u_3^3 - k u_3) \left(\frac{k - 2}{4} \right)^6 2^2.$$

Proof of Theorem 2. We have the identity

$$\left(\frac{4u_j^2 + k}{4u_j} \right)^2 - k = \left(\frac{4u_j^2 - k}{4u_j} \right)^2$$

and by Lemma 2 for at least one $j \leq 3$ we have $\sqrt{(4u_j^2 - k)/4u_j} \in F$.

The following problem related to the proof of Lemma 2 remains open.

Problem. *Let* $f \in \mathbb{Z}[x]$ *have the leading coefficient positive and assume that the congruence* $f(x) \equiv y^2 \pmod{m}$ *is solvable for every natural number* m. *Does there exist an odd integer* $k > 0$ *and integers* $x_1, \ldots, x_k$ *such that* $\prod_{i=1}^{k} f(x_i)$ *is a square?*

A. Schinzel and M. Skałba
Institute of Mathematics
Polish Academy of Sciences
00-956 Warszawa, Poland
E-mail: schinzel@impan.gov.pl
skalba@impan.gov.pl

Received July 16, 2004;
received in final form July 28, 2004 (7406)