BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 55, No. 2, 2007

NUMBER THEORY

Rational Points on Certain Hyperelliptic Curves over Finite Fields

by

Maciej ULAS

Presented by Andrzej SCHINZEL

Dedicated to the memory of Andrzej Mąkowski

Summary. Let K be a field, $a, b \in K$ and $ab \neq 0$. Consider the polynomials $g_1(x) = x^n + ax + b$, $g_2(x) = x^n + ax^2 + bx$, where n is a fixed positive integer. We show that for each $k \geq 2$ the hypersurface given by the equation

$$S_k^i: \quad u^2 = \prod_{j=1}^{k} g_i(x_j), \qquad i = 1, 2,$$

contains a rational curve. Using the above and van de Woestijne's recent results we show how to construct a rational point different from the point at infinity on the curves C_i : $y^2 = g_i(x)$, $(i = 1, 2)$ defined over a finite field, in polynomial time.

1. Introduction. R. Schoof showed in [4] how to count the rational points on the elliptic curve $E : y^2 = x^3 + ax + b$ defined over the finite field $\mathbb{F}_p$, where $p > 3$ is a prime, in polynomial time. Surprisingly, this algorithm yields the order of the group $E(\mathbb{F}_p)$ without providing any point (different from the point at infinity) on the curve E explicitly. In [4] the problem was posed to construct an algorithm determining a rational point $P \in E(\mathbb{F}_p) \setminus \{\mathcal{O}\}$ in polynomial time.

To the author's best knowledge, the first work concerning this problem appeared in 2004. A. Schinzel and M. Skałba showed in [3] how to determine efficiently a rational point on the curve of the form $y^2 = x^n + a$, where

2000 *Mathematics Subject Classification*: Primary 11D25, 11D41; Secondary 14G15.

Key words and phrases: hyperelliptic curves, rational points, diophantine equations, finite fields.

The author is a scholarship holder of the Stanisław Estreicher Fund.

$n = 3, 4$, $a \in \mathbb{F}_q$ and $q = p^m$. In case $n = 3$, they gave explicit elements $y_1, y_2, y_3, y_4 \in \mathbb{F}_q$ such that for at least one $i \leq 4$ the equation $y_i^2 = x^3 + a$ has a solution in $\mathbb{F}_q$. In case $n = 4$, they constructed $y_1, y_2, y_3 \in \mathbb{F}_q$ such that for at least one $i \leq 3$, the equation $y_i^2 = x^4 + a$ has a solution in $\mathbb{F}_q$.

A solution of the subproblem of finding the x-coordinate of a rational point on the elliptic curve

$$E: \quad y^2 = x^3 + ax + b =: f(x)$$

in case $a, b \in \mathbb{F}_q$, $a \neq 0$, $q = p^m$ and $p > 3$, was provided in [7] (for many applications the y-coordinate is not needed). The key element of the proof was a construction of non-constant rational functions $x_1, x_2, x_3, u \in K(t)$ which satisfy the equation

$$u^2 = f(x_1)f(x_2)f(x_3). \tag{1.1}$$

We know that the multiplicative group $\mathbb{F}_q^*$ is cyclic. This fact plus the parametric solution obtained prove that for at least one $i \leq 3$, the element $f(x_i)$ is a square in $\mathbb{F}_q$. If now $q = p$ or $q = p^m$ and an element $v \in \mathbb{F}_q \setminus \mathbb{F}_q^2$ is given, then using Schoof's and Tonnelli–Shanks' algorithm (given in [6]) respectively, we can calculate a square root of $f(x_i)$ in polynomial time.

In his PhD dissertation [8], Ch. van de Woestijne showed how in polynomial time, for given $b_0, b_1, \ldots, b_n \in \mathbb{F}_q^*$, we can find integers i, j with $0 \leq i < j \leq n$ and an element $b \in \mathbb{F}_q^*$ such that $b_i/b_j = b^n$. Note that to calculate this nth root, it is not necessary to have the element $v \in \mathbb{F}_q \setminus \mathbb{F}_q^n$, and the algorithm which computes this root is deterministic. It is easy to see that having x_1, x_2, x_3 satisfying the identities (1.1) for some $u \in \mathbb{F}_q$ and using van de Woestijne's result we can find a rational point on the curve $y^2 = f(x)$ in polynomial time. This idea was used in [5]. The authors constructed a rational curve (different from the one in [7]) on the hypersurface $u^2 = f(x_1)f(x_2)f(x_3)$, where f is a given polynomial of degree three. However, in order to obtain an explicit form of the curve, it is necessary to solve the equation $\alpha x^2 + \beta y^2 = \gamma$ in $\mathbb{F}_q$ for some α, β, γ (this can be done in deterministic polynomial time, but of course it lengthens the time needed to compute a rational point on E). The authors also showed how to construct rational points on elliptic curves defined over finite fields of characteristic 2 and 3.

A natural question arising here concerns the existence of rational curves on a hypersurface of the form

$$S_k: \quad u^2 = \prod_{i=1}^{k} g(x_i), \tag{1.2}$$

where $g \in \mathbb{Z}[x]$ has no multiple roots. Note that in this case S_k is smooth. It appears that this problem has not been considered so far. Papers [7] and [5] show that for k odd, finding rational curves on the hypersurface S_k can be useful in finding rational points on hyperelliptic curves (defined over a finite field) of the form

$$C: \quad y^2 = g(x).$$

Note moreover that if $\deg g = 2, 3, 4$ and k is even number, then it is easy to find rational curves on S_k. Indeed, if $k = 2$, then on S_2 we have the rational curve $(x_1, x_2, u) = (t, t, g(t))$. If now $\deg g = 2$, then using a standard procedure we can parametrize the rational solutions of the equation $u^2 = g(t)g(x)$. For $\deg g = 3$ or $\deg g = 4$ we act similarly, except that this time we use an algorithm of adding points on a curve of genus one with known rational points. In this way we obtain infinitely many rational curves on S_2. As an immediate consequence of the above reasoning, we obtain curves on S_k for any even integer $k > 2$.

However, if $\deg g > 4$ or k is an odd integer, then the task seems to be much more difficult and the crucial question arises whether for a given $g \in \mathbb{Z}[x]$ there is an odd k such that S_k contains a rational curve.

Let now $a, b \in K$, $ab \neq 0$, and consider the polynomials

$$g_1(x) = x^n + ax + b, \qquad g_2(x) = x^n + ax^2 + bx,$$

where n is a fixed positive integer. In this paper we prove that if $g = g_1$ or $g = g_2$, then for each $k \geq 2$ there is a rational curve on the surface S_k.

Together with Woestijne's results this shows that rational points on the curve $C_i : y^2 = g_i(x)$ can be found in polynomial time. Let us also note that if n is even, then $g_i(-b/a) = (b/a)^n$ and the finite point $P = (-b/a,\ (b/a)^{n/2})$ lies on the curve $y^2 = g_i(x)$, so in this case the problem of existence of rational points on C_i is easy. However, this of course does not provide a rational curve on S_k when n is even.

2. Rational curves on S_k^i. In this section we consider the hypersurface

$$S_k^i: \quad u^2 = \prod_{j=1}^{k} g_i(x_j),$$

where $i \in \{1, 2\}$ is fixed. As direct examination of the existence of rational curves on S_k^i is difficult, we reduce the problem to examining simpler objects.

Let $a, b, c, d \in K$ satisfy the condition

$$(*) \qquad (a \neq 0 \text{ or } c \neq 0) \quad \text{and} \quad (b \neq 0 \text{ or } d \neq 0).$$

Let m, n be fixed positive integers and consider the surfaces

$$S^1: \quad g_1(x)z^m = y^n + cy + d,$$
$$S^2: \quad g_2(x)z^m = y^n + cy^2 + dy.$$

We will prove that a rational curve lies on each of these surfaces. Using these curves we will construct curves on S_2^i and S_3^i. Since each positive integer ≥ 2 is of the form $2k+3l$, as an immediate consequence we obtain the existence of rational curves on S_k^i for each $k \geq 2$.

We start with the following

Lemma 2.1. *Let $n, m \in \mathbb{N}_+$ and let $a, b, c, d \in K$ satisfy $(*)$. Then on each of the surfaces S^1, S^2 there is a rational curve.*

Proof. Let $F_1(x,y,z) := g_1(x)z^m - (y^n + cy + d)$ and $F_2(x,y,z) := g_2(x)z^m - (y^n + cy^2 + dy)$. Set $x = T$, $y = t^m T$, $z = t^n$. It is easy to see that the equation $F_1(T, t^m T, t^n) = 0$ has the root

$$T = -\frac{bt^{mn} - d}{at^{mn} - ct^m},$$

which gives us a parametric curve L_1 on S^1 given by

$$L_1: \quad x(t) = -\frac{bt^{mn} - d}{at^{mn} - ct^m}, \qquad y(t) = -\frac{bt^{mn} - d}{at^{m(n-1)} - c}, \qquad z(t) = t^n.$$

The same method can be applied to find a rational curve on S^2. In this case the equation $F_2(T, t^m T, t^n) = 0$ has two roots, $T = 0$ and

$$T = -\frac{bt^{m(n-1)} - d}{at^{m(n-1)} - ct^m}.$$

A rational curve L_2 on S^2 is given by the equations

$$L_2: \quad x(t) = -\frac{bt^{m(n-1)} - d}{at^{m(n-1)} - ct^m}, \qquad y(t) = -\frac{bt^{m(n-1)} - d}{at^{m(n-2)} - c}, \qquad z(t) = t^n.$$

Note that the condition $(*)$ is crucial in both cases. ∎

Remark 2.2. The surface S^1 appeared in [2] with the additional assumption $a = c, b = d, m = 2, n = 3$. In this case the curve L_1 was used to show that for a given $j \neq 0, 1728$ there are infinitely many elliptic curves with j-invariant equal to j and Mordell–Weil rank ≥ 2.

A special case of the surface S^1, when $m = 2$, $n = 3$, was also considered in [1]. In this case the curve L_1 was used to show that on S^1 the set of rational points is dense in the topology of $\mathbb{R}^3$.

Using the above lemma we can prove the following

Theorem 2.3. *Let K be a field and set $g_1(x) = x^n + ax + b$, $g_2(x) = x^n + ax^2 + bx$, where $a, b \in K, ab \neq 0$. Let t, u be variables.*

(1) *If $n \geq 3$ is a positive integer*, *set*

$$X_1(t) = -\frac{b}{a}\,\frac{t^{2n} - 1}{t^{2n} - t^2}, \qquad X_2(t) = t^2 X_1(t), \qquad U(t) = t^n g_1(X_1(t)).$$

Then

$$U(t)^2 = g_1(X_1(t))g_1(X_2(t)).$$

If now

$$X_1(t) = -\frac{b}{a}\,\frac{t^{2(n-1)}-1}{t^{2(n-1)}-t^2}, \qquad X_2(t) = t^2X_1(t), \quad U(t) = t^n g_1(X_1(t)),$$

then

$$U(t)^2 = g_2(X_1(t))g_2(X_2(t)).$$

(2) *If n is an odd integer, set*

$$\begin{aligned} X_1(t,u) &= u, \\ X_2(t,u) &= -\frac{b}{a}\,\frac{t^{2n}g_1(u)^n - 1}{g_1(u)(t^{2n}g_1(u)^{n-1}-t^2)}, \\ X_3(t,u) &= t^2 g_1(u)X_2(t,u), \\ U(t,u) &= t^n g_1(u)^{(n+1)/2} g_1(X_2(t,u)). \end{aligned}$$

Then

$$U(t,u)^2 = g_1(X_1(t,u))g_1(X_2(t,u))g_1(X_3(t,u)).$$

If now

$$\begin{aligned} X_1(t,u) &= u, \\ X_2(t,u) &= -\frac{b}{a}\,\frac{t^{2(n-1)}g_2(u)^{n-1} - 1}{g_2(u)(t^{2(n-1)}g_2(u)^{n-2}-t^2)}, \\ X_3(t,u) &= t^2 g_2(u)X_2(t,u), \\ U(t,u) &= t^n g_2(u)^{(n+1)/2} g_2(X_2(t,u)), \end{aligned}$$

then

$$U(t,u)^2 = g_2(X_1(t,u))g_2(X_2(t,u))g_2(X_3(t,u)).$$

Proof. We consider the surfaces S^1 and S^2 from Lemma 2.1 with $m=2$. To prove (1), note that the change of variables $z = z_1/g_1(x)$ shows that S^1 is birational to the surface

$$S' : \quad z_1^2 = (x^n + ax + b)(y^n + cy + d). \tag{2.1}$$

Putting now $a = c$, $b = d$ and using the equations of the curve L_1 from the proof of Lemma 2.1, we obtain the statement of our theorem.

Now we take the equations defining the curve L_2 from the proof of Lemma 2.1 and repeat the above reasoning for the surface S^2. This ends the proof of (1).

To prove (2), consider again the surface S' given by (2.1). If we now put $c = a/g_1(u)^{n-1}$, $d = b/g_1(u)^n$ and perform a change of variables

$$u = X_1, \quad x = X_2, \quad y = \frac{X_3}{g_1(u)}, \quad z_1 = U_1 g_1(u)^{-(n+1)/2}, \tag{2.2}$$

then after elementary calculations the equation of S' is of the form

$$U_1^2 = g_1(X_1)g_1(X_2)g_1(X_3).$$

If now x, y, z are rational functions defining the curve L_1 on the surface S^1 for $c = a/g_1(u)^{n-1}$, $d = b/g_1(u)^n$, then calculating X_1, X_2, X_3 from (2.2), we obtain a two-parameter solution of the above equation as given in the statement of our theorem.

The proof of (2) for $g_2(x) = x^n + ax^2 + bx$ is similar, with one difference: we substitute $a/g_2(u)^{n-2}$ and $b/g_2(u)^{n-1}$ for c, d respectively. ∎

Remark 2.4. If K is a finite field with $\operatorname{char} K > 3$, $a, b \in K, ab \neq 0$ and we look for a rational point on the elliptic curve

$$E: \quad y^2 = x^3 + ax + b =: f(x),$$

then our rational curve lying on the hypersurface S: $u^2 = f(x_1)f(x_2)f(x_3)$ is much simpler than that obtained by Skałba. If $x_i = X_i(t)$, $i = 1, 2, 3$, are the equations defining the curve on S, then if $X_1X_2X_3 = N/D$ for some relatively prime polynomials $N, D \in K[t]$, then $\deg N \leq 26$, $\deg D \leq 25$ for the parametrization obtained by Skałba, while $\deg N \leq 8$, $\deg D \leq 6$ for our parametrization (with $u \in K$ such that $f(u) \neq 0$) from Theorem 2.3. The multiplicative structure of the functions X_i is also very simple in our case, which influences the speed of calculations.

Moreover, our parametrization has the advantage over the one obtained by Shallue and van de Woestijne that it does not require solving an equation of the form $\alpha x^2 + \beta y^2 = \gamma$ in K.

Since for n even we have $g_i(-a/b) = ((b/a)^{n/2})^2$, from the above theorem we obtain

Corollary 2.5. *Let K be a field, $a, b \in K$, $ab \neq 0$. Then for each positive integer $k \geq 2$ there is a rational curve on the hypersurface*

$$S_k^i: \quad u^2 = \prod_{j=1}^{k} g_i(x_j), \qquad i = 1, 2.$$

Because the case $k = 3$ and $K = \mathbb{F}_q$, $q = p^m$, is especially interesting for us, we have to decide about the assumptions that would permit calculating the values of $X_i(u, t)$ for $i = 1, 2, 3$ from the second part of Theorem 2.3. We limit our considerations to the case of g_1 of odd degree n. For g_2 the reasoning is similar.

First, the functions $X_i(t, u)$ for $i = 1, 2, 3$ are non-constant. Moreover, X_2 and X_3 have the same denominator which equals

$$D(t, u) = g_1(u)t^2 \, \frac{(t^2g_1(u))^{n-1} - 1}{t^2g_1(u) - 1}.$$

We know that $v^{p^m-1} = 1$ for each $v \in \mathbb{F}_q$. There are $p^m - n$ elements $u \in \mathbb{F}_q$ for which $g_1(u) \neq 0$. If we fix such a u, then because $\deg_t D(t, u) =$

$2(n-1)$ and $t^2 \mid D(t,u)$, there are at least $p^m - 2(n-1)+1$ elements $t \in \mathbb{F}_q$ for which $D(t,u) \neq 0$. Thus there are at least $(p^m - n)(p^m - 2(n-1)+1)$ elements (t,u) in $\mathbb{F}_q \times \mathbb{F}_q$ for which $D(t,u) \neq 0$. Hence if $p > 2(n-1)-1$ then we can find $t, u \in \mathbb{F}_q$ such that $g_1(X_j(t,u))$ is a square for at least one $j \in \{1,2,3\}$.

3. Some remarks and questions. Define T to be the set of pairs $(t,u) \in \mathbb{F}_q \times \mathbb{F}_q$ for which we can compute $X_i(t,u)$, $i = 1,2,3$, from the preceding section. Then we can define a map $\varPhi$ from T to the curve $C : y^2 = g_1(x)$ by

$$\varPhi(t,u) = \big(X_j(t,u), \sqrt{g_1(X_j(t,u))}\big),$$

where the square root is taken in $\mathbb{F}_q$ and $j = \min\{i : g_1(X_i(t,u)) \text{ is a square}\}$. Note that there are at most $2q$ rational points on C over $\mathbb{F}_q$, while T, as we have proved, contains at least $(q-n)(q-2(n-1)+1)$ elements. This suggests the following

QUESTION 3.1. *Is the map $\varPhi : T \ni (t,u) \mapsto \varPhi(t,u) \in C$ surjective?*

Another question which comes to mind is the following.

QUESTION 3.2. *Fix $g \in \mathbb{Z}[x]$ without multiple roots. Is there an integer $k \geq 2$ such that on the hypersurface*

$$S_k : \quad u^2 = \prod_{j=1}^{k} g(x_j)$$

there are infinitely many rational points with $u \neq 0$? Here we are interested in non-trivial points on S_k, i.e. $(x_1, \ldots, x_k, u)$ such that $g(x_i) \neq g(x_j)$ for $i \neq j$.

It would also be interesting to know whether there are rational curves on S_k if we consider this hypersurface over $\mathbb{C}$ (instead of $\mathbb{Q}$).

It seems that the following question is much more difficult.

QUESTION 3.3. *Fix $g \in \mathbb{Z}[x]$ without multiple roots and a positive integer $k \geq 2$. Is there a non-trivial rational point with $u \neq 0$ on the hypersurface S_k?*

If the k in Question 3.3 is odd we should also assume that for each $p \in \mathbb{P} \cup \{\infty\}$ the curve $y^2 = g(x)$ has a point over $\mathbb{Q}_p$ (as usual $\mathbb{Q}_\infty = \mathbb{R}$). It is clear that the assumption concerning local solubility is necessary. For example, consider the polynomial $g(x) = 3 - x^2$. There are no $\mathbb{Q}_3$-rational points on the curve $y^2 = g(x)$, which immediately implies that there are none on S_k.

If g satisfies $x^n g(1/x) = g(x)$ (such polynomials are called *reciprocal*), then we have a rational curve $x_1 = t^2$, $x_2 = 1/t^2$, $u = t^n g(1/t^2)$ on the surface S_2. As an immediate consequence we conclude that if k is even, then there is a rational curve on S_k. Additionally, if the degree of g is odd, then on S_3 we have a rational curve given by

$$x_1 = t, \quad x_2 = g(t), \quad x_3 = \frac{1}{g(t)}, \quad u = g(t)^{(n+1)/2} g\left(\frac{1}{g(t)}\right),$$

and hence for each $k \geq 2$ there is a rational curve on S_k.

If $g(x) = x^4 + 1$, then on S_3 we have a rational curve with $x_i = x_i(t)$, $i = 1, 2, 3$, given by

$$x_1 = \frac{2t+1}{3t^2+3t+1}, \quad x_2 = \frac{3t^2+2t}{3t^2+3t+1}, \quad x_3 = \frac{3t^2+4t+1}{3t^2+3t+1}.$$

It would be very interesting to construct other families of polynomials with the property that for each $k \geq 2$ there are rational curves (or infinitely many non-trivial rational points) on S_k.

Acknowledgments. I would like to thank the anonymous referee for his valuable comments, and Professors A. Schinzel and K. Rusek for remarks improving the presentation. I am also grateful to Dr. M. Skałba who acquainted me with van de Woestijne's paper [8].

References

[1] M. Kuwata and L. Wang, *Topology of rational points on isotrivial elliptic surfaces*, Int. Math. Res. Not. 1993, no. 4, 113–123.

[2] J. F. Mestre, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris Sér. I Math. 314 (1992), 919–922.

[3] A. Schinzel and M. Skałba, *On equations $y^2 = x^n + k$ in a finite field*, Bull. Polish Acad. Sci. Math. 52 (2004), 223–226.

[4] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. 44 (1985), 483–494.

[5] A. Shallue and Ch. van de Woestijne, *Construction of rational points on elliptic curves over finite fields*, in: Algorithmic Number Theory, Lecture Notes in Comput. Sci. 4076, Berlin, 2006, 510–524.

[6] D. Shanks, *Five number-theoretic algorithms*, Congr. Numer. 7 (1972), 51–70.

[7] M. Skałba, *Points on elliptic curves over finite fields*, Acta Arith. 117 (2005), 293–301.

[8] Ch. van de Woestijne, *Deterministic equation solving over finite fields*, PhD thesis, Univ. Leiden, 2006.

Maciej Ulas
Institute of Mathematics
Jagiellonian University
Reymonta 4
30-059 Kraków, Poland
E-mail: Maciej.Ulas@im.uj.edu.pl

Received February 19, 2007;
received in final form April 26, 2007 (7583)