ACTA ARITHMETICA
117.3 (2005)

Points on elliptic curves over finite fields

by

M. Skałba (Warszawa)

The main result of the present paper asserts that given a polynomial $f(X) = X^3 + AX + B \in \mathbb{Q}[X]$ with $A \neq 0$ we can find $X_1, X_2, X_3, U \in \mathbb{Q}$ satisfying

$$f(X_1)f(X_2)f(X_3) = U^2.$$

In fact our method gives a two-parameter solution, but even the problem of the existence of any solution is non-trivial.

As the first application we give a deterministic polynomial time algorithm which produces points other than the point at infinity on a given elliptic curve $E : Y^2 = X^3 + AX + B$ defined over a finite field $\mathbb{F}_q$, provided $A \neq 0$ and a certain $n \in \mathbb{F}_q \setminus \mathbb{F}_q^2$ is given. Remarkably, no subexponential algorithm for this problem has been known before (according to N. Koblitz's remarks on p. 129 of his book [2]). But the first recognition of the problem can be attributed to R. Schoof, who writes in his classical paper [7]:*... in practice there is no problem in finding a point P, but I do not know how to prove that computing a point in $E(\mathbb{F}_q)$ is easy.*

The restriction to $A \neq 0$ is essential for our method. Fortunately we can refer to Theorem 1 of [6], where an effective method for finding points on $E : Y^2 = X^3 + B$ is provided.

Our second application concerns patterns of quadratic residues. We will prove some result related to a conjecture of E. Lehmer and R. K. Guy. Moreover we interpret this conjecture in the language of elliptic curves and supplement another conjecture.

I am greatly indebted to Prof. A. Schinzel for his help and encouragement at every stage of writing this paper.

Theorem 1. *Let F be any field of characteristic unequal to 2 or 3 and $f(X) = X^3 + AX + B$, with $A, B \in F$ and $A \neq 0$. Put*

$$X_j(t) = \frac{N_j(t)}{D_j(t)} \quad \text{for } j = 1, 2, 3,$$

2000 *Mathematics Subject Classification*: 11G20, 11G05.

where

$$N_1(t)=A^2t\sum_{j=0}^{4}\Big(\sum_{2a+3b=3j} n_{a,b}^{(1)}A^aB^b\Big)t^j,\quad D_1(t)=\sum_{j=0}^{5}\Big(\sum_{2a+3b=3j} d_{a,b}^{(1)}A^aB^b\Big)t^j,$$

$$N_2(t)=\sum_{j=0}^{6}\Big(\sum_{2a+3b=3j} n_{a,b}^{(2)}A^aB^b\Big)t^j,\quad D_2(t)=144At\sum_{j=0}^{4}\Big(\sum_{2a+3b=3j} d_{a,b}^{(2)}A^aB^b\Big)t^j,$$

$$N_3(t)=\sum_{j=0}^{15}\Big(\sum_{2a+3b=3j+3} n_{a,b}^{(3)}A^aB^b\Big)t^j,$$

$$D_3(t)=A\sum_{j=0}^{5}\Big(\sum_{2a+3b=3j} d_{a,b}^{(31)}A^aB^b\Big)t^j\cdot\sum_{j=0}^{10}\Big(\sum_{2a+3b=3j} d_{a,b}^{(32)}A^aB^b\Big)t^j,$$

and the coefficients $n_{a,b}^{(i)}$ *and* $d_{a,b}^{(i)}$ *are given in the tables at the end of the paper. Then*

$$f(X_1(t^2))f(X_2(t^2))f(X_3(t^2))=U^2 \quad \textit{for some } U\in F(t) \tag{1}$$

and $X_1(t), X_2(t), X_3(t)$ *are not constant.*

THEOREM 2. *Let* $\mathbb{F}_q$ *be a finite field of* q *elements,* $\gcd(q,6)=1$, *and consider an elliptic curve* $E: Y^2=X^3+AX+B$, *where* $A,B\in\mathbb{F}_q$ *and* $A\neq 0$. *Let* $T\subseteq\mathbb{F}_q$ *satisfy the condition: if* $t\in T$ *then* $-t\notin T$. *Define a map* $\Phi: T\to E(\mathbb{F}_q)$ *as follows:*

$$\Phi(t)=(X_j(t^2),\sqrt{f(X_j(t^2))}),\quad \textit{where}\quad j=\min\{1\le i\le 3 \mid f(X_i(t^2))\in\mathbb{F}_q^2\},$$

and $X_i(t)$ $(i=1,2,3)$ *are defined in Theorem* 1. *Then* Φ *is well defined for at least* $|T|-25$ *values of* t *and*

$$|\operatorname{Im}\Phi|\ge\left\lceil\frac{|T|-25}{26}\right\rceil. \tag{2}$$

COROLLARY 1. *Let* F *be a finite field of characteristic unequal to* 2 *or* 3, $E: Y^2=X^3+AX+B$ *an elliptic curve defined over* F, *where* $A\neq 0$, *and suppose a certain* $n\in F\setminus F^2$ *is given. Then we can compute a point* $P\in E(F)\setminus\{\infty\}$ *in time polynomial in* $\log|F|$. *The relevant* O*-constant is absolute.*

Thus, according to N. Koblitz's remarks ([2, p. 129]), we can say that *the main obstacle to a deterministic polynomial time algorithm for finding a point on* E has been overcome. The remaining obstacle, the theoretical difficulty of extracting square roots, can also be overcome in the following special case.

COROLLARY 2. *Let* $E: Y^2=X^3+AX+B$ *be an elliptic curve, where* $A,B\in\mathbb{Z}$ *and* $A\neq 0$. *If* $p\nmid 4A^3+27B^2$ *then we can find a point*

$P \in E(\mathbb{F}_p) \setminus \{\infty\}$ *in time polynomial in* $\log p$. *The relevant* O*-constant depends only on* $|B|$.

REMARK. Our method of finding points in $E(\mathbb{F}_q)$, based on Theorem 2, gives actually any number of points that is of polynomial growth in $\log q$, in time polynomial in $\log q$. For the sake of simplicity of formulation we have confined ourselves in the above corollaries to single points $P \neq \infty$.

There are many papers devoted to investigation of patterns of power residues. We are interested in the following special problem. Let $a < b$ be positive integers. Denote (after E. Lehmer and R. K. Guy [1, Problem F6]) by $\Omega(a,b)$ the least number such that for all $p > p(a,b)$ there exists $n \leq \Omega(a,b)$ such that each of $n, n+a, n+b$ is a quadratic residue modulo p; moreover, write $\Omega(a,b) = \infty$ if there is no such finite number. There is a conjecture of R. K. Guy and E. Lehmer ([1, Problem F6]) that

if $(a,b) \not\equiv (1,2) \bmod 3, (1,3) \bmod 5, (2,3) \bmod 5, (2,4) \bmod 5, (1,5) \bmod 7, (2,3) \bmod 7, (4,6) \bmod 7$, *then* $\Omega(a,b) < \infty$.

Our modest task at the moment is to formulate this conjecture using explicitly the language of elliptic curves.

CONJECTURE 1. *Consider the elliptic curve* $E : Y^2 = X(X+a)(X+b)$ *where* $a < b$ *are natural numbers. Assume that for each prime* p *satisfying* $p \nmid ab(b-a)$, *the duplication does not send all points of* $E(\mathbb{F}_p)$ *to the point* ∞ (*equivalently* $|E(\mathbb{F}_p)| > 4$). *Then* $\Omega(a,b) < \infty$.

The equivalence of both conjectures is easily obtainable by H. Hasse's estimate

$$||E(\mathbb{F}_p)| - (p+1)| < 2\sqrt{p},$$

which implies that $|E(\mathbb{F}_p)| > 4$ for $p \geq 11$. Hence the only candidates for *delay primes* (using the terminology of E. Lehmer [3]) can be $3, 5$ or 7. It is a very elementary verification that $E(\mathbb{F}_p) \cong C_2 \times C_2$ if and only if (a,b) appears in the above list of R. K. Guy and E. Lehmer.

We prove the following result related to Conjecture 1.

THEOREM 3. *For any rational numbers* $a \neq b$ *there exist rational numbers* r_1, r_2, r_3 *satisfying*: *for every sufficiently large prime number* p *there exists* $j \in \{1,2,3\}$ *such that*

$$\left(\frac{r_j}{p}\right) = \left(\frac{r_j + a}{p}\right) = \left(\frac{r_j + b}{p}\right) = +1$$

where $\left(\frac{-}{p}\right)$ *stands for the Legendre symbol and the numerators are considered modulo* p.

For the sake of completeness we formulate a conjecture which is even more basic than Conjecture 1 (see also Problem in [6]).

CONJECTURE 2. *Consider the elliptic curve* $E : Y^2 = X^3 + AX^2 + BX + C$, *where* A, B, C *are given integers. Assume that for each prime number* p *at which* E *has good reduction, the reduced curve* $E(\mathbb{F}_p)$ *contains at least one affine point (equivalently* $|E(\mathbb{F}_p)| > 1$*). Then there exists a constant* $C(E)$ *such that for each sufficiently large prime* p *there exist integers* X, Y *satisfying the congruence*

$$Y^2 \equiv X^3 + AX^2 + BX + C \pmod{p}$$

and additionally $1 \le X \le C(E)$.

For the proofs we need three lemmas.

LEMMA 1. *If* $f(X) = X^3 + AX + B$ *then the following identity holds*:

$$f\left(\frac{\alpha^3 + 4B}{-4A - 3\alpha^2}\right) = \left(\frac{\alpha^3 + 4A\alpha - 8B}{-4A - 3\alpha^2}\right)^2 \cdot \frac{\alpha^3 + A\alpha + B}{-4A - 3\alpha^2}.$$

LEMMA 2. *Let* F *be a field of characteristic unequal to* 2 *or* 3 *and consider the algebraic set* V *defined over* F *by the equation*

$$y^2 + 12Ax^2 = z^3 + Az + B =: f(z), \quad \text{where } A, B \in F \text{ and } A \neq 0. \tag{3}$$

Then V *is irreducible and if we put*

$$X_1 = \frac{yz + 4Ax}{y - 3xz}, \quad X_2 = \frac{z^3 + 4B}{-4A - 3z^2}, \quad X_3 = \frac{X_1^3 + 4B}{-4A - 3X_1^2},$$

then

$$f(X_1)f(X_2)f(X_3) = \left(\frac{(X_1^3 + AX_1 + B)(X_1^3 + 4AX_1 - 8B)(z^3 + 4Az - 8B)(y - 3xz)}{(-4A - 3X_1^2)(-4A - 3z^2)^2}\right)^2,$$

where both sides are to be understood as elements of $F(V)$, *the function field of* V.

Proof. For the proof of irreducibility of V we refer to [5, p. 68, Corollary 2 and Corollary 3]. By Lemma 1 we obtain

$$f(X_2) = \left(\frac{z^3 + 4Az - 8B}{-4A - 3z^2}\right)^2 \cdot \frac{z^3 + Az + B}{-4A - 3z^2},$$

$$f(X_3) = \left(\frac{X_1^3 + 4AX_1 - 8B}{-4A - 3X_1^2}\right)^2 \cdot \frac{X_1^3 + AX_1 + B}{-4A - 3X_1^2},$$

and hence

$$f(X_1)f(X_2)f(X_3) = \frac{z^3 + Az + B}{(-4A - 3X_1^2)(-4A - 3z^2)} \times \left(\frac{(X_1^3 + AX_1 + B)(X_1^3 + 4AX_1 - 8B)(z^3 + 4Az - 8B)}{(-4A - 3X_1^2)(-4A - 3z^2)}\right)^2.$$

We use the equation defining V and transform further

$$\frac{z^3+Az+B}{(-4A-3X_1^2)(-4A-3z^2)} = \frac{y^2+12Ax^2}{(-4A-3X_1^2)(-4A-3z^2)} = \left(\frac{y-3xz}{-4A-3z^2}\right)^2.$$

Now the assertion follows by combining the above formulas.

LEMMA 3. *Let V be the variety given by* (3). *Then we have rational morphism*

$$\Psi : F^2 \to V(F),$$

given by the formulas

$$\Psi(t,s) = (x(t,s), y(t,s), z(t,s)),$$

where

$$\begin{aligned} x = x(t,s) &= 3m^2r - 4Amtr + A^2t^2r - 12Ar^3 - 12A^2rs^2 \\ &\quad + 3Bmts - ABt^2s + 12ABs^3, \\ y = y(t,s) &= m^3 - 2Am^2t + A^2mt^2 - 36Amr^2 - 12A^2ms^2 \\ &\quad + B^2t^3 + 24A^2tr^2 - 36ABtrs, \\ z = z(t,s) &= m^2 + 12Ar^2, \\ m = m(t,s) &:= \frac{At^2-12As^2}{2t}, \qquad r = r(t,s) := \frac{Bt^2-1}{24As}. \end{aligned}$$

Proof. This result belongs to Mordell. It is a special case of Theorem 1 on page 113 of his classical treatise [4]. We have only performed all detailed elementary calculations to make the solution as explicit as possible.

Proof of Theorem 1. We apply Lemmas 2 and 3. When we substitute $s = t$ in the formulas for x, y, z in Lemma 3 and then compute X_1, X_2, X_3 of Lemma 2 we shall obtain $X_1(t^2), X_2(t^2), X_3(t^2)$, where $X_1(t), X_2(t), X_3(t)$ are displayed in Theorem 1. Now we will verify that $D_1(t)D_2(t)D_3(t) \neq 0$ and that $X_1(t), X_2(t), X_3(t)$ are non-constant. The lowest term in the product $D_1(t)D_2(t)D_3(t)$ is $144A^2t$ (this follows from the tables given at the end of the paper). Since $A \neq 0$ and $\operatorname{char} F \neq 2, 3$ we obtain $144A^2 \neq 0$ and hence $D_1(t)D_2(t)D_3(t) \neq 0$.

The equality $N_1(t)/D_1(t) = c_1 \in F$ would imply $N_1(t) = 0$. From Table 1 we see that the coefficients $212A^2$, $208A^2B$ and $161568A^5 + 264A^2B^2$ vanish. The fact that $212A^2 = 0$, while A is not zero, implies that $\operatorname{char} F = 53$. Since $208 \not\equiv 0 \pmod{53}$, we have $B = 0$ and hence, as $161568 \not\equiv 0 \pmod{53}$, we find $A = 0$, a contradiction.

Next $X_2(t) \notin F$ because $N_2(0) \neq 0$ and $D_2(0) = 0$. For the proof that $X_3(t) \notin F$ we use the formula

$$X_3(t) = \frac{X_1(t)^3 + 4B}{-4A - 3X_1(t)^2}.$$

The equality $X_3(t) = c_3 \in F$ would give

$$X_1(t)^3 + 3c_3X_1(t)^2 + (4B + 4c_3A) = 0,$$

but $c_3 = X_3(0) = -B/A$, which leads to

$$X_1(t)^2\left(X_1(t) - \frac{3B}{A}\right) = 0,$$

a contradiction with $X_1(t) \notin F$.

Proof of Theorem 2. The set

$$\{t \in T \mid D_1(t^2)D_2(t^2)D_3(t^2) = 0\}$$

has no more than $\deg D_1(t) + \deg D_2(t) + \deg D_3(t) \leq 25$ elements. For the remaining values of t the map Φ is well defined because of (1) and the fact that $\mathbb{F}_q^*$ is cyclic. In the worst case the same point in $E(\mathbb{F}_q)$ can be obtained by our procedure for $\deg X_1(t) + \deg X_2(t) + \deg X_3(t) \leq 26$ values of $t \in T$, and this ends the proof of inequality (2).

Proof of Corollary 1. Obviously we can assume that $|F| > 49$. First, take a subset T of F satisfying $T \cap (-T) = \emptyset$ and $|T| = 26$. Secondly, using Theorem 2 find $X \in F$ such that $f(X) \in F^2$. Finally, compute the relevant square root $Y = \sqrt{f(X)}$ using $n \in F \setminus F^2$ and the well known "approximation" procedure due to D. Shanks [8], in time polynomial in $\log|F|$.

First proof of Corollary 2. We distinguish two cases. If $f(0) = B$ is a quadratic residue mod p we compute $y = \sqrt{B} \bmod p$, using the algorithm of R. Schoof [7], in time $O((|B|^{1/2+\varepsilon}\log p)^9)$. If B is a quadratic non-residue we put $n = B$ and apply Corollary 1.

Second (direct) proof of Corollary 2. The proof differs from the above only in the case $\left(\frac{B}{p}\right) = -1$. So we can compute all square roots which appear in what follows in deterministic polynomial time. By Lemma 1 it is sufficient to find $\alpha \in \mathbb{Z}$ satisfying

$$\left(\frac{-4A - 3\alpha^2}{p}\right) = -1. \tag{4}$$

Consider the quadratic form

$$g(u, v) = -4Au^2 - 3v^2.$$

If we find $u, v \in \mathbb{F}_p$ such that

$$\left(\frac{g(u,v)}{p}\right) = -1 \quad \text{and} \quad uv \neq 0, \tag{5}$$

then we put $\alpha = v/u$ and (4) holds. If either $-4A = g(1,0)$ or $-3 = g(0,1)$ is a quadratic non-residue mod p then we easily find $u, v \in \mathbb{F}_p^*$ satisfying $g(u,v) = -4A$ or $g(u,v) = -3$ (respectively) and (5) holds. If both $-4A$

and -3 are squares mod p we first find $c, d \in \mathbb{F}_p^*$ such that

$$c^2 = -4A, \quad d^2 = -3.$$

In new variables $s = cu, t = dv$ the form $g(u, v)$ transforms to $G(s, t) = s^2 + t^2$. Let n_0 be the unique number in the interval $[2, p-1]$ satisfying $n_0 \equiv B \bmod p$ and define

$$n_{j+1} = n_j - [\sqrt{n_j}]^2 \quad \text{for } j = 0, 1, \ldots.$$

For $J = \max\{j \geq 0 \mid \left(\frac{n_j}{p}\right) = -1\}$ we obtain

$$n_J = G(f, [\sqrt{n_J}])$$

with $f \in \mathbb{F}_p^*$ satisfying $f^2 = n_{J+1}$. Since $J \ll \log\log p$ we have arrived at $u = f/c$, $v = [\sqrt{n_J}]/d$ satisfying (5) in polynomial time.

Proof of Theorem 3. Consider the elliptic curve

$$\widetilde{E} : \widetilde{Y}^2 = \widetilde{X}(\widetilde{X} + a)(\widetilde{X} + b) =: g(\widetilde{X}).$$

The map

$$\widetilde{X} \mapsto X = \widetilde{X} + \frac{a+b}{3}, \quad \widetilde{Y} \mapsto Y$$

gives an isomorphism of $\widetilde{E}$ onto $E : Y^2 = X^3 + AX + B$, where $A = (ab - a^2 - b^2)/3 \neq 0$. We apply Theorem 1 to obtain rational numbers $\widetilde{X}_1, \widetilde{X}_2, \widetilde{X}_3, \widetilde{U}$ such that

$$g(\widetilde{X}_1)g(\widetilde{X}_2)g(\widetilde{X}_3) = \widetilde{U}^2 \quad \text{and} \quad \widetilde{U} \neq 0. \tag{6}$$

Now we define

$$r_j = \frac{(\widetilde{X}_j - ab)^2}{4g(\widetilde{X}_j)}$$

and verify that

$$r_j + a = \frac{(\widetilde{X}_j^2 + 2a\widetilde{X}_j + ab)^2}{4g(\widetilde{X}_j)}, \quad r_j + b = \frac{(\widetilde{X}_j^2 + 2b\widetilde{X}_j + ab)^2}{4g(\widetilde{X}_j)}. \tag{7}$$

If a prime number p appears neither in the numerators nor in the denominators of $g(\widetilde{X}_j)$ $(j = 1, 2, 3)$, then using the fact that $\mathbb{F}_p^*$ is cyclic and (6) we infer that at least one of $g(\widetilde{X}_j)$ is a square in $\mathbb{F}_p$. The desired assertion follows now by the definition of r_j and (7).

Table 1 $(i = 1)$

$$n_{0,0}^{(1)} = 212; \quad n_{0,1}^{(1)} = -208; \quad n_{3,0}^{(1)} = -161568, \; n_{0,2}^{(1)} = -264;$$
$$n_{3,1}^{(1)} = 441408, \; n_{0,3}^{(1)} = 304; \quad n_{6,0}^{(1)} = -92765376, \; n_{3,2}^{(1)} = -127776, \; n_{0,4}^{(1)} = -44;$$
$$d_{0,0}^{(1)} = -1; \quad d_{0,1}^{(1)} = 5; \quad d_{3,0}^{(1)} = 10536, \; d_{0,2}^{(1)} = -10; \quad d_{3,1}^{(1)} = 9480, \; d_{0,3}^{(1)} = 10;$$
$$d_{6,0}^{(1)} = 4024944, \; d_{3,2}^{(1)} = -4488, \; d_{0,4}^{(1)} = -5; \quad d_{6,1}^{(1)} = 2108304, \; d_{3,3}^{(1)} = 2904, \; d_{0,5}^{(1)} = 1.$$

Table 2 $(i = 2)$

$$n^{(2)}_{0,0} = -1; \quad n^{(2)}_{0,1} = 6; \quad n^{(2)}_{3,0} = -4356,\ n^{(2)}_{0,2} = -15; \quad n^{(2)}_{3,1} = -424944,\ n^{(2)}_{0,3} = 20;$$
$$n^{(2)}_{6,0} = -6324912,\ n^{(2)}_{3,2} = -26136,\ n^{(2)}_{0,4} = -15;$$
$$n^{(2)}_{6,1} = 12649824,\ n^{(2)}_{3,3} = 17424,\ n^{(2)}_{0,5} = 6;$$
$$n^{(2)}_{9,0} = -3061257408,\ n^{(2)}_{6,2} = -6324912,\ n^{(2)}_{3,4} = -4356,\ n^{(2)}_{0,6} = -1;$$
$$d^{(2)}_{0,0} = 1; \quad d^{(2)}_{0,1} = -4; \quad d^{(2)}_{3,0} = 5976,\ d^{(2)}_{0,2} = 6; \quad d^{(2)}_{3,1} = -5808,\ d^{(2)}_{0,3} = -4;$$
$$d^{(2)}_{6,0} = 2108304,\ d^{(2)}_{3,2} = 2904,\ d^{(2)}_{0,4} = 1.$$

Table 3 $(i = 3, 31, 32)$

$$n^{(3)}_{0,1} = 1; \quad n^{(3)}_{3,0} = 0,\ n^{(3)}_{0,2} = -15; \quad n^{(3)}_{3,1} = -31608,\ n^{(3)}_{0,3} = 105;$$
$$n^{(3)}_{6,0} = -2382032,\ n^{(3)}_{3,2} = 287640,\ n^{(3)}_{0,4} = -455;$$
$$n^{(3)}_{6,1} = 327958320,\ n^{(3)}_{3,3} = -1124496,\ n^{(3)}_{0,5} = 1365;$$
$$n^{(3)}_{9,0} = 5446134144,\ n^{(3)}_{6,2} = -949378416,\ n^{(3)}_{3,4} = 2369808,\ n^{(3)}_{0,6} = -3003;$$
$$n^{(3)}_{9,1} = -940697745408,\ n^{(3)}_{6,3} = -185899568,\ n^{(3)}_{3,5} = -2531880,\ n^{(3)}_{0,7} = 5005;$$
$$n^{(3)}_{12,0} = -1023635467008,\ n^{(3)}_{9,2} = -4041852271488,$$
$$n^{(3)}_{6,4} = 3844905120,\ n^{(3)}_{3,6} = -14904,\ n^{(3)}_{0,8} = -6435;$$
$$n^{(3)}_{12,1} = -1271178606627072,\ n^{(3)}_{9,3} = -557953136640,$$
$$n^{(3)}_{6,5} = -5637798432,\ n^{(3)}_{3,7} = 4402080,\ n^{(3)}_{0,9} = 6435;$$
$$n^{(3)}_{15,0} = -3711755775062016,\ n^{(3)}_{12,2} = -3365703371771136,$$
$$n^{(3)}_{9,4} = 1809225932544,\ n^{(3)}_{6,6} = 2558454048,\ n^{(3)}_{3,8} = -7401888,\ n^{(3)}_{0,10} = -5005;$$
$$n^{(3)}_{15,1} = -502999567986972672,\ n^{(3)}_{12,3} = -924766944152832,$$
$$n^{(3)}_{9,5} = -3401013749760,\ n^{(3)}_{6,7} = 1784103840,\ n^{(3)}_{3,9} = 7013304,\ n^{(3)}_{0,11} = 3003;$$
$$n^{(3)}_{18,0} = 447914759358173184,\ n^{(3)}_{15,2} = -981669643253544960,\ n^{(3)}_{12,4} = 329477012308224,$$
$$n^{(3)}_{9,6} = 913161021696,\ n^{(3)}_{6,8} = -3372070032,\ n^{(3)}_{3,10} = -4408920,\ n^{(3)}_{0,12} = -1365;$$
$$n^{(3)}_{18,1} = -73786028437373497344,\ n^{(3)}_{15,3} = -459570852044992512,$$
$$n^{(3)}_{12,5} = -977913669655296,\ n^{(3)}_{9,7} = 439245379584,$$
$$n^{(3)}_{6,9} = 2438317040,\ n^{(3)}_{3,11} = 1904112,\ n^{(3)}_{0,13} = 455;$$
$$n^{(3)}_{21,0} = 1042769766152244658176,\ n^{(3)}_{18,2} = -84332284536876355584,$$
$$n^{(3)}_{15,4} = 5961076345331712,\ n^{(3)}_{12,6} = -43484326592256,$$
$$n^{(3)}_{9,8} = -707241693312,\ n^{(3)}_{6,10} = -1030036656,\ n^{(3)}_{3,12} = -555120,\ n^{(3)}_{0,14} = -105;$$
$$n^{(3)}_{21,1} = -28488742630826030530 56,\ n^{(3)}_{18,3} = -63482146340076490752,$$
$$n^{(3)}_{15,5} = -101522561076541440,\ n^{(3)}_{12,7} = 69490543161600,$$
$$n^{(3)}_{9,9} = 280657428480,\ n^{(3)}_{6,11} = 255430032,\ n^{(3)}_{3,13} = 100584,\ n^{(3)}_{0,15} = 15;$$

$$n^{(3)}_{24,0} = 19957113916647077176934 4,\ n^{(3)}_{21,2} = 824674128787069304832,$$
$$n^{(3)}_{18,4} = -7951403445605351424,\ n^{(3)}_{15,6} = -37420516674680832,\ n^{(3)}_{12,8} = -66000709716480,$$
$$n^{(3)}_{9,10} = -61039617408,\ n^{(3)}_{6,12} = -31603264,\ n^{(3)}_{3,14} = -8712,\ n^{(3)}_{0,16} = -1;$$
$$d^{(31)}_{0,0} = -1;\quad d^{(31)}_{0,1} = 5;\quad d^{(31)}_{3,0} = 10536,\ d^{(31)}_{0,2} = -10;\quad d^{(31)}_{3,1} = 9480,\ d^{(31)}_{0,3} = 10;$$
$$d^{(31)}_{6,0} = 4024944,\ d^{(31)}_{3,2} = -4488,\ d^{(31)}_{0,4} = -5;$$
$$d^{(31)}_{6,1} = 2108304,\ d^{(31)}_{3,3} = 2904,\ d^{(31)}_{0,5} = 1;$$
$$d^{(32)}_{0,0} = 1;\quad d^{(32)}_{0,1} = -10;\quad d^{(32)}_{3,0} = 12636,\ d^{(32)}_{0,2} = 45;\quad d^{(32)}_{3,1} = 20256,\ d^{(32)}_{0,3} = -120;$$
$$d^{(32)}_{6,0} = 51578784,\ d^{(32)}_{3,2} = -158448,\ d^{(32)}_{0,4} = 210;$$
$$d^{(32)}_{6,1} = 426572352,\ d^{(32)}_{3,3} = 149472,\ d^{(32)}_{0,5} = -252;$$
$$d^{(32)}_{9,0} = 74892394368,\ d^{(32)}_{6,2} = -178487712,\ d^{(32)}_{3,4} = 146472,\ d^{(32)}_{0,6} = 210;$$
$$d^{(32)}_{9,1} = 42705805824,\ d^{(32)}_{6,3} = -194173056,\ d^{(32)}_{3,5} = -328224,\ d^{(32)}_{0,7} = -120;$$
$$d^{(32)}_{12,0} = 38682048607488,\ d^{(32)}_{9,2} = 217678171392,$$
$$d^{(32)}_{6,4} = 339663456,\ d^{(32)}_{3,6} = 208656,\ d^{(32)}_{0,8} = 45;$$
$$d^{(32)}_{12,1} = -44449457564160,\ d^{(32)}_{9,3} = -122450296320,$$
$$d^{(32)}_{6,5} = -126498240,\ d^{(32)}_{3,7} = -58080,\ d^{(32)}_{0,9} = 10;$$
$$d^{(32)}_{15,0} = 6454061238316032,\ d^{(32)}_{12,2} = 22224728782080,$$
$$d^{(32)}_{9,4} = 30612574080,\ d^{(32)}_{6,6} = 21083040,\ d^{(32)}_{3,8} = 7260,\ d^{(32)}_{0,10} = 1.$$

References

[1] R. K. Guy, *Unsolved Problems in Number Theory*, 2nd ed., Springer, 1994.

[2] N. Koblitz, *Algebraic Aspects of Cryptography*, Springer, Berlin, 1998.

[3] E. Lehmer, *Patterns of power residues*, J. Number Theory 17 (1983), 37–46.

[4] L. J. Mordell, *Diophantine Equations*, Academic Press, London and New York, 1969.

[5] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Cambridge Univ. Press, 2000.

[6] 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.

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

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

Institute of Mathematics
Polish Academy of Sciences
00-956 Warszawa, Poland
E-mail: skalba@impan.gov.pl

Institute of Mathematics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland

Received on 1.10.2004
and in revised form on 18.1.2005 (4858)