Elliptic curve analogues of a pseudorandom generator

Katalin Gyarmati

Abstract

Using the discrete logarithm in [7] and [9] a large family of pseudorandom binary sequences was constructed. Here we extend this construction. An interesting feature of this extension is that in certain special cases we get sequences involving points on elliptic curves.

2000 AMS Mathematics Subject Classification: 11K45.

List of keywords and phrases: pseudorandom, elliptic curve.

1 Introduction

In a series of papers Mauduit and Sárközy (partly with further coauthors) studied finite pseudorandom binary sequences

$$E_N = \{e_1, e_2, \dots, e_N\} \in \{-1, +1\}^N.$$

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K67676 and PD72264 and the János Bolyai Research Fellowship.

In particular, in Part I [12] first they introduced the following measures of pseudorandomness:

Write

$$U(E_N, t, a, b) = \sum_{j=0}^{t-1} e_{a+jb}$$

and, for $D = (d_1, \dots, d_\ell)$ with non-negative integers $d_1 < \cdots < d_\ell$,

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell}.$$

Then the *well-distribution measure* of E_N is defined as

$$W(E_N) = \max_{a,b,t} |U(E_N(t, a, b)| = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|,$$

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \leq a \leq a + (t-1)b \leq N$, while the *correlation measure of order* ℓ of E_N is defined as

$$C_\ell(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \dots, d_\ell)$ and M such that $1 \leq d_1 < d_2 < \cdots < d_\ell < M + d_\ell \leq N$.

Then the sequence E_N is considered as a "good" pseudorandom sequence if both measures $W(E_N)$, $C_\ell(E_N)$ (at least for small ℓ) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$).

Numerous binary sequences have been tested for pseudorandomness by J. Cassaigne, Z. Chen, X. Du, L. Goubin, S. Ferenczi, S. Li, H. Liu, C. Mauduit, L. Mérai, S. Oon, J. Rivat, A. Sárközy, G. Xiao and others. In the best constructions we have $W(E_N) \ll N^{1/2}(\log N)^c$ and $C_\ell(E_N) \ll N^{1/2}(\log N)^{c_\ell}$, where $c, c_2, c_3, \dots$ are positive constants. However, most of these constructions produced only a "few" pseudorandom sequences; usually for a fixed integer N, the construction provided only one pseudorandom sequence E_N of length N. First L. Goubin, C. Mauduit, A. Sárközy [6] succeeded in constructing a large family of pseudorandom binary sequences. Since then numerous other large families of pseudorandom sequences have been constructed (see [7], [8], [9], [10], [11] and [13]). Specially, I generalized the construction of Sárközy [14] in [7], [8] and [9]. Indeed, in [7] and [9] I studied a faster version of [8], this faster construction was the following:

Construction A *Let p be an odd prime, g be a primitive root modulo p. For $(n,p)=1$ define* ind n *by*

$$g^{\text{ind } n} \equiv n \pmod p \quad \text{ and } 1 \le \text{ind } n \le p-1.$$

Let

$$m \mid p-1$$

with $m \in \mathbb{N}$, and define $\text{ind}^* n$ *by*

$$\text{ind}^* n \equiv \text{ind } n \pmod m \quad \text{ and } 1 \le \text{ind}^* n \le m.$$

Define the sequence $E_{p-1} = \{e_1, \dots, e_{p-1}\}$ by

$$e_n = \begin{cases} +1 & \text{if } 1 \le \text{ind}^* f(n) \le \frac{m}{2}, \\ -1 & \text{if } \frac{m}{2} < \text{ind}^* f(n) \le m \text{ or } p \mid f(n). \end{cases}$$

In [7] and [9] I proved the following:

Theorem A *Let p be an odd prime, $m \mid p-1$ and $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree k, which has no multiple roots. Suppose that m is even. Then*

$$W(E_{p-1}) \ll kp^{1/2} \log p \log m.$$

Moreover suppose that at least one of the following 4 conditions holds:

a) *f is irreducible;*

b) *if f has the factorization $f = \varphi_1\varphi_2\dots\varphi_u$ where φ_i's are irreducible over $\mathbb{F}_p$, then there exists a β such that exactly one or two φ_i's are of degree β;*

c) $\ell = 2$;

d) $(4\ell)^k < p$ *or* $(4k)^\ell < p$.

Then

$$C_\ell(E_{p-1}) < 9k\ell 4^\ell p^{1/2}(\log p)^{\ell+1}.$$

Here we further generalize this construction:

Construction 1 *Let p be an odd prime and define m and $\mathrm{ind}^* n$ as in Construction A. Let $\mathcal{A}$ and $\mathcal{B}$ two disjoint sets such that $\mathcal{A}\cup\mathcal{B} = \{1, 2, 3, \dots, m\}$, $\mathcal{A}\cap\mathcal{B} = \emptyset$. Now define the sequence $E_{p-1} = \{e_1, \dots, e_{p-1}\}$ by*

$$e_n = \begin{cases} +1 & \textit{if } \mathrm{ind}^* f(n) \in \mathcal{A}, \\ -1 & \textit{if } \mathrm{ind}^* f(n) \in \mathcal{B} \textit{ or } p \mid f(n). \end{cases} \tag{1}$$

Clearly, in this way we get a large family of pseudorandom sequences. Not only the polynomial $f(x) \in \mathbb{F}_p[x]$ can be chosen p^k ways, but also the sets $\mathcal{A}$ and $\mathcal{B}$ can be chosen many different ways.

However not every sequence in this family has strong pseudorandom properties. For example, if A and $\mathcal{B}$ are of nearly the same cardinality then it is proved that the sequence has poor pseudorandom properties. For $|\mathcal{A}| = |\mathcal{B}|$ we give sufficient conditions for small well-distribution measure and correlation measures.

Theorem 1 *Let p be an odd prime, $m \mid p-1$ and $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree k, which has no multiple roots. Define the sequence $E_{p-1} = \{e_1, e_2, \dots, e_{p-1}\}$ by* (1)*. Then*

$$W(E_{p-1}) = \frac{||\mathcal{A}| - |\mathcal{B}||}{m} p + O(kmp^{1/2} \log p). \tag{2}$$

Moreover suppose that at least one of the 4 conditions a), b), c) and d) holds in Theorem A. Then we have

$$C_\ell(E_{p-1}) = \left(\frac{||\mathcal{A}| - |\mathcal{B}||}{m} \right)^\ell p + O(k\ell m^{2\ell} p^{1/2} \log p). \tag{3}$$

If $|\mathcal{A}| = |\mathcal{B}|$ and m is small in terms of p, then both measures $W(E_{p-1})$ and $C_\ell(E_{p-1})$ are small; they are less than $cp^{1/2} \log p$ with a constant c depending only on k and ℓ.

Recently, several pseudorandom constructions using elliptic curves have been presented (see for example [2], [3], [4], [5]). In most of these constructions the coordinates of multiples of a point P are used. Here we will present another construction which combines Theorem 1 with elliptic curves. Unlike the previous constructions, our new constructions use *two* elliptic curves.

Corollary 1 *Let $p = 4k+1$ be a prime number and Z a quadratic non-residue modulo p. Consider two elliptic curves over $\mathbb{F}_p$:*

$$E_1 : \ y^2 = x^3 + Ax + B,$$
$$E_2 : \ y^2 = x^3 + AZ^2x + BZ^3,$$

where x^3+Ax+B has no multiple roots. For $1 \le n \le p-1$ either E_1 contains a point P_n of form (n, y_n) or E_2 contains a point Q_n of form (Zn, y_n). Now *we may define* $E_{p-1} = \{e_1, e_2, \dots, e_{p-1}\}$ *by*

$$e_n = \begin{cases} \left(\frac{y_n}{p}\right) = \left(\frac{-y_n}{p}\right) & \text{if } p \nmid y_n, \\ 1 & \text{if } p \mid y_n. \end{cases}$$

This sequence has strong pseudorandom properties:

$$W(E_N) = O(p^{1/2} \log p)$$

and for $(4\ell)^3 < p$

$$C_\ell(E_N) = O(16^\ell \ell p^{1/2} \log p).$$

The case of primes of form $4k+3$ is more complicated. Then $\left(\frac{y_n}{p}\right) = -\left(\frac{-y_n}{p}\right)$, so we must determine which point we use in the construction: (n, y_n) or $(n, -y_n)$, (Zn, y_n) or $(Zn, -y_n)$? We also slightly modify the definition of the elements of the sequence.

Corollary 2 *Let* $p = 4k+3 \geq 7$ *be a prime number. Consider two elliptic curves over* $\mathbb{F}_p$*:*

$$E_1 : \ y^2 = x^3 + Ax + B,$$

$$E_2 : \ y^2 = x^3 + Ax - B,$$

where $x^3 + Ax + B$ *has no multiple roots. For* $1 \leq n \leq p-1$ *either* E_1 *contains a point* P_n *of form* (n, y_n) *where* y_n *is a quadratic residue, or* E_2 *contains a point* Q_n *of form* $(-n, y_n)$ *where* y_n *is a quadratic residue. Let* $m \mid p-1$ *and if* m *is odd let* $m' = m$ *and let* $\mathcal{A}$,$\mathcal{B}$ *be two disjoint sets such that* $\mathcal{A} \cup \mathcal{B} = \{1, 2, 3, \dots, m\}$, $\mathcal{A} \cap \mathcal{B} = \emptyset$. *If* m *is even let* $m' = m/2$ *and let*

$\mathcal{A}$,$\mathcal{B}$ be two disjoint sets such that $\mathcal{A}\cup\mathcal{B}=\{2,4,6,\dots,m\}$, $\mathcal{A}\cap\mathcal{B}=\emptyset$. Now we may define $E_{p-1}=\{e_1,e_2,\dots,e_{p-1}\}$ by

$$e_n=\begin{cases}1 & \textit{if } \operatorname{ind}^* y_n\in\mathcal{A},\\ -1 & \textit{if } \operatorname{ind}^* y_n\in\mathcal{B} \textit{ or } p\mid y_n.\end{cases}$$

Then

$$W(E_N)=\frac{||\mathcal{A}|-|\mathcal{B}||}{m'}p+O(mp^{1/2}\log p) \tag{4}$$

and for $(4\ell)^3<p$

$$C_\ell(E_N)=\left(\frac{||\mathcal{A}|-|\mathcal{B}||}{m'}\right)^\ell p+O(\ell m'^{2\ell}p^{1/2}\log p). \tag{5}$$

Thus for $|\mathcal{A}|\approx|\mathcal{B}|$ and for properly chosen m, E_{p-1} has strong pseudorandom properties.

Finally we remark that we may also consider hyperelliptic curves $y^2=f(x)$ and $y^2=Zf(x)$ in place of E_1 and E_2.

We mention that E_2 is a twist of E_1 in Corollaries 1 and 2, see [16]. It is well-known that both in Corollary 1 and Corollary 2 we have that for $1\le n\le p-1$ either E_1 contains a point P_n of form (n,y_n) or E_2 contains a point Q_n of form (Zn,y_n) (where in case of Corollary 1 Z is the quadratic non-residue, while in case of Corollary 2 $Z=-1$) see e.g. [16].

2 Proof of Theorem 1

The proof of the theorem is very similar to the proof of Theorem 1-3 in [9] and Theorem 1 in [7]. By the formula

$$\frac{1}{m}\sum_{\chi:\chi^m=1}\overline{\chi}^j(a)\chi(b)=\begin{cases}1 & \text{if } m \mid \operatorname{ind} a-\operatorname{ind} b,\\ 0 & \text{if } m \nmid \operatorname{ind} a-\operatorname{ind} b,\end{cases}$$

we obtain

$$e_n = 2\sum_{\substack{a\in\mathcal{A}\\ \operatorname{ind} f(n)\equiv a \pmod m}} 1 - 1 = \frac{2}{m}\sum_{a\in\mathcal{A}}\sum_{\chi:\chi^m=1}\overline{\chi}(f(n))\chi(g^a)-1.$$

By this and $m=|\mathcal{A}|+|\mathcal{B}|$

$$\begin{aligned} e_n &= \frac{2}{m}\sum_{a\in\mathcal{A}}\sum_{\chi\neq\chi_0:\chi^m=1}\overline{\chi}(f(n))\chi(g^a)+\frac{2\,|\mathcal{A}|}{m}-1\\ &= \frac{2}{m}\sum_{a\in\mathcal{A}}\sum_{\chi\neq\chi_0:\chi^m=1}\overline{\chi}(f(n))\chi(g^a)+\frac{|\mathcal{A}|-|\mathcal{B}|}{m}. \end{aligned} \tag{6}$$

Assume now that $1\leq a\leq a+(t-1)b\leq N$. Then we have

$$\begin{aligned} |U(E_{p-1},t,a,b)| &= \left|\frac{|\mathcal{A}|-|\mathcal{B}|}{m}t+\right.\\ &\quad\left.+\frac{2}{m}\sum_{\chi\neq\chi_0:\chi^m=1}\left(\sum_{i=0}^{t-1}\overline{\chi}(f(a+ib))\right)\left(\sum_{j\in\mathcal{A}}\chi(g^j)\right)\right|\\ &= \frac{||\mathcal{A}|-|\mathcal{B}||}{m}t+O(S), \end{aligned}$$

where

$$S=\left|\frac{2}{m}\sum_{\chi\neq\chi_0:\chi^m=1}\left(\sum_{i=0}^{t-1}\overline{\chi}(f(a+ib))\right)\left(\sum_{j\in\mathcal{A}}\chi(g^j)\right)\right|. \tag{7}$$

We will prove the following:

$$S=O\left(kmp^{1/2}(\log p)\right), \tag{8}$$

from which (2) immediately follows.

We will use the following lemma:

Lemma 1 *Suppose that p is a prime, χ is a non-principal character modulo p of order d, $f \in \mathbb{F}_p[x]$ has s distinct roots in $\overline{\mathbb{F}}_p$, and it is not the constant multiple of the d-th power of a polynomial over $\mathbb{F}_p$. Let y be a real number with $0 < y \le p$. Then for any $x \in \mathbb{R}$:*

$$\left| \sum_{x<n\le x+y} \chi(f(n)) \right| < 9sp^{1/2} \log p.$$

Poof of Lemma 1

This is a trivial consequence of Lemma 1 in [1]. Indeed, there this result is deduced from Weil theorem, see [18].

Since f has no multiple roots, by Lemma 1 we have:

$$\left| \sum_{i=0}^{t-1} \overline{\chi}(f(a+ib)) \right| \le 9kp^{1/2} \log p$$

and thus by (7) and $|\mathcal{A}| \le m$

$$\begin{aligned} S &\le \frac{18kp^{1/2}\log p}{m} \sum_{\chi\neq\chi_0:\chi^m=1} \left| \sum_{j\in\mathcal{A}} \chi^j(g^j) \right| \\ &\le \frac{18kp^{1/2}\log p}{m} m\,|\mathcal{A}| \le 18kmp^{1/2}\log p, \end{aligned}$$

which was to be proved.

To prove (3), consider any $\mathcal{D} = \{d_1, d_2, \ldots, d_\ell\}$ with non-negative integers $d_1 < d_2 < \cdots < d_\ell$ and positive integers M with $M + d_\ell \le p - 1$. Let $z = \frac{|\mathcal{A}|-|\mathcal{B}|}{m}$. Then by (6)

$$e_n = z + \frac{2}{m} \sum_{a\in\mathcal{A}} \sum_{\chi\neq\chi_0:\ \chi^m=\chi_0} \overline{\chi}(f(n))\chi(g^a).$$

So

$$
\begin{aligned}
V(E_N, M, \mathcal{D}) &= \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k} \\
&= \sum_{n=1}^{M} \left(z + \frac{2}{m} \sum_{a \in \mathcal{A}} \sum_{\substack{\chi \neq \chi_0: \\ \chi^m = \chi_0}} \overline{\chi}(f(n+d_1)) \chi(g^a) \right) \dots \\
&\left(z + \frac{2}{m} \sum_{a \in \mathcal{A}} \sum_{\substack{\chi \neq \chi_0: \\ \chi^m = \chi_0}} \overline{\chi}(f(n+d_\ell)) \chi(g^a) \right) \\
&= \sum_{n=1}^{M} \sum_{j=0}^{\ell} z^{\ell-j} \sum_{\{i_1,\dots,i_j\} \subseteq \{1,\dots,\ell\}} \sum_{a_{i_1} \in \mathcal{A}} \cdots \sum_{a_{i_j} \in \mathcal{A}} \sum_{\substack{\chi_{i_1} \neq \chi_0: \\ \chi_{i_1}^m = \chi_0}} \dots \\
&\sum_{\substack{\chi_{i_j} \neq \chi_0: \\ \chi_{i_j}^m = \chi_0}} \overline{\chi_{i_1}}(f(n+d_{i_1})) \dots \overline{\chi_{i_j}}(f(n+d_{i_j})) \chi_{i_1}(g^{a_{i_1}}) \dots \chi_{i_j}(g^{a_{i_j}}) \\
&= z^\ell M + O\Bigg(\sum_{n=1}^{M} \sum_{j=1}^{\ell} z^{\ell-j} \sum_{\{i_1,\dots,i_j\} \subseteq \{1,\dots,\ell\}} \sum_{a_{i_1} \in \mathcal{A}} \cdots \sum_{a_{i_j} \in \mathcal{A}} \sum_{\substack{\chi_{i_1} \neq \chi_0: \\ \chi_{i_1}^m = \chi_0}} \dots \\
&\sum_{\substack{\chi_{i_j} \neq \chi_0: \\ \chi_{i_j}^m = \chi_0}} \overline{\chi_{i_1}}(f(n+d_{i_1})) \dots \overline{\chi_{i_j}}(f(n+d_{i_j})) \chi_{i_1}(g^{a_{i_1}}) \dots \chi_{i_j}(g^{a_{i_j}}) \Bigg).
\end{aligned}
\tag{9}
$$

Here

$$O\Bigg(\sum_{n=1}^{M} \sum_{j=1}^{\ell} z^{\ell-j} \sum_{\{i_1,\dots,i_j\}\subseteq\{1,\dots,\ell\}} \sum_{a_{i_1}\in\mathcal{A}} \cdots \sum_{a_{i_j}\in\mathcal{A}} \sum_{\substack{\chi_{i_1}\neq\chi_0:\\ \chi_{i_1}^m=\chi_0}} \cdots \sum_{\substack{\chi_{i_j}\neq\chi_0:\\ \chi_{i_j}^m=\chi_0}}$$

$$\overline{\chi_{i_1}}(f(n+d_{i_1}))\dots\overline{\chi_{i_j}}(f(n+d_{i_j}))\chi_{i_1}(g^{a_{i_1}})\dots\chi_{i_j}(g^{a_{i_j}}) \Bigg)$$

$$= O\Bigg(\sum_{j=1}^{\ell} z^{\ell-j} \sum_{\{i_1,\dots,i_j\}\subseteq\{1,\dots,\ell\}} \sum_{a_{i_1}\in\mathcal{A}} \cdots \sum_{a_{i_j}\in\mathcal{A}} \Bigg| \sum_{\substack{\chi_{i_1}\neq\chi_0:\\ \chi_{i_1}^m=\chi_0}} \cdots \sum_{\substack{\chi_{i_j}\neq\chi_0:\\ \chi_{i_j}^m=\chi_0}}$$

$$\sum_{n=1}^{M} \overline{\chi_{i_1}}(f(n+d_{i_1}))\dots\overline{\chi_{i_j}}(f(n+d_{i_j}))\chi_{i_1}(g^{a_{i_1}})\dots\chi_{i_j}(g^{a_{i_j}}) \Bigg|\Bigg)$$

$$= O\Bigg(\sum_{j=1}^{\ell} z^{\ell-j} \sum_{\{i_1,\dots,i_j\}\subseteq\{1,\dots,\ell\}} \sum_{a_{i_1}\in\mathcal{A}} \cdots \sum_{a_{i_j}\in\mathcal{A}} \Bigg| \sum_{\substack{\chi_{i_1}\neq\chi_0:\\ \chi_{i_1}^m=\chi_0}} \cdots \sum_{\substack{\chi_{i_j}\neq\chi_0:\\ \chi_{i_j}^m=\chi_0}}$$

$$\sum_{n=1}^{M} \overline{\chi_{i_1}}(f(n+d_{i_1}))\dots\overline{\chi_{i_j}}(f(n+d_{i_j})) \Bigg|\Bigg)$$

$$= O\Bigg(\sum_{j=1}^{\ell} z^{\ell-j} \sum_{\{i_1,\dots,i_j\}\subseteq\{1,\dots,\ell\}} |\mathcal{A}|^j \sum_{\substack{\chi_{i_1}\neq\chi_0:\\ \chi_{i_1}^m=\chi_0}} \cdots \sum_{\substack{\chi_{i_j}\neq\chi_0:\\ \chi_{i_j}^m=\chi_0}}$$

$$\Bigg| \sum_{n=1}^{M} \overline{\chi_{i_1}}(f(n+d_{i_1}))\dots\overline{\chi_{i_j}}(f(n+d_{i_j})) \Bigg|\Bigg). \tag{10}$$

Now let χ be a modulo p character of order m; for simplicity we will choose χ as the character uniquely defined by $\chi(g) = e\left(\frac{1}{m}\right)$. Let $\chi_u = \chi^{\delta_u}$ for $u = 1, 2, \dots, \ell$, whence by $\chi_{i_1} \neq \chi_0, \dots, \chi_{i_j} \neq \chi_0$, we may take

$$1 \leq \delta_{i_u} < m.$$

Thus in (10) we have

$$\begin{aligned}
&\left|\sum_{n=1}^{M} \chi_1(f(n+d_{i_1}))\dots\chi_\ell(f(n+d_{i_j}))\right| \\
&= \left|\sum_{n=1}^{M} \chi^{\delta_{i_1}}(f(n+d_{i_1}))\dots\chi^{\delta_{i_j}}(f(n+d_{i_j}))\right| \\
&= \left|\sum_{n=1}^{M} \chi\left(f^{\delta_{i_1}}(n+d_{i_1})\dots f^{\delta_{i_j}}(n+d_{i_j})\right)\right|.
\end{aligned}$$

If $f^{\delta_{i_1}}(n+d_{i_1})\cdots f^{\delta_{i_j}}(n+d_{i_j})$ is not the constant multiple of a perfect m-th power, then this sum can be estimated by Lemma 1, whence

$$\left|\sum_{n=1}^{M} \chi(f^{\delta_{i_1}}(n+d_{i_1})\cdots f^{\delta_{i_j}}(n+d_{i_j}))\right| \le 9k\ell p^{1/2}\log p.$$

Therefore by (9), (10) and the triangle-inequality we get:

$$\begin{aligned}
|V(E_N,M,D)| &= z^\ell M + O\left(\sum_{j=1}^{\ell} z^{\ell-j}\,|\mathcal{A}|^j \sum_{\{i_1,\dots,i_j\}\subseteq\{1,\dots,\ell\}} \sum_{\substack{\chi_{i_1}\neq\chi_0:\\ \chi_{i_1}^m=\chi_0}} \cdots \sum_{\substack{\chi_{i_j}\neq\chi_0:\\ \chi_{i_j}^m=\chi_0}} 9k\ell p^{1/2}\log p\right. \\
&= z^\ell M + O\left(\sum_{j=1}^{\ell} z^{\ell-j}\,|\mathcal{A}|^j \binom{\ell}{j}(m-1)^j k\ell p^{1/2}\log p\right) \\
&= z^\ell M + O\left((|\mathcal{A}|(m-1)+|z|)^\ell k\ell p^{1/2}\log p\right) \qquad (11) \\
&= z^\ell M + O(k\ell m^{2\ell}p^{1/2}\log p)
\end{aligned}$$

which proves (8).

It remains to prove that $f^{\delta_{i_1}}(n+d_{i_1})\cdots f^{\delta_{i_j}}(n+d_{i_j})$ is never the constant multiple of a perfect m-th power. This follows from Lemma 1 in [7].

3 Proof of Corollary 1

First suppose that $\left(\frac{n^3+An+B}{p}\right) = 1$. Then P_n is a point on E_1. Clearly,

$$\begin{aligned} y_n^2 &= n^3 + An + B, \\ 2\text{ind } y_n &\equiv \text{ind } (n^3 + An + B) \pmod{p-1}. \end{aligned}$$

y_n is a quadratic residue if and only if ind y_n is even. Then 2ind y_n is divisible by 4, so ind $(n^3 + An + B)$ is divisible by 4. In this case we get

$$e_n = \begin{cases} +1 & \text{if } 4 \mid \text{ind } (n^3 + An + B), \\ -1 & \text{if ind } (n^3 + An + B) \equiv 2 \pmod 4. \end{cases}$$

Suppose that $p \mid n^3 + An + B$. Then P_n and Q_n are points on E_1 and E_2 and $y_n = 0$. Then $e_n = -1$.

Finally let $\left(\frac{n^3+An+B}{p}\right) = -1$. Then Q_n is a point on E_2 since

$$\begin{aligned} y_n^2 &= (nZ)^3 + AZ^2(nZ) + BZ^3, \\ y_n^2 &= Z^3(n^3 + An + B). \end{aligned} \tag{12}$$

Both Z^3 and $n^3 + An + B$ are quadratic non-residue thus (12) has a solution in $\mathbb{F}_p$. Then

$$2\text{ind } y_n \equiv 3\text{ind } Z + \text{ind } (n^3 + An + B).$$

y_n is a quadratic residue if and only if 3ind $Z +$ ind $(n^3 + An + B)$ is divisible by 4. Thus

$$e_n = \begin{cases} +1 & \text{if ind } (n^3 + An + B) \equiv \text{ind } Z \pmod 4, \\ -1 & \text{if ind } (n^3 + An + B) \equiv 4 - \text{ind } Z \pmod 4. \end{cases}$$

By choosing $m = 4$, $\mathcal{A} = \{\text{ind}^* Z, 4\}$ and $\mathcal{B} = \{2, 4 - \text{ind}^* Z\}$ we get

$$e_n = \begin{cases} +1 & \text{if } \text{ind}^*(n^3 + An + B) \in \mathcal{A}, \\ -1 & \text{if } \text{ind}^*(n^3 + An + B) \in \mathcal{B} \text{ or } p \mid n^3 + An + B. \end{cases}$$

Thus we may use Theorem 1. It easy to see that condition d) holds, thus we get (4) and (5), which was to be proved.

4 Proof of Corollary 2

Since p is a prime of form $4k + 3$, thus $(p + 1)/4$ is an integer. Consider the equation

$$y^2 \equiv a \pmod p \tag{13}$$

in $\mathbb{F}_p$. By the Tonelli-Shanks algorithm [15], [17] this congruence has two solutions, namely

$$y = \pm a^{(p+1)/4} = \pm a^{(3p-1)/2}.$$

For odd k let $\alpha = (p + 1)/4$, for even k let $\alpha = (3p - 1)/4$. Then α is even and $(\alpha, p - 1) = 2$. By the Tonelli-Shanks algorithm [15], [17]

$$y = a^\alpha$$

is a solution of (13) and since α is even, this y is a quadratic residue.

If $n^3 + An + B$ is a quadratic residue let

$$f(n) = n^3 + An + B.$$

Now consider the sequence $E_{p-1} = \{e_1, e_2, \dots, e_{p-1}\}$. By the definition of e_n

and the previous argument

$$e_n = \begin{cases} +1 & \text{if } \mathrm{ind}^*(f(n)^\alpha) \in \mathcal{A}, \\ -1 & \text{if } \mathrm{ind}^*(f(n)^\alpha) \in \mathcal{B} \text{ or } p \mid n^3 + An + B. \end{cases} \tag{14}$$

Similarly, if $n^3 + An + B$ is a quadratic non-residue let

$$f'(n) = -(n^3 + An + B).$$

(In this case by the definition of y_n we have $y_n^2 = (-n)^3 + A(-n) - B = -(n^3 + An + B)$.) Since α is even $f(n)^\alpha = (f'(n))^\alpha$ thus (14) always holds.

Define $r_s(a)$ by

$$r_s(a) \equiv a \pmod{s}, \quad 1 \le r_s(a) \le s.$$

If m is odd let

$$\mathcal{A}' = \{r_m(\alpha^{-1}a) : \ a \in \mathcal{A}\},$$
$$\mathcal{B}' = \{r_m(\alpha^{-1}b) : \ b \in \mathcal{B}\}.$$

If m is even

$$\mathcal{A}' = \{r_{m/2}\left(\left(\frac{\alpha}{2}\right)^{-1} \frac{a}{2}\right) : \ a \in \mathcal{A}\},$$
$$\mathcal{B}' = \{r_{m/2}\left(\left(\frac{\alpha}{2}\right)^{-1} \frac{b}{2}\right) : \ b \in \mathcal{B}\}.$$

Then

$$e_n = \begin{cases} +1 & \text{if } \mathrm{ind}^* f(n) \in \mathcal{A}', \\ -1 & \text{if } \mathrm{ind}^* f(n) \in \mathcal{B}' \text{ or } p \mid n^3 + An + B, \end{cases}$$

which is a special case of Construction 1. By using Theorem 1 d) we get the statement.

I would like to thank to Professor András Sárközy for the valuable discussions.

References

[1] R. Ahlswede, C. Mauduit, A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity, Part I, Part II.* General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 293-325.

[2] Z. Chen, *Elliptic curve analogue of Legendre sequences*, Monatsh. Math. 154 (2008), 1-10.

[3] Z. Chen, S. Li, G. Xiao, *Construction of Pseudo-random Binary Sequences from Elliptic Curves by Using Discrete Logarithm*, Lecture Notes in Computer Science 4086, Springer, Berlin, 2006, Sequences and Their Applications - SETA 2006, 285-294.

[4] Z. Chen, N. Zhang, G. Xiao, *Pseudo-Randomness of Discrete-Log Sequences from Elliptic Curves*, Lecture Notes in Computer Science 4990, Springer Berlin / Heidelberg 2008, Information Security and Cryptology, 231-245.

[5] Z. Chen, G. Xiao, *'Good' Pseudor-Random Binary Sequences from Elliptic Curves*, http://eprint.iacr.org/2007/275.pdf.

[6] L. Goubin, C. Mauduit, A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), 56-69.

[7] K. Gyarmati, *A note to the paper "On a fast version of a pseudorandom generator"*, Ann. Univ. Sci. Budapest. Eötvös, Sect. Math. 49 (2006), 87-93..

[8] K. Gyarmati,*On a family of pseudorandom binary sequences*, Period. Math. Hungar. 49 (2004), 45-63.

[9] K. Gyarmati, *On a fast version of a pseudorandom generator*, Lecture Notes in Computer Science 4123, General Theory of Information Transfer and Combinatorics, Springer Berlin / Heidelberg 2006, 326-342.

[10] K. Gyarmati, A. Sárközy, A. Pethő, *On linear recursion and pseudorandomness*, Acta Arith. 118 (2005), 359-374.

[11] Christian Mauduit, Joël Rivat, András Sárközy, *Construction of pseudorandom binary sequences using additive characters*. Monatsh. Math. 141 (2004), 197-208.

[12] C. Mauduit, A. Sárközy, *On finite pseudorandom binary sequence I: Measures of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (1997), 365-377.

[13] Joël Rivat, András Sárközy, *Modular construction of pseudorandom binary sequences with composite moduli*. Period. Math. Hungar. 51 (2005), 75-107.

[14] A. Sárközy, *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. 38 (2001), 377-384.

[15] D. Shanks, *Five Number Theoretic Algorithms*, Proc. of the Second Manitoba Conference on Numerical Mathematics (1973), 51-70.

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, 1986, expanded 2nd edition 2009.

[17] A. Tonelli, *Bemerkung über die Auflösung quadratischer Congruenzen*, Nachrichten von der Königl. Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen 1891, 344-346.

[18] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.

Katalin Gyarmati

Department of Algebra and Number Theory

Eötvös Loránd University

H-1117 Budapest, Pázmány Péter sétány 1/c

Hungary

email: gykati@cs.elte.hu