Sequences of PRN's from Algebraic Curves over the Ring $\mathbb{Z}_{p^m}$

Sergey Varbanets and Yakov Vorobyov

Abstract In this work there is considered the method of producing the sequences of pseudorandom numbers basing on solutions of congruences of two variables modulo the power of prime number. The estimates of discrepant function of constructed sequences of pseudorandom numbers have been obtained.

Keywords Pseudorandom numbers · Elliptic curve and Exponential sum · Discrepancy

1 Introduction

Following the revelation of public-key cryptography that arose at the last quarter of twentieth century, in 1985 Nil Koblitz and Victor Miller have found that the elements over the group of points from elliptic curve over finite field are able to store the secrete information due to of complexity on addition operation. And it would serve as motive to study the cryptography on elliptic curves. The sequences of pseudorandom number at every time was being intrinsic part of cryptography, and therefore for the last 20 years the theory of elliptic curves has application in problem of generating of sequences of pseudorandom numbers. The useful survey in this direction belongs to Shparlinskii [4].

In our paper we consider the algorithm of producing the sequences of pseudorandom numbers from algebraic curves over the ring $\mathbb{Z}_{p^m}$ of residue classes of prime power modulus. The according elements of such sequences accept the polynomial representation over $\mathbb{Z}_{p^m}$. We demonstrate this concept to construct the sequences of

S. Varbanets (✉)
Department of Computer Algebra and Discrete Mathematics, Odessa I.I. Mechnikov National University, Dvoryanskaya street 2, Odessa, Ukraine
e-mail: varb@sana.od.ua

Y. Vorobyov (✉)
Department of Mathematics, Informatics and Information Activities, Izmail State University of Humanities, Repina Street 12, Odessa, Ukraine
e-mail: yashavoro@gmail.com

C. H. Skiadas and Y. Dimotikalis (eds.), *14th Chaotic Modeling and Simulation International Conference*, Springer Proceedings in Complexity,
https://doi.org/10.1007/978-3-030-96964-6_35

pseudorandom numbers of algebraic curves

$$y^2 \equiv x^3 + ax + b \pmod{p^m}$$

and

$$ax^3 + y^3 \equiv 1 \pmod{p^m}.$$

The constructed sequences have the fixed period $\tau = p^{m-1}$ that can be grown as for the growth of prime number p or factor m.

Notations. The letter p denotes a prime number, $p \geq 3$. For $n \in \mathbb{N}$ the notations $\mathbb{Z}_{p^m}$(accordingly, $\mathbb{Z}^*_{p^m}$) denote the complete (accordingly, reduced) system of residues modulo p^m. We write (a, b) for notation a great common divisor of a and b. For $z \in \mathbb{Z}$, $(z, p) = 1$ let z' or z^{-1} be the multiplicative inverse of a modulo p^m. We write $\nu_p(A)$ if $p^{\nu_p(A)} | A$, $p^{\nu_p(A)+1} \nmid A$. Landau symbol "O" is equivalent to Vinogradov symbol "$\ll$". The notation $f(x) \ll g(x)$ means that for $x \to \infty$ the inequality $|f(x)| \leq C \cdot g(x)$ holds with arbitrary constant C. Through $[x]$ we will denote the integral part of real number x.

2 Auxiliary Results

Let $E(\mathbb{F}_p)$ be an elliptic curve defined over $\mathbb{F}_p$ given by an affine Weierstraβ equation of the form

$$Y^2 + (a_1X + a_3)Y = X^3 + a_2X^2 + a_4X + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_p$ such that the partial derivations $\frac{\partial F}{\partial X}$ and $\frac{\partial F}{\partial Y}$ for the function

$$F(X, Y) = Y^2 + (a_1X + a_3)Y - X^3 - a_2X^2 - a_4X - a_6$$

do not become zero simultaneously at the points of the curve $(x, y) \in E(\overline{\mathbb{F}}_p)$ over the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$.

For the case $p > 3$ the previous equation can be deduce to form

$$Y^2 = X^3 + ax + b \tag{1}$$

for some $a, b \in \mathbb{F}_p$ with $4a^3 + 27b^2 \neq 0$.

We recall that the set of points of curve $E(\mathbb{F}_p)$ together with point at infinity $\mathcal{O}$, relatively to a special operation $\oplus$, forms the abelian group E_p of order $\mathcal{N}(E_p)$ which satisfies inequality

$$\left|\mathcal{N}(E_p) - p - 1\right| \leq 2p^{\frac{1}{2}}.$$

For a point $Q \in E(\mathbb{F}_p)$ we use $x(Q)$, $y(Q)$ to denote its coordinates, that is, $(x(Q), y(Q))$.

For $m > 1$ we denote $E_p(m)$ as the set of solutions (x, y) satisfying to the congruence

$$y^2 \equiv x^3 + ax + b \pmod{p^m} \tag{2}$$

The set $E_p(m)$ we will call the elliptic curve over the ring $\mathbb{Z}_{p^m}$ and $\mathcal{N}(E_p(m))$ be a number of solutions of (2) with condition $(y, p) = 1$.

Lemma 1 *Let (x_0, y_0) be a solution of (2) with $(y_0, p) = 1$ and $m = 1$. Then for any integer t the congruence*

$$y^2(t) \equiv (x_0 + pt)^3 + a(x_0 + pt) + b \pmod{p^m} \tag{3}$$

has just two incongruent solutions modulo p^m for every positive m.

The assertion of this lemma follows from the fact that any solution (x_0, y_0) of congruence (3) with $m = 1$ we can grow to the solutions $y_1(t) = y(t), y_2(t) = -y(t)$.

Denote by $y_i(t)$, $i = 1, 2$ the solution of congruence (3).

Lemma 2 *Let $p > 2$ be a prime, $m \geq 3$ be an integer, $s = \left[\frac{p-1}{p-2}m\right]$. There exist the polynomial $\varphi(t) \in \mathbb{Z}_{p^m}[t]$ of degree s*

$$\varphi(t) = \phi_0(x_0) + p^{\lambda_1}\phi_1(x_0)t + \cdots + p^{\lambda_s}\phi_s(x_0) \cdot t^s,$$

where $(\phi_i(x_0), p) = 1$, $i = 0, 1, \ldots, s$, and $\lambda_1, \lambda_2, \ldots, \lambda_s \in \mathbb{N}$, moreover

$$\lambda_j \geq j\frac{p-2}{p-1}, \quad j = 1, \ldots, s.$$

such that

$$y_i(t) = y_i(0)\varphi(t) \pmod{p^m}, \quad i = 1, 2,$$

and the points $(x_0 + pt, y_i(t))$, $i = 1, 2$, belong to the elliptic curves (2).

Proof Let (x_0, y_0) is the solution of (2) for $m = 1$, $(y_0, p) = 1$. For every $t, 0 \leq t \leq p^{m-1} - 1$, we denote $y_1(t), y_2(t)$ as two different solutions of the congruence

$$y^2(t) \equiv (x_0 + pt)^3 + a(x_0 + pt) + b \pmod{p^m}.$$

Denote by x_0' the multiplicative inverse of $x_0^3 + ax_0 + b$, i.e.

$$x_0'(x_0^3 + ax_0 + b) \equiv 1 \pmod{p^m}.$$

Such solution exists since $(y_0, p) = 1$.
Hence, we find that (3) is equivalent to

$$y^2(t) \equiv (x_0^3 + ax_0 + b)(1 + (3ptx_0^2 + 3p^2t^2x_0 + p^3t^3)x_0').$$

Let $U^2(\omega) = (1 + (3\omega x_0^2 + 3\omega^2 x_0 + \omega^3)x_0')$.
Expanding the function $U(\omega)$ to series in powers of ω

$$U(\omega) = \sum_{i=0}^{\infty} X_i(x_0, x_0')\omega^i$$

and its logarithmic derivation

$$\frac{d\log U(\omega)}{d\omega} = \frac{U'(\omega)}{U(\omega)} = \frac{\sum_{i=1}^{\infty} i X_i(x_0, x_0')\omega^{i-1}}{\sum_{i=0}^{\infty} X_i(x_0, x_0')\omega^i}$$

gives the following recursion formulas for $j = 2, 3, \ldots$:

$$\begin{aligned} X_{j+1} = & -\frac{2j+1}{2(j+1)}(3x_0^2x_0' + ax_0)X_j \\ & -\frac{3(j-2)}{j+1}x_0x_0'X_{j-1} \\ & -\frac{2j-7}{2(j+1)}x_0'X_{j-2}, \end{aligned} \tag{4}$$

$$X_0 = 1,$$

$$X_1 = \frac{1}{2}(3x_0^2x_0' + ax_0),$$

$$X_2 = \frac{1}{2}3x_0x_0' - \frac{1}{8}(3x_0^2x_0' + ax_0')^2.$$

Let show that the formal p-adic series for $U(pt)$ converges in p-adic metric and modulo p^m the congruence

$$U(pt) \equiv \varphi(t) \pmod{p^m},$$

where

$$\varphi(t) = \phi_0(x_0) + p^{\lambda_1}\phi_1(x_0)t + \cdots + p^{\lambda_s}\phi_s(x_0)\cdot t^s, \tag{5}$$

and $\varphi_j(x_0) \in \mathbb{Z}$, $\lambda_j \in \mathbb{N}$ and $\lambda_j \geq m$ for $j > s$. holds.

In our reasoning we will use p-adic analysis by schema of Postnikova [3].

Let us introduce the variables Y_j, Z_j, $j = 1, 2, \ldots, s$ defined by the conditions

$$Y_1 = 0,\ \ Y_2 = 1,\ \ Y_3 = \frac{1}{2}(3x_0^2 x_0' + a x_0'),$$
$$Z_1 = 0,\ \ Z_2 = 0,\ \ Z_3 = 1$$

and for $j \geq 4$ Y_j, Z_j be determined by recursion formulas of type (4).

Let us consider determinants

$$\Delta_j = \begin{vmatrix} X_{j-2} & X_{j-1} & X_j \\ Y_{j-2} & Y_{j-1} & Y_j \\ Z_{j-2} & Z_{j-1} & Z_j \end{vmatrix}, \quad j = 3, 4, \ldots, s.$$

In particular, we have modulo p^m

$$\Delta_3 = \frac{1}{2}(3x_0 x_0' + a x_0').$$

From this moment on, we suppose that $-3a$ is the non-quadratic residue modulo p. Therefore, we have

$$(x_0', p) = 1,\ \ (3x_0^2 + a, p) = 1.$$

(since otherwise the congruence $x^2 \equiv -3a \pmod{p}$ has the solution).

But then $\nu_p(\Delta_3) = 0$.

Also for $j \geq 4$ we easily obtain

$$\begin{aligned} \Delta_j &= -\frac{2j-9}{2j} x_0' \Delta_{j-1} \\ &\cdots = (-x_0')^{j-s} \frac{(2j-9)(2j-11)\cdots 3 \cdot 1 \cdot (-1)}{2^{j-s} j(j-1)\cdots 4} \Delta_3 \\ &= (-x_0')^{j-3} \frac{(2j-9)! \cdot 6}{2^{2j-7} j!(j-4)!} \Delta_3. \end{aligned}$$

Let $\nu_p(X_j p^j) = \lambda_j$, $\nu_p(Y_j p^j) = \mu_j$, $\nu_p(Z_j p^j) = \tau_j$.

Now let take out a common factor $p^{\min(\lambda_{j-1}, \lambda_j, \lambda_{j-2})}$ from the first row of determinant Δ_j. From the second and third rows let do the same with $p^{\min(\mu_{j-1}, \mu_j, \mu_{j-2})}$ and $p^{\min(\tau_{j-1}, \tau_j, \tau_{j-2})}$, respectively.

It easy prove that

$$\lambda_j \geq j\frac{p-2}{p-1}, \quad \mu_j \geq j\frac{p-2}{p-1}, \quad \tau_j \geq j\frac{p-2}{p-1}.$$

Now, taking into account the relation between Δ_j and Δ_3 we easily find

$$\min(\lambda_j, \lambda_{j-1}, \lambda_{j-2}) \le 3j - 3 - 2(j-2)\tfrac{p-2}{p-1} + \sum_{k=1}^{\infty}\left[\tfrac{2j-9}{p^k}\right] - \sum_{k=1}^{\infty}\left[\tfrac{j}{p^k}\right] - \sum_{k=1}^{\infty}\left[\tfrac{j-4}{p^k}\right].$$

Also take into account that $[2x] \le 2[x] + 1$ for $x \ge 0$, and the quantity of nonzero summand in sum $\sum_{k=1}^{\infty}\left[\frac{2j-9}{p^k}\right]$ be at most $\frac{2j-9}{p} < \frac{2j}{p-1}$.

Then we have

$$\min(\lambda_j, \lambda_{j-1}, \lambda_{j-2}) \le j + 1 + \frac{4(j-1)}{p-1}.$$

Bringing up the definition for $\varphi(t)$ (5) we at once obtain the proof of Lemma 2. □

Corollary 1 *In the conditions of Lemma 2 we obtain p-adic description of the solutions of the congruence*

$$y^2 \equiv x^3 + ax + b \pmod{p^m}$$

in the form

$$x = x_0 + pt, \quad y_i(t) = y_i(0)(1 + A_1 pt + A_2 p^2 t^2 + A_3 p^{\lambda_3} t^3 + \cdots) \ (\pmod{p^m}),$$

where

$$\lambda_1 = 1, \ \lambda_2 = 2, \ \lambda_3 \ge 3, \ j = 3, 4, \ldots;$$
$$A_0 = 1, \ A_1 = 2^{-1}(3x_0^2 x_0' + a x_0'), \ A_2 = 3 \cdot 2^{-1} x_0 x_0' - 2^{-3}(3x_0^2 x_0' + a x_0')^2;$$
$$(A_i, p) = 1, \ i = 1, 2, 3, \ldots.$$

(here 2^{-1} be the multiplicative inverse for 2 modulo p^m).

Corollary 2 *For the fixed $x_0, y_0 \in E_p$ and $y_i(0)$, $i = 1, 2$ we have*

$$y_i(t_1) \equiv y_i(t_2) \pmod{p^m}$$

if and only if $t_1 \equiv t_2 \pmod{p^{m-1}}$. And hence, the sequences $y_i(t)$, $t = 0, 1, \ldots, p^{m-1} - 1$ have the least period $\tau = p^{m-1}$ (here $i = 1$ or 2, $y_2(t) = -y_1(t)$). Thus we obtain the family of different sequences $\{y(t)\}$, which define by selection of initial point (x_0, y_0) on the curve E_p and by selection of index $i \in \{1, 2\}$.

Bellow we will show that the sequence of real numbers $\{\frac{y(t)}{p^m}\}$, $t = 0, 1, \ldots, p^{m-1} - 1$ be the sequence of real numbers from $[0, 1)$ that may be considered as the sequence of pseudorandom numbers passes the serial test on pseudorandomness.

Note that the same point (x_0, y_0) of elliptic curve E_p generate two sequences $y_i(t)$ defined by Lemma 2, the selection of which defines by the values of $y_i(0)$ as the solution of congruence

$$y^2 \equiv x^3 + ax + b \pmod{p^m}.$$

If $0 < y(0) < \frac{p}{2}$ then $y_i(t)$ denotes by $y_1(t)$, otherwise we have $y_2(t)$.

Over constructed set of sequences $\{y(t)\}$ we can define operation "*" by the following way:

$$y'(t) * y''(t) = y'''(t),$$

where $y'''(t)$ defines by sum of two points (x_0', y_0') and (x_0'', y_0'') of elliptic curve E_p

$$(x_0', y_0') \oplus (x_0'', y_0'')$$

and by Lemma 2, where $0 < y'''(0) < \frac{p}{2}$ if $y'(0)$ and $y''(0)$ simultaneously belong to $\left[0, \frac{p}{2}\right]$ or $\left[\frac{p}{2}, p\right]$. Otherwise, $y'''(0)$ is selected from interval $\left[\frac{p}{2}, p\right]$.

Similarly, we can construct the sequence $\{y(t)\}$ same to the sequence from Lemma 2 produced by the congruence

$$y^\ell \equiv f(x) \pmod{p^m},$$

where $f(x)$ be the polynomial with integer coefficients of degree ≥ 3.

In particular, let see the congruence

$$ax^3 + y^3 \equiv 1 \pmod{p^m}. \tag{6}$$

We will assume that p be the prime number of form $6k - 1$.

Define by $y(t)$ the solution of congruence

$$y^3 \equiv 1 - a(x_0 + pt)^3 \pmod{p^m}. \tag{7}$$

where (x_0, y_0) be the anyone solution of congruence

$$y^3 \equiv 1 - ax^3 \pmod{p}.$$

with $1 - ax_0^3 \not\equiv 0 \pmod{p}$. Every of such x_0 uniquely define the respective y_0. So, the solution $y(t)$ of congruence (7) defines uniquely.

Lemma 3 *Let* $s = \left[\frac{p-1}{p-2}m\right]$. *There exists the polynomial of degree* s

$$\varphi(t) = \Phi_0(x_0) + p^{\lambda_1}\Phi_1(x_0)t + \cdots + p^{\lambda_s}\Phi_s(x_0)t^s,$$

where $(\Phi_i(x_0), p) = 1$, $i = 0, 1, \ldots, s$; $\lambda_1, \ldots, \lambda_s$ *are the natural numbers satisfy the inequalities* $\lambda_j \geq j\frac{p-2}{p-1}$, *such that*

$$y(t) \equiv y(0)\varphi(t) \pmod{p^m}.$$

The proof of this lemma passes simultaneously to proof of Lemma 2 and the respective coefficients $\Phi_j(x_0)$ define by recurrent relation

$$\Phi_{j+1} = \frac{3j-1}{j+1} a x_0^2 x_0' \Phi_j + \frac{3j-5}{j+1} a x_0 x_0' \Phi_{j-1} + \frac{j-3}{j+1} a x_0' \Phi_{j-2},$$

moreover,

$$\Phi_0 = 1, \ \Phi_1 = -a x_0^2 x_0', \ \Phi_2 = -a x_0 x_0' - a^2 x_0^4 x_0'^2.$$

Here, x_0' is the multiplicative inverse modulo p^m for $1 - a x_0^3$.

3 Discrepancy

Let $\{x_n\}$ be the sequence of points from $[0, 1)$. As characteristic property of equidistribution of such sequences the following discrepant function D_N is used

$$D_N(x_0, x_2, \dots, x_{N-1}) = D_N := \sup_{\Delta \subset [0,1)} \left| \frac{A_N(\Delta)}{N} - |\Delta| \right|,$$

where $A_N(\Delta)$ is the number of points among $x_0, x_2, \dots, x_{N-1}$ falling into Δ, and $|\Delta|$ denotes the length of Δ.

In the same way there is defined the discrepancy for the sequence of s-dimensional points $X_n \subset [0, 1)^s$.

From definition of equidistribution of sequences of s-dimensional points we can conclude that for $D_N^{(s)} \to 0$ with $N \to \infty$ we can obtain better uniformly distributed sequences $\{X_n^{(s)}\}$.

Every sequence $\{x_n\}$, $x_n \in [0, 1)$ defines the sequence of s-dimensional points $X_n^{(s)}$, where $X_n^{(s)} = (x_n, x_{n+1}, \dots, x_{n+s-1})$.

It is clear that for every equidistributed sequence $\{x_n\}$, which elements are statistically independent (unpredictable) for every integer $s \in \mathbb{N}$, the according sequence $\{X_n^{(s)}\} = \{x_n, x_{n+1}, \dots, x_{n+s-1}\}$ be the equidistributed sequence.

We say that the sequence $\{x_n\}$, $x_n \in [0, 1)$ passes s-dimensional test on pseudorandomness if every sequence $\{X_n^{(s)}\}$, $s = 1, 2, \dots, s$ be the equidistributed on s-dimensional unit interval $[0, 1)^s$.

To estimate the s-dimensional discrepant function of sequence $\{X_n^{(s)}\}$ the following lemmas is used.

For integers $s \geq 1$ and $q \geq 2$, let $C_s(q)$ be the set of all nonzero lattice points $\mathbf{h} = (h_1, \dots, h_s) \in \mathbb{Z}^s$ with $-\frac{q}{2} < h_j \leq \frac{q}{2}$ for $1 \leq j \leq s$. Define for $\mathbf{h} \in C_s(q)$

$$r(h,q) = \begin{cases} 1 & if\ \ h = 0, \\ q \sin(\pi \frac{|h|}{q}) & if\ \ h \neq 0, \end{cases}$$
$$r(\mathbf{h},q) = \prod_{j=1}^{s} r(h_j,q) \tag{8}$$

Lemma 4 *Let $N \geq 1$ and $q \geq 2$ be integers. Suppose that $\mathbf{y_0}, \mathbf{y_1}, \ldots, \mathbf{y_{N-1}} \in \mathbb{Z}_q^s$. Then the discrepancy of the points $\mathbf{t_k} = \frac{\mathbf{y_k}}{q} \in [0,1)^s$, $k = 0, 1, \ldots, N-1$, satisfies*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}}) \leq \frac{s}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(q)} \frac{1}{r(\mathbf{h},q)} \left| \sum_{k=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_k}) \right| \tag{9}$$

(Proof of this lemma see in [1],[2]).

From the last statement it follows the classical statement of Turan-Erdös-Koksma inequality.

Lemma 5 *Let $T \geq N \geq 1$ and $q \geq 2$ be integers, $\mathbf{y_k} \in \{0, 1, \ldots, q-1\}^s$ for $k = 0, 1, \ldots, N-1$; $\mathbf{t_k} = \frac{\mathbf{y_k}}{q} \in [0,1)^s$. Then*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}}) \leq \frac{s}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(q)} \sum_{h_0 \in \left(-\frac{T}{2}, \frac{T}{2}\right]} \frac{1}{r(\mathbf{h},q) r(h_0,T)} \times \left| \sum_{k=0}^{T} e(\mathbf{h} \cdot \mathbf{t_k} + \frac{k h_0}{T}) \right| \tag{10}$$

This assertion follows from Lemma 4 and from an estimate of incomplete exponential sum through complete exponential sum.

Lemma 6 (Niederreiter, [1]). *Let $q \geq 2$, $T > 1$ be integers. Then*

$$\sum_{\substack{\mathbf{h} \in C_s(q) \\ \mathbf{h} \equiv 0 (\pmod{v})}} r(\mathbf{h},q) < \frac{1}{v} \left(\frac{2}{\pi} \log q + \frac{7}{5} \right)^s$$

for any divisor v of q with $1 \leq v < q$, and

$$\sum_{h_0 \in \left(-\frac{T}{2}, \frac{T}{2}\right]} \frac{1}{r(h_0,T)} \leq \frac{2}{\pi} \log T + \frac{7}{5} \tag{11}$$

Lemma 7 *The discrepancy of N arbitrary points $\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}} \in [0,1)^2$ satisfies*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}}) \geq \frac{1}{2(\pi+2)|h_1 h_2|N} \left| \sum_{k=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_k}) \right| \tag{12}$$

for any lattice point $\boldsymbol{h} = (h_1, h_2) \in \mathbb{Z}^2$ *with* $h_1 h_2 \neq 0$.

(It is the special version of Niederreiter result in [1]).

From these lemmas we can to see that the character of equidistribution of sequence $\{x_n\}$, $x_n \in [0, 1)$ completely defines by estimate of exponential sum

$$S_N := \sum_{n=1}^{N} e^{2\pi i h x_n}, \ h \in \mathbb{N}.$$

In Sect. 2 we constructed two sequences $\{x_t\}$, $x_t = \frac{y(t)}{p^m}$ that were being produced by the algebraic curves over the ring $\mathbb{Z}_{p^m}$ defined by the congruences (2) and (6). From Lemmas 2 and 3 it is clear to see that $y(t)$ are defining by special polynomials from the ring $\mathbb{Z}_{p^m}[t]$. These polynomials have the form

$$y(t) = A_0 + A_1 pt + A_2 p^2 t^2 + A_3 p^{\lambda_3} t^3 + \cdots,$$

moreover, $\lambda_j \geq 3$, $(A_j, p) = 1$ for $j \geq 3$.

The according sums S_N can be estimated by use of the generalized Gauss sums and the last can be estimated using the following lemma.

Lemma 8 (see, [5], Lemma 3). *Let* $p > 2$ *be a prime number,* $m \geq 2$ *be a positive integer,* $m_0 = \left[\frac{m}{2}\right]$, $f(x)$, $g(x)$, $h(x)$ *be polynomials over* $\mathbb{Z}$

$$\begin{aligned} f(x) &= A_1 x + A_2 x^2 + \cdots, \\ g(x) &= B_1 x + B_2 x^2 + \cdots, \\ h(x) &= C_\ell x + C_{\ell+1} x^{\ell+1} + \cdots, \ \ell \geq 1, \end{aligned}$$

$$\nu_p(A_j) = \lambda_j, \quad \nu_p(B_j) = \mu_j, \quad \nu_p(C_j) = \nu_j,$$

and, moreover,

$$\begin{aligned} &k = \lambda_2 < \lambda_3 \leq \cdots, \quad 0 = \mu_1 < \mu_2 < \mu_3 \leq \cdots, \\ &\nu_p(C_\ell) = 0, \ \nu_p(C_j) > 0, \ j \geq \ell + 1. \end{aligned}$$

Then the following bounds occur

$$\left|\sum_{x\in\mathbb{Z}_{p^m}} e_m(f(x))\right| \le \begin{cases} 2p^{\frac{m+k}{2}} & if\ \nu_p(A_1)\ge k, \\ 0 & if\ \nu_p(A_1)<k; \end{cases}$$

$$\left|\sum_{x\in\mathbb{Z}^*_{p^m}} e_m(f(x)+g(x^{-1}))\right| \le I(p^{m-m_0})p^{\frac{m}{2}}$$

$$\left|\sum_{x\in\mathbb{Z}^*_{p^m}} e_m(h(x))\right| \le \begin{cases} 1\ if\ \ell=1, \\ 0\ if\ \ell>1, \end{cases}$$

where $I(p^{m-m_0})$ *is a number of solutions of the congruence*

$$y\cdot f'(y)\equiv g'(y^{-1})\cdot y^{-1} \pmod{p^{m-m_0}},\ y\in\mathbb{Z}^*_{p^{m-m_0}}.$$

This lemma is the estimation of complete generalized Gauss sum. The incomplete generalized Gauss sum

$$\sum_{t=1}^{N} e^{2\pi i\frac{f(t)}{p^m}},\ \ 1\le N\le p^m$$

we can estimate by using the inequality

$$\left|\sum_{t=1}^{N} e^{2\pi i\frac{f(t)}{p^m}}\right| \le \sum_{k=1}^{p^m}\frac{1}{\max(k,\,p^m-k)}\left|\sum_{t=1}^{p^m} e^{2\pi i\frac{f(t)+kt}{p^m}}\right| =$$

$$= \max_{1\le k\le p^m}\left|\sum_{t=1}^{p^m} e^{2\pi i\frac{f(t)+kt}{p^m}}\right|\log p^m \ll p^{\frac{m}{2}}\log p^m.$$

Now we can obtain the estimate of discrepancy for sequences generated in Lemmas 2 and 3.

Indeed, the function $y(t)$ for the sequence generated by elliptic curve (2) as the function $y(t)$ for the sequence generated by (6) both satisfy for all conditions of Lemma 8 and so the sum $\sum_{t=1}^{p^m} e^{2\pi i\frac{y(t)}{p^m}}$ can be estimated as $O(p^{\frac{m+1}{2}}\log p^m)$. And now using Lemmas 4 and 5 we obtain the estimate of discrepancy for the sequence $\{x_t\}$, where $x_t=\frac{y(t)}{p^m}$, $t=1,2,\ldots,N$, $N\le p^{m-1}$

$$D_N^{(1)} \le \frac{3p^{\frac{m+1}{2}}}{N}\log N$$

This proves the equidistribution of the sequence $\{x_t\}$. Moreover, $h_1y(t) + h_2y(t+1) + \cdots + h_sy(t+s-1)$ be the polynomial which for the nontrivial set of coefficients $h_1, \ldots, h_s$ generates the polynomial $Y(t)$ that satisfies to condition of Lemma 8 and so the discrepancy of s-dimensional sequence $\{X_n^{(s)}\}$ has an estimate

$$\frac{s}{N} + \frac{p^{\frac{m+1}{2}}}{N}(3\log N)^s.$$

Therefore, the sequences produced by congruences (2) and (6) pass serial test for $s \le p-2$.

To obtain the lower bounds for discrepancy of sequences generated from elliptic curve we apply Lemma 7.

From Corollary 1 we can write

$$y(t) = y(0)(1 + A_1pt + A_2p^2t^2 + A_3p^{\lambda_3}t^3 + \cdots) \pmod{p^m}$$

Therefore, we have

$$\begin{aligned} y(t+k) = y(0)&(1 + A_1p + 2A_2p^2 + 3A_3p^{\lambda_3} + \cdots)t \\ &+ (A_2t^2 + 3A_3p^{\lambda_3} + \cdots)t^2 \\ &+ (A_3p^{\lambda_3} + 2p^{\lambda_4}A_4 + \cdots)t^3 + \cdots \end{aligned}$$

And hence,

$$\begin{aligned} h_1y(t) + h_2y(t+1) = &\textit{free term} + (A_1h_1 + A_1h_2 + 2A_2h_2p)pt \\ &+ (A_2h_1 + A_2h_2 + 3A_3h_2p)p^2t^2 \\ &+ p^{\lambda_3}t^3\psi(t) \end{aligned}$$

where $\psi(t)$ is a polynomial with coefficients from $\mathbb{Z}_{p^m}$.

By form of coefficients for A_1 and A_2 it is clear that we can find x_0 such that the coefficient at t in the last equality is divided at least by p^2 but the coefficient at t^2 exactly divided by p^2. Let define this conditions as (*).

Now Lemma 8 gives

$$\left|\sum_{t=0}^{p^{m-1}-1} e^{2\pi i\frac{h_1y(t)+h_2y(t+1)}{p^{m-1}}}\right| = \begin{cases} p^{\frac{m+v}{2}} & if \text{ conditions (*) hold,} \\ 0 & otherwise. \end{cases}$$

Theorem 1 *Let $\{x_t\}$ be the sequence of PRN's produced by elliptic curve $y^2 \equiv x^3 + ax + b \pmod{p^m}$. There exists the point (x_0, y_0), $y_0 \ne 0, \infty$ on the curve $y^2 \equiv x^3 + ax + b \pmod{p}$ such that the sequence of two-dimensional points $\{X_t\}$, $X_t = (x_t, x_{t+1})$ has discrepancy $D_\tau^{(2)}$, $\tau = p^{m-1}$ for which the following inequalities*

$$\frac{1}{4(\pi+2)h^*}p^{-\frac{m-1}{2}} \le D_\tau^{(2)} \le 3p^{-\frac{m-1}{2}}\log^2 p^m,$$

hold, where $h^* = \min(h_1, h_2)$, (h_1, h_2) *is a point from* $(\mathbb{Z}^*_{p^{m-1}})^2$ *with conditions (*).*

This theorem together with Lemma 8 shows that the obtained upper bound is, in general, the best possible up to the logarithmic factor for any inversive congruential sequence $\{(x_t, x_{t+1})\}$, $t \ge 0$ (defined by the congruence (2)).

Hence, on the average, the discrepancy $D_\tau^{(2)}$ has an order of magnitude between $p^{-(\frac{m-1}{2}-\nu)}$ and $p^{-(\frac{m-1}{2}-\nu)}\log^2 p^m$. In the certain sense, inversive congruential pseudorandom numbers model the random numbers very closely.

4 Conclusion

In conclusion let introduce the step by step algorithm of constructing the sequences of PRN's with a period $\tau = p^{m-1}$, associated with elliptic curve over finite ring $\mathbb{Z}_{p^m}$, $p > 3$ be a prime, $m \ge 3 \in \mathbb{N}$, that can be described by the following way.

First of all for $(x_0, y_0) \in E_p$, $(y_0, p) = 1$, i.e. for the point of elliptic curve $y^2 \equiv x^3 + ax + b \pmod p$ over $\mathbb{Z}_p$ with non-quadratic residue $-3a$ we construct the points $(x(t), y(t))$, $0 \le t \le p^{m-1} - 1$ which belongs to elliptic curve over $\mathbb{Z}_{p^m}$. Then

(1) we select (x_0, y_0), where $y_0 \ne 0$ and $y_0 \ne \infty$;
(2) calculate $x(t) \equiv x_0 + pt \pmod{p^m}$;
(3) calculate $y_i(0)$, $i = 1, 2$ as the solutions of congruence

$$y^2 \equiv x_0^3 + ax_0 + b \pmod{p^m};$$

(4) we will use the Taylor series for the function of ω at the point $\omega = 0$ in form

$$\sqrt{1 + (3\omega x_0^2 + 3\omega^2 x_0 + \omega^3)x_0'} = X_0 + X_1\omega + X_2\omega^2 + \cdots. \qquad (13)$$

(here x_0' is the multiplicative inverse modulo p^m for $x_0^3 + ax_0^2 + b$).
(5) In (13) we put $\omega = pt$ and then modulo p^m we construct the following polynomial:

$$\begin{aligned}\varphi(t) &\equiv 1 + X_1 pt + X_2 p^2 t^2 + \cdots + X_s p^s t^s \\ &\equiv \Phi_0(x_0) + p^{\lambda_1}\Phi_1(x_0)t + \cdots + p^{\lambda_s}\Phi_s(x_0)t^s \pmod{p^m},\end{aligned}$$

where $\Phi_j(x_0) \in \mathbb{Z}$, $(\Phi_j(x_0), p) = 1$, $\lambda_j \in \mathbb{N}$, $\lambda_j \ge j\frac{p-2}{p-1}$, $j = 1, 2, \ldots, s$.
(6) This polynomials and the solutions $y_i(0)$, $i = 0, 1$ we use to construct the following representations modulo p^m:

$$y_i(t) \equiv y_i(0)(\Phi_0(x_0) + \Phi_1(x_0)p^{\lambda_1 t} + \cdots + \Phi_s(x_0)p^{\lambda_s t^s})$$

$$\equiv y_i(0)(1 + A_1 pt + A_2 p^2 t^2 + A_3 p^{\lambda_3} t^3 + \cdots + A_s p^{\lambda_s} t^s)$$

for each $i = 1, 2$, which produce two sequences of PRN's

$$\left\{ \frac{y_i(t)}{p^m} \right\}, \ t = 0, 1, \ldots$$

with the period $\tau = p^{m-1}$.

Using the results obtained in previous sections we can say that the constructed sequence of PRN's, associated with elliptic curve $y^2 \equiv x^3 + ax + b \pmod{p^m}$, passes the serial test on pseudorandomness, and therefore may be used in cryptographic applications.

References

1. H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods* (SIAM, Philadelphia, 1992)
2. H. Niederreiter, Quasi-Monte Carlo methods and pseudorandom numbers. Bull. Amer. Math. Soc. **84**, 957–1041 (1978)
3. L.P. Postnikova, Distribution of solutions of the congruence $x^2 + y^2 \equiv 1 \ (mod \ p^n)$. Matem. sb. **65**(2), 228–238 (1964) (in Russian)
4. I. Shparlinski, Pseudorandom number generators from elliptic curves. Contemp. Math. **477**, 121–141 (2009)
5. S. Varbanets, Exponential sums over the sequences of PRN's produced by inversive generators. Annales Univ. Sci. Budapest. Sect. Comp. **48**, 225–232 (2018)