Числа Фибоначчи для оценки базисов рекуррентных последовательностей.

Ф.М. Малышев

2026

$$\{x_i\}, \quad i \in \mathbb{Z}, \quad x_i \in X$$

$$x_{i+m} = f\left(x_i, x_{i+k_1}, \ldots, x_{i+k_s}\right) \tag{1}$$

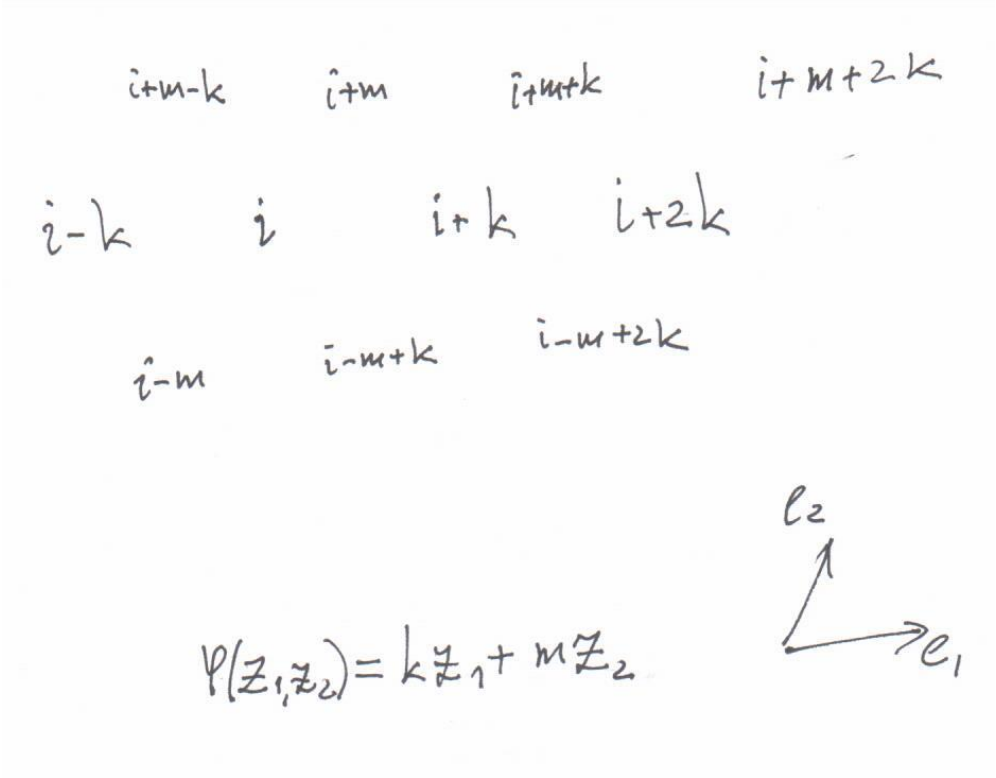
$$0 = k_0 < k_1 < \ldots < k_s < k_{s+1} = m,$$

$$\text{НОД}(k_1, \ldots, k_s, m) = 1,$$

$$s \geqslant 1,$$

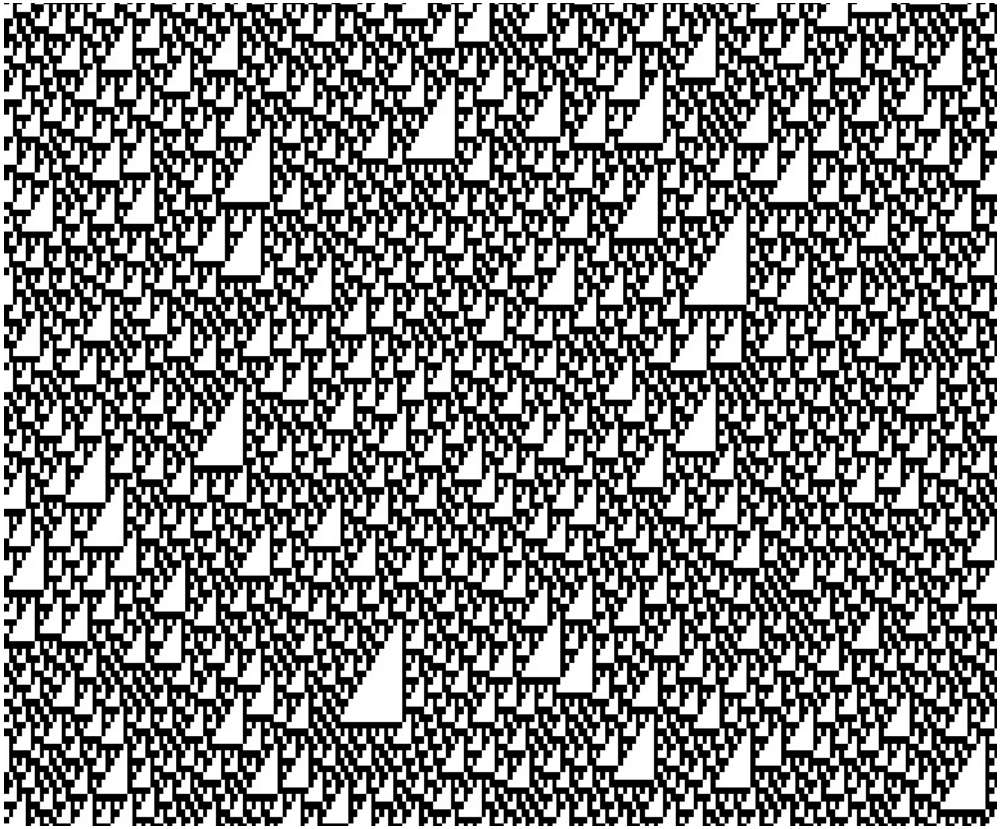
$$s = 1, \quad X = GF(2)$$

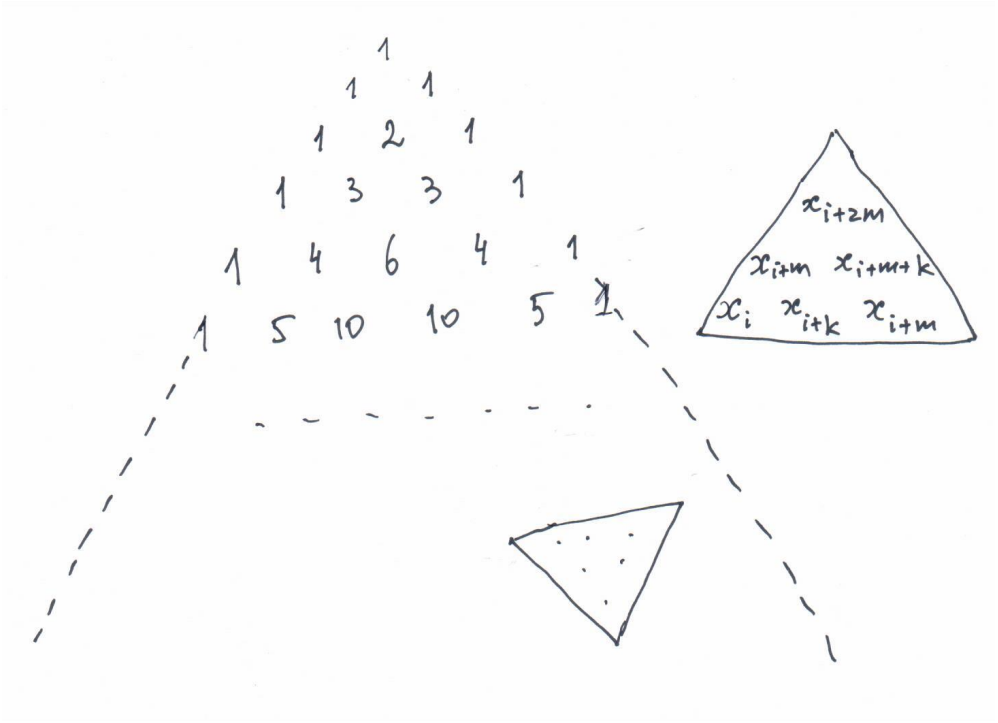
$$x_{i+m} = x_i + x_{i+k}$$



$$\varphi\colon \mathbb{Z}^2 \to \mathbb{Z}, \quad (z_1, z_2) \mapsto kz_1 + mz_2, \quad (k, m) = 1$$

$$\mathbb{Z} \cong \mathbb{Z}^2 / \ker \varphi \subset \mathbb{R}^2 / \ker \varphi$$




1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
x_{i+2m}
x_{i+m} x_{i+m+k}
x_i x_{i+k} x_{i+m}


n

Δ_n – булев треугольник Паскаля, ξ – число единиц в нём

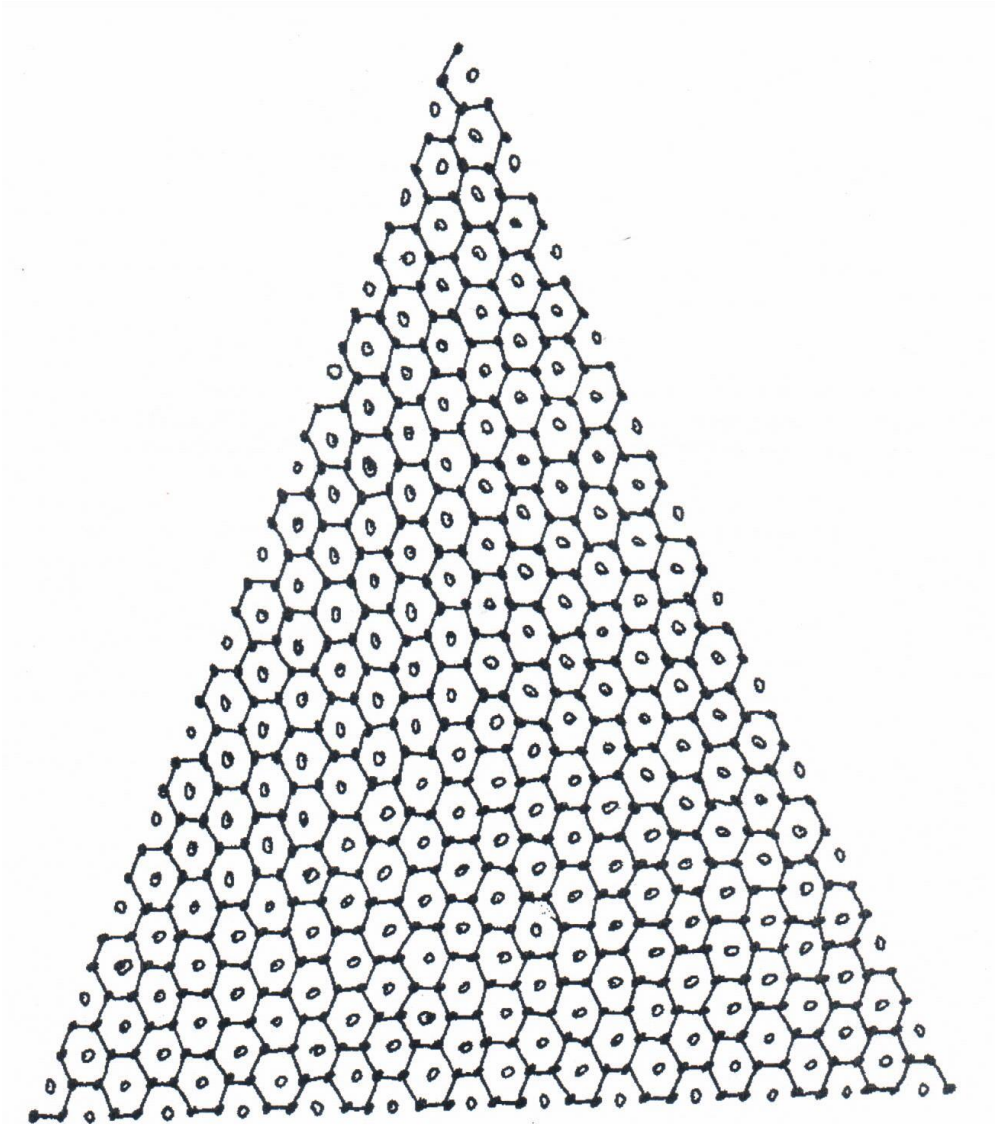
$$\text{Th. } \xi \in (\chi_i n - \delta_i, \chi_i n + \delta_i)$$

$$0 = \chi_0 < 1 = \chi_1 < \chi_2 < \chi_3 < \ldots.$$

$$\chi_0 = 0,\ \chi_1 = 1,\ \chi_2 = 1\frac{1}{2},\ \chi_3 = 2,\ \chi_4 = 2\frac{1}{4},\ \chi_5 = 2\frac{1}{2},\ \chi_6 = 2\frac{3}{4},\ \chi_7 = 3,$$
$$\chi_8 = 3\frac{1}{4},\ \chi_9 = 3\frac{3}{8},\ \chi_{10} = 3\frac{1}{2},\ \chi_{11} = 3\frac{3}{4},\ \chi_{12} = 3\frac{7}{8},\ \chi_{13} = 4,\ \ldots.$$

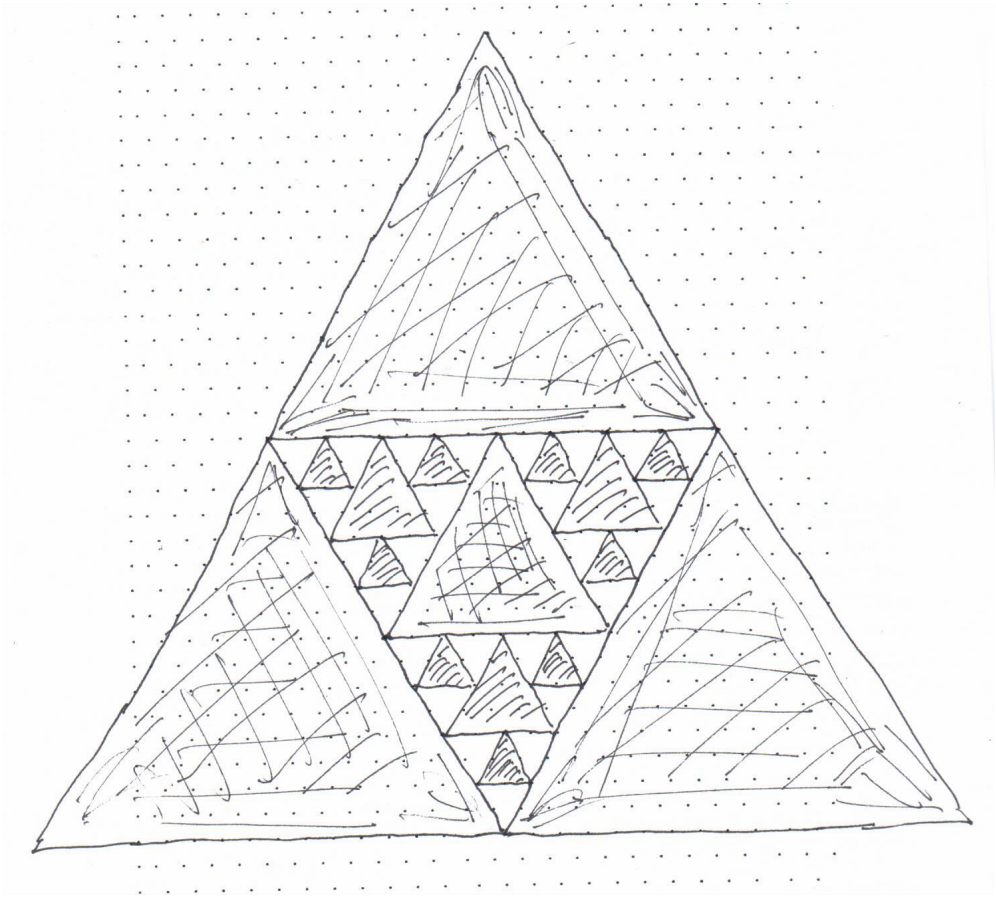
$$N_0 = 1, N_1 = 3, N_2 = 6, N_3 = 15, N_4 = N_5 = 12, N_6 = 36, N_7 = 61,$$
$$N_8 = 72, N_9 = 24, N_{10} = 78, N_{11} = 192, N_{12} = 48, N_{13} = 192.$$

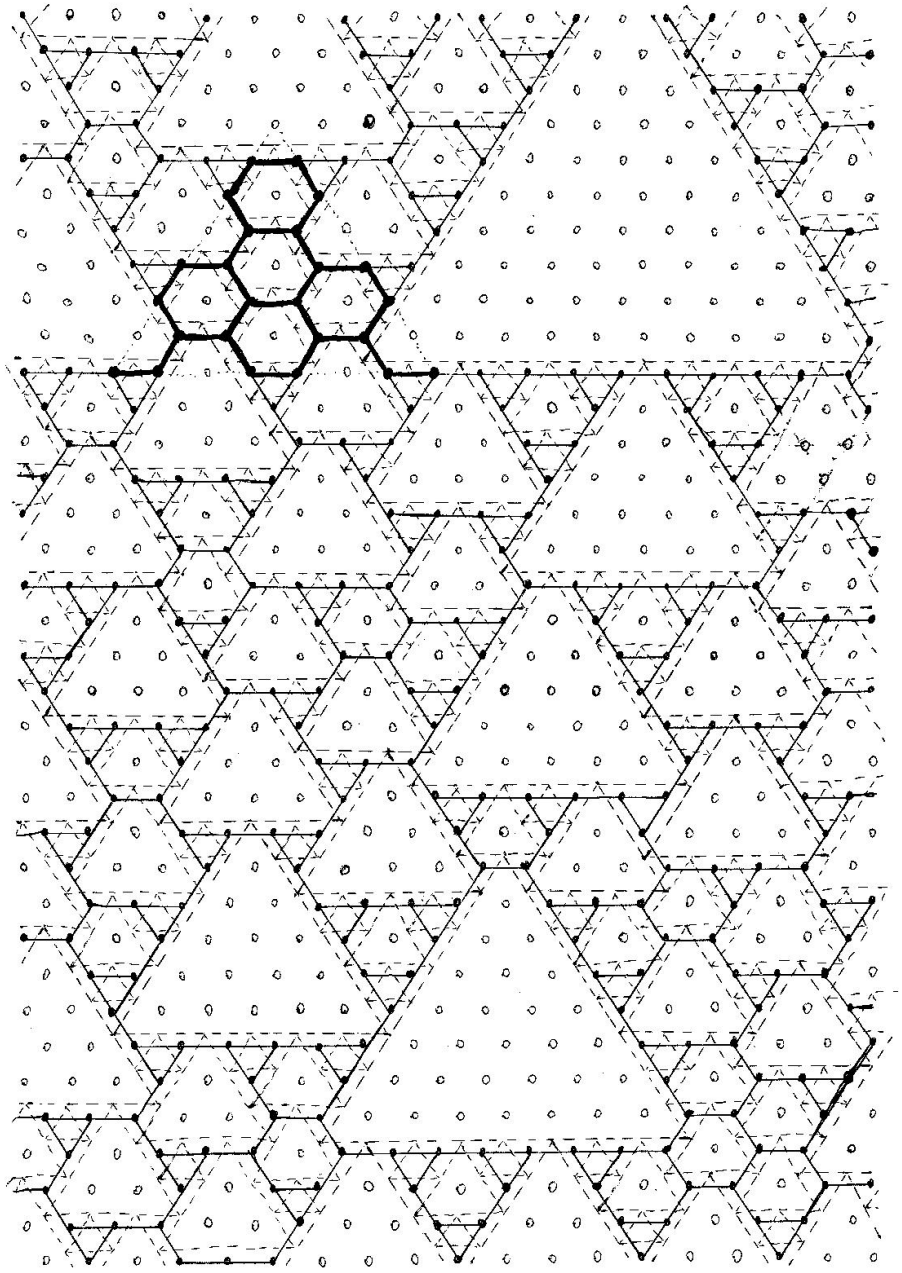
Малышев Ф.М., Кутырева Е.В. О распределении числа единиц в булевом треугольнике Паскаля. Дискр. матем. **18**:2 (2006), 123–131.



$$\text{Th. } \xi \in \left(\frac{n(n+1)}{3} - \chi_i n - \delta_i, \frac{n(n+1)}{3} - \chi_i n + \delta_i\right)$$

Малышев Ф.М. Распределение крайних значений числа единиц в булевых аналогах треугольника Паскаля. Дискр. матем. **28**:3 (2016), 59–96.





$$x_{i+m} = f\left(x_i, x_{i+k_1}, \ldots, x_{i+k_s}\right)$$

Минимальный порождающий набор – $S \subset \mathbb{Z}$: x_t, $t \geqslant T$, выражаются формулой, содержащей символы f и x_i, $i \in S$. Для $S' \subsetneq S$ это не выполняется.

$$x_t = f\left(x_{t-m}, x_{t-m+k_1}, \ldots, x_{t-m+k_s}\right)$$

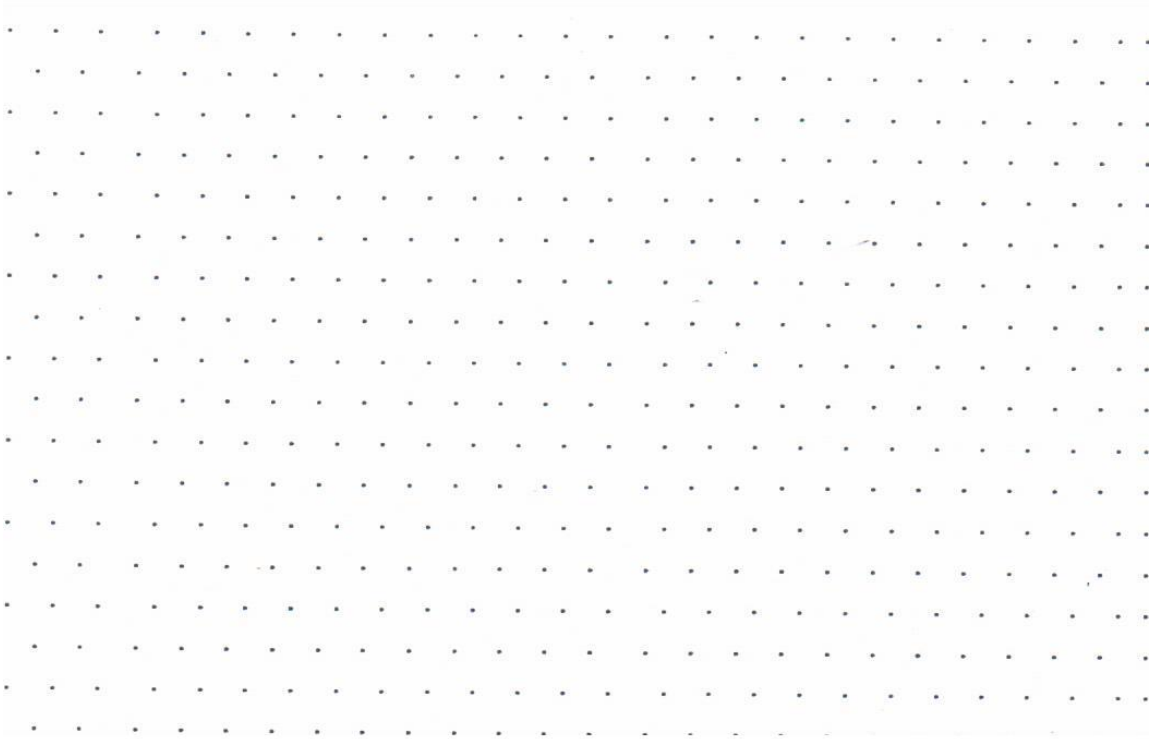
Базисный набор – когда $|S| = m$ минимально возможная.

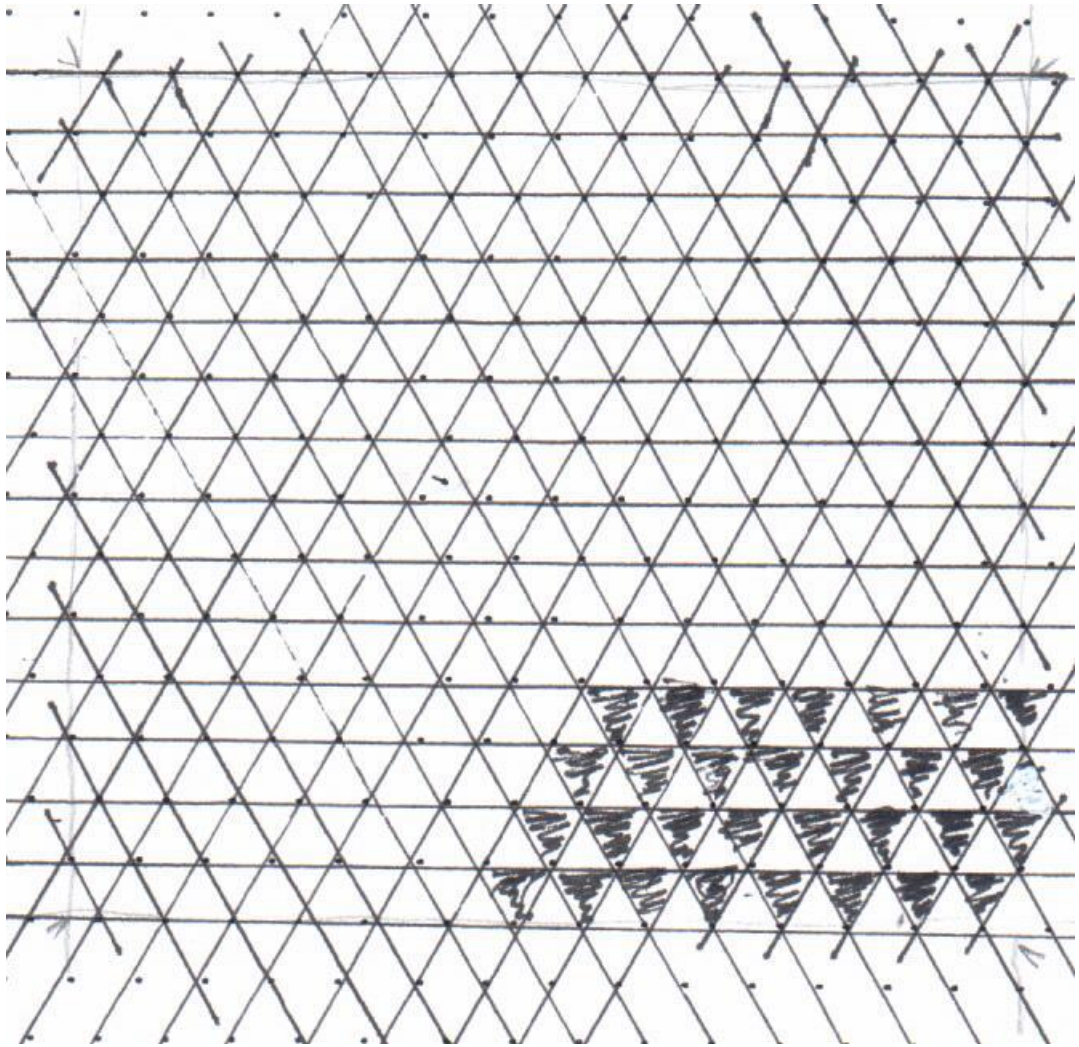
$$\varphi\colon \mathbb{Z}^{s+1} \to \mathbb{Z}, \quad (z_1, \ldots, z_s, z_{s+1}) \mapsto k_1 z_1 + \ldots + k_s z_s + m z_{s+1},$$

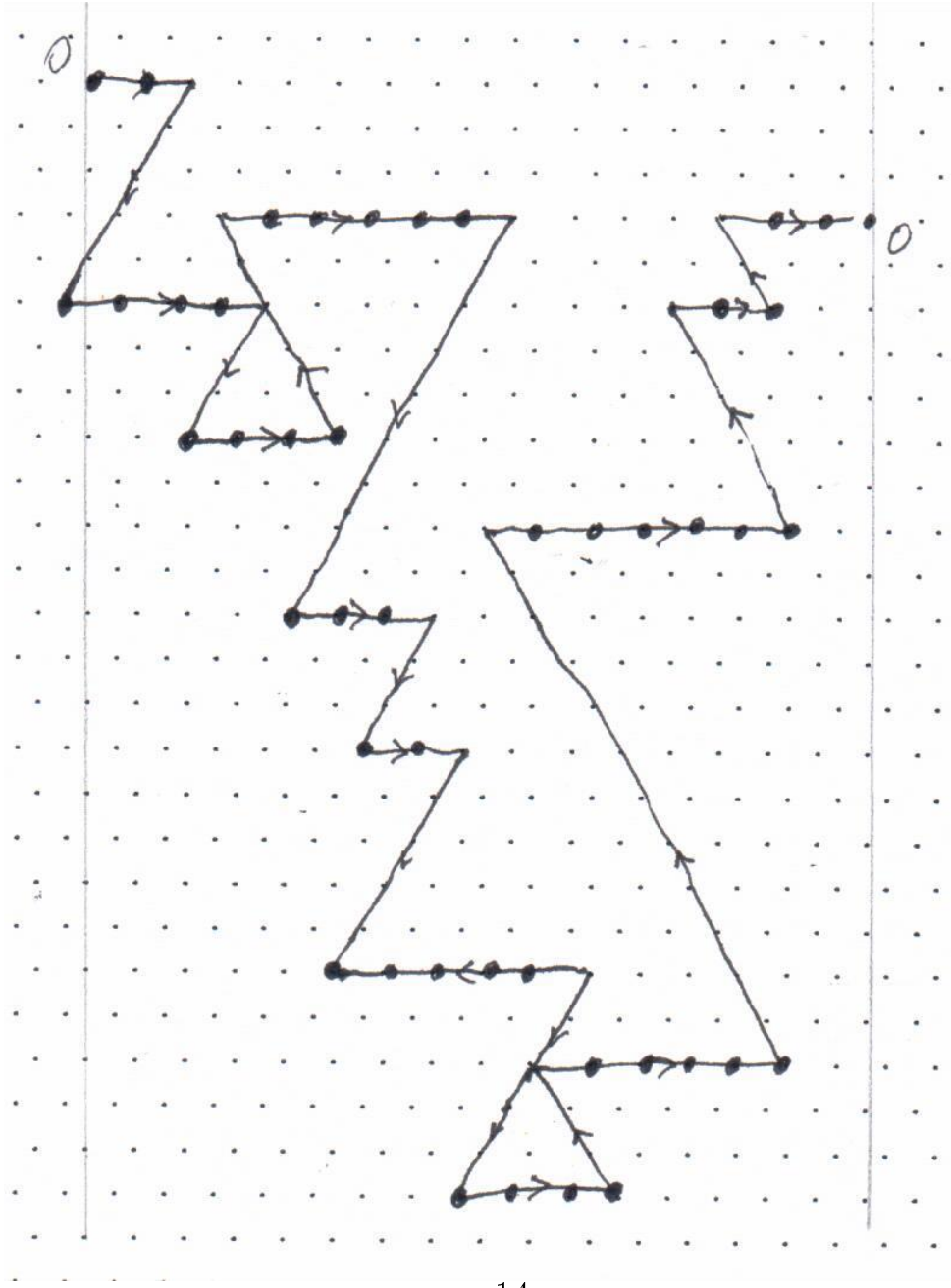
$$\mathbb{Z} \cong \mathbb{Z}^{s+1} \big/ \ker\varphi \subset \mathbb{R}^{s+1} \big/ \ker\varphi = C^s \times \mathbb{R}$$

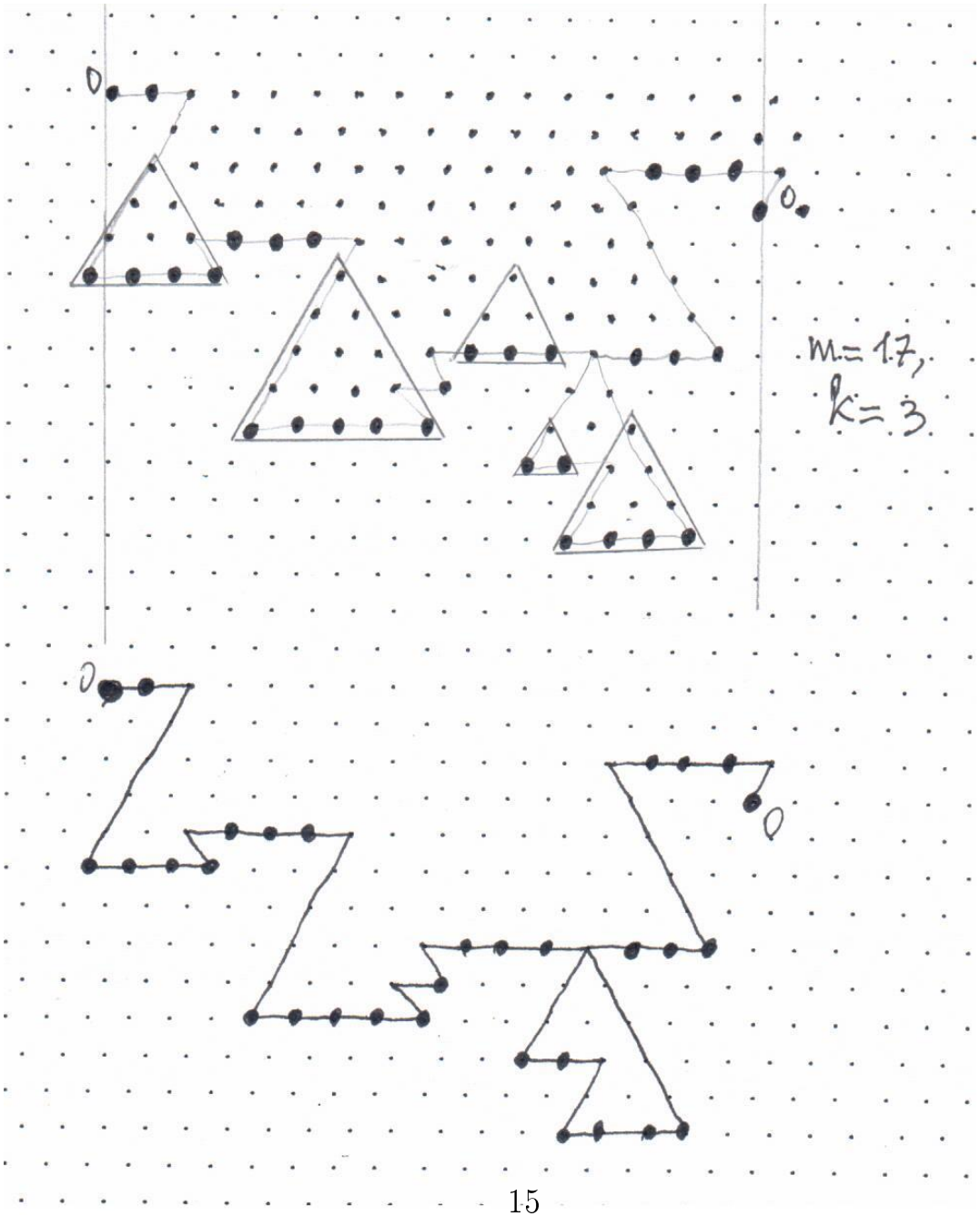
Малышев Ф.М. Порождающие наборы элементов рекуррентных последовательностей. Труды по дискретной математике, **11**:2 (2008), 86–111.

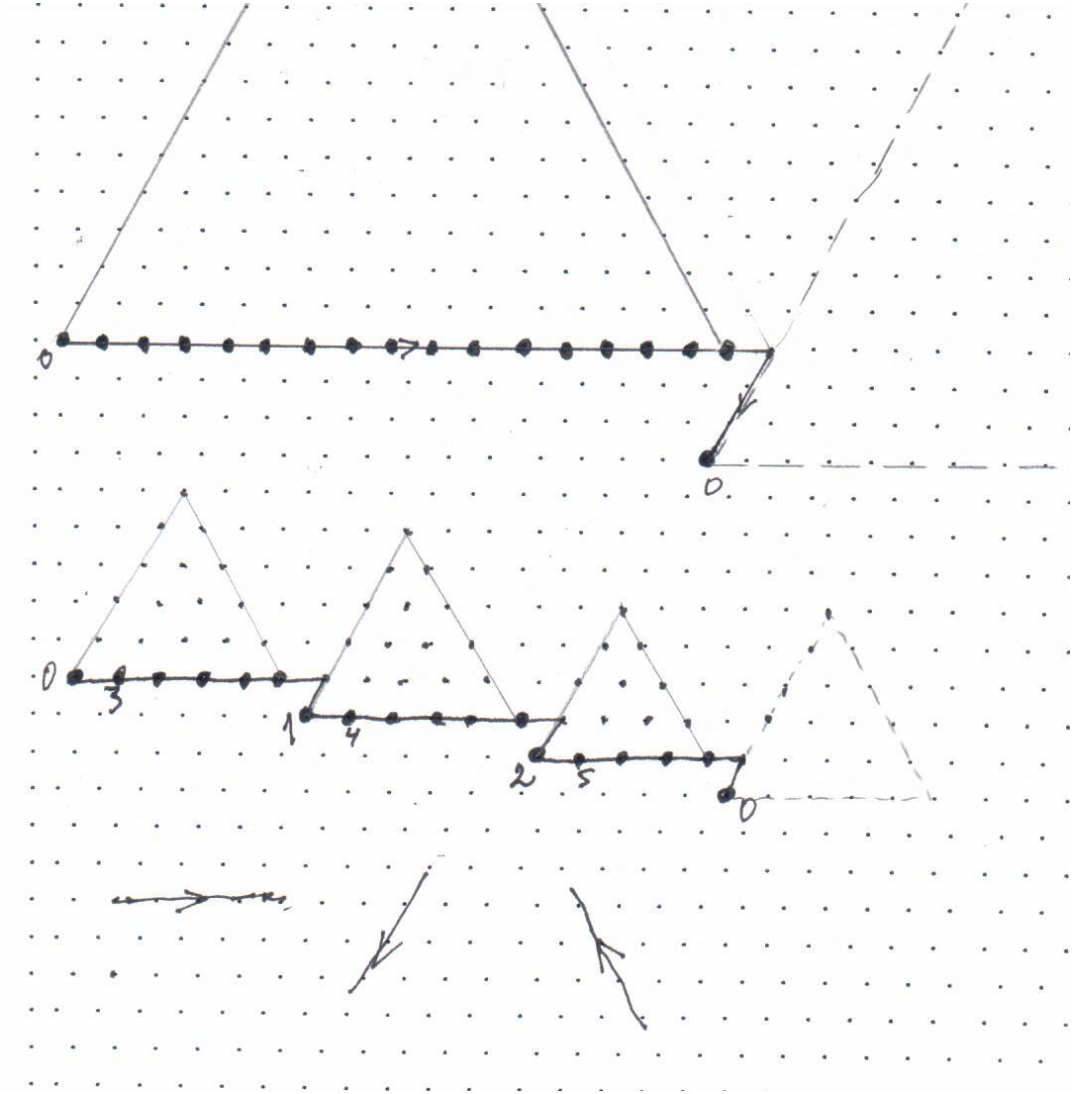
$s = 1$

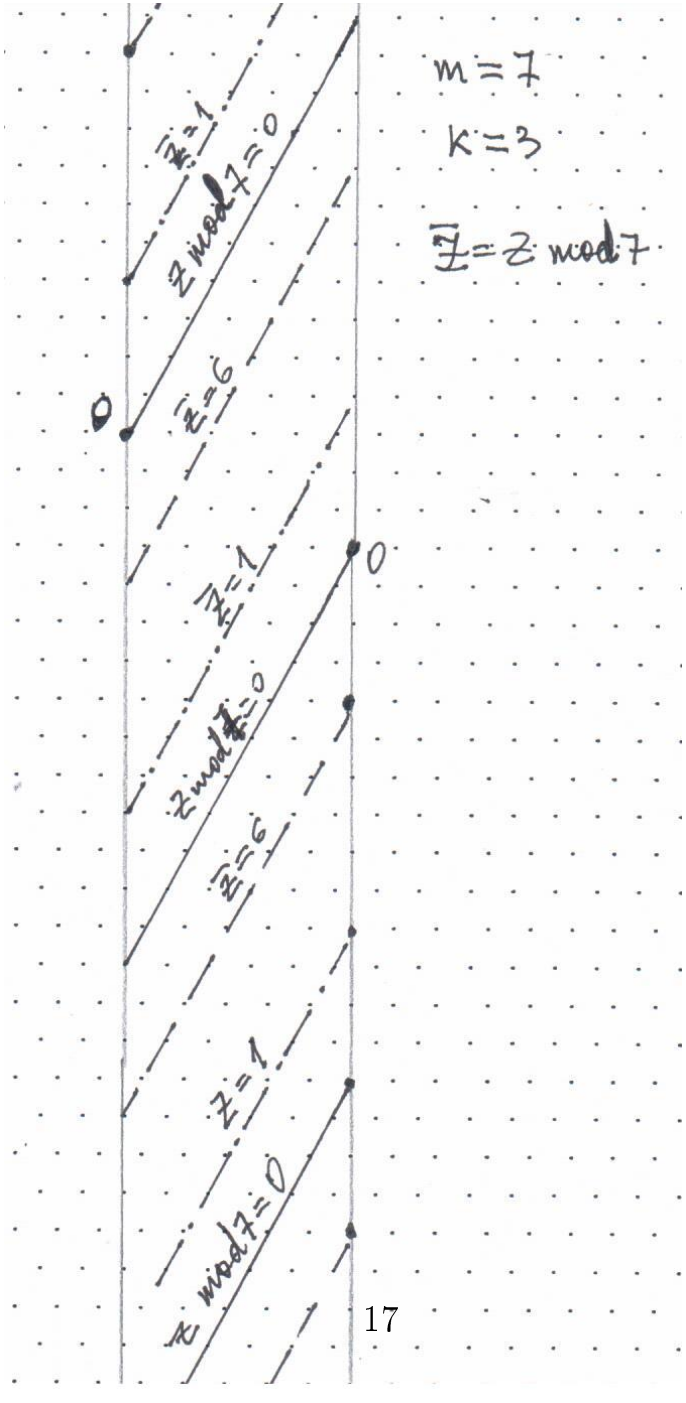





0
0


m = 17,
k = 3


0
0
0
3
1
4
2
5
0


m=7
k=3
z=z mod 7
z=1
z mod 7=0
z=6
0
z=1
z mod 7=0
z=6
z=1
z mod 7=0

$$s \geqslant 2, \quad \mathbb{Z}_m \subset C^s$$

$$\pi \colon \mathbb{Z} \to \mathbb{Z}_m, \ \ z \mapsto z \bmod m$$

$$\sigma \colon \mathbb{Z}_m \to \mathbb{Z}, \ \ \pi(\sigma(y)) = y, \, \forall y \in \mathbb{Z}_m$$

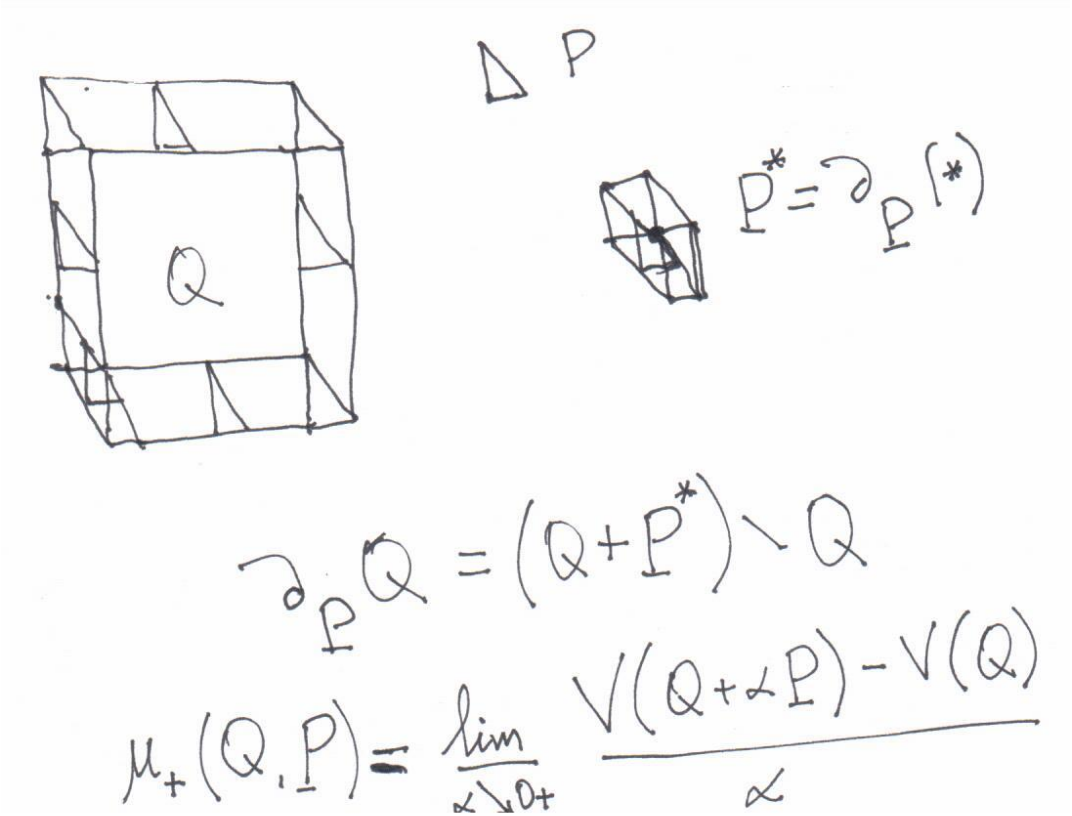
$$\operatorname{Im} \sigma \text{ – базисный набор} \Leftrightarrow$$

$$\sigma(y + \pi(k_i)) \leqslant \sigma(y) + k_i$$

$$\text{для всех } y \in \mathbb{Z}_m \text{ и } i = 1, \ldots, s$$

Малышев Ф.М. Порождающие наборы элементов рекуррентных последовательностей. Труды по дискретной математике, **11**:2 (2008), 86–111.

Малышев Ф.М. Базисы рекуррентных последовательностей. Чебышевский сборник, **16**:2 (2015), 155–185.



Малышев Ф.М. Оптимизационная задача для неравенства Брунна–Минковского. Труды МИАН, **218** (1997), 262–265.

Малышев Ф.М. Доказательство теоремы Брунна–Минковского рассечениями Брунна. Математические заметки, **111**:1 (2022), 80–92.

$$s = 1, \quad x_{i+m} = f(x_i, x_{i+k}), \quad (m, k) = 1$$

$$x_i = f^{(0)}(x_{i+m}, x_{i+k}), \quad x_{i+k} = f^{(1)}(x_{i+m}, x_i), \quad i \in \mathbb{Z}$$

$S \subset \mathbb{Z}$ – базисный набор, если расширение

$$[S] = \{t \in \mathbb{Z} |\, x_t = \mathcal{F}(f, f^{(0)}, f^{(1)}, x_i, i \in S\}$$

содержит все целые числа $z \in \mathbb{Z}$

Теорема. *Если S – базисный набор, то*

$$m \leqslant |S| \leqslant \psi(m)$$

Обратно, для любого целого s, $m \leqslant s \leqslant \psi(m)$ имеется базисный набор мощности s.

Малышев Ф.М. Базисы множества целых чисел относительно многоместных операций сдвига. Математические вопросы криптографии, **2**:1 (2011), 29–73.

$$m = \varphi_{n_0} + \varphi_{n_1} + \varphi_{n_2} + ...$$

$$n_0 \gg n_1 \gg n_2 ... \geqslant 0$$

$$\psi(m) = 2^{n_0} + 2^{n_1+1} + 2^{n_2+2} + ... + 2^{n_i+i} + ...$$

$$\varphi_{-1} = \varphi_0 = 1, \quad \varphi_i = \varphi_{i-1} + \varphi_{i-2}, \quad n_i - n_{i+1} \geqslant 2$$

$$m = 1c_{n-1}c_{n-2}...c_1c_0 = \varphi_n + \sum_{i=0}^{n-1} c_i\varphi_i$$

$$m = 1(\nu_l)1(\nu_{l-1})1...1(\nu_1)1(\nu_0)$$

$$\psi(m) = 1(\nu_l - 1)1(\nu_{l-1} - 1)1...1(\nu_1 - 1)1(\nu_0 + l)$$

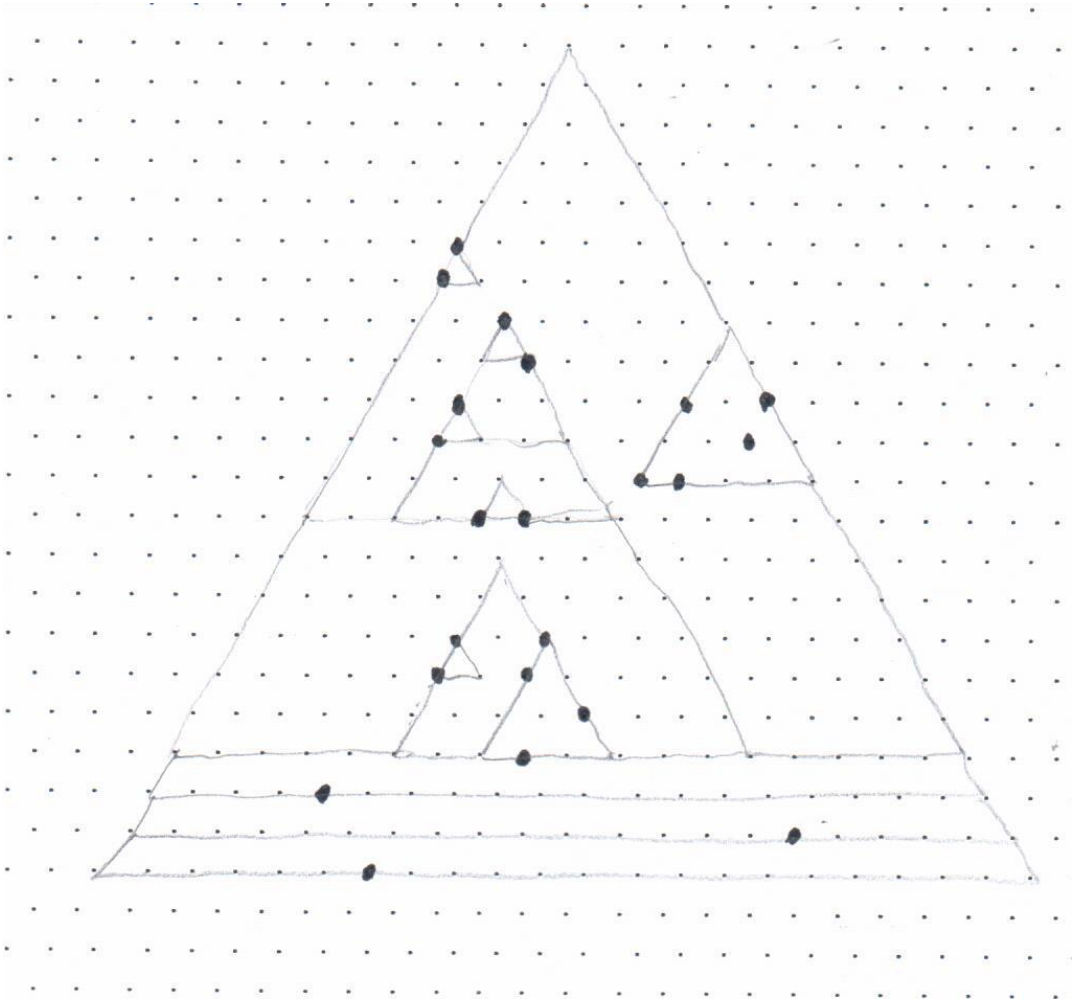
$$\psi\colon \mathbb{R} \to \mathbb{R}$$

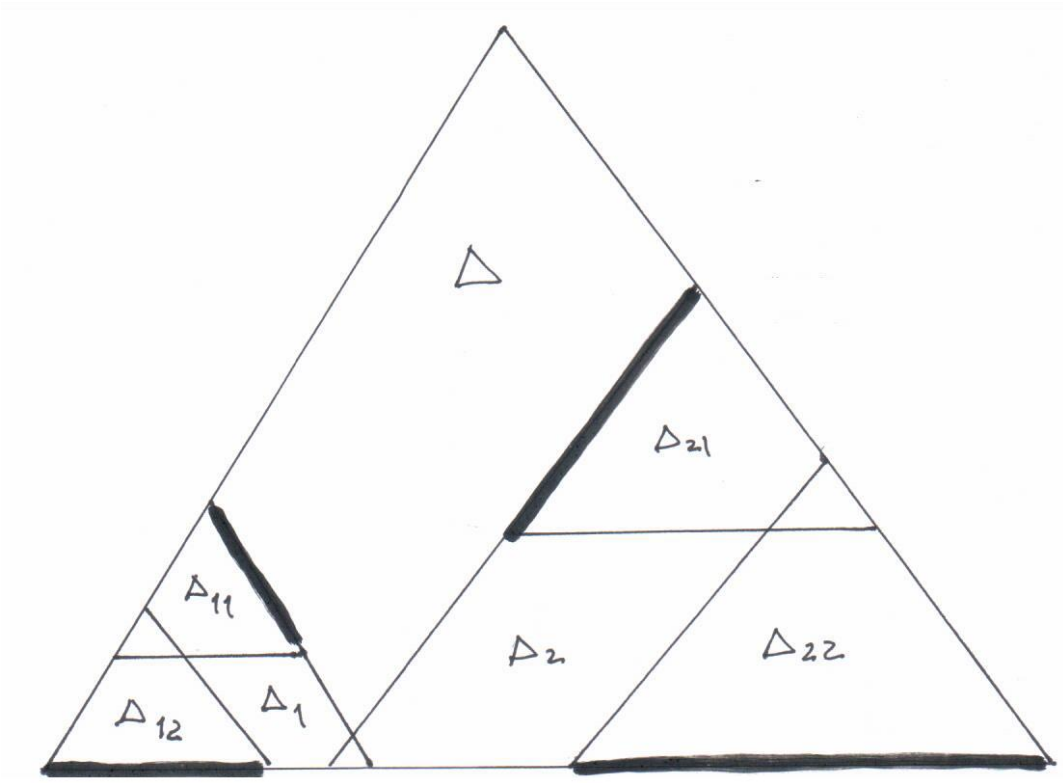
$$\psi(x) = x, \quad x \in [0, 2];$$

$$\psi(\varphi_{n+1} + x) = 2^{n+1} + 2\psi(x), \quad x \in [0, \varphi_n], \quad n \geqslant 0$$

$$0.719m^{\tau} < \psi(m) < 0.797m^{\tau} + 0.25,$$

$$\tau = \log_{\frac{\sqrt{5}+1}{2}} 2$$




Δ
Δ21
Δ11
Δ2
Δ22
Δ12
Δ1

References

[1] Малышев Ф.М. Оптимизационная задача для неравенства Брунна–Минковского. Труды МИАН, **218** (1997), 262–265.

[2] Малышев Ф.М., Кутырева Е.В. О распределении числа единиц в булевом треугольнике Паскаля. Дискр. матем. **18**:2 (2006), 123–131.

[3] Малышев Ф.М. Порождающие наборы элементов рекуррентных последовательностей. Труды по дискретной математике, **11**:2 (2008), 86–111.

[4] Малышев Ф.М. Базисы множества целых чисел относительно многоместных операций сдвига. Математические вопросы криптографии, **2**:1 (2011), 29–73.

[5] Малышев Ф.М. Метрические свойства вложений множества целых чисел в цилиндр. Математические вопросы криптографии, **3**:3 (2012), 57–79.

[6] Малышев Ф.М. Базисы рекуррентных последовательностей. Чебышевский сборник, **16**:2 (2015), 155–185.

[7] Малышев Ф.М. Распределение крайних значений числа единиц в булевых аналогах треугольника Паскаля. Дискр. матем. **28**:3 (2016), 59–96.

[8] Малышев Ф.М. Доказательство теоремы Брунна для школьников. Геометрические аспекты в преподавании математики в высшей и средней школе, Материалы международной

конференции “Классическая и современная геометрия” (к 100-летию со дня рождения Л. С. Атанасяна), МПГУ, М., 2022, 130–138.

[9] Малышев Ф.М. Доказательство теоремы Брунна–Минковского рассечениями Брунна. Математические заметки, **111**:1 (2022), 80–92.

[10] Малышев Ф.М. Сложность восстановления начальных знаков фильтрующих генераторов одного класса. Математические вопросы криптографии, **6**:1 (2015), 109–116.

[11] Малышев Ф.М. Криптографически слабые функции для трёхчленных линейных рекуррентных последовательностей. Математические вопросы криптографии, **8**:1 (2017), 69–80.