Фазовая намотка числовой прямой, фазовая плоскость и двойное решето

Короткие определения, простые леммы и заготовки рисунков

Автор: *Горюшкин Сергей Владимирович zz.vexel@gmail.com*

23 августа 2025 г.

Аннотация

Документ даёт *максимально простое* описание фазовой намотки: как каждое целое число получает координаты *уровень + высота*, как разворачивается цилиндр в плоскость, что такое *минимальный треугольник* формата $A_0 + B_0 = C_0$, и как формулируется *двойное решето* для $6k \pm 1$. Предназначен для вставки готовых рисунков: цилиндр, фазовая плоскость, решето.

Содержание

1 Намотка: как число n получает координаты

Фиксируем модуль $m \in \mathbb{Z}_{\geq 1}$. **Наматываем** числовую прямую на цилиндр так, что каждые m шагов по оси попадаем на тот же угол.

Определение 1.1 (Координаты числа при намотке)**.** *Для $n \in \mathbb{Z}$ определим*

$$\begin{aligned} \textit{уровень (фаза):} \quad v(n) &:= n \bmod m \in \{0, 1, \ldots, m-1\}, \\ \textit{высота (номер витка):} \quad h(n) &:= \left\lfloor \frac{n}{m} \right\rfloor \in \mathbb{Z}. \end{aligned}$$

На цилиндре фаза v отображается в угол $\theta = \frac{2\pi}{m} v$, а высота h — в осевую координату. При развёртке *цилиндра в плоскость точке n сопоставляется пара $(h(n), v(n)) \in \mathbb{Z} \times \{0, \ldots, m-1\}$.*

Замечание 1.2. *Говорим:* “число n лежит на уровне v и на высоте h”*. При увеличении n на m уровень не меняется, а высота растёт на* 1.

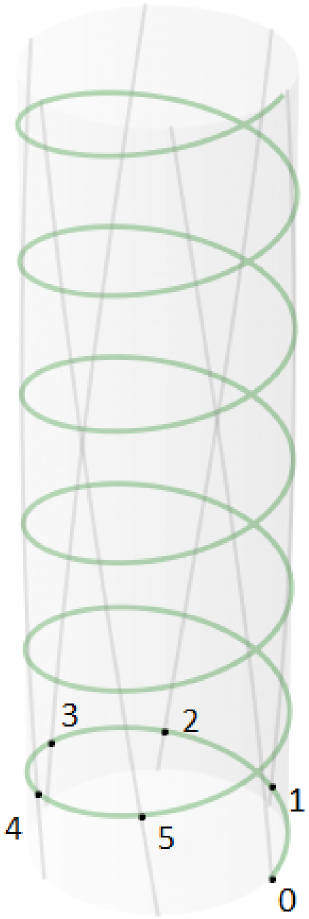


Рис. 1: Фазовая намотка числовой прямой на цилиндр ($m = 6$). Числа с одинаковым остатком лежат на одной образующей.

2 Фазовая плоскость (развёртка цилиндра)

Разворачиваем цилиндр вдоль образующей: получаем **фазовую плоскость** с прямоугольными координатами (h, v), где $h \in \mathbb{Z}$ (высота) и $v \in \{0, \dots, m-1\}$ (уровень), периодически повторяющийся по v с периодом m.

Утверждение 2.1 (Точка → прямая уровня)**.** *Множество $\{n \in \mathbb{Z} : \ v(n) = r\}$ при развёртке образует горизонтальную прямую уровня $v = r$. Все уровни $v = 0, 1, \dots, m-1$ — параллельны.*

Утверждение 2.2 (Повороты/степени по фазе)**.** *Если считать фазу как угол $\theta = \frac{2\pi}{m} v$, то операция "n-я степень" действует по фазе как умножение: $v \mapsto (n \cdot v) \bmod m$. На плоскости это замена уровня v на $nv \mod m$.*

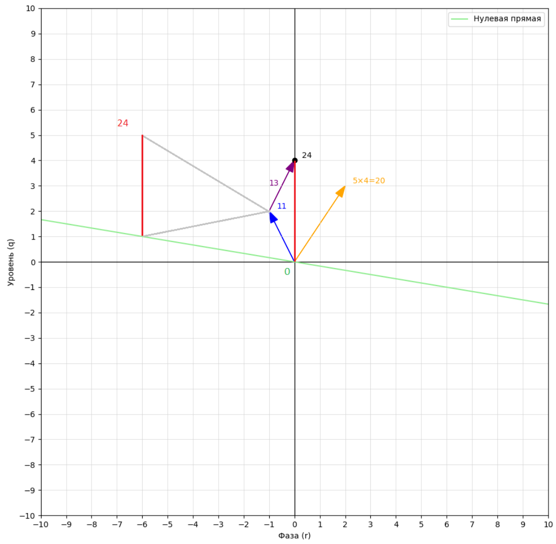


Рис. 2: Фазовая плоскость: развёртка цилиндра. Горизонтальные линии соответствуют фиксированным фазам (остаткам по модулю m).

Определение 2.3 (Минимальный треугольник; якорная версия)**.** *Пусть фиксирован модуль* $m \geq 1$ *и остатки* $(A_0, B_0, C_0) \in \{0, \dots, m-1\}^3$ *удовлетворяют* $A_0 + B_0 \equiv C_0 \pmod{m}$. Якорным семейством *(с якорем* A*) называем множество решений*

$$\mathcal{S}_{A_0} \;:=\; \big\{(A, B, C) : \;A = A_0, \quad B = B_0 + km, \quad C = C_0 + km, \;k \in \mathbb{Z}\big\}.$$

Интуитивно: A *фиксирован как «фазовый якорь», а* (B, C) *поднимаются синхронно на один виток.*

Лемма 2.4 (Эквивалентность с полной решёточной параметризацией)**.** *Полная параметризация решений*

$$A = A_0 + mx, \qquad B = B_0 + my, \qquad C = C_0 + m(x + y) \qquad (x, y \in \mathbb{Z})$$

содержит якорное семейство как срез $x = 0$, $y = k$*. Наоборот, любое решение с* $A \equiv A_0 \pmod{m}$ *можно свести к якорной форме: выбрав* x *из равенства* $A = A_0 + mx$ *и положив* $k = y$*, получаем* $(A, B, C) \in \mathcal{S}_{A_0}$ *после вычитания* mx *из* B *и* C*.*

Замечание 2.5 (Пример при $m = 6$)**.** *Для минимального треугольника* $(A_0, B_0, C_0) = (1, 2, 3)$ *якорное семейство по* A*:*

$$(1, \;2 + 6k, \;3 + 6k), \qquad k \in \mathbb{Z},$$

что эквивалентно общей формуле при $x = 0$, $y = k$*. Аналогично можно якорить* B *или* C*:* $(A, B, C) = (A_0 + km, \;B_0, \;C_0 + km)$ *или* $(A_0 + km, \;B_0 + km, \;C_0)$*.*

3 Двойное решето для 6k±1

Фиксируем $z \geq 5$, множество простых $\mathcal{P}(z) = \{p : \;5 \leq p \leq z\}$, и $M = \prod_{p \in \mathcal{P}(z)} p$. Для $p \in \mathcal{P}(z)$ пусть $t_p \equiv 6^{-1} \pmod{p}$.

Лемма 3.1 (Двойное решето)**.** *Множество индексов*

$$S(z) = \big\{\, k \in \mathbb{Z} : \;\forall p \in \mathcal{P}(z) \;\; k \not\equiv \pm t_p \;(\mathrm{mod} p) \,\big\}$$

имеет период M и в одном периоде содержит ровно

$$\varphi_2(M) = \prod_{p\in\mathcal{P}(z)} (p-2)$$

разрешённых классов. Каждому разрешённому классу $k \equiv r \pmod M$ соответствует двойная *прогрессия* $6(r+jM)\pm 1$ *без делителей $\le z$.*

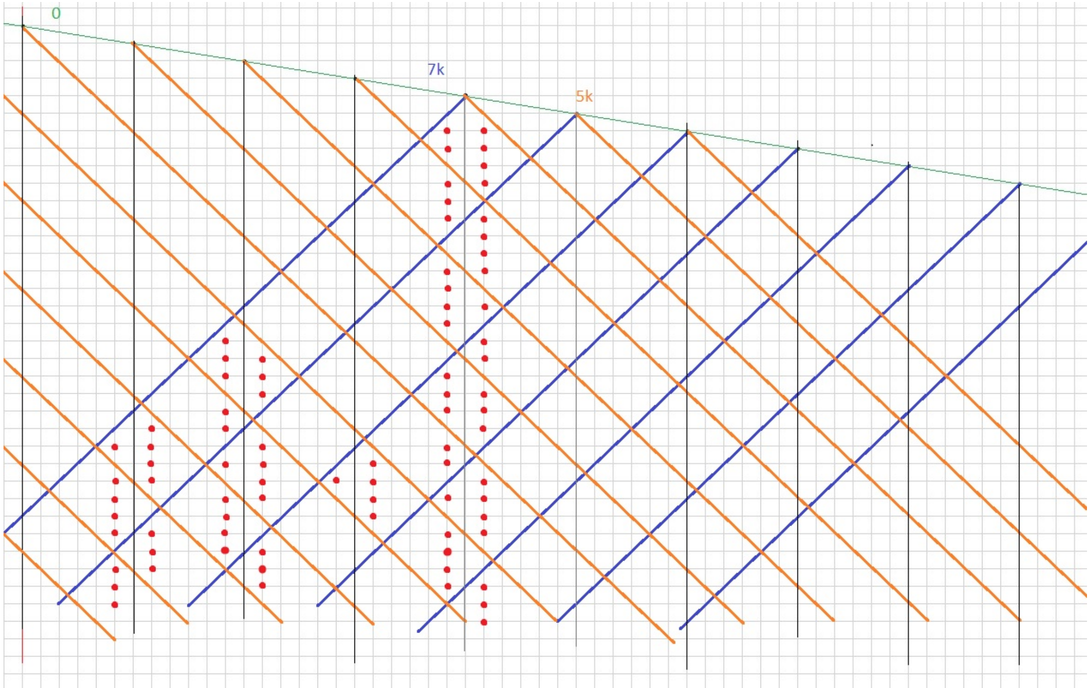


Рис. 3: Двойное решето для $m = 30$. Красные точки показывают вероятного простого.

Замечание 3.2 (Пояснение к рисунку двойного решета)**.** *На рисунке изображены два ситовых слоя:*

- ***левое решето*** $5k$ *(запреты по простому $p = 5$),*
- ***правое решето*** $7k$ *(запреты по простому $p = 7$).*

Они даны в виде наклонных прямых, которые образуют перекрёстную решётку на фазовой плоскости.

Вдоль нулевой оси (вертикаль $6k$) вниз идут каналы $6k\pm1$. По обе стороны от неё нанесены красные точки — кандидаты на простые. До момента пересечения $5\cdot7 = 35$ все эти точки являются потенциально простыми:

$$11,\ 13,\ 17,\ 19,\ 23,\ 29,\ldots$$

Некоторые из них будут выбиваться последующими решётами (по большим простым).

Характерные места:

- *на левом канале (через $v = 5$) видно последовательность* $11, 13, 19, \ldots,$ *но в точке* 25 *срабатывает решето* $5k$*;*
- *на правом канале (через $v = 1$) идут* $11, 17, 23, 29,$ *а затем в точке* 35 *срабатывает* двойное пересечение *решёт* $5k$ *и* $7k$*.*

Таким образом рисунок демонстрирует: каждый красный маркер — это «живое место» ситовой решётки, пока его не исключит одно из следующих простых.

4 Гипотеза щита

Определение (щитового окна). Пусть $p < q$ — *соседние простые числа*. Определим *щитовым окном* интервал

$$W(p) \ := \ \big(p^2,\ q^2\big).$$

Внутри $W(p)$ сито на каналах $6k \pm 1$ действует только ограничениями от простых $\le p$; следующий простой q «включается» лишь на правой границе q^2.

Наблюдение (пример $p = 5,\ q = 7$). В окне $W(5) = (25, 49)$ на каналах $6k \pm 1$ остаются простые

$$29,\ 31,\ 37,\ 41,\ 43,\ 47,$$

в частности появляется *пара близнецов* $29, 31$. Здесь новые ситовые ограничения начинают работать только с числа $49 = 7^2$.

Формулировка (гипотеза щита). Если в некотором щитовом окне $W(p) = (p^2, q^2)$ существует пара близнецов $(u, u+2)$, то пары близнецов существуют и в бесконечно многих последующих окнах $W(p')$ при $p' \to \infty$.

Индуктивная эвристика. Структура запретов в $W(p)$ описывается периодом

$$M(p) = \prod_{5 \le r \le p} r$$

по китайской теореме об остатках. Наличие пары близнецов означает, что в этом слове из «живых» и «дыр» есть два соседних разрешённых места. При переходе к следующему окну $W(p')$ этот шаблон поднимается по модулю $M(p)$ (и его расширениям). Таким образом, *если пара близнецов появилась в одном щитовом окне, то по индукции она будет появляться и в последующих окнах*, сохраняясь в бесконечной последовательности.

5 Провал радикала: что это и как он ограничен

Лемма 5.1 (Провал радикала: общий vs якорный режим)**.** *Пусть $m \ge 1$, $A_0 + B_0 \equiv C_0 \pmod m$ и*

$$A = A_0 + mx, \quad B = B_0 + my, \quad C = C_0 + m(x+y).$$

Обозначим $C_0' = \operatorname{rad}\big(\gcd(A_0, B_0)\gcd(A_0, C_0)\gcd(B_0, C_0)\big)$ и $C_m = \operatorname{rad}(m)$. Тогда

$$\Delta(A,B,C) = \frac{\operatorname{rad}(A)\operatorname{rad}(B)\operatorname{rad}(C)}{\operatorname{rad}(ABC)} \le \begin{cases} C_0'\,C_m^2, & \textbf{\textit{общий случай}},\\ C_0'\,C_m, & \textbf{\textit{якорный режим}}\ (\text{якорим } A;\ x = 0,\ B = B_0 + my,\ C = \end{cases}$$

Замечание 5.2 (Уточнение якорного режима)**.** *В якорном режиме вклад простых $p \mid m$ зависит только от остатков A_0, B_0, C_0. Если дополнительно $\gcd(A_0, m) = 1$, то для всех $p \mid m$ имеем $k_p \le 1$ и*

$$\Delta(A,B,C) \le C_0'.$$

Вообще всегда справедлива более тонкая оценка

$$\Delta(A,B,C) \ \le \ C_0' \operatorname{rad}\big(\gcd(A_0, m)\big),$$

а грубая линейная $C_0'C_m$ удобна как универсальная «короткая» граница.

Замечание 5.3 (Коэффициент качества)**.** *Введём* коэффициент качества *класса*

$$\kappa_{\mathrm{gen}}(m) := \mathrm{rad}(m)^2, \qquad \kappa_{\mathrm{anc}}(A_0; m) := \mathrm{rad}(m) \quad \textit{(или тоньше } \mathrm{rad}(\gcd(A_0, m))\textit{)}.$$

Тогда $\Delta \le C_0' \kappa$, и чем меньше κ, тем «чище» тройка по смыслу ABC: якорение и взаимная простота A_0 с m минимизируют провал радикала.

Идея доказательства. Пусть k_p — число из $\{0, 1, 2, 3\}$, равное количеству компонент A, B, C, делящихся на простой p. Тогда вклад p в Δ равен p^{k_p-1}, откуда общий верхний предел $k_p - 1 \le 2$ даёт $\mathrm{rad}(m)^2$. В якорном случае из $A_0 + B_0 \equiv C_0 \pmod{p}$: если $p \nmid A_0$, то B_0 и C_0 не могут одновременно делиться на p ($k_p \le 1$); если $p \mid A_0$ и класс минимален (не все три делятся на p), то $k_p \le 2$, что даёт множитель не выше p. Если кроме того $\gcd(A_0, m) = 1$, то для всех $p \mid m$ имеем $k_p \le 1$ и вклад равен 1. □

Рис. 4: Провал радикала Δ в якорном режиме: $A = A_0$ фиксирован, $(B, C) = (B_0 + my,\ C_0 + my)$. Резкие падения соответствуют появлению общего простого делителя, границы сверху соответствуют оценкам из леммы ($C_0' C_m$ или тоньше $C_0' \mathrm{rad}(\gcd(A_0, m))$).

Замечание 5.4 (Геометрия провала на графике)**.** *В якорном режиме A фиксирован, а $(B, C) = (B_0 + my,\ C_0 + my)$ сдвигаются синхронно. Поэтому соседние точки y дают почти совпадающие величины B и C (различаются на шаг m), а при попадании общего простого делителя в обе компоненты радикал $\mathrm{rad}(ABC)$ резко "схлопывается", что видно как скачок вниз у Δ на графике (*провал*).*

6 TOR: двухфазная намотка и китайская теорема об остатках

Определение 6.1 (Двухфазная намотка и тор)**.** *Пусть $m_1, m_2 \in \mathbb{Z}_{\ge 1}$. Для $n \in \mathbb{Z}$ зададим две фазы*

$$v_1(n) := n \bmod m_1, \qquad v_2(n) := n \bmod m_2.$$

Отображение

$$\Phi: \ \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}), \qquad \Phi(n) = (v_1(n), v_2(n))$$

— это двухфазная намотка на тор $S^1 \times S^1$ (комбинаторно — прямоугольная решётка остатков).

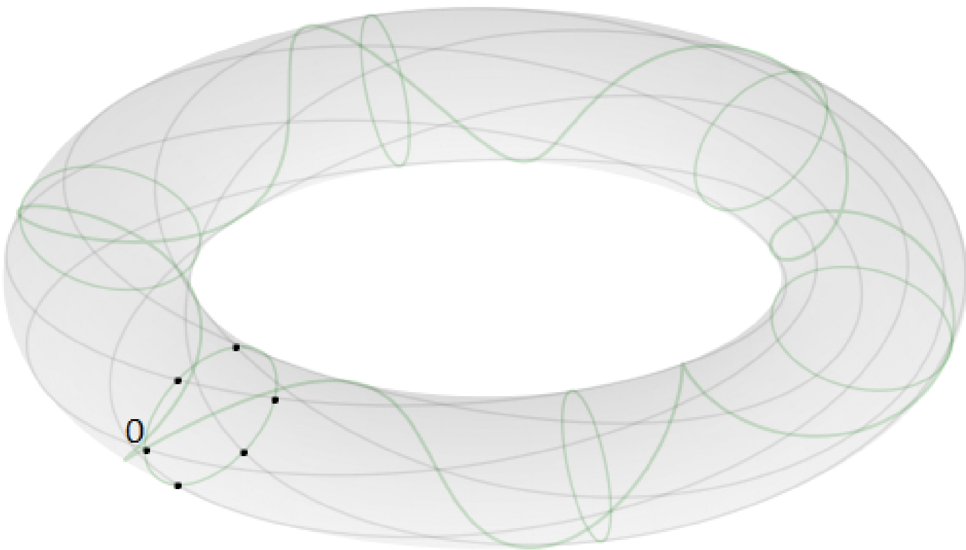
Утверждение 6.2 (Аналог КТО на торе). *Если* $\gcd(m_1, m_2) = 1$*, то для любых остатков* $a \pmod{m_1}$*,* $b \pmod{m_2}$ *существует единственный класс* $n \pmod{M}$*,* $M = m_1 m_2$*, такой что*

$$n \equiv a \pmod{m_1}, \qquad n \equiv b \pmod{m_2}.$$

Эквивалентно: орбита $\{\Phi(n) : n \in \mathbb{Z}\}$ *проходит по всем клеткам решётки ровно один раз за период* M*. Если* $g = \gcd(m_1, m_2) > 1$*, орбита распадается на* g *циклов длины* M/g*.*

Замечание 6.3 (Длинная развёртка (идея)). *Разворачивая тор в прямоугольник* $[0, m_1) \times [0, m_2)$*, траектория* $n \mapsto (v_1(n), v_2(n))$ *визуализируется как прямая с рациональным наклоном, замыкающаяся с периодом* M*. Это геометрическая форма китайской теоремы об остатках.*

Замечание 6.4 (Эллиптическая кривая на торе (набросок)). *Наложив алгебраическое условие (например,* $y^2 = x^3 + Ax + B$ *на одной фазе) и сочетая его с второй фазой, получаем кривую на торе с выделенной «центральной» точкой — геометрическим образом точки на бесконечности. Этот пункт даёт направление для дальнейшего анализа и визуализаций.*



Заключение

В работе построена геометрическая интерпретация числовой прямой через намотку на цилиндр и фазовую развёртку. Мы выделили минимальные треугольники как базовые шаблоны для троек $A + B = C$, а также показали, что операции сдвига и подъёма согласуются с векторными операциями на фазовой плоскости.

Далее введена *гипотеза щита*: в каждом окне $(p^2, (p+1)^2)$ для соседних простых $p < p+1$ остаётся ненулевая конфигурация кандидатов на простые, и наличие пары близнецов в одном окне эвристически гарантирует их повторение в последующих окнах.

Мы уточнили понятие *провала радикала*: в общем случае он ограничен $C_0' \operatorname{rad}(m)^2$, а в якорном режиме — $C_0' \operatorname{rad}(m)$, что даёт простую эвристику оценки качества троек (A, B, C) в терминах гипотезы ABC.

Наконец, введён *тор* как геометрический аналог китайской теоремы об остатках: двухфазная намотка $n \mapsto (n \bmod m_1, n \bmod m_2)$ реализует структуру CRT на поверхности $S^1 \times S^1$. Это открывает путь к дальнейшим конструкциям (в частности, к эллиптическим кривым на торе).

Таким образом, добавленные фрагменты (щит, провал радикала, тор) формируют целостную картину: геометрическая интерпретация даёт не только наглядность, но и комбинаторные эвристики для классических задач теории чисел.

Контакты автора: zz.vexel@gmail.com/ GitHub zzVex .