РАВНОМЕРНО РАСПРЕДЕЛЕННЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ ЦЕЛЫХ p–АДИЧЕСКИХ ЧИСЕЛ, II

В. С. Анашин

1. Введение.

При решении целого ряде прикладных задач из области компьютерного моделирования, численных методов (в особенности квази-Монте-Карло) и криптографии возникает необходимость строить некоторым регулярным образом числовые последовательности с равномерным законом распределения. Методам построения таких последовательностей посвящена столь обширная литература, что мы не имеем возможности перечислить здесь даже основные монографии, посвященные этому вопросу – сошлемся лишь на [2], где имеется подробный обзор и основательная библиография. Как правило, упомянутые методы предполагают построение членов последовательности с помощью некоторых рекурсивных процедур, а также могут рассматриваться и как автоматы. Последние обычно называют псевдослучайными (или квазислучайными) генераторами.

Типичным примером служит предложенный более полувека назад линейный конгруэнтный метод, состоящий в том, что искомая последовательность $\{x_n : n = 0, 1, 2, \dots\}$ реализуется как рекуррентная последовательность первого порядка с законом рекурсии $x_{n+1} \equiv a + bx_n \pmod m$, где a, b – рациональные целые, а $m > 1$ – натуральное число. Равномерная распределенность такой последовательности эквивалентна тому, что она имеет период, длина которого в точности равна m; при выполнении последнего условия *каждый* элемент из множества $\{0, 1, \dots, m-1\}$ (обычно отождествляемого с кольцом вычетов $\mathbb{Z}/m$ кольца $\mathbb{Z}$ всех рациональных целых чисел по модулю m) встречается на периоде *в точности один* раз, и наоборот. Необходимые и достаточные условия, которым при данном m должны отвечать a и b, чтобы период вырабатываемой последовательности имел максимально возможную длину (т.е. в точности равную m), хорошо известны – см. [2, п. 3.2.1.2, теорема A].

К несомненным достоинствам линейного конгруэнтного генератора относится простота его программной реализации (особенно при $m = 2^k$), а одна из основных причин его недостатков, т.е. неудовлетворительных для некоторых задач статистических качеств вырабатываемой последовательности, кроется как раз в его линейности. Например, ввиду того, что в законе рекурсии $f(x) = a+bx$ есть полином степени 1, вырабатываемая последовательность имеет над кольцом $\mathbb{Z}/m$ линейную сложность 2, т.е. является линейной рекуррентной последовательностью порядка 2 над $\mathbb{Z}/m$. Именно, $x_{n+2} \equiv (1+b)x_{n+1} - bx_n \pmod m$ и, значит, точки вида $(\frac{x_{n+2}}{m}, \frac{x_{n+1}}{m}, \frac{x_n}{m})$ всегда, *каково бы ни было* m, попадают на параллельные друг другу плоскости $c + X - (1+b)Y + bZ$ с целым

c, пересекающие единичный куб трехмерного евклидова пространства. Известный результат Георга Марсальи [7] утверждает, что схожая ситуация имеет место и в размерностях > 3 – все точки оказываются сосредоточенными в относительно небольшом количестве параллельных друг другу гиперплоскостей, а не заполняют этот куб более или менее равномерно, и причиной этому опять-таки служит то, что $\deg f = 1$.

Этот факт в течение последних десятилетий стимулировал интенсивную раработку различных альтернатив линейному конгруэнтному методу. Значительная часть их представляет собой *нелинейные* конгруэнтные методы, состоящие в том, что в законе рекурсии в качестве f используются полиномы над $\mathbb{Z}$ степени > 1, в частности, квадратичные (см. [2]), или более высоких степеней ([15]), а также другие преобразования, отличные от полиномиальных (например, экспоненциальные вида $f(x) = a^{g(x)}$ или т.н. инверсивные, построенные с использованием возведения в отрицательные степени, см. обзор в [2]). При этом для увеличения линейной сложности вырабатываемой последовательности авторы довольно часто отказываются от требования максимальности длины периода, т.е. предлагают использовать в законе рекурсии такие преобразования f, с помощью которых генерируются последовательности с длинами периодов заведомо меньшими, чем m, и, значит, строго говоря, заведомо не являющиеся равномерно распределенными в $\mathbb{Z}/m$. В этом случае авторы неизбежно сталкиваются с необходимостью не только оценивать длины периодов, но и выбирать начальное состояние x_0 рекуррентной последовательности таким образом, чтобы попасть на достаточно длинный период. За увеличение степени полинома, а равно и за применение других арифметических функций, типа возведения в отрицательную степень или экспоненцирования, обычно тоже приходится платить определенным увеличением сложности программной реализации. При этом особенно неприятным является не столько это, сколько тот факт, что сложность программной реализации и качество псевдослучайной последовательности обычно оказываются в обратной зависимости: увеличение качества приводит к уменьшению быстродействия, а при увеличении быстродействия приходится жертвовать качеством.

В свете сказанного, актуальной представляется задача описания преобразований $f\colon \mathbb{Z}/m \to \mathbb{Z}/m$, которые, во-первых, обеспечивали бы максимально возможное, т.е. в точности равное m, значение длины периода последовательности, генерируемой по закону $x_{n+1} \equiv f(x_n) \pmod m$ и тем самым ее равномерное распределение в $\mathbb{Z}/m$ (такие преобразования f мы называем транзитивными по модулю m), во-вторых, гарантировали бы достаточно высокую линейную над кольцом $\mathbb{Z}/m$ сложность этой последовательности, т.е. отсутствие в ней «коротких» линейных зависимостей вида $\sum_{i=0}^{r-1} c_i x_{n+i} \equiv 0 \pmod m$ $(n = 0, 1, 2, \dots)$ и, в третьих, в принципе допускали бы относительно простую программную реализацию, а именно, были бы достаточно «гибкими», т.е. имели бы ряд определяющих быстродействие соответствующих программ параметров, которые можно было бы варьировать, добиваясь нужной скорости работы, но не ухудшая при этом вышеупомянутых характеристик качества вырабытываемой последовательности. В данной работе мы описываем широкие классы преобразований, в определенной мере отвечающих этим требованиям.

В первую очередь, мы находим условия транзитивности по модулю m для

преобразований, которые могут быть реализованы в виде композиций как арифметических (сложения, умножения), так и стандартных машинных операций, типа поразрядных логических операций, сдвигов, наложения маски и т.п . В эти композиции могут включаться такие операции, как экспоненцирование и взятие обратного элемента, а значит, и возведение в степени с отрицательными показателями (см. в связи с этими операциями 4.9, 4.11 и 2.5) и/или такие машинные операции как $\mathrm{OR}, \mathrm{XOR}, \mathrm{AND}$ и т.п. (см. 2.5, 2.8).

В частности, мы находим обширные классы транзитивных по модулю m функций, которые могут быть заданы как полиномы с рациональными, но не обязательно целыми коэффициентами (см. 4.7), или как мероморфные, в частности, рациональные функции (см. 4.9, 4.11, 4.12), или как аналитические функции (см. 4.11, 4.9, 2.5). Упомянутые условия легко проверяемы и позволяют строить транзитивные по модулю m преобразования в явном виде — см., например, 2.3, 2.4, или 2.5–2.8 (а также 4.11, 4.12) вместе с 2.1, и другие примеры, приведенные в данной работе.

Проиллюстрируем сказанное некоторыми из этих примеров: как следует из доказанных ниже теоремы 2.7 и леммы 4.11, транзитивно по *каждому* модулю $m = 2^k$ $(k = 1, 2, \dots)$ любое преобразование вида

$$f(x) = 1 + x + 2(g(x+1) - g(x)),$$

где g есть *произвольная* композиция арифметических операций — сложения $(y, z) \mapsto y + z$, умножения $(y, z) \mapsto yz$, экспоненцирования $(y, z) \mapsto (1 + 2y)^z$ (в частности, взятия обратного элемента, $y \mapsto (1 + 2y)^{-1}$), поразрядных логических операций — конъюнкции $(y, z) \mapsto y \,\mathrm{AND}\, z$, дизъюнкции $(y, z) \mapsto y \,\mathrm{OR}\, z$, исключительного «или» $(y, z) \mapsto y \,\mathrm{XOR}\, z$, отрицания $z \mapsto \mathrm{NEG}\, z$, и «машинных» операций (которые, в сущности, являются производными операциями от перечисленных выше) — сдвига на s шагов в сторону старших значащих разрядов $z \mapsto 2^s z$, маскирования $z \mapsto z \,\mathrm{AND}\, M$ с маской M, приведения по модулю 2^s, состоящая в отбрасывании всех старших значащих бит $z \mapsto z \bmod 2^s = z \,\mathrm{AND}(2^s - 1)$, и некоторых других. При этом предполагается, что все вышеуказанные операции осуществляются над элементами кольца $\mathbb{Z}/2^k$, причем логические операции производятся поразрядно над операндами, представленными в двоичной системе счисления: так, $2 = 1 \,\mathrm{XOR}\, 3 = 2 \,\mathrm{AND}\, 7 \equiv \mathrm{NEG}\, 13 \pmod 8$, $3^{-1} \equiv 11 \equiv -5 \pmod{16}$, $3^{-\frac{1}{3}} \equiv 3^{11} \equiv 3^{-5} \equiv 11 \pmod{16}$ и т.п. При таких соглашениях функции g и f определены на $\mathbb{Z}/m$ корректно, а сложность их программной реализации определяется исключительно соотношением и количеством «быстрых» и «медленных» операций в композиции g, т.е. может произвольно варьироваться в зависимости от требований к быстродействию.

Подчеркнем еще раз, в приведенном выше примере транзитивность преобразования f по модулю $m = 2^k$ *никак не зависит* ни от k, ни от конкретного вида композиции g — и при $g(x) = x \,\mathrm{XOR}(2x + 1)$, и при

$$g(x) = \left(1 + 2\frac{x \,\mathrm{AND}\, x^2 + x^3 \,\mathrm{OR}\, x^4}{3 + 4(5 + 6x^5)^{x^6 \,\mathrm{XOR}\, x^7}}\right)^{7 + \frac{8x^8}{9 + 10x^9}}$$

последовательность $\{x_n\}$ с законом рекурсии $x_{n+1} \equiv 1 + x_n + 2(g(x_n + 1) - g(x_n)) \pmod{2^k}$ равномерно распределена в $\mathbb{Z}/2^k$ при любом значении $k = 1, 2, 3 \dots$.

Именно, эта последовательность является строго периодической с периодом длины 2^k, и *каждый* элемент из множества $\{0, 1, \dots, 2^k - 1\}$ встречается на ее периоде *в точности один* раз.

Похожего рода утверждения справедливы и для произвольного составного m: например, из доказанных ниже утверждений 4.11 и 4.12 вытекает, что преобразование

$$f(x) = 1 + x + \pi(m)^2 u(x)(1 + \pi(m)v(x))^{w(x)},$$

где $\pi(m)$ есть произведение всех простых чисел, делящих m, транзитивно по модулю m, каковы бы ни были полиномы $u(x), v(x), w(x) \in \mathbb{Z}[x]$ над кольцом $\mathbb{Z}$. Многочисленные аналоги этого последнего утверждения для полиномов с рациональными (не обязательно целыми) коэффициентами могут быть получены с помощью техники из раздела 4. Отметим попутно, что приведенный пример показывает, что с помощью небольших изменений закона рекурсии можно обеспечивать транзитивность как т.н. инверсивных псевдослучайных генераторов (т.е. с $f(x) = a + bx^{-1}$ или с $f(x) = (a + bx)^{-1}$), так экспоненциальных (т.е. с $f(x) = a^x$): при $v(x) = const \neq 0$ мы получаем генератор экспоненциального типа, при $w(x) = const = -1$ – инверсивного.

Что же касается наличия в построенных таким способом последовательностях $\{x_n \equiv f(x_{n-1}) \pmod m : n = 1, 2, \dots\}$ линейных зависимостей вида $\sum_{i=0}^{r-1} c_i x_{n+i} \equiv 0 \pmod m$ $(n = 0, 1, 2, \dots)$, длина r которых не зависит от m, то в этом отношении линейные конгруэнтные генераторы оказываются в классе всех конгруэнтных генераторов скорее исключением, чем правилом. Например, если для некоторого простого p функция $f\colon \mathbb{Z} \to \mathbb{Z}$ может быть задана транзитивным по модулю $m = p^k$ $(k \geqslant 3)$ полиномом степени $\geqslant 2$ с рациональными целыми коэффициентами, то таких соотношений с r *и* c_i *не зависящими от* k заведомо не будет. Более того, минимальный ранг линейной над $\mathbb{Z}/p^k$ рекуррентной последовательности, с помощью которой можно задать выходную последовательность такого генератора, неограниченно растет вместе с k. На самом деле, справедливо значительно более общее утверждение — см. 5.1–5.4 для точных формулировок.

В работе изучаются также равновероятные по модулю m функции, т.е. такие отображения F s-ой декартовой степени $(Z/m)^{(s)}$ на t-ю декартову степень $(Z/m)^{(t)}$ кольца $\mathbb{Z}/m$, $(s \geqslant t)$, при котором полные прообразы всех элементов равномощны. В частности, при $s = t$ равновероятные по модулю m функции задают биекции соответствующих колец, и потому называются биективными по модулю m. Весьма частным случаем изучаемых в работе равновероятных по модулю m функций являются т.н. подстановочные полиномы по модулю m, т.е. полиномы с целыми коэффициентами, задающие биекцию кольца $\mathbb{Z}/m$ на себя. Полученные условия равновероятности по модулю m обобщают известные (см. [8]) результаты о подстановочных полиномах на значительно более широкие классы функций— см. по этому поводу раздел 3 данной работы. Мотивом для такого изучения послужил тот факт, что применение равновероятных по модулю m функций позволяет строить из равномерно распределенных в $\mathbb{Z}/M$ периодических последовательностей с периодом длины M равномерно распределенные в $\mathbb{Z}/N$ (где N делит M) периодческие последовательности с периодом той же длины M; другими словами, каждый элемент из $\mathbb{Z}/N$ встретится на

периоде полученной последовательности одинаковое число (но не обязательно один) раз. Применение равновероятных по модулю m преобразований к последовательностям, полученным описанными выше методами, оказывается полезным при построении и обосновании криптографической стойкости поточных шифраторов — однако эта тема составляет содержание последующей статьи и лежит вне рамок данной работы.

Отметим, что при доказательстве основных утверждений нами используется техника p-адического анализа. Поставленные выше задачи сначала переформулируются на этом языке.

Фактически, в работе описываются эргодические относительно меры Хаара, а также сохраняющие эту меру или равновероятные относительно этой меры функции, заданные на пространстве $\mathbb{Z}_p$ всех целых p-адических чисел, принимающие значения в $\mathbb{Z}_p$ и принадлежащие классу всех функций, удовлетворяющих относительно p-адической метрики условию Липщица с коэффициентом 1. В этом смысле результаты данной работы могут оказаться полезными для теории неархимедовых динамических систем: ряд результатов легко интерпретируется как описание эргодических динамических систем с дискретным временем на компакте $\mathbb{Z}_p$.

Работа продолжает исследования автора, начатые в [11]: мы приводим доказательства некоторых результатов, анонсированных в [11, 12, 14, 17], формулируем и доказываем новые результаты.

Переходя к точным формулировкам, для удобства читателя напомним некоторые сведения из p-адического анализа и теории равномерно распределенных последовательностей, следуя [6], [3] и [2], а также приведем необходимые результаты, определения и обозначения из [11].

Везде далее p — простое число. Если $z = z_0 + z_1 p + z_2 p^2 + \dots$, где $z_j \in \{0, 1, \dots, p-1\}$ $(j = 0, 1, 2, \dots)$, — каноническая запись целого p-адического числа $z \neq 0$, то $\operatorname{ord}_p z = \min\{j : z_j \neq 0\}$ — показатель максимальной степени p, делящей z. По определению, $\|z\|_p = p^{-\operatorname{ord}_p z}$ есть p-адическая норма z, $\|0\|_p = 0$. Норма $\| \ \|_p$ стандартным образом распространяется на все поле $\mathbb{Q}_p$ p-адических чисел, которое есть поле частных кольца целых p-адических чисел $\mathbb{Z}_p$, и задает на $\mathbb{Q}_p$ метрику $d_p(u, v) = \|u - v\|_p$, относительно которой $\mathbb{Q}_p$ является пополнением пространства рациональных чисел $\mathbb{Q}$. Кольцо $\mathbb{Z}_p = \{u \in \mathbb{Q}_p : \|u\|_p \leqslant 1\}$ есть компакт в пространстве $\mathbb{Q}_p$, являющийся замыканием множества $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. Таким образом, $\mathbb{Z}_p$ есть сепарабельное компактное метрическое пространство. Множество всех различных смежных классов $a + p^k\mathbb{Z}_p$ по всем идеалам кольца $\mathbb{Z}_p$ образует базу соответствующего топологического пространства. Каждое множество $a + p^k\mathbb{Z}_p$ $(a \in \mathbb{Z}_p$, $k = 0, 1, 2, \dots)$ есть открытый (и одновременно замкнутый) шар радиуса p^{-k}.

Пространство $\mathbb{Z}_p$ наделяется мерой μ: положив $\mu(a + p^k\mathbb{Z}_p) = p^{-k}$, продолжим эту меру на все σ-кольцо множеств, порожденное компактами из $\mathbb{Z}_p$ (последние являются в точности всеми замкнутыми множествами в $\mathbb{Z}_p$). Это продолжение единственно, является мерой Хаара на $\mathbb{Z}_p$ и представляет собой неотрицательную σ-аддитивную регулярную нормированную борелевскую меру. Таким образом, μ — естественная вероятностная мера на пространстве $\mathbb{Z}_p$. Аналогично задается вероятностная мера на n-мерном пространстве $\mathbb{Z}_p^{(n)}$

— как соответствующая нормированная мера Хаара.

Пусть теперь $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ есть функция, сохраняющая все конгруэнции кольца $\mathbb{Z}_p$, т.е. такая, что $a\theta b$ влечет $f(a)\theta f(b)$ для любой конгруэнции θ и любых $a, b \in \mathbb{Z}_p$. Поскольку каждая конгруэнция кольца $\mathbb{Z}_p$ есть отношение сравнимости по модулю некоторого идеала $p^k\mathbb{Z}_p$ (которое везде далее обозначается через $\cdot \equiv \cdot \pmod{p^k}$), то нетрудно показать, что функция f сохраняет все конгруэнции кольца $\mathbb{Z}_p$ тогда и только тогда, когда она удовлятворяет условию Липшица с коэффициентом 1: $\|f(x)-f(y)\|_p \leqslant \|x-y\|_p$. Функцию, сохраняющую все конгруэнции некоторой универсальной алгебры, называют *совместимой*. Мы будем использовать этот термин вместо термина «консервативный» из [11], поскольку за последним в работах по алгебраическим системам закрепилось другое значение (см. [8, стр. 45]).

Класс совместимых функций весьма широк: в нем лежат все функции, задаваемые полиномами с рациональными целыми или p-адическими целыми коэффициентами, целозначные аналитические над $\mathbb{Z}_p$ функции, а также целозначные рациональные над $\mathbb{Z}_p$ функции, знаменатели которых не обращаются в 0 по модулю p. Ряд других примеров приведен ниже.

Напомним, что функция, заданная на некотором поле F и принимающая значения в F, называется *целозначной*, если все ее значения на целых элементах поля F являются целыми элементами поля F. В дальнейшем мы изучаем целозначные функции на поле $\mathbb{Q}_p$ всех целых p-адических чисел (и, стало быть, принимающие целые p-адические значения во всех точках из $\mathbb{Z}_p$), в частности, целозначные на поле $\mathbb{Q}$ рациональных чисел функции. Полином над полем F называется целозначным, если целозначна задаваемая им на F функция. Отметим, что целозначная на F функция f, очевидно, задает на кольце Z целых элементов поля F функцию $f|_Z : Z \to Z$, которая не обязательно является совместимой на Z, т.е. не обязательно сохраняет все конгруэнции кольца Z; однако если $f|_Z$ совместима как функция на Z, то в случаях, когда это не приводит к недоразумениям, применительно функции f (а если она задается полиномом над F, то и к этому полиному) будет использоваться термин «совместимый».

Отметим, что понятия целозначности и совместимости естественным образом переносятся и на функции нескольких переменных — норма (и, следовательно, метрика) пространства $\mathbb{Z}_p$ естественным образом индуцирует норму (и, следовательно, метрику) n-мерного пространства $\mathbb{Z}_p^{(n)}$: для $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}_p^{(n)}$ полагаем $\|\mathbf{u}\|_p = \max\{\|u_i\|_p : i = 1, 2, \ldots, n\}$. Таким образом, функция

$$F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$$

совместима тогда и только тогда, когда она удовлетворяет условию Липшица с коэффициентом 1. В частности, все совместимые функции на $\mathbb{Z}_p$ непрерывны как p-адические функции.

Этот простой вывод является весьма важным для приложений. Именно, каждое машинное слово, т.е. слово некоторой конечной длины в алфавите $\{0, 1\}$, можно интерпретировать как неотрицательное рациональное целое число, записанное в двоичной системе счисления. Тогда все вышеупомянутые поразрядные логические и машинные операции естественным образом продолжаются на

все множество $\mathbb{Z}_2$ целых 2-адических чисел, представленных в канонической форме. Кроме того, на $\mathbb{Z}_2$ продолжаются и вышеупомянутые арифметические операции. Несложно показать, что все эти операции (т.е. их продолжения на $\mathbb{Z}_2$), а значит, и все их композиции, являются совместимыми функциями: для экспоненцирования $(y,z)\mapsto(1+2y)^z$, и, в частности, взятия обратного элемента $y\mapsto(1+2y)^{-1}$ см. 4.11, для остальных операций это сразу следует из их определений. Следовательно, все эти операции являются непрерывными на $\mathbb{Z}_2$ функциями в 2-адической метрике. Отметим, что сдвиг на m шагов двоичной записи числа в сторону младших разрядов, т.е. операция $\lfloor\frac{\cdot}{2^m}\rfloor$ деления на 2^m с последующим отбрасыванием дробной части, тоже является непрерывной на $\mathbb{Z}_2$, хотя и не совместимой функцией (откуда следует, что результаты статьи остаются справедливыми и для композиций, включающими также и эту последнюю операцию, но при условии, что вся композиция остается совместимой функцией).

Сказанное дает потенциальную возможность применять к изучению ряда свойств функций, реализуемых как композиции вышеуказанных операций, методы неархимедова (т.е. p-адического) анализа. Разумеется, этот аппарат возможно применять к изучению тех свойств, которые допускают некоторую естественную формулировку в терминах анализа, т.е. на языке мер, метрик, сходимостей, производных и т.п.

Оказывается, ряд свойств функций, традиционно изучаемых в рамках дискретной математики, допускают такую переформулировку. С одним из них — совместимостью — мы уже познакомились. Отметим, что известные в теории автоматов т.н. детерминированные функции на множестве всех сверхслов (т.е. бесконечных последовательностей) в алфавите $\{0,1\}$ (естественным образом отождествляемых с элементами из $\mathbb{Z}_2$) есть совместимые функции на $\mathbb{Z}_2$.

Есть и другие свойства, допускающие такую переформулировку. Рассмотрим, например, свойство совместимой функции $F=(f_1,\dots,f_m)\colon {\mathbb{Z}_p}^{(n)}\to {\mathbb{Z}_p}^{(m)}$ быть *равновероятной по модулю* p^k. Последнее по определению означает, что F индуцирует на n-ой декартовой степени $(\mathbb{Z}/p^k)^{(n)}$ кольца $\mathbb{Z}/p^k$ вычетов по модулю p^k равновероятную функцию $\bar F=(\bar f_1,\dots,\bar f_m)\colon(\mathbb{Z}/p^k)^{(n)}\to(\mathbb{Z}/p^k)^{(m)}$, т.е. такую, что каждая точка из ${(\mathbb{Z}/p^k)}^{(m)}$ имеет в ${(\mathbb{Z}/p^k)}^{(n)}$ одно и то же число F-прообразов. В частности, при $m=n$ равновероятность по модулю p^k есть ни что иное как *биективность по модулю* p^k. Мы будем рассматривать также важное для построения псевдослучайных генераторов свойство функции F быть *транзитивной по модулю* p^k, т.е. задавать на ${(\mathbb{Z}/p^k)}^{(n)}$ подстановку, имеющую только один цикл (т.н. полноцикловую подстановку).

Отметим, что при определении понятий равновероятности, биективности или транзитивности функции F по модулю p^k мы пользовались совместимостью этой функции. Значение индуцированной функции $\bar f_i(x)$ в кольце $\mathbb{Z}/p^k$ вычетов по модулю p^k по определению есть наименьший неотрицательный вычет $f_i(x)\bmod p^k$ по модулю p^k значения функции $f_i(x)$, т.е. $f_i(x)\bmod p^k=\alpha\in\{0,1,\dots,p^k-1\}$, причем $\|f_i(x)-\alpha\|_p\leqslant p^{-k}$. В силу совместимости функции f_i значение функции $\bar f_i(x)$ не зависит от выбора представителя x смежного класса кольца $\mathbb{Z}_p^{(n)}$ (которое есть прямая сумма n изоморфных копий кольца $\mathbb{Z}_p$) по идеалу $(p^k\mathbb{Z}_p)^{(n)}$, а значит, функция F корректно задает на кольце

$(\mathbb{Z}/p^k)^{(n)}$ функцию $F \bmod p^k = (f_1(x) \bmod p^k, \dots, f_m(x) \bmod p^k)$, принимающую значения в $(\mathbb{Z}/p^k)^{(m)}$. В дальнейшем в случаях, когда это не приведет к недоразумению, для этой последней функции мы будем использовать наряду с обозначением $F \bmod p^k$ и обозначение $\bar{F}$.

Напомним некоторые определения из теории измеримых функций (см., например, [1]). Пусть S и T — пространства с неотрицательными нормированными мерами μ и τ, соответственно, и пусть $f\colon S \to T$ — измеримая функция (т.е. полный f-прообраз $f^{-1}(U)$ множества $U \subseteq T$ μ-измерим при любом τ-измеримом U). Функцию f назовем (μ,τ)-*пропорциональной*, если для каждых двух τ-измеримых подмножеств $U, V \subseteq T$ равенство $\tau(U) = \tau(V)$ влечет равенство $\mu(f^{-1}(U)) = \mu(f^{-1}(V))$. Если обе меры μ, τ суть вероятностные меры (например, должным образом нормированные меры Хаара), то f называется (μ,τ)-*равновероятной* (или *равновероятной относительно* μ и τ) тогда и только тогда, когда $\mu(f^{-1}(U)) = \tau(U)$ для каждого τ-измеримого $U \subseteq T$. В случае, когда $S = T$ и $\mu = \tau$ говорят, что f *сохраняет меру* μ, если равенство $\mu(f^{-1}(U)) = \mu(U)$ выполняется при каждом μ-измеримом U. Наконец, если f сохраняет меру μ и для μ-измеримого множества U равенство $f^{-1}(U) = U$ имеет место лишь в случае, когда либо $\mu(U) = 0$, либо $\mu(U) = 1$, то говорят, что функция f является μ-*эргодической* (или *эргодической относительно меры* μ). Отметим, что в метрической теории функций вместо терминов «функция, сохраняющая меру» и «равновероятная функция» используются, соответственно, термины «метрический эндоморфизм» и «метрический гомоморфизм», а в теории динамических систем вместо эргодичности говорят также о «метрической транзитивности». Поскольку во всей статье в качестве меры рассматривается только нормированная мера Хаара, то в дальнейшем указание на это опускается, и сохраняющие меру Хаара, равновероятные (соответственно, эргодические) относительно меры Хаара функции называются просто *сохраняющими меру*, *равновероятными* (соответственно, *эргодическими* или *эргодичными*).

Справедлива следующая

1.1 Теорема. *Совместимая функция* $F = (f_1, \dots, f_m)\colon {\mathbb{Z}_p}^{(n)} \to {\mathbb{Z}_p}^{(m)}$ *равновероятна* (*соответственно, сохраняет меру или эргодична*) *тогда и только тогда, когда она равновероятна* (*соответственно, биективна или транзитивна*) *по модулю* p^k *для всех* $k = 1, 2, \dots$. *Совместимая и сохраняющая меру функция* F *биективна* (*и, стало быть, является метрическим автоморфизмом*)*; кроме того, она является изометрией пространства* $\mathbb{Z}_p^{(n)}$.

Отметим, что везде в дальнейшем в данной работе при доказательстве эргодичности (равновероятности) той или иной функции относительно меры Хаара мы, фактически, доказываем ее транзитивность (равновероятность) по каждому модулю p^k, $k = 1, 2, \dots$, т.е. непосредственно устанавливаем именно те свойства, которые нас и интересуют в свете поставленных выше задач. В силу этого мы позволим себе опустить доказательство теоремы 1.1 как не имеющей прямого отношения к целям данной работы. Тем не менее, везде далее в работе мы будем употреблять соответствующую терминологию (например, говорить о функции «эргодическая» вместо «транзитивная по модулю p^k для всех $k = 1, 2, \dots$», и т.п.)

В связи с теоремой 1.1, однако, уместно заметить здесь, что результаты

данной работы в части, относящейся к описанию сохраняющих меру или эргодических функций можно трактовать как описание неархимедовых (или ультраметрических) динамических систем $(\mathbb{Z}_p^{(n)}, F)$ на фазовом пространстве $\mathbb{Z}_p^{(n)}$ с дискретным временем, где F — нерастягивающее отображение (т.е. применение F к любой паре точек не увеличивает расстояния между ними). В такой трактовке теорема 2.2, например, может рассматриваться как полное описание эргодических динамических систем из упомянутого класса при условии $p = 2$ и $n = 1$, а совместно с теоремой 3.11 дает полное описание дважды целозначных (т.е. имеющих всюду целозначную производную) эргодических динамическх систем для любого n. Эти вопросы, однако, лежат вне рамок данной работы и составят содержание одной из последующих статей.

Возвращаясь к основной теме работы, отметим, что для широкого класса совместимых функций, в некотором (точно определенном в разделе 3) смысле близких к равномерно дифференцируемым на $\mathbb{Z}_p$ функциям, свойство быть биективной по модулю p^k для некоторого определенного k эквивалентно тому, что функция сохраняет меру; последнее же эквивалентно тому, что функция биективна по модулю p^k для всех $k = 1, 2, 3, \dots$.

Свойство функции быть транзитивной по модулю p^k некоторого определенного k оказалось эквивалентным тому, что функция эргодична; последнее же эквивалентно тому, что функция транзитивна по модулю p^k для всех $k = 1, 2, 3, \dots$. Наконец, из равновероятности функции по модулю p^k для некоторого определенного k вытекает ее равновероятность; последнее же свойство эквивалентно равновероятности функции по модулю p^k для всех $k = 1, 2, 3 \dots$. Доказательства результатов такого характера приведены в разделе 3 данной работы.

Эти результаты демонстрируют впервые проявившийся в лемме Гензеля эффект гензелевского подъема, состоящий в том, что поведение функции по модулю p^{k_0} для некоторого k_0 определяет ее поведение по модулю p^k для всех $k = k_0 + 1, k_0 + 2, \dots$ и на всем пространстве $\mathbb{Z}_p$. Этот эффект уже возникал при изучении транзитивности тех или иных преобразований.

Например, необходимые и достаточные условия транзитивности полинома $f(x) = a + bx$ степени 1 с целыми рациональными коэффициентами a, b (см., например, [2; 3.2.1.2, теорема A]) могут быть сформулированы следующим образом: полином $a + bx$ транзитивен по модулю p^k для некоторого $k \geqslant 2$ тогда и только тогда, когда он транзитивен по модулю p, если p нечетно, или по модулю p^2, если $p = 2$.

Общий критерий транзитивности по модулю p^k полинома f произвольной степени с целыми рациональными коэффициентами, полученный в [15], также также демонстрирует этот эффект: при $p \neq 2, 3$ полином f транзитивен по модулю p^k, $k \geqslant 3$, тогда и только тогда, когда он транзитивен по модулю p^2; если же $p = 2$ или $p = 3$, то тогда и только тогда, когда он транзитивен по модулю p^3. Отметим попутно, что этот последний результат остается справедливым для значительно более широкого класса функций, не обязательно даже аналитических (см. 4.9–4.10).

Полученные в разделе 3 данной работы результаты показывают, что эффект гензелевского подъема таких свойств функции, как биективность или транзи-

тивность по модулю p^k, обусловлен спецификой p-адической метрики и имеет место для различных весьма широких классов функций. В разделе 4 уточняются границы значений k_0, с которых начинается этот подъем.

Результаты вышеуказанного типа полезны, если для данной функции f необходимо узнать, обладает ли она некоторым свойством (например, транзитивностью или биективностью) по модулю p^k для конкретного достаточно большого k, исключающего возможность прямой проверки. Если же, например, требуется построить из заранее заданных операций функцию, заведомо являющуюся транзитивной или биективной по модулю p^k , то предпочтительнее явные формулы. Такие формулы для биективных по модулю 2^k полиномов над кольцом рациональных целых чисел $\mathbb{Z}$ получены в [13], для транзитивных по модулю 2^k полиномов над $\mathbb{Z}$ — в [15]. Явные формулы для эргодических и сохраняющих меру совместимых функций (в частности, совместимых целозначных полиномов над $\mathbb{Q}$) на $\mathbb{Z}_2$ приведены в [11]. В данной работе приведены явные формулы, задающие совместимые эргодические или сохраняющие меру функции на $\mathbb{Z}_p$ для нечетных простых p — см. следующий раздел.

2. Явные формулы.

Напомним (см. [3]), что любая функция $f\colon \mathbb{N}_0 \to \mathbb{Z}_p$ (соответственно, $f\colon \mathbb{N}_0 \to \mathbb{Z}$) допускает единственное представление в виде т.н. *интерполяционного ряда*

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i}, \qquad (\diamondsuit)$$

где $\binom{x}{i} = \dfrac{x(x-1)\cdots(x-i+1)}{i!}$ для $i = 1, 2, \ldots$, и $\binom{x}{0} = 1$; $a_i \in \mathbb{Z}_p$ (соответственно, $a_i \in \mathbb{Z}$), $i = 0, 1, 2, \ldots$.

Если f равномерно непрерывна на $\mathbb{N}_0$ относительно p-адической метрики, то ее можно единственным образом продолжить до равномерно непрерывной на $\mathbb{Z}_p$ функции. Следовательно, интерполяционный ряд функции f сходится равномерно на $\mathbb{Z}_p$. Справедливо утверждение: ряд $f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i}$, $\quad (a_i \in \mathbb{Q}_p,\ i = 0, 1, 2, \ldots \overset{p}{)}$ сходится равномерно на $\mathbb{Z}_p$ тогда и только тогда, когда $\lim\limits_{i\to\infty} a_i = 0$, где $\lim\limits_{p}$ есть предел по p-адической метрике; при этом ряд задает равномерно непрерывную на $\mathbb{Z}_p$ функцию. Эта функция целозначна тогда и только тогда, когда $a_i \in \mathbb{Z}_p$, $i = 0, 1, 2, \ldots$.

Везде далее в этом разделе $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ равномерно непрерывная на $\mathbb{Z}_p$ функция, представленная в виде $(\diamondsuit)$. Справедливы следующие теоремы (см. [11]):

2.1 Теорема. (См. 4.3 из [11], см. также [5]) *Функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ совместима тогда и только тогда, когда*

$$a_i \equiv 0 \pmod{p^{\lfloor \log_p i \rfloor}}$$

для всех $i = p,\ p+1,\ p+2, \ldots$. (Здесь и далее $\lfloor \alpha \rfloor$ для действительного α обозначает ближайшее к α целое рациональное число, не превосходящее α.)

2.2 Теорема. (См. 4.5 из [11]) *Функция $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ совместима и сохраняет меру тогда и только тогда, когда она может быть представлена в следующем виде:*

$$f(x) = c_0 + x + \sum_{i=1}^{\infty} c_i\, 2^{\lfloor \log_2 i \rfloor + 1} \binom{x}{i},$$

где $c_0, c_1, c_2 \ldots \in \mathbb{Z}_2$.

2.3 Теорема. (См. 4.7 из [11]) *Функция $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ совместима и эргодична тогда и только тогда, когда она может быть представлена в следующем виде:*

$$f(x) = 1 + x + \sum_{i=0}^{\infty} c_i\, 2^{\lfloor \log_2 (i+1) \rfloor + 1} \binom{x}{i},$$

где $c_0, c_1, c_2 \ldots \in \mathbb{Z}_2$.

Хотя для произвольного простого p необходимость условий теорем 2.2 и 2.3 уже не имеет места, их достаточность остается справедливой. Именно, в данном разделе мы доказываем следующее утверждение.

2.4 Теорема. *Функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, где p — нечетное простое число, представленная в форме ($\diamondsuit$), совместима и сохраняет меру, если одновременно выполняются следующие сравнения:*

$$\begin{gathered} a_1 \not\equiv 0 \pmod{p}; \\ a_i \equiv 0 \pmod{p^{\lfloor \log_p i \rfloor + 1}}, \quad (i = 2, 3, \ldots). \end{gathered}$$

Функция f совместима и эргодична, если одновременно выполняются следующие сравнения:

$$\begin{gathered} a_0 \not\equiv 0 \pmod{p}; \\ a_1 \equiv 1 \pmod{p}; \\ a_i \equiv 0 \pmod{p^{\lfloor \log_p (i+1) \rfloor + 1}}, \quad (i = 2, 3, \ldots). \end{gathered}$$

Для доказательства нам понадобятся два вспомогательных результата, которые полезны и сами по себе.

2.5 Лемма. *Пусть p — произвольное простое число, $v\colon \mathbb{Z}_p \to \mathbb{Z}_p$ — совместимая функция, и пусть c, d — p-адические целые числа, причем $c \not\equiv 0 \pmod{p}$. Тогда функция $g(x) = d + cx + pv(x)$ сохраняет меру, а функция $h(x) = c + x + p\Delta v(x)$ эргодична.* (Здесь и далее Δ — оператор взятия разности: $\Delta v(x) = v(x+1) - v(x)$. Отметим, что и g, и h, очевидно, совместимы, т.к. они обе являются композициями совместимых функций.)

Доказательство леммы 2.5. Сначала индукцией по l мы покажем, что g биективна по модулю p^l для всех $l = 1, 2, 3, \ldots$. Предположение, очевидно, выполняется для $l = 1$.

Пусть, далее, предположение верно для $l = 1, 2, \ldots, k-1$. Докажем, что тогда оно выполняется и для $l = k$. Пусть $g(a) \equiv g(b) \pmod{p^k}$ для некоторых p-адических целых a, b. Тогда $a \equiv b \pmod{p^{k-1}}$ по предположению индукции. Отсюда следует, что $pv(a) \equiv pv(b) \pmod{p^k}$, поскольку v совместима. Далее, из сравнения $g(a) \equiv g(b) \pmod{p^k}$ следует, что $ca + pv(a) \equiv cb + pv(b) \pmod{p^k}$, а значит, что $ca \equiv cb \pmod{p^k}$. Поскольку $c \not\equiv 0 \pmod{p}$, из последнего сравнения вытекает, что $a \equiv b \pmod{p^k}$, что доказывает первое утверждение леммы.

Для доказательства оставшегося утверждения леммы отметим вначале, что из уже доказанного первого утверждения следует, что h сохраняет меру. Для доказательства транзитивности h по модулю p^k для всех $k = 1, 2, 3, \ldots$ вновь применим индукцию по k.

Очевидно, что h транзитивна по модулю p. Допустим, что h транзитивна по модулю p^{k-1}. Тогда, поскольку h индуцирует подстановку на кольце вычетов $\mathbb{Z}/p^k$ и является совместимой функцией, то длина любого цикла этой подстановки кратна p^{k-1}; поэтому для доказательства того, что эта подстановка имеет единственный цикл, достаточно показать, что функция

$$h^{p^{k-1}}(x) = \underbrace{h(h \ldots (h}_{p^{k-1} \text{ раз}}(x)) \ldots)$$

индуцирует подстановку с единственным циклом на идеале (p^{k-1}) кольца $\mathbb{Z}/p^k$, порожденном элементом p^{k-1}. Другими словами, достаточно показать, что функция $\frac{1}{p^{k-1}} h^{p^{k-1}}(p^{k-1}x)$ транзитивна по модулю p.

С помощью очевидных прямых вычислений последовательно получаем, что

$$h^1(x) = c + x + pv(x+1) - pv(x),$$

$$\ldots \qquad \ldots \qquad \ldots$$

$$h^j(x) = h(h^{j-1}(x)) = cj + h^{j-1}(x) + pv(h^{j-1}(x)+1) - pv(h^{j-1}(x))$$
$$= cj + x + p\sum_{i=0}^{j-1} v(h^i(x)+1) - p\sum_{i=0}^{j-1} v(h^i(x)),$$

и т.д. Напомним, что $h^0(x) = x$ по определению. Таким образом,

$$h^{p^{k-1}}(x) = cp^{k-1} + x + p\sum_{i=0}^{p^{k-1}-1} v(h^i(x)+1) - p\sum_{i=0}^{p^{k-1}-1} v(h^i(x)). \qquad (1)$$

Так как h транзитивна по модулю p^{k-1} и совместима, то

$$\sum_{i=0}^{p^{k-1}-1} v(h^i(x)+1) \equiv \sum_{i=0}^{p^{k-1}-1} v(h^i(x)) \equiv \sum_{z=0}^{p^{k-1}-1} v(z) \pmod{p^{k-1}},$$

значит, из (1) следует, что $h^{p^{k-1}}(x) \equiv cp^{k-1} + x \pmod{p^k}$. Поскольку $c \not\equiv 0 \pmod{p}$, функция $cp^{k-1} + x$, очевидно, индуцирует на идеале (p^{k-1}) подстановку, имеющую только один цикл, что и завершает доказательство леммы. $\square$

2.6 Следствие. *В условиях леммы 2.5, если p нечетно, а $r \equiv 1 (\mathrm{mod} p)$, то функция $c + rx + p\Delta v(x)$ совместима и эргодична.*

Доказательство следствия 2.6. Имеем $r = 1 + ps$ для подходящего $s \in \mathbb{Z}_p$. Далее, поскольку p нечетно, то функция $s\binom{x}{2}$ совместима; значит, и функция $v_1(x) = s\binom{x}{2} + v(x)$ совместима. Однако $\Delta v_1(x) = sx + \Delta v(x)$, и нам достаточно лишь применить лемму 2.5 для завершения доказательства следствия. □

Доказательство теоремы 2.4. Заметим, что в силу 2.1 совместимая функция $v(x)$ может быть представлена в следующем виде:

$$v(x) = a + \sum_{i=1}^{\infty} b_i p^{\lfloor \log_p i \rfloor} \binom{x}{i},$$

где $a, b_1, b_2, \ldots \in \mathbb{Z}_p$. Поскольку $\lfloor \log_p i \rfloor = \lfloor \log_p (i+1) \rfloor$ для всех $i = 1, 2, \ldots$, кроме $i = p^t - 1$, $(t = 1, 2, 3, \ldots)$, и так как

$$\Delta v(x) = \sum_{i=1}^{\infty} b_i p^{\lfloor \log_p i \rfloor} \binom{x}{i-1}, \tag{1}$$

мы завершаем доказательство теоремы, применяя 2.5 и 2.6. □

При $p = 2$ доказанные выше результаты позволяют получить еще один полезный критерий того, когда функция совместима и сохраняет меру (или является эргодической).

2.7 Теорема. *Функция $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ совместима и сохраняет меру (соответственно, совместима и эргодична) тогда и только тогда, когда ее можно представить в виде $f(x) = c + x + 2v(x)$ (соответственно, $f(x) = 1 + x + 2\Delta v(x)$), где $c \in \mathbb{Z}_2$, а $v(x)$ — совместимая функция.*

Доказательство. Легко следует из 2.1–2.3 и 2.5 в комбинации с равенством (1) из доказательства теоремы 2.4. □

Лемму 2.5, следствие 2.6 и теорему 2.7 можно применить к задаче построения сохраняющих меру или эргодических функций как композиций заранее заданных совместимых функций. Например, полагая $v(x) = (x^2)\,\mathrm{XOR}(x + 32\,\mathrm{AND}\,x)$ (эта функция совместима как композиция совместимых функций) мы получаем, что функция

$$7 + x + 2((x^2 + 2x + 1)\,\mathrm{XOR}(x + 1 + 32\,\mathrm{AND}(x+1))) - 2(x^2\,\mathrm{XOR}(x + 32\,\mathrm{AND}\,x))$$

эргодична — факт, который непросто установить непосредственным применением теорем 2.2 и 2.3. Кстати, для случая $p = 2$ теорему 2.7 можно слегка переформулировать, сделав чуть более простым ее применение для построения эргодических функций с помощью операции сложения и поразрядных логических операций типа поразрядного исключительного «или», XOR, поразрядного «и», AND или NEG, поразрядной инверсии. Именно, легко видеть, что в кольце $\mathbb{Z}_2$ выполняется следующее тождество: $z + \mathrm{NEG}(z) = -1$. Значит, $\Delta v(x) = v(x+1) - v(x) = v(x+1) + \mathrm{NEG}(v(x)) + 1$, и мы получаем следующее

2.8 Предложение. *Функция $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ совместима и эргодична тогда и только тогда, когда она может быть представлена в любом из следующих видов:*

$$f(x) = 1 + x + 2(v(x+1) + \mathrm{NEG}\, v(x)),$$
$$f(x) = 2 + x + 2v(x+1) + \mathrm{NEG}(2v(x)),$$
$$f(x) = 3 + x + 2v(x+1) + 2\mathrm{NEG}v(x),$$

где $v\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ – произвольная совместимая функция.

Поскольку умножение на 2 есть просто сдвиг двоичной записи числа на 1 разряд в сторону старших разрядов, предложение 2.8 можно применять при построении псевдослучайных генераторов на основе «быстрых» компьютерных команд типа сложения, поразрядных логических операций и сдвигов в сторону старших разрядов, задавая функцию v как композицию этих операций.

Также стоит отметить, что все функции, описанные в 2.4 – 2.8 «аффинны по модулю p», т.е. задают на $\mathbb{Z}/p$ преобразования вида $x \mapsto a + bx$.

3. Гензелевский подъем.

В данном разделе мы изучаем условия, при которых функция, обладающая одним важным (определяемым ниже) свойством равномерной дифференцируемости по модулю p^k, будет равновероятной, или эргодичной, или сохраняющей меру. Результаты этого раздела, как правило, демонстрируют упомянутый во введении эффект: из того, что функция F обладает некоторым свойством по модулю p^{k_0} вытекает, что она обладает этим свойством по любому модулю p^n для всех $n \geqslant k_0$. Кроме того, уместно заметить, что результаты этого раздела, в отличие от результатов предыдущего, позволяют строить сохраняющие меру или эргодические функции, которые не обязательно аффинны по модулю p. Фактически, на основе результатов этого раздела может быть развита некоторая техника, позволяющая «поднимать» произвольное транзитивное преобразование кольца $\mathbb{Z}/p^{k_0}$ до функции на $\mathbb{Z}_p$, транзитивной по модулю p^k для всех $k = k_0, k_0+1, k_0+2, \dots$. Именно по этой причине мы вводим ниже понятие асимптотически совместимой функции. Сама же эта техника не рассматривается здесь, а составит предмет следующей статьи.

Вначале напомним несколько определений, обобщающих некоторые из наших основных понятий (см. 5.1 из [11]).

3.1 Определение. Пусть $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ — некоторая функция, не обязательно совместимая. Функция F называется (*асимптотически*) *равновероятной*, если для всех $k = 1, 2, \dots$ (соответственно, всех достаточно больших $k \in \mathbb{N}$) она *равновероятна по модулю* p^k, т.е. ограничение $F \bmod p^k = (f_1 \bmod p^k, \dots, f_m \bmod p^k)$ функции F на множество $\{0, 1, \dots, p^k - 1\}^{(n)}$ есть равновероятная функция. (Отметим, что мы в случаях, когда это не вызывает недоразумений, отождествляем множество $\{0, 1, \dots, p^k - 1\}^{(n)}$ со множеством всех элементов кольца $(\mathbb{Z}/p^k)^{(n)}$). Аналогично, мы говорим, что F *асимптотически сохраняет меру* (соответственно, что F *асимптотически эргодична*), если $F \bmod p^k$ есть биективная (соответственно, транзитивная) функция

на $(\mathbb{Z}/p^k)^{(n)}$ для всех достаточно больших k. Наконец, будем говорить, что F *асимптотически совместима*, если найдется положительное рациональное целое N такое, что для всех $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_p^{(n)}$ и всех $k \geqslant N$ из сравнения $\mathbf{a} \equiv \mathbf{b} \pmod{p^k}$ вытекает сравнение $F(\mathbf{a}) \equiv F(\mathbf{b}) \pmod{p^k}$.

По определению, для $\mathbf{a} = (a_1, \dots, a_n)$ и $\mathbf{b} = (b_1, \dots, b_n)$ из $\mathbb{Q}_p^{(n)}$ сравнение $\mathbf{a} \equiv \mathbf{b} \pmod{p^s}$ означает, что $\|a_i - b_i\|_p \leqslant p^{-s}$ (или, что то же самое, что $a_i = b_i + c_i p^s$ для подходящих $c_i \in \mathbb{Z}_p$), $i = 1, 2, \dots, s$, т.е. что $\|\mathbf{a} - \mathbf{b}\|_p \leqslant p^{-s}$. Другими словами, функция асимптотически совместима, если для некоторого $N \in \mathbb{N}_0$ она удовлетворяет условию Липшица с коэффициентом 1 для всех пар точек, находящихся одна от другой на расстоянии меньшем, чем p^{-N}. Ввиду компактности пространства $\mathbb{Z}_p^{(n)}$ сказанное означает, что функция F асимптотически совместима тогда и только тогда, когда она удовлетворяет условию Липщица с константой 1 локально.

Для удобства читателя напомним еще некоторые сведения из [11]. Функция $F = (f_1, \dots, f_m) \colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ называется *дифференцируемой по модулю* p^k в точке $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{Z}_p^{(n)}$, если найдутся положительное рациональное целое N и матрица $F'_k(\mathbf{u})$ размера $n \times m$ над $\mathbb{Q}_p$ (называемая *матрицей Якоби по модулю* p^k функции F в точке $\mathbf{u}$) такие, что для любого положительного рационального целого $K \geqslant N$ и любого $\mathbf{h} = (h_1, \dots, h_n) \in \mathbb{Z}_p^{(n)}$ при выполнении неравенства $\|\mathbf{h}\|_p \leqslant p^{-K}$ выполняется сравнение

$$F(\mathbf{u} + \mathbf{h}) \equiv F(\mathbf{u}) + \mathbf{h}F'_p(\mathbf{u}) \pmod{p^{k+K}}. \qquad (\heartsuit)$$

В случае $m = 1$ матрица Якоби по модулю p^k называется *дифференциалом по модулю* p^k. При $m = n$ определитель матрицы Якоби по модулю p^k называется *якобианом по модулю* p^k. Элементы матрицы Якоби по модулю p^k называются *частными производными по модулю* p^k функции F в точке $\mathbf{u}$. Частную производную (соответственно, дифференциал) по модулю p^k будем иногда обозначать как $\frac{\partial_k f_i(\mathbf{u})}{\partial_k x_j}$ (соответственно, как $d_k F(\mathbf{u}) = \sum_{i=1}^n \frac{\partial_k F(\mathbf{u})}{\partial_k x_i} d_k x_i$).

Из приведенного определения сразу следует, что частные производные по модулю p^k функции F определены с точностью до целого p-адического слагаемого с нормой, не превосходящей p^{-k}. В случае, когда все частные производные по модулю p^k во всех точках из $\mathbb{Z}_p^{(n)}$ являются целыми p-адическими числами, будем говорить, что функция F имеет *целозначную производную по модулю* p^k; при этом каждой частной производной по модулю p^k сопоставляется однозначно определенный элемент кольца вычетов $\mathbb{Z}/p^k$, а матрица Якоби по модулю p^k в каждой точке $u \in \mathbb{Z}_p^{(n)}$ рассматривается как матрица над кольцом $\mathbb{Z}/p^k$.

При таком соглашении «правила дифференцирования по модулю p^k» имеют ту же форму, что и в случае обычного дифференцирования. , с той лишь разницей, что равенства заменяются на сравнения по модулю p^k. Например, если функции $G \colon \mathbb{Z}_p^{(s)} \to \mathbb{Z}_p^{(n)}$ и $F \colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ обе дифференцируемы по модулю p^k в точках, соответственно, $\mathbf{v} = (v_1, \dots, v_s)$ и $\mathbf{u} = G(\mathbf{v})$, причем их частные производные по модулю p^k в этих точках являются целыми p-адическими числами, то композиция $F \circ G \colon \mathbb{Z}_p^{(s)} \to \mathbb{Z}_p^{(m)}$ этих функций дифференцируема по модулю p^k в точке $\mathbf{v}$, значения всех ее частных производных по модулю p^k в этой точке являются целыми p-адическими числами, и $(F \circ G)'_k(\mathbf{v}) \equiv G'_k(\mathbf{v}) F'_k(\mathbf{u}) \pmod{p^k}$.

По аналогии с классическим определением для функции F вводится понятие *равномерной дифференцируемости на $\mathbb{Z}_p^{(n)}$ по модулю p^k*; наименьшее $K \in \mathbb{N}$ такое, что ($\heartsuit$) выполняется сразу для всех $\mathbf{u} \in \mathbb{Z}_p^{(n)}$ как только $\|h_i\|_p \leqslant p^{-K} (i = 1, 2, \ldots, n)$ обозначается через $N_k(F)$. Этот последний параметр играет важную роль в дальнейшей теории.

Напомним, что, согласно 2.12 из [11], если функция F равномерно дифференцируема по модулю p^k на $\mathbb{Z}_p^{(n)}$, то все ее частные производные по модулю p^k являются периодическими функциями с периодом $p^{N_k(F)}$. Это, в частности, означает, что каждую частную производную по модулю p^k можно рассматривать как функцию, заданную на кольце вычетов $\mathbb{Z}/p^{N_k(F)}$. Более того, если функция $F = (f_1, \ldots, f_m)\colon \mathbb{N}_0^{(n)} \to \mathbb{N}_0^{(m)}$ может быть продолжена до равномерно дифференцируемой по модулю p^k функции на все пространство $\mathbb{Z}_p^{(n)}$, то она может быть продолжена вместе со всеми своими производными по модулю p^k.

Везде далее $F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ и $f\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p$ — равномерно дифференцируемые по модулю p функции. Это относительно слабое ограничение, поскольку все равномерно дифференцируемые на $\mathbb{Z}_p^{(n)}$ функции, а также все равномерно дифференцируемые по модулю p^k для некоторого $k \geqslant 1$ функции равномерно дифференцируемы по модулю p на $\mathbb{Z}_p^{(n)}$.

Примеры функций, не являющихся равномерно дифференцируемыми, но тем не менее равномерно дифференцируемых по модулю p дают функция $f(x, y) = x \operatorname{XOR} y$ при $p = 2$ и ее соответствующие аналоги при $p \neq 2$; все частные производные по модулю p этих функций сравнимы с 1 по модулю p во всех точках (см. [11]). Заметим кстати, что функция «приведения по модулю p^n», т.е. введенная ранее функция $\mathrm{mod} p^n\colon \mathbb{Z}_p \to \mathbb{Z}/p^n$ равномерно дифференцируема на $\mathbb{Z}_p$ (ее производная равна 0 во всех точках); функция $f(x, y) = x \operatorname{AND} y$ не является дифференцируемой по модулю 2 ни в одной точке из $\mathbb{Z}_2^{(2)}$ (как функция двух переменных), однако она равномерно дифференцируема по x при каждом $y \in \mathbb{Z}$: ее производная равна 0 если $y \geqslant 0$, и 1 в противном случае.

Оказывается, свойство функции асимптотически сохранять меру или быть асимптотически совместимой, налагает определенные ограничения на значения нормы производной по модулю p.

3.2 Предложение. *Если функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ асимптотически сохраняет меру, то $\|f_1'(u)\|_p \geqslant 1$ во всех точках $u \in \mathbb{Z}_p$.*

Доказательство. Поскольку каждая частная производная по модулю p^k функции f периодична с периодом $p^{N_k(f)}$, утверждение достаточно доказать лишь для точек $u \in \mathbb{N}_0$. Из определения дифференцируемости по модулю p^k следует, что при $K \geqslant N_1(f)$ и $u \in \mathbb{N}_0$ условие

$$f(u + h) \equiv f(u) + h f_1'(u) \pmod{p^{K+1}} \tag{1}$$

выполняется как только $\|h\|_p \leqslant p^{-K}$. Если бы $\|f_1'(u)\|_p < 1$ для некоторого $u \in \mathbb{N}_0$, то из условия $f_1'(u) \equiv 0 \pmod p$ и сравнения (1) следовало бы, что $f(u + p^K) \equiv f(u) \pmod{p^{K+1}}$. Последнее сравнение означает, что для всех $K \geqslant N_1(f)$, таких что $u + p^K \leqslant p^{K+1} - 1$ функция f не является биективной по модулю p^{K+1}. Противоречие. $\square$

3.3 Следствие. *Если в условиях 3.2 функция f равномерно дифференцируема, то $\|f'(u)\|_p \geqslant 1$ для всех $u \in \mathbb{Z}_p$.*

Доказательство. Из определения производной по модулю p немедленно следует, что

$$f_1'(u) \equiv f'(u) \pmod{p}$$

для всех $u \in \mathbb{Z}_p$. Поэтому $f'(u) = f_1'(u) + ps(u)$ для подходящей функции $s\colon \mathbb{Z}_p \to \mathbb{Z}_p$. Однако если $\|f_1'(u)\|_p \geqslant 1$, то из последнего равенства с очевидностью вытекает, что $\|f'(u)\|_p \geqslant 1$ по свойствам p-адической метрики. Теперь утверждение следует из 3.2. $\square$

Утверждение, обратное к 3.2 неверно: очевидным контрпримером служит функция $\frac{x^2-x}{2}$ на $\mathbb{Z}_2$. Она обращается в 0 в точках 0 и 1, но ее производная имеет норму 2. Тем не менее, функции такого типа локально инъективны. Более точно, справедливо следующее

3.4 Предложение. *Если функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ равномерно дифференцируема по модулю p, и если $\|f_1'(u)\|_p \geqslant 1$, то пространство $\mathbb{Z}_p$ можно представить в виде объединения конечного числа попарно непересекающихся открытых (эквивалентно, замкнутых) шаров U, для которых справедливо следующее: если $a, b \in U$, $k \geqslant N_1(f)$ и $a \not\equiv b \pmod{p^k}$, то $f(a) \not\equiv f(b) \pmod{p^k}$.*

Доказательство. Рассмотрим объединение

$$\mathbb{Z}_p = \bigcup_{a=0}^{p^N-1} (a + p^N\mathbb{Z}_p),$$

где $N = N_1(f)$. Каждое множество $U = a + p^N\mathbb{Z}_p$ есть открытый и одновременно замкнутый шар радиуса p^{-N} (см. [3]). Пусть $u, v \in U$, и пусть $u \neq v$. Тогда $v = u + h$, где $\|h\|_p = p^{-K}$ для некоторого положительного рационального целого $K \geqslant N$. Из определения дифференцируемости по модулю p следует, что

$$f(u + h) \equiv f(u) + hf_1'(u) \pmod{p^{K+1}}. \tag{1}$$

Поэтому, если $f(u) \equiv f(v) \pmod{p^K}$, то из (1) вытекает, что $\|f_1'(u)\|_p = p^{-1} < 1$. Противоречие. $\square$

Из этого предложения следует, что если норма производной по модулю p некоторой равномерно дифференцируемой по модулю p функции не менее 1 всюду на $\mathbb{Z}_p$, то функция, может быть, «склеивает по модулю p^k» при достаточно больших k лишь те точки, которые лежат в разных шарах, упомянутых в 3.4. Отсюда следует

3.5 Предложение. *Пусть $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ — равномерно дифференцируемая по модулю p функция. Она асимптотически сохраняет меру тогда и только тогда, когда одновременно выполняются следующие условия:*

(1) $\|f_1'(u)\|_p \geqslant 1$ *во всех точках* $u \in \mathbb{Z}_p$;
(2) $f(a) \not\equiv f(b) \pmod{p^n}$ *для всех* $n, a, b \in \mathbb{N}_0$ *таких, что* $\|a - b\|_p \geqslant p^{-N_1(f)}$ *и* $0 \leqslant a, b \leqslant p^n - 1$. $\square$

А.А.Нечаев заметил, что функция $f(x) = \frac{x^2+x}{2}$ на $\mathbb{Z}_2$ асимптотически сохраняет меру (это может быть выведено также из 3.5). Поэтому, если $g\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ — совместимая функция, сохраняющая меру (все такие функции описаны, см. 2.2), то композиция $h(x) = g(f(x))$ есть равномерно дифференцируемая по модулю $p = 2$ функция, асимптотически сохраняющая меру, причем $\|g_1'(u)\|_2 = 2$ во всех точках из $u \in \mathbb{Z}_2$. Других равномерно дифференцируемых по модулю p функций $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, асимптотически сохраняющих меру и имеющих производные по модулю p, норма которых не меньше чем 1 нигде на $\mathbb{Z}_p$, не существует (см. [10]). Доказательство этого последнего утверждения использует не только аппарат p-адического анализа, но и методы алгебраической геометрии.

Последнее замечание, в частности, иллюстрирует тот факт, что второе из условий критерия 3.5 достаточно сложно проверяемо, поскольку необходимо вычислять значения функции в бесконечном числе точек. Но проблему можно упростить, наложив на исследуемую функцию f дополнительное ограничение. Именно, будем считать, что f отображает каждый шар радиуса p^{-M} (где $M \geqslant N_1(f)$) в шар радиуса p^{-M}, (следовательно, является асимптотически совместимой). Это ограничение эквивалентно тому, что функция f имеет целозначную производную по модулю p.

3.6 Предложение. *Если для некоторого $M \geqslant N_1(f)$ равномерно дифференцируемая по по модулю p функция f отображает каждый шар радиуса p^{-M} в шар радиуса p^{-M}, то $f_1'(a) \in \mathbb{Z}_p$ для всех $a \in \mathbb{Z}_p$. Обратно, равномерно дифференцируемая по модулю p функция, имеющая целозначную производную по модулю p, отображает каждый шар радиуса p^{-M} в шар радиуса p^{-M} для всех $M \geqslant N_1(f)$.*

Доказательство. Если $M \geqslant N_1(f)$ и $\|h\|_p \leqslant p^{-M}$, то из определения равномерной дифференцируемости по модулю p^k (см. 2.4 из [11]) следует, что

$$f(u+h) \equiv f(u) + hf_1'(u) \pmod{p^{M+1}} \tag{1}$$

для всех $u \in \mathbb{Z}_p$. С другой стороны, из включения $f(a + p^M\mathbb{Z}_p) \subseteq f(a) + p^M\mathbb{Z}_p$ следует, что

$$\|f(u+h) - f(u)\|_p \leqslant p^{-M} \tag{2}$$

для всех h таких, что $\|h\|_p \leqslant p^{-M}$. Сравнивая (1) и (2), мы видим, что $\|f_1'(u)\|_p \leqslant 1$. Обратное утверждение эквивалентно асимптотической совместимости функции f (см 2.10 из [11]). $\square$

Везде далее мы дополнительно считаем, что функции f и F имеют целозначные производные по модулю p. В частности, это означает, что функции f и F асимптотически совместимы (см. 2.10 и 2.11 из [11]). Сформулируем теперь необходимые и достаточные условия того, чтобы функция F сохраняла меру, и достаточные условия того, чтобы функция F была равновероятной.

3.7 Теорема. *Пусть $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ — равномерно дифференцируемая по модулю p функция, имеющая целозначные производные по модулю*

p всюду на $\mathbb{Z}_p$. Тогда F асимптотически равновероятна, если она равновероятна по модулю p^k для некоторого $k \geqslant N_1(F)$ и ранг ее матрицы Якоби $F_1'(u)$ по модулю p равен m во всех точках $u = (u_1, \dots, u_n) \in (\mathbb{Z}/p^k)^{(n)}$.

Доказательство. Для $\xi \in (\mathbb{Z}/p^s)^{(m)}$ обозначим $F_s^{-1}(\xi) = \{\gamma \in (\mathbb{Z}/p^s)^{(n)} : F(\gamma) \equiv \xi \pmod{p^s}\}$. Пусть $s \geqslant k \geqslant N_1(F)$. Так как F асимптотически совместима, то, поскольку F есть сумма совместимой функции и периодической функции с периодом $p^{N_1(F)}$ (см. 2.10 из [11]), мы заключаем, что если $\eta \in F_{s+1}^{-1}(\xi)$, то $\bar{\eta} \in F_s^{-1}(\bar{\xi})$. Здесь, как мы условились во введении, $\bar{\alpha} = (\bar{\alpha}_1, \dots, \bar{\alpha}_m) \in (\mathbb{Z}/p^s)^{(m)}$ обозначает $\alpha \bmod p^s = (\alpha_1 \bmod p^s, \dots, \alpha_m \bmod p^s)$, где $\alpha = (\alpha_1, \dots, \alpha_m) \in (\mathbb{Z}/p^{s+1})^{(m)}$. Положим $\lambda = \bar{\eta} + p^s\sigma \in (\mathbb{Z}/p^{s+1})^{(n)}$, где $\sigma \in (\mathbb{Z}/p)^{(n)}$. Ввиду равномерной дифференцируемости функции F по модулю p, (см. ($\heartsuit$)) имеем

$$F(\lambda) \equiv F(\eta) + p^s\sigma F_1'(\bar{\eta}) \pmod{p^{s+1}}. \tag{1}$$

Поскольку $F(\bar{\eta}) \equiv \bar{\xi} + p^k\beta \pmod{p^{s+1}}, \xi = \bar{\xi} + p^s\gamma$ для подходящих $\beta, \gamma \in (\mathbb{Z}/p)^{(m)}$, то из (1) следует, что $\lambda \in F_{s+1}^{-1}(\xi)$ тогда и только тогда, когда $\bar{\lambda} \in F_s^{-1}(\xi)$ (т.е. когда $\bar{\eta} \in F_s^{-1}(\xi)$) и координаты вектора α удовлетворяют следующей системе линейных уравнений над полем $\mathbb{Z}/p$:

$$\beta + \alpha F_1'(\bar{\eta}) = \gamma. \tag{2}$$

Таким образом, если столбцы матрцы $F_1'(\bar{\eta})$ линейно независимы над полем $\mathbb{Z}/p$, то система (2) имеет в точности p^{n-m} различных решений при любых $\beta, \gamma \in (\mathbb{Z}/p)^{(m)}$. Отсюда следует, что

$$|F_{s+1}^{-1}(\xi)| = |F_s^{-1}(\xi)|p^{n-m}. \tag{3}$$

Значит, если F равновероятна по модулю p^k (т.е., если $|F_s^{-1}(\bar{\xi})|$ не зависит от $\bar{\xi}$) и ранг матрицы $F_1'(\bar{\eta})$ равен m, то из (3) следует, что F равновероятна по модулю p^{s+1}. $\square$

3.8 Следствия. 1° *Положим $m = 1$ в условиях теоремы 3.7. Тогда F асимптотически равновероятна, если F равновероятна по модулю p^k для некоторого $k \geqslant N_1(F)$, и дифференциал d_1F по модулю p функции F не обращается в 0 ни в одной точке из $(\mathbb{Z}/p^k)^{(n)}$.*

2° *Пусть $f(x_1, \dots, x_n)$ — полином с целыми p-адическими коэффициентами от переменных $x_1, \dots, x_n$. Полином f равновероятен, если он равновероятен по модулю p и все его частные производные не обращаются одновременно в 0 по модулю p ни в одной точке из $(\mathbb{Z}/p)^{(n)}$.*

Доказательство. Утверждение 1° есть тривиальное следствие теоремы 3.7. В свою очередь, 2° сразу следует из 1°, поскольку для всех $f \in \mathbb{Z}[x_1, \dots, x_n]$ имеет место $N_1(f) \leqslant 1$. Осталось доказать последнее неравенство.

По формуле Тейлора,

$$f(x_1 + h_1, \dots, x_n + h_n) = f(x_1, \dots, x_n) + \sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i} + Q \tag{1}$$

где $Q \in \mathbb{Z}[x_1, \dots, x_n, h_1, \dots, h_n]$, и каждый моном в каноническом представлении полинома Q имеет по переменным $h_1, \dots, h_n$ степень не менее 2. Поэтому при $\|(h_1, \dots, h_n)\|_p = p^{-s}$, где $s \geqslant 1$, для всех значений $x_1, \dots, x_n$ мы имеем $Q \equiv 0 \pmod{p^{2s}}$. Ввиду (1) это доказывает утверждение. $\square$

В случае $m = n$ сформулированные выше достаточные условия равновероятности являются и необходимыми.

3.9 Теорема. *Равномерно дифференцируемая по модулю p функция $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(n)}$, имеющая целозначную производную по модулю p, асимптотически сохраняет меру тогда и только тогда, когда она биективна по модулю $p^{N_1(F)}$ и якобиан по модулю p функции F не обращается в 0 ни в одной точке из $(\mathbb{Z}/p^{N_1(F)})^{(n)}$ (эквивалентно, тогда и только тогда, когда она биективна по модулю $p^{N_1(F)+1}$).*

Доказательство. Если F биективна по модулю $p^{N_1(F)}$ и ее якобиан по модулю p нигде не обращается в 0, то ввиду 3.7 функция F асимптотически равновероятна, и поскольку $m = n$, то F асимптотически сохраняет меру.

Обратно, пусть F асимптотически сохраняет меру, т.е. пусть F биективна по модулю p^k для всех $k \geqslant N$, где N – некоторое положительное рациональное целое. Пусть $k \geqslant \max\{N, N_1(F)\}$, тогда из определения равномерной дифференцируемости по модулю p следует, что

$$F(u + p^k\alpha) \equiv F(u) + p^k\alpha F_1'(u) \pmod{p^{k+1}} \tag{1}$$

для всех $u, \alpha \in \mathbb{Z}_p$. Здесь $F_1'(u)$ – матрица размера $n \times n$ над полем $\mathbb{Z}/p$. Если $\det F_1'(u) \equiv 0 \pmod{p}$ для некоторого $u \in \mathbb{Z}_p^{(n)}$ (или, эквивалентно, для некоторого $u \in \{0, 1, \dots, p^{N_1(F)} - 1\}^{(n)}$ ввиду периодичности частных производных по модулю p), то существует $\alpha \in \{0, 1, \dots, p-1\}^{(n)}, \alpha \not\equiv (0, \dots, 0) \pmod{p}$, такое, что $\alpha F_1'(u) \equiv (0, \dots, 0) \pmod{p}$. Но в этом случае из (1) следует, что $F(u + p^k\alpha) \equiv F(u) \pmod{p^{k+1}}$. Это противоречит биективности функции F по модулю p^{k+1}, поскольку для $u \in \{0, 1, \dots, p^{N_1(F)} - 1\}^{(n)}$ имеем $u, u + p^k\alpha \in \{0, 1, \dots, p^{k+1} - 1\}^{(n)}$ и $u + p^k\alpha \neq u$.

Теперь докажем критерий в эквивалентной формулировке. Пусть F – биективная по модулю $p^{N_1(F)}$ функция. Тогда, полагая $k = N_1(F)$ в проведенном выше рассуждении, получаем, что $\det F_1'(u) \not\equiv 0 \pmod{p}$ для всех $u \in \mathbb{Z}_p^{(n)}$. Согласно 3.7, отсюда вытекает, что F асимптотически сохраняет меру.

Допустим, что F асимптотически сохраняет меру, но не является биективной по модулю p^k для некоторого $k \geqslant N_1(F)$. Докажем, что в этом случае F не будет биективна по модулю p^{k+1}. Выберем $u, v \in \{0, 1, \dots, p^k - 1\}^{(n)}$ так, чтобы $u \neq v$ и $F(u) \equiv F(v) \pmod{p^k}$. Тогда либо $F(u) \equiv F(v) \pmod{p^{k+1}}$ (т.е. F не биективна по модулю p^{k+1}), либо $F(u) \not\equiv F(v) \pmod{p^{k+1}}$. Однако в последнем случае $F(u) \equiv F(v) + p^k\alpha \pmod{p^{k+1}}$ для некоторого $\alpha \in \{0, 1, \dots, p-1\}^{(n)}$, $\alpha \not\equiv (0, \dots, 0) \pmod{p}$. Рассмотрим $u_1 = u + p^k\beta$, где $\beta \in \{0, 1, \dots, p-1\}^{(n)}$, причем $\beta \not\equiv (0, \dots, 0) \pmod{p}$ и $\beta F_1'(u) + \alpha \equiv (0, \dots, 0) \pmod{p}$. Такой элемент β существует, поскольку F асимптотически сохраняет меру и, следовательно, $\det F_1'(u) \not\equiv 0 \pmod{p}$, как только что было доказано. Из определения равномерной дифференцируемости по модулю p следует тогда, что

$$F(u+p^k\beta) \equiv F(u)+p^k\beta F_1'(u) \equiv F(v)+p^k\alpha+p^k\beta F_1'(u) \equiv F(v) \pmod{p^{k+1}}, \tag{2}$$

где $u + p^k\beta \in \{0, 1, \dots, p^{k+1} - 1\}^{(n)}$ и $u + p^k\alpha \neq v$ (так как $u \neq v$). Поэтому из (2) совместно с нашим предположением вытекает, то F не биективна по модулю p^{k+1}. Повторяя это рассуждение необходимое число раз, заключаем, что F не биективна по модулю p^s для всех $s \geqslant k$. Однако в то же время F асимптотически сохраняет меру. Противоречие. $\square$

3.10 Следствия. 1° *Если $n = 1$ в условиях теоремы 3.9, то F асимптотически сохраняет меру в том и только в том случае, когда она биективна по модулю $p^{N_1(F)}$ и ее производная по модулю p не обращается в 0 на множестве $\{0, 1, \dots, p^{N_1(F)} - 1\}$.*

2° (см. [8] , гл. 4, разделы 4 и 5) *Пусть $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(n)}$, где $f_i(x_1, \dots, x_n) \in \mathbb{Z}_p[x_1, \dots, x_n]$, $i = 1, 2, \dots, n$. Тогда F сохраняет меру в том и только в том случае, когда F биективна по модулю p и $\det F'(u) \not\equiv 0 \pmod p$ для всех $u \in \{0, 1, \dots, p-1\}^{(n)}$ (эквивалентно, тогда и только тогда, когда F биективна по модулю p^2).*

3° *Если $A = \langle \mathbb{Z}_p; \Omega \rangle$ – универсальная алгебра с конечной сигнатурой Ω, и если все операции из Ω являются равномерно дифференцируемыми по модулю p функциями с целозначными производными по модулю p, то полином над A задает асимптотически сохраняющую меру функцию он биективен по модулю $p^{k(A)}$, где $k(A) = \max\{N_1(\omega) : \omega \in \Omega\} + 1$.*

Доказательство. Утверждение 1° тривиально следует из 3.9. Утверждение 2° справедливо ввиду 3.9, поскольку $N_1(F) \leqslant 1$ (см. доказательство следствия 3.8). Композиция $F \circ G$ функций F и G, которые обе равномерно дифференцируемы по модулю p и имеют целозначные производные по модулю p, сама равномерно дифференцируема по модулю p, имеет целозначную производную по модулю p и $N_1(F \circ G) \leqslant \max\{N_1(F), N_1(G)\}$. Последнее доказывает утверждение 3°. $\square$

При сравнении утверждений 3.7 и 3.9 возникает естественный вопрос, не являются ли достаточные условия из 3.7 также и необходимыми. Ответ на него отрицателен: соответствующий контрпример может быть построен на основе результатов из [9].

Рассмотрим функцию $f(x, y) = 2x + y^3$ на $\mathbb{Z}_2$. Так как f – полином над $\mathbb{Z}$, то он является равномерно дифференцируемой функцией с целозначной производной, и $df = 2dx + 3y^2dy$. Таким образом, $df \equiv 0 \pmod 2$, если $y \equiv 0 \pmod 2$. Тем не менее, f индуцирует равновероятную функцию $(\mathbb{Z}/2^n)^{(2)} \to \mathbb{Z}/2^n$ при каждом $n = 1, 2, \dots$. Докажем это.

При $n = 1$ имеем, что $f(x, y) \equiv y \pmod 2$ равновероятна на $\mathbb{Z}/2$. Пусть $n > 1$. Покажем, что для каждого $z \in \mathbb{Z}/2^n$ существует в точности 2^n пар (x, y) таких, что $f(x, y) \equiv z \pmod{2^n}$ и $(x, y) \in \{0, 1, \dots, 2^n - 1\}^{(2)}$.

В самом деле, если $z = 1 + 2r$ для некоторого $r \in \{0, 1, \dots, 2^{n-1} - 1\}$, то тогда $y = 1 + 2k$ для некоторого $k \in \{0, 1, \dots, 2^{n-1} - 1\}$. Таким образом, из сравнения $2x + (1 + 2k)^3 \equiv 1 + 2r \pmod{2^n}$ следует, что $x + 3k + 6k^2 + 4k^3 \equiv r \pmod{2^{n-1}}$. Левая часть последнего сравнения есть полиномиальная функция $\varphi(x, k)$ от переменных x, k. Она равновероятна ввиду 3.8, 2°, поскольку $d\varphi \equiv dx + dk \pmod 2$ (и, следовательно, этот дифференциал нигде не обращается в 0 по модулю 2) и $\varphi \equiv x + k \pmod 2$, т.е., очевидно, равновероятна по модулю 2.

Отсюда следует, что сравнение $\varphi(x,k) \equiv r \pmod{2^{n-1}}$ с неизвестными x, k имеет в точности 2^{n-1} решений в $\{0,1,\dots,2^{n-1}-1\}^{(2)}$.

Если $z = 2r$ для некоторого $r \in \{0,1,\dots,2^{n-1}-1\}$, то тогда $y = 2k$ для подходящего $k \in \{0,1,\dots,2^{n-1}-1\}$ и, следовательно, из сравнения $f(x,y) \equiv z \pmod{2^n}$ вытекает сравнение $x+4k^3 \equiv r \pmod{2^{n-1}}$. И опять функция $\psi(x,k)$ в левой части последнего сравнения равновероятна ввиду 3.8, 2°, поскольку $d\psi \equiv dx \pmod 2$ не обращается в 0 по модулю 2 нигде на $(\mathbb{Z}/2)^{(2)}$ и $\psi \equiv x \pmod 2$ равновероятна по модулю 2. Отсюда следует, что сравнение $f(x,y) \equiv 2r \pmod{2^n}$ с неизвестными x, y имеет в точности 2^n решений в $\{0,1,\dots,2^n-1\}^{(2)}$. Окончательно заключаем, что f равновероятна.

Мы начинаем изучать асимптотически эргодические функции в классе всех равномерно дифференцируемых по модулю p функций, имеющих целозначные производные по модулю p. Оказывается, такие функции существуют только в размерности 1. Точнее, справедливо следующая

3.11 Теорема. *Пусть $F = (f_1,\dots,f_n)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(n)}$ – равномерно дифференцируемая по модулю p и асимптотически эргодическая функция, имеющая целозначную производную по модулю p. Тогда $n = 1$.*

Доказательство. Нам понадобятся две леммы.

3.12 Лемма. *Если $f\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p$ – равномерно дифференцируемая по модулю p функция, имеющая целозначную производную по модулю p и обращающаяся для некоторого $k > N_1(f)$ в 0 по модулю p^k во всех точках из $\mathbb{Z}_p^{(n)}$, то каждая частная производная по модулю p функции f обращается в 0 по модулю p во всех точках из $\mathbb{Z}_p^{(n)}$.*

Доказательство леммы 3.12. При произвольных фиксированных значениях переменных $x_0, x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n$ функция

$$g_i(x_0,x_1,\dots,x_n) = x_i + x_0 f(x_1,\dots,x_n)$$

биективна по модулю p^k как функция переменной x_i, $(i = 1,2,\dots,n)$. Поскольку $k > N_1(g_i) = N_1(f)$, то, согласно 3.9, функция g_i асимптотически сохраняет меру, а значит, ее производная по модулю p не обращается в 0 нигде на $\mathbb{Z}_p$. Более того, справедливо следующее:

$$\frac{\partial_1}{\partial_1 x_i} g_i(u_0,\dots,u_n) = 1 + u_0 \cdot \frac{\partial_1}{\partial_1 x_i} f(u_1,\dots,u_n) \not\equiv 0 \pmod p \qquad (1)$$

для всех $u_0,\dots,u_n \in \mathbb{Z}_p$. Если бы

$$\frac{\partial_1}{\partial_1 x_i} f(u_1,\dots,u_n) \equiv d \not\equiv 0 \pmod p$$

для некоторых $u_1,\dots,u_n \in \mathbb{Z}_p$, тогда, выбрав u_0 таким, чтобы $u_0 d \equiv -1 \pmod p$, мы получили бы противоречие с (1). Это доказывает лемму. $\square$

3.13 Лемма. *Пусть $H\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(n)}$ – равномерно дифференцируемая по модулю p функция, имеющая целозначную производную по модулю p. Если H биективна по модулю p^k и индуцирует тождественную подстановку на $\mathbb{Z}/p^{k-1}$ для некоторого $k > N_1(H) + 1$, то H индуцирует на $(\mathbb{Z}/p^k)^{(n)}$ либо тривиальную (т.е. тождественную) подстановку, либо подстановку порядка p.*

Доказательство леммы 3.13. Пусть G – произвольная функция, удовлетворяющая условиям леммы, и пусть $N_1(G) = N_1(H)$. Представим H и G в следующем виде:

$$H(x_1, \dots, x_n) = (x_1, \dots, x_n) + U(x_1, \dots, x_n);$$
$$G(x_1, \dots, x_n) = (x_1, \dots, x_n) + V(x_1, \dots, x_n).$$

Тогда U и V – равномерно дифференцируемые по модулю p функции, имеющие целозначные производные по модулю p и $N_1(U) = N_1(V) = N_1(H)$. Более того, U и V равны 0 по модулю p^{k-1} всюду на $\mathbb{Z}_p^{(n)}$ и $k-1 > N_1(H)$. Тогда из леммы 3.12 следует, что $U_1' = V_1' = 0$ во всех точках из $\mathbb{Z}_p^{(n)}$. Поскольку $\|U\|_p \leqslant p^{-k+1}$ и $\|V\|_p \leqslant p^{-k+1}$ всюду на $\mathbb{Z}_p^{(n)}$, тогда из определения равномерной дифференцируемости по модулю p получаем, что для всех $h_1, \dots, h_n \in \mathbb{Z}_p$ выполняются следующие сравнения:

$$\begin{aligned} H(G(h_1, \dots, h_n)) &= H((h_1, \dots, h_n) + V(h_1, \dots, h_n)) \\ &\equiv H(h_1, \dots, h_n) + V(h_1, \dots, h_n) H_1'(h_1, \dots, h_n) \\ &\equiv H(h_1, \dots, h_n) + V(h_1, \dots, h_n) + V(h_1, \dots, h_n) U_1'(h_1, \dots, h_n) \\ &\equiv (h_1, \dots, h_n) + U(h_1, \dots, h_n) + V(h_1, \dots, h_n) \pmod{p^k}. \end{aligned}$$

В частности, отсюда следует, что для всех $s \in \mathbb{N}$ выполняется сравнение

$$\begin{aligned} H^s(h_1, \dots, h_n) = \underbrace{H(\dots H}_{s \text{ раз}}(h_1, \dots, h_n)\dots) \\ \equiv (h_1, \dots, h_n) + sU(h_1, \dots, h_n) \pmod{p^k}. \end{aligned}$$

Так как функция U тождественно равна 0 по модулю p^{k-1}, то из последнего сравнения следует, что $H^p(h_1, \dots, h_n) \equiv (h_1, \dots, h_n) \pmod{p^k}$ для всех $h_1, \dots, h_n \in \mathbb{Z}_p$, что и доказывает лемму. $\square$

Для доказательства теоремы 3.11 выберем $k > N_1(F) + 1$ так, чтобы F была транзитивной по модулю p^n для всех $n \geqslant k-1$. Функция F индуцирует подстановку на $(\mathbb{Z}/p^k)^{(n)}$, которую мы обозначим как $\sigma_k(F)$. Рассмотрим подстановку $\sigma = \sigma_k(F)^{p^{(k-1)n}}$. Поскольку F транзитивна по модулю p^k, то порядок подстановки σ равен p^n (и следовательно, σ – нетривиальная подстановка).

С другой стороны, $\sigma = \sigma_k(F^{p^{(k-1)n}})$. Но $F^{p^{(k-1)n}}$ биективна по модулю p^k и индуцирует тождественную подстановку на $\mathbb{Z}/p^{k-1}$ (последнее вытекает из транзитивности F по модулю p^{k-1}). Поскольку σ – нетривиальная подстановка, то ввиду 3.13 порядок подстановки σ должен быть равен p. Однако, согласно предыдущему рассуждению, порядок подстановки σ равен p^n, поэтому необходимо $n = 1$. $\square$

Получить описание асимптотически эргодических функций в классе всех равномерно дифференцируемых по модулю p функций, имеющих целозначные производные по модулю p, пока не удалось, однако при более сильном предположении, состоящем в том, что функция равномерно дифференцируема по модулю p^2, такое описание получено. Метод доказательства следующей теоремы, по сути дела, представляет собой обобщение на случай p-адических функций того метода, который первоначально применил М.В.Ларин при описании транзитивных по модулю n полиномов над $\mathbb{Z}$ (см. [15]).

3.14 Теорема. *Пусть $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ – равномерно дифференцируемая по модулю p^2 функция, имеющая целозначную производную по модулю p^2. Тогда f асимптотически эргодична в том и только в том случае, когда она транзитивна по модулю $p^{N_2(f)+1}$, если p – нечетное простое число, или, соответственно, по модулю $2^{N_2(f)+2}$, если $p = 2$.*

Доказательство. Нам понадобится следующая

3.15 Лемма. *Пусть $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ – равномерно дифференцируемая по модулю p функция, имеющая целозначную производную по модулю p. Если f транзитивна по модулю p^k для некоторого $k > N_1(f)$, то f индуцирует на $\mathbb{Z}/p^{k+1}$ подстановку, которая есть либо цикл длины p^{k+1}, либо произведение p независимых циклов длины p^k каждый.*

Доказательство леммы 3.15. Для $i = 0, 1, 2, \dots$ обозначим через $x_i = \delta_i(x) \in \{0, 1, \dots, p-1\}$ значение i-го разряда в каноническом представлении целого p-адического числа $x \in \mathbb{Z}_p$. Тогда из определения равномерной дифференцируемости по модулю p вытекает, что для всех $x \in \mathbb{Z}_p$ и $s \geqslant N_1(f) = N$ справедливо сравнение $f(x_0 + x_1 p + \dots + x_{s-1}p^{s-1} + x_s p^s) \equiv f(x_0 + x_1 p + \dots + x_{s-1}p^{s-1}) + x_s p^s f_1'(x_0 + x_1 p + \dots + x_{s-1}p^{s-1}) \pmod{p^{s+1}}$, откуда следует, что

$$\delta_s(f(x)) \equiv \Phi_s(x_0, \dots, x_{s-1}) + x_s f_1'(x) \pmod{p}, \tag{1}$$

где $\Phi_s(x_0, \dots, x_{s-1}) = \delta_s(f(x_0 + x_1 p + \dots + x_{s-1}p^{s-1}))$.

Так как частная производная $f_1'(x)$ по модулю p периодична с периодом p^N, то она зависит только от $x_0, \dots, x_{N-1}$, поэтому (1) можно переписать в виде

$$\delta_s(f(x)) \equiv \Phi_s(x_0, \dots, x_{s-1}) + x_s \Psi(x_0, \dots, x_{N-1}) \pmod{p}, \tag{2}$$

где $\Psi(x_0, \dots, x_{N-1}) = f_1'(x)$. Применяя упомянутое в начале данного раздела «правило дифференцирования по модулю p^k композиции функций», заключаем, что для всех $r = 1, 2, \dots$ имеет место сравнение

$$(f^r(x))_1' \equiv \prod_{j=0}^{r-1} f_1'(f^j(x)) \pmod{p}, \tag{3}$$

где, напоминаем, $f^r(x) = \underbrace{f(\dots f}_{r \text{ раз}}(x)\dots)$, $f^0(x) = x$. Поскольку f асимптотически совместима, то из транзитивности f по модулю p^k для некоторого $k > N$ следует транзитивность f по модулю p^n для всех n таких, что $k \geqslant n \geqslant N$

(см. [11], теоремы 2.10 и 1.4). Так как f_1' зависит только от $x_0, \dots, x_{N-1}$, а f транзитивна по модулю p^N, то из (3) следует, что

$$(f^{p^n}(x))_1' \equiv \left(\prod_{u_0,\dots,u_{N-1}=0}^{p-1} \Psi(u_0, \dots, u_{N-1}) \right)^{p^{n-N}} \pmod{p}. \tag{4}$$

Обозначим произведение, стоящее в скобках в правой части сравнения (4), через Π. Тогда, поскольку $f^{p^n}(x)$ равномерно дифферецируема по модулю p и имеет целозначную производную по модулю p, ввиду (2) и (4) мы заключаем, что

$$\delta_n(f^{p^n}(x)) \equiv \varphi_n(x_0, \dots, x_{n-1}) + x_n \Pi^{p^{n-N}} \pmod{p}, \tag{5}$$

где $\varphi_n(x_0, \dots, x_{n-1}) = \delta_n(f^{p^n}(x_0 + x_1 p + \dots + x_{n-1}p^{n-1}))$.

Так как f транзитивна по модулю p^{n+1} при $k > n \geqslant N$, то функция f^{p^n}, с одной стороны, индуцирует тождественную подстановку по модулю p^n, а с другой стороны, задает на каждом смежном классе $a + p^n(\mathbb{Z}/p^{n+1})$ кольца $\mathbb{Z}/p^{n+1}$ подстановку, являющуюся циклом длины p. Сказанное означает, в частности, что функция, стоящая в правой части сравнения (5), как функция переменной x_n должна быть подстановкой на $\{0, 1, \dots p-1\}$, и более того — циклом длины p. Хорошо известно, однако, что полином $c + dy \in \mathbb{Z}[y]$ транзитивен по модулю p тогда и только тогда, когда $d \equiv 1 \pmod{p}$ и $c \not\equiv 0 \pmod{p}$ (см., например, [2], Гл. 3, Теорема А). Но тогда необходимо, чтобы $\Pi^{p^{n-N}} \equiv 1 \pmod{p}$, а значит, чтобы $\Pi \equiv 1 \pmod{p}$. Окончательно получаем, что

$$\begin{aligned} f^{p^k}(x) &\equiv f^{p^k}(x_0 + x_1 p + \dots + x_k p^k) \\ &\equiv x_0 + x_1 p + \dots + x_{k-1}p^{k-1} + p^k(\varphi_k(x_0, \dots, x_{k-1}) + x_k) \pmod{p^{k+1}}. \end{aligned} \tag{6}$$

Из последнего сравнения вытекает, что f индуцирует подстановку σ на кольце вычетов $\mathbb{Z}/p^{k+1}$. Более того, оказывается, что если $\varphi_k(x_0, \dots, x_{k-1}) \not\equiv 0 \pmod{p}$ при каких-то конкретных (эквивалентно, при всех) значениях переменных $x_0, \dots, x_{k-1}$ на множестве $\{0, 1, \dots, p-1\}$, то f транзитивна по модулю p^{k+1}; в ином случае σ есть произведение p независимых циклов длины p^k каждый.

Для доказательства этого утверждения зафиксируем какие-нибудь значения $u_0, \dots, u_k$ из $\{0, 1, \dots, p-1\}$ и обозначим через C тот цикл подстановки σ, который содержит элемент $u_0 + u_1 p + \dots + u_{k-1}p^{k-1} + u_k p^k \in \mathbb{Z}/p^{k+1}$. Так как f транзитивна по модулю p^k, то ввиду (6) длина $|C|$ цикла C должна быть кратна p^k. Если $\varphi_k(u_0, \dots, u_{k-1}) \not\equiv 0 \pmod{p}$, то из (6) следует, что

$$\begin{aligned} f^{p^k}(u_0 + u_1 p + \dots + u_{k-1}p^{k-1} + u_k p^k) \\ \not\equiv u_0 + u_1 p + \dots + u_{k-1}p^{k-1} + u_k p^k \pmod{p^{k+1}}, \end{aligned} \tag{7}$$

т.е., что $|C| > p^k$. С другой стороны, из (6) следует, что $|C|$ делит p^{k+1}. Окончательно мы заключаем, что в рассматриваемом случае $|C| = p^{k+1}$, т.е. что f транзитивна по модулю p^{k+1}.

Если же сравнение $\varphi_k(u_0,\dots,u_{k-1}) \equiv 0 \pmod p$ выполняется на некотором наборе $u_0,\dots,u_{k-1} \in \{0,1,\dots,p-1\}$, то оно выполняется на любом наборе $u_0,\dots,u_{k-1} \in \{0,1,\dots,p-1\}$ (в противном случае из доказанного выше вытекала бы транзитивность f по модулю p^{k+1}, что означало бы справедливость (7) для всех $u_0,\dots,u_k \in \{0,1,\dots,p-1\}$, т.е., в силу (6), что $\varphi_k(u_0,\dots,u_{k-1}) \not\equiv 0 \pmod p$ при всех $u_0,\dots,u_{k-1} \in \{0,1,\dots,p-1\}$; противоречие). Но тогда (6) означает, что σ^{p^k} – тождественная подстановка, т.е. что $|C| = p^k$, поскольку p^k делит $|C|$. Лемма доказана. $\square$

Теперь мы приступаем к доказательству теоремы 3.14. В ходе доказательства предшествующей леммы мы установили, что если f транзитивна по модулю p^k для некоторого $k \geqslant N_1(f)$, то f транзитивна по модулю p^n для всех $k \geqslant n \geqslant N_1(f)$. Поскольку $N_2(f)+1 > N_1(f)$, то необходимость условий теоремы доказана.

Осталось показать, что если $n \geqslant N_2(f)+1$ (соотв., если $n \geqslant N_2(f)+2$ при $p=2$), и если f транзитивна по модулю p^n, то она транзитивна по модулю p^{n+1}. Для этого ввиду леммы 3.15 достаточно показать, что при некотором $x \in \mathbb{Z}_p$ выполняется следующее условие:

$$f^{p^n}(x) \not\equiv x \pmod{p^{n+1}}. \tag{1}$$

Поскольку транзитивность по модулю p^n влечет транзитивность по модулю p^{n-1}, то ввиду леммы 3.15 имеет место равенство

$$f^{p^{n-1}}(x) = x + p^{n-1}\xi(x), \tag{2}$$

где $\xi\colon \mathbb{Z}_p \to \mathbb{Z}_p$ и $\xi(x) \not\equiv 0 \pmod p$ для всех $x \in \mathbb{Z}_p$ (в противном случае из 3.15 следовало бы, что f не транзитивна по модулю p^n, вопреки предположению).

Далее, поскольку функция f равномерно дифференцируема по модулю p^2 и имеет целозначную производную по модулю p^2, то для всех $r = 1,2,\dots$ композиция f^r равномерно дифференцируема по модулю p^2 и имеет целозначную производную по модулю p^2, причем $(f^r(x))'_2 \equiv \prod\limits_{j=0}^{r-1} f'_2(f^j(x)) \pmod{p^2}$ (см. (3) из 3.15). Теперь, так как $n-1 \geqslant N_2(f)$, то, применяя эти соображения и очевидное (вытекающее из (2)) равенство $f^{sp^{n-1}}(x) = f^{(s-1)p^{n-1}}(x+p^{n-1}\xi(x))$, где $s = 1,2,\dots$, мы последовательно вычисляем

$$\begin{aligned}
f^{p^n}(x) &\equiv f^{(p-1)p^{n-1}}(x) + p^{n-1}\xi(x) \prod_{j=0}^{(p-1)p^{n-1}-1} f'_2(f^j(x)) \\
&\equiv f^{(p-2)p^{n-1}}(x) + p^{n-1}\xi(x)\left(\prod_{j=0}^{(p-2)p^{n-1}-1} f'_2(f^j(x)) + \prod_{j=0}^{(p-1)p^{n-1}-1} f'_2(f^j(x))\right) \\
&\equiv \dots \equiv x + p^{n-1}\xi(x)\left(1 + \sum_{i=1}^{p-1} \prod_{j=0}^{(p-i)p^{n-1}-1} f'_2(f^j(x))\right) \pmod{p^{n+1}}.
\end{aligned} \tag{3}$$

Однако f_2' есть периодическая функция с периодом $p^{N_2(f)}$, а f транзитивна по модулю p^{n-1}; поэтому мы заключаем, что для любых $i, j \in \mathbb{N}$ выполняется сравнение $f_2'(f^j(x)) \equiv f_2'(f^{j+ip^{n-1}}(x)) \pmod{p^2}$. Ввиду транзитивности функции f по модулю p^{n-1} из последнего сравнения следует, что $\prod\limits_{j=0}^{(p-i)p^{n-1}-1} f_2'(f^j(x)) \equiv \alpha(x)^{p-i} \pmod{p^2}$, где $\alpha(x) = \prod\limits_{j=0}^{p^{n-1}-1} f_2'(f^j(x))$. В силу (3) мы теперь заключаем, что

$$f^{p^n}(x) \equiv x + p^{n-1}\xi(x)\left(1 + \sum_{i=1}^{p-1} \alpha(x)^i\right) \pmod{p^{n+1}}. \tag{4}$$

Далее, из того, что функция f_2' по модулю p^2 периодична с периодом $p^{N_2(f)}$, а функция f транзитивна по модулю p^{n-1} при $n-1 \geqslant N_2(f)$, вытекает, что значение $\alpha(x)$ по модулю p^2 не зависит от x. Более того, мы утверждаем, что $\alpha(x) \equiv 1 \pmod{p}$.

Действительно, в ходе доказательства леммы 3.15 мы уже установили, что если $k \geqslant N_1(f)$, а f — равномерно дифференцируемая по модулю p^k функция, имеющая целозначную производную по модулю p, то

$$\prod_{j=0}^{p^{N_1(f)}-1} f_1'(f^j(x)) \equiv 1 \pmod{p} \tag{5}$$

для всех $x \in \mathbb{Z}_p$ (см. доказательство сравнения (6) из 3.15). Из определения производной по модулю p^2 следует, что $f_2'(x) \equiv f_1'(x) \pmod{p}$; значит,

$$\alpha(x) \equiv 1 + p\beta \pmod{p^2} \tag{6}$$

для подходящего $\beta \in \mathbb{N}_0$. Ввиду (5) и (6) из (4) теперь следует, что

$$f^{p^n}(x) \equiv x + p^{n-1}\xi(x)\left(p + p\beta\sum_{i=1}^{p-1} i\right) \pmod{p^{n+1}}; \tag{7}$$

поэтому при $p \neq 2$ заключаем, что

$$f^{p^n}(x) \equiv x + p^n\xi(x) \pmod{p^{n+1}}.$$

Последнее в силу 3.15 доказывает теорему при $p \neq 2$, поскольку $\xi(x) \not\equiv 0 \pmod{p}$ (см. текст, следующий за равенством (2)).

Если же $p = 2$, то из сравнения (7) вытекает, что

$$f^{2^n}(x) \equiv x + 2^n(1 + \beta) \pmod{2^{n+1}}, \tag{8}$$

и для завершения доказательства теоремы достаточно теперь показать, что β четно.

Если $n \geqslant N_2(f)+2$, то из транзитивности функции f по модулю 2^n вытекает ее транзитивность по модулю $2^{N_2(f)+2}$, поэтому из определения производной по модулю p^2 получаем, что

$$f^{2^N}(x+2^N\xi) \equiv f^{2^N}(x) + 2^N\xi \prod_{j=0}^{2^N-1} f_2'(f^j(x)) \pmod{2^{N+2}}, \tag{9}$$

где $N = N_2(f)$, $\xi \in \mathbb{Z}_2$. Так как f транзитивна по модулю 2^{N+2}, то для произвольного $x \in \{0,1,\dots,2^N-1\}$ отображение $\varphi_x\colon \xi \mapsto \delta_N(f^{2^N}(x+2^N\xi)) + 2\delta_{N+1}(f^{2^N}(x+2^N\xi))$, где $\xi \in \{0,1,2,3\}$, есть цикл длины 4 на $\mathbb{Z}/4$. Из (6) следует, что $\prod_{j=0}^{2^N-1} f_2'(f^j(x)) \equiv 1+2\beta \pmod 4$, а тогда из (9) вытекает, что

$$\varphi_x(\xi) \equiv c(x) + \xi(1+2\beta) \pmod 4, \tag{10}$$

где $c(x) = \delta_N(f^{2^N}(x)) + 2\delta_{N+1}(f^{2^N}(x))$. Но отображение φ_x транзитивно по модулю 4 при каждом x, а тогда из (10) сразу следует, что $\beta \equiv 0 \pmod 2$ (см. также упомянутый критерий транзитивности полиномов степени 1 в [2] , Гл. 3, Теорема A). $\square$

Замечание. Аналог теоремы 3.14 для функций, равномерно дифференцируемых по модулю p, в общем случае неверен. Именно, для любого $n \in \mathbb{N}$ можно указать такую равномерно дифференцируемую по модулю 2 совместимую функцию $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$, у которой $f_1' = 1$ всюду на $\mathbb{Z}_2$, $N_1(f) = 1$, которая транзитивна по модулю 2^k при $k = 1,2,\dots,n$, но не транзитивна по модулю 2^k при всех $k > n$. (Способом, похожим на описанный ниже, можно построить аналогичный пример и при $p \neq 2$.)

Представим $x \in \mathbb{Z}_2$ в каноническом виде $x = x_0 + x_1\cdot 2 + x_2\cdot 2^2 + \dots$, где $x_0, x_1, x_2 \dots \in \{0,1\}$. Рассмотрим функцию $f(x) = \sum_{i=0}^{\infty} \varphi_i(x_0,\dots,x_i)\cdot 2^i$, где каждый $\varphi_i(x_0,\dots,x_i)$ — линейный по переменному x_i булев многочлен. Другими словами, в фактор-кольце $\mathbb{Z}/2[x_0,\dots,x_i]/(x_0^2-x_0,\dots,x_i^2-x_i)$ кольца многочленов $\mathbb{Z}/2[x_0,\dots,x_i]$ от переменных $x_0,\dots,x_i$ над $\mathbb{Z}/2$ по идеалу, порожденному $x_0^2-x_0,\dots,x_i^2-x_i$, выполняется равенство $\varphi_i(x_0,\dots,x_i) = \psi_i(x_0,\dots,x_{i-1}) + x_i$, причем $\psi_0 = 1$. Несложно увидеть, что такая функция f совместима (см. 3.9 из [11]). Прямые вычисления показывают, что для любых $s \in \mathbb{N}$ и $h \in \mathbb{Z}_2$ справедливо сравнение $f(x+2^sh) \equiv f(x) + 2^sh \pmod{2^{s+1}}$, т.е. что функция f равномерно дифференцируема по модулю 2, причем $f_1' = 1$ всюду на $\mathbb{Z}_2$ и $N_1(f) = 1$.

Далее, в теории булевых функций хорошо известны необходимые и достаточные условия транзитивности по модулю 2^n функции f рассматриваемого вида: именно, она транзитивна по модулю 2^n тогда и только тогда, когда $\varphi_i(x_0,\dots,x_i) = \psi_i(x_0,\dots,x_{i-1}) + x_i$ для $i = 1,2,\dots,n-1$, причем каждый булев многочлен $\psi_i(x_0,\dots,x_{i-1})$ при $i = 1,2,\dots,n-1$ имеет нечетный вес (т.е. число всех наборов значений переменных, на которых он принимает значение 1, нечетно), а $\psi_0 = 1$. (Этот результат, критерий транзитивности по модулю 2^n так называемых преобразований треугольного вида, относится к математическому фольклору, поэтому указать его первоисточник затруднительно, однако доказательство можно найти, например, в [11], лемма 4.8).

Таким образом, выбрав для данного $n \in \mathbb{N}$ функцию f так, чтобы $\psi_0 = 1$, каждый булев многочлен $\psi_i(x_0, \dots, x_{i-1})$ при $i = 1, 2, \dots, n-1$ имел нечетный вес, а булев многочлен $\psi_n(x_0, \dots, x_{n-1})$ имел четный вес, получим функцию, которая транзитивна по модулю 2^k при $k = 1, 2, \dots, n$, но не транзитивна по модулю 2^{n+1}. Но тогда она не будет транзитивна и по каждому модулю 2^k при $k > n$, поскольку ввиду совместимости функции f из транзитивности f по модулю 2^{k+1} вытекала бы ее транзитивность по модулю 2^k.

3.16 Следствие. *Пусть $A = \langle \mathbb{Z}_p; \Omega \rangle$ — универсальная алгебра с конечной сигнатурой Ω, и пусть все операции из Ω — равномерно дифференцируемые по модулю p^2 функции, имеющие целозначные производные по модулю p^2. Тогда существует такое $k(A) \in \mathbb{N}$, что полином $f(x) \in A[x]$ асимптотически эргодичен тогда и только тогда, когда он транзитивен по модулю $p^{k(A)}$.*

Доказательство. Аналогично доказательству 3.10, 3°, а потому детали опускаются. Можно положить $k(A) = \max\{N_2(\omega) : \omega \in \Omega\} + \varepsilon$, где $\varepsilon = 1$ если p нечетно, или $\varepsilon = 2$ в противном случае. □

4. Границы, с которых начинается подъем.

Результаты предыдущего раздела показывают, что для класса $\mathcal{D}_1$ (соответственно, $\mathcal{D}_2$) всех равномерно дифференцируемых по модулю p (соответственно, по модулю p^2) функций, имеющих целозначные производные по модулю p (соответственно, по модулю p^2) можно указать такую функцию $\zeta\colon \mathcal{D}_1 \to \mathbb{N}$ ($\eta\colon \mathcal{D}_2 \to \mathbb{N}$), что функция $f \in \mathcal{D}_1$ ($f \in \mathcal{D}_2$) асимптотически сохраняет меру (асимптотически эргодична) тогда и только тогда, когда она биективна (транзитивна) по модулю $p^{\zeta(f)}$ ($p^{\eta(f)}$). Теоремы 3.9 и 3.14 дают соответствующие оценки величин $\zeta(f)$ и $\eta(f)$.

Эти оценки точны в том смысле, что существует совместимая функция $f \in \mathcal{D}_1$ ($f \in \mathcal{D}_2$) такая, что f биективна (транзитивна) по модулю $p^{N_1(f)}$ (по модулю $p^{N_2(f)}$ при $p \neq 2$ или по модулю $2^{N_2(f)+1}$ при $p = 2$), но не сохраняет меру (не эргодична). Например, полином $f(x) = 1 + x^p$ биективен по модулю p, $N_1(f) = 1$, но в силу 1° из 3.10, полином f не биективен по модулю p^2, поскольку $f'(z) \equiv 0 \pmod{p}$ для всех $z \in \mathbb{Z}_p$.

В качестве соответствующего примера к теореме 3.14 при $p \neq 2$ можно взять функцию $f(x) = (x+1) \odot_p 1$, где $\odot_p$ — операция поразрядного умножения по модулю p целых p-адических чисел: $\delta_i(x \odot_p y) \equiv \delta_i(x)\delta_i(y) \pmod{p}$ для всех $i \in \mathbb{N}_0$. Функция f равномерно дифференцируема, ее производная равна 0 всюду на $\mathbb{Z}_p$, а $N_2(f) = 1$; при этом f транзитивна по модулю p, но даже не биективна (и тем более, не транзитивна) по модулю p^2.

Тем не менее, оценки величин $\zeta(f)$ и $\eta(f)$, которые дают, соответственно, теоремы 3.9 и 3.14, могут сильно отличаться от их истинных значений для различных подклассов из $\mathcal{D}_1$ и $\mathcal{D}_2$. Например, для функции $f(x) = (ax + b) \operatorname{XOR} c$, где $a, b, c \in \mathbb{N}$, теорема 3.14 утверждает, что $f(x)$ асимптотически эргодична тогда и только тогда, когда она транзитивна по модулю $2^{\lfloor \log_2 c \rfloor + 2}$, поскольку эта функция равномерно дифференцируема и имеет производную, равную a всюду на $\mathbb{Z}_2$, а $N_2(f) = \lfloor \log_2 c \rfloor$. Однако непосредственное применение упомянутых выше критериев транзитивности по модулю 2^n для полиномов степени

1 над $\mathbb{Z}$ и для преобразований треугольного вида дает, что рассматриваемая функция асимптотически эргодична тогда и только тогда, когда она транзитивна по модулю 4. Поэтому представляет интерес задача нахождения уточненных оценок величин $\zeta(f)$ и $\eta(f)$ для различных важных в том или ином смысле классов функций, более узких, нежели классы $\mathcal{D}_1$ и $\mathcal{D}_2$.

В данном разделе мы рассматриваем класс $\mathcal{A}$ всех совместимых функций $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ таких, что коэффициенты их интерполяционных рядов убывают как $i!$ или быстрее (напомним, что $\lim\limits_{i\to\infty}\limits^{p} i! = 0$). Точнее, функция f, представленная в виде интерполяционного ряда $(\diamondsuit)$ (см. раздел 2) с целыми p-адическими коэффициентами a_i, содержится в $\mathcal{A}$ тогда и только тогда, когда она совместима и последовательность $\{\|\frac{a_i}{i!}\|_p : i = 0, 1, 2, \dots\}$ ограничена, т.е. $\|\frac{a_i}{i!}\|_p \leqslant p^{\rho(f)}$ для некоторого $\rho(f) \in \mathbb{N}_0$. Напомним, что, согласно теореме 2.1, функция f вида $(\diamondsuit)$ совместима тогда и только тогда, когда $\|a_i\|_p \leqslant p^{-\lfloor \log_p i \rfloor}$ для всех $i \in \mathbb{N}$.

Класс $\mathcal{A}$ довольно широк: он содержит, например, все целозначные совместимые аналитические на $\mathbb{Z}_p$ функции, в частности, совместимые функции, задаваемые целозначными полиномами над $\mathbb{Q}_p$. Известно, (см. [3], гл. 4, теорема 4, стр. 224), что функция f вида $(\diamondsuit)$ аналитична на $\mathbb{Z}_p$ тогда и только тогда, когда $\lim\limits_{i\to\infty}\limits^{p} \frac{a_i}{i!} = 0$.

В оставшейся части этого раздела мы считаем, что $f \in \mathcal{A}$. Положим

$$\lambda(f) = \min\left\{k \in \mathbb{N} : 2\frac{p^k - 1}{p - 1} - k > \rho(f)\right\}.$$

Справедлива следующая

4.1 Теорема. *Пусть $f \in \mathcal{A}$, и пусть p — нечетное простое число. Функция f эргодична тогда и только тогда, когда она транзитивна по модулю $p^{\lambda(f)+1}$ (если $p \neq 3$), или по модулю $3^{\lambda(f)+2}$ (если $p = 3$).*

Поскольку f совместима, то в силу 2.1 ее можно представить в виде

$$f(x) = b_0 + \sum_{i=1}^{\infty} b_i p^{\lfloor \log_p i \rfloor} \binom{x}{i},$$

где $b_j \in \mathbb{Z}_p$ для $j = 0, 1, 2, \dots$. Далее везде в доказательстве мы предполагаем, что функция f представлена в этом виде. В дальнейшем мы обозначаем $\lambda(f)$ через λ, а через p — нечетное простое число. Нам понадобятся некоторые технические результаты.

4.2 Лемма. *В предположениях теоремы 4.1 справедливы следующие сравнения:*

$$b_i \equiv \begin{cases} 0 \pmod{p}, & \text{если } i \geqslant 2p^{\lambda}; \\ 0 \pmod{p^2}, & \text{если } i \geqslant 3p^{\lambda}. \end{cases}$$

Доказательство леммы 4.2. При $b_i = 0$ утверждение леммы тривиально.

Пусть $b_i \neq 0$. Представим f в виде

$$f(x) = b_0 + \sum_{i=1}^{\infty} \frac{1}{i!} b_i p^{\lfloor \log_p i \rfloor} (x)_i,$$

где, напомним, $(x)_i = x(x-1)\cdots(x-i+1)$. Поскольку $f \in \mathcal{A}$, т.е. $\left\| b_i p^{\lfloor \log_p i \rfloor} \right\|_p \leqslant p^{\rho(f)} \|i!\|_p$, то

$$\operatorname{ord}_p b_i \geqslant \operatorname{ord}_p i! - \lfloor \log_p i \rfloor - \rho(f), \tag{1}$$

для всех $i = 1, 2, \ldots$. Напомним, что для $a \in \mathbb{N}$ выполняется $\log_p \|a\|_p = -\operatorname{ord}_p a$; таким образом, максимальная степень p, делящая a, в точности равна $p^{\operatorname{ord}_p a}$.

Далее, функция $\varkappa(i) = \operatorname{ord}_p i! - \lfloor \log_p i \rfloor$ как функция аргумента i, является неубывающей. Для доказательства этого заметим, что, очевидно, $\operatorname{ord}_p i! \geqslant \operatorname{ord}_p (i-1)!$, а потому, если $\lfloor \log_p i \rfloor = \lfloor \log_p (i-1) \rfloor$, то $\varkappa(i-1) \leqslant \varkappa(i)$.

Допустим, что $\lfloor \log_p j \rfloor > \lfloor \log_p (j-1) \rfloor$ для некоторого положительного рационального целого j. Ясно, что $\lfloor \log_p j \rfloor + 1$ есть число всех значащих цифр в p-ичном представлении j. Следовательно, рассматриваемый случай имеет место тогда и только тогда, когда $j-1 = (p-1)+(p-1)p+\cdots+(p-1)p^n = p^{n+1}-1$ для некоторого $n \in \mathbb{N}_0$. Однако тогда $\operatorname{ord}_p j! = \operatorname{ord}_p (j-1)! + n$, $\lfloor \log_p (j-1) \rfloor = n$, $\lfloor \log_p j \rfloor = n+1$, и, следовательно, $\varkappa(j) > \varkappa(j-1)$.

Для завершения доказательства леммы теперь достаточно показать, что $\varkappa(2p^\lambda) - \rho(f) \geqslant 1$ и $\varkappa(3p^\lambda) - \rho(f) \geqslant 2$. Напомним, что $\operatorname{ord}_p i! = \frac{1}{p-1}(i - \operatorname{wt}_p i)$, где $\operatorname{wt}_p i$ есть сумма всех цифр в p-ичном представлении i (т.е. если $i = i_0 + i_1 p + \cdots + i_s p^s$, где $i_0, \ldots, i_s \in \{0, 1, \ldots, p-1\}$, то $\operatorname{wt}_p i = i_0 + \cdots + i_s$, см., например, [6] , гл.1, раздел 2, упражнение 13).

Поскольку $p \neq 2$, то $\varkappa(2p^\lambda) - \rho(f) = \frac{1}{p-1}(2p^\lambda - 2) - \lambda - \rho(f) \geqslant 1$, согласно определению $\lambda = \lambda(f)$. Значит, если $p \neq 3$, то

$$\varkappa(3p^\lambda) - \rho(f) = \frac{1}{p-1}(3p^\lambda - 3) - \lambda - \rho(f) = \varkappa(2p^\lambda) + \frac{1}{p-1}(p^\lambda - 1) - \rho(f) \geqslant 2,$$

что доказывает лемму при $p \neq 3$.

Наконец, пусть $p = 3$. Тогда

$$\varkappa(3p^\lambda) - \rho(f) = \varkappa(3^{\lambda+1}) - \rho(f) = \frac{1}{2}(3^{\lambda+1} - 1) - \lambda - 1 - \rho(f) \geqslant 2,$$

ибо в противном случае ввиду неравенства

$$3^\lambda - 1 - \lambda > \rho(f),$$

вытекающего непосредственно из определения $\lambda = \lambda(f)$, выполнялось бы и неравенство

$$\frac{1}{2}(3^{\lambda+1} - 1) - \lambda - 1 - 3^\lambda + 1 + \lambda < 1,$$

т.е. $3^\lambda - 1 < 2$, откуда $\lambda < 1$, вопреки определению $\lambda = \lambda(f)$. Лемма 4.2 доказана. $\square$

4.3 Следствие. *В условиях теоремы 4.1 для $i \in \mathbb{N}$ справедливы следующие сравнения:*

$$\frac{\Delta^i f(x)}{i} \equiv \begin{cases} 0 \pmod{p^2}, & \text{если } i \geqslant 2p^\lambda + 1; \\ 0 \pmod{p}, & \text{если } i \geqslant p^\lambda + 1. \end{cases}$$

Доказательство следствия 4.3. Поскольку $\Delta^j \binom{x}{i} = \binom{x}{i-j}$ при $i \geqslant j$, и $\Delta^j \binom{x}{i} = 0$ при $i < j$, то

$$\frac{\Delta^i f(x)}{i} = \frac{1}{\hat{\imath}} \sum_{j=i}^{\infty} b_j p^{\lfloor \log_p j \rfloor - \operatorname{ord}_p j} \binom{x}{j-i},$$

где $\hat{\imath} = ip^{-\operatorname{ord}_p i} \in \mathbb{Z}_p$, $\operatorname{ord}_p \hat{\imath} = 0$. Теперь результат очевиден ввиду леммы 4.2. $\square$

4.4 Предложение. *В условиях теоремы 4.1, функция f равномерно дифференцируема по модулю p^2 (причем $N_2(f) \leqslant \lambda(f) + 1$), имеет целозначную производную по модулю p^2, и*

$$f_2'(x) \equiv \sum_{i=1}^{2p^\lambda} (-1)^{i-1} \frac{\Delta^i f(x)}{i} \pmod{p^2}.$$

Доказательство предложения 4.4. Для доказательства первой части утверждения предложения 4.4 покажем, что существует функция $f_2' \colon \mathbb{Z}_p \to \mathbb{Z}_p$ такая, что для всех $x, h \in \mathbb{Z}_p$ и всех $m \geqslant \lambda(f) + 1$ выполняется следующее сравнение:

$$f(x + p^m h) \equiv f(x) + p^m h f_2'(x) \pmod{p^{m+2}}. \tag{1}$$

Ввиду совместимости функции f достаточно установить справедливость сравнения (1) лишь для $h \in \{1, 2, \ldots, p^2 - 1\}$ (случай $h = 0$ тривиален). Применяя справедливую для любого $n \in \mathbb{N}_0$ формулу Ньютона

$$f(x + n) = \sum_{i=0}^{n} \binom{n}{i} \Delta^i f(x)$$

при $n = p^m h$ получаем, что

$$f(x + p^m h) = f(x) + p^m h \varphi_m(x, h), \tag{2}$$

где

$$\varphi_m(x, h) = \sum_{i=1}^{p^m h} \binom{p^m h - 1}{i - 1} \frac{\Delta^i f(x)}{i}. \tag{3}$$

Отсюда ввиду 4.3 для $m \geqslant \lambda + 1$ получаем:

$$\varphi_m(x, h) \equiv \sum_{i=1}^{2p^\lambda} \binom{p^m h - 1}{i - 1} \frac{\Delta^i f(x)}{i} \pmod{p^2}. \tag{4}$$

Далее, для всех $i = 1, 2, \dots, 2p^\lambda$ выполняются следующие очевидные равенства:

$$\binom{p^m h - 1}{i-1} = \prod_{k=0}^{i-2} \frac{p^m h - (k+1)}{k+1} = \prod_{j=1}^{i-1} \left(\frac{h}{\hat{j}} p^{m - \operatorname{ord}_p j} - 1 \right). \tag{5}$$

Здесь $\hat{j} = jp^{-\operatorname{ord}_p j}$, т.е. элемент $\hat{j}$ имеет в $\mathbb{Z}_p$ мультипликативный обратный $\frac{1}{\hat{j}} \in \mathbb{Z}_p$; следовательно, каждый сомножитель произведения из правой части равенства (5) есть p-адическое целое число.

Если $i \leqslant p^\lambda$, то $m - \operatorname{ord}_p j \geqslant 2$ для всех $j = 1, 2, \dots, i-1$; поэтому из (5) следует, что

$$\binom{p^m h - 1}{i-1} \equiv (-1)^{i-1} \pmod{p^2}. \tag{6}$$

Если же $p^\lambda + 1 \leqslant i \leqslant 2p^\lambda$ и $j \in \{1, 2, \dots, i-1\}$, то равенство $m - \operatorname{ord}_p j = 1$ выполняется тогда и только тогда, когда одновременно $j = p^\lambda$ и $m = \lambda + 1$; в остальных же случаях $m - \operatorname{ord}_p j \geqslant 2$. Однако если $m - \operatorname{ord}_p j = 1$, то

$$\frac{\Delta^i f(x)}{i} \equiv 0 \pmod{p}$$

ввиду 4.3; значит, во всех случаях справедливо сравнение

$$\left(\frac{h}{\hat{j}} p^{m - \operatorname{ord}_p j} - 1 \right) \frac{\Delta^i f(x)}{i} \equiv -\frac{\Delta^i f(x)}{i} \pmod{p^2}.$$

Отсюда ввиду (5) заключаем, что

$$\binom{p^m h - 1}{i-1} \frac{\Delta^i f(x)}{i} \equiv (-1)^{i-1} \frac{\Delta^i f(x)}{i} \pmod{p^2} \tag{7}$$

для всех $i = 1, 2, \dots, 2p^\lambda$. Теперь (4), (6), (7) совместно дают

$$\varphi_m(x, h) \equiv \sum_{i=1}^{2p^\lambda} (-1)^{i-1} \frac{\Delta^i f(x)}{i} \pmod{p^2},$$

что ввиду (2), (3), (4) завершает доказательство предложения 4.4. $\square$

4.5 Лемма. *При выполнении условий теоремы 4.1 найдется функция $\theta\colon \mathbb{Z}_p \to \mathbb{Z}_p$ такая, что для произвольных $x, h \in \mathbb{Z}_p$ выполняется сравнение*

$$f(x + p^\lambda h) \equiv f(x) + p^\lambda h f_2'(x) + p^{\lambda+1} h^2 \theta(x) \pmod{p^{\lambda+2}}.$$

Функция θ обладает следующим свойством: для любых $a, b \in \mathbb{Z}_p$ сравнение $a \equiv b \pmod{p^\lambda}$ влечет сравнение $\theta(a) \equiv \theta(b) \pmod{p}$. Кроме того, можно положить

$$\theta(x) = \sum_{j=2}^{p-1} (-1)^j \sum_{i=1}^{j-1} \frac{1}{i} \cdot \frac{\Delta^{jp^{\lambda-1}} f(x)}{jp^{\lambda-1}} + \sum_{k=1}^{p-1} (-1)^{k-1} \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^\lambda} + \frac{\Delta^{2p^\lambda} f(x)}{2p^{\lambda+1}}.$$

Доказательство леммы 4.5. Докажем вначале, что функция θ, заданная последним равенством из формулировки леммы, принимает целые p-адические значения во всех точках из $\mathbb{Z}_p$. Поскольку ввиду совместимости функции f каждая дробь $\frac{\Delta^s f(x)}{s}$, где $s = 1, 2, 3, \dots$, есть целое p-адическое число (см. 3.1 из [11]), то достаточно доказать лишь, что определенные ниже функции $\alpha(x)$ и $\beta_k(x)$ принимают целые p-адические значения при всех $x \in \mathbb{Z}_p$ и $k \in \{1, 2, \dots, p-1\}$. По определению,

$$\alpha(x) = \frac{\Delta^{2p^\lambda} f(x)}{2p^{\lambda+1}}; \quad \beta_k(x) = \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^\lambda}.$$

Поскольку

$$\Delta^i f(x) = \sum_{j=i}^{\infty} b_j p^{\lfloor \log_p j \rfloor} \binom{x}{j-i} \tag{1}$$

для $i = 1, 2, 3, \dots$, и $b_j p^{\lfloor \log_p j \rfloor} \equiv 0 \pmod{p^{\lambda+1}}$ для всех рациональных целых $j \geqslant 2p^\lambda$ (см. 4.2), то $\alpha(x) \in \mathbb{Z}_p$. Если $j \geqslant kp^{\lambda-1} + p^\lambda$, то $\lfloor \log_p j \rfloor \geqslant \lambda$; значит, из (1) вытекает, что $\beta_k(x) \in \mathbb{Z}_p$.

Теперь докажем что для всех $a, b \in \mathbb{Z}_p$ из справедливости сравнения $a \equiv b \pmod{p^\lambda}$ следует справедливость сравнения $\theta(a) \equiv \theta(b) \pmod{p}$. Из (1) and 4.2 следует, что

$$\alpha(x) \equiv \frac{1}{2} \sum_{j=2p^\lambda}^{3p^\lambda-1} \frac{1}{p} b_j \binom{x}{j-2p^\lambda} \pmod{p}. \tag{2}$$

Напомним формулировку известной теоремы Люка (доказательство см., например, в [4]): если $a = \sum_{i=0}^{\infty} a_i p^i$ и $b = \sum_{i=0}^{N} b_i p^i$ есть, соответственно, канонические p-адические представления целого p-адического числа a и неотрицательного рационального целого числа b (т.е. $a_i, b_i \in \{0, 1, \dots, p-1\}$ для $i = 0, 1, 2, \dots$), то

$$\binom{a}{b} \equiv \binom{a_0}{b_0} \binom{a_1}{b_1} \cdots \binom{a_N}{b_N} \pmod{p}.$$

Поэтому, если $a \equiv b \pmod{p^\lambda}$, то из теоремы Люка следует, что для всех $j = 2p^\lambda, 2p^\lambda + 1, \dots, 3p^\lambda - 1$ справедливо следующее сравнение:

$$\binom{a}{j-2p^\lambda} \equiv \binom{b}{j-2p^\lambda} \pmod{p}.$$

Таким образом, из (2) теперь следует, что

$$\alpha(a) \equiv \alpha(b) \pmod{p}. \tag{3}$$

Далее, комбинируя (1) и 4.2, получаем, что

$$\beta_k(x) \equiv \frac{1}{k} \sum_{j=kp^{\lambda-1}+p^\lambda}^{2p^\lambda-1} b_j \binom{x}{j-kp^{\lambda-1}-p^\lambda} \pmod{p}$$

для всех $k = 1, 2, \ldots, p-1$. Вновь применяя теорему Люка, заключаем, что

$$\beta_k(a) \equiv \beta_k(b) \pmod{p}, \tag{4}$$

если $a \equiv b \pmod{p^\lambda}$.

Наконец, полагая

$$\gamma_k(x) = \frac{\Delta^{kp^{\lambda-1}} f(x)}{kp^{\lambda-1}},$$

ввиду (1) заключаем, что для $k = 1, 2, \ldots, p-1$ справедливо следующее сравнение:

$$\gamma_k(x) \equiv \frac{1}{k} \sum_{j=kp^{\lambda-1}}^{p^\lambda-1} b_j \binom{x}{j-kp^{\lambda-1}} \pmod{p}.$$

Еще раз применяя теорему Люка, получаем, что

$$\gamma_k(a) \equiv \gamma_k(b) \pmod{p}, \tag{5}$$

если $a \equiv b \pmod{p^\lambda}$. Следовательно, ввиду (3)–(5) из сравнения $a \equiv b \pmod{p^\lambda}$ вытекает сравнение $\theta(a) \equiv \theta(b) \pmod{p}$.

Теперь докажем оставшуюся часть утверждения леммы. Поскольку f совместима, то в процессе доказательства можем считать, что $h \in \mathbb{N}$ (случай $h = 0$ тривиален). Рассуждая так же, как при доказательстве 4.4 (см. там (2)–(5)), заключаем, что справедливо сравнение

$$f(x + p^\lambda h) \equiv f(x) + p^\lambda h \varphi(x, h) \pmod{p^{\lambda+2}}, \tag{6}$$

где

$$\varphi(x, h) \equiv \sum_{i=1}^{2p^\lambda} \binom{p^\lambda h - 1}{i-1} \frac{\Delta^i f(x)}{i} \pmod{p^2}, \tag{7}$$

и, кроме того, при $i = 1, 2, \ldots, 2p^\lambda$ — равенство

$$\binom{p^\lambda h - 1}{i-1} = \prod_{j=1}^{i-1} \left(\frac{h}{j} p^{\lambda - \operatorname{ord}_p j} - 1\right). \tag{8}$$

Поскольку f совместима, то, согласно 3.4 из [11],

$$\frac{\Delta^i f(x)}{i} \equiv 0 \pmod{p}$$

во всех случаях, кроме, быть может, случая, когда i имеет вид $i = tp^s$ для подходящих $t \in \{1, 2, \dots p-1\}$ и $s \in \mathbb{N}_0$. Поэтому, если $i \leqslant p^{\lambda-1}$, или если одновременно $p^{\lambda-1} < i < p^\lambda$ и $p^{\lambda-1}$ не делит i, то из (8) следует, что

$$\binom{p^\lambda h - 1}{i-1} \frac{\Delta^i f(x)}{i} \equiv (-1)^{i-1} \frac{\Delta^i f(x)}{i} \pmod{p^2}. \tag{9}$$

Пусть $i = kp^{\lambda-1}$, где $k \in \{2, 3, \dots, p-1\}$. Тогда из (8) следует, что

$$\binom{p^\lambda h - 1}{i-1} \equiv (-1)^{kp^{\lambda-1}-1} + (-1)^k ph \sum_{j=1}^{k-1} \frac{1}{j} \pmod{p^2}. \tag{10}$$

Далее, если $p^\lambda \leqslant i \leqslant 2p^\lambda$ и $\operatorname{ord}_p i \neq \lambda, \lambda - 1$, то

$$\frac{\Delta^i f(x)}{i} \equiv 0 \pmod{p^2} \tag{11}$$

(см. (1) и следующее за ним сравнение).

Осталось рассмотреть два случая: $i = \nu p^\lambda$, где $\nu \in \{1, 2\}$, и $i = kp^{\lambda-1} + p^\lambda$, где $k \in \{1, 2, \dots, p-1\}$. В последнем из них ввиду 4.3 и (8) выполняется сравнение

$$\binom{p^\lambda h - 1}{i-1} \frac{\Delta^i f(x)}{i} \equiv (-1)^{i-1} \frac{\Delta^i f(x)}{i} + (-1)^{k-1} h \frac{\Delta^i f(x)}{i} \pmod{p^2}. \tag{12}$$

Далее, при $k = 1, 2, \dots, p-1$ в поле $\mathbb{Q}_p$ имеет место следующее тривиальное равенство:

$$\left(1 + \frac{p}{k}\right) \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1} + p^\lambda} = \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1}}. \tag{13}$$

Отсюда ввиду 4.3 заключаем, что

$$\frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1} + p^\lambda} \equiv 0 \pmod{p},$$

а так как $\frac{p}{k} \in \mathbb{Z}_p$ и $\operatorname{ord}_p \frac{p}{k} = 1$, то из (13) следует, что

$$\frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1} + p^\lambda} \equiv \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1}} \pmod{p^2}.$$

Теперь, применяя (12) для $i = kp^{\lambda-1} + p^\lambda$, заключаем, что

$$\begin{aligned} &\binom{p^\lambda h - 1}{kp^{\lambda-1} + p^\lambda - 1} \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1} + p^\lambda} \\ &\qquad = (-1)^{kp^{\lambda-1}+p^\lambda-1} \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1} + p^\lambda} + (-1)^{k-1} ph\beta_k(x) \pmod{p^2}. \end{aligned} \tag{14}$$

В случае, когда $i = p^\lambda$, из (8) вытекает, что

$$\binom{p^\lambda h - 1}{p^\lambda - 1} \equiv (-1)^{p^\lambda - 1} - ph \sum_{j=1}^{p-1} \frac{1}{j} \equiv (-1)^{p^\lambda - 1} \pmod{p^2}, \tag{15}$$

поскольку при $p \neq 2$ в $\mathbb{Q}_p$ выполняются сравнения

$$\sum_{j=1}^{p-1} \frac{1}{j} \equiv \sum_{j=1}^{p-1} j \equiv 0 \pmod{p}.$$

Наконец, при $i = 2p^\lambda$, в силу (8) и 4.3, мы заключаем, что

$$\begin{aligned}\binom{p^\lambda h - 1}{2p^\lambda - 1} \frac{\Delta^{2p^\lambda} f(x)}{2p^\lambda} &\equiv (-1)^{2p^\lambda - 1} \frac{\Delta^{2p^\lambda} f(x)}{2p^\lambda} + h \frac{\Delta^{2p^\lambda} f(x)}{2p^\lambda} \\ &\equiv (-1)^{2p^\lambda - 1} \frac{\Delta^{2p^\lambda} f(x)}{2p^\lambda} + hp\alpha(x) \pmod{p^2}. \end{aligned} \tag{16}$$

Теперь, комбинируя (6), (7), (9), (11), (14), (15), (16) с 4.4, мы завершаем доказательство леммы 4.5. □

4.6 Лемма. *В предположениях теоремы 4.1, для всех $x, h \in \mathbb{Z}_p$ справедливо следующее сравнение:*

$$f_2'(x + p^\lambda h) \equiv f_2'(x) + 2ph\theta(x) \pmod{p^2}.$$

Здесь θ — функция, определенная в формулировке леммы 4.5.

Доказательство леммы 4.6. Ввиду 4.4, справедливо следующее сравнение:

$$f_2'(x + p^\lambda h) \equiv \sum_{i=1}^{2p^\lambda} (-1)^{i-1} \frac{\Delta^i f(x + p^\lambda h)}{i} \pmod{p^2}. \tag{1}$$

При $i = 1, 2, \ldots, 2p^\lambda$ из предыдущей леммы следует, что

$$\begin{aligned}\frac{\Delta^i f(x + p^\lambda h)}{i} \equiv \frac{\Delta^i f(x)}{i} &+ hp^{\lambda - \operatorname{ord}_p i} \frac{\Delta^i f_2'(x)}{\hat{\imath}} + \\ &+ h^2 p^{\lambda + 1 - \operatorname{ord}_p i} \frac{\Delta^i \theta(x)}{\hat{\imath}} \pmod{p^2}, \end{aligned} \tag{2}$$

где $\hat{\imath} = ip^{-\operatorname{ord}_p i}$ имеет в кольце $\mathbb{Z}_p$ мультипликативный обратный $\frac{1}{\hat{\imath}} \in \mathbb{Z}_p$.

Член второго порядка относительно h в сравнении (2) может не обращаться в 0 по модулю p^2 лишь в случае, когда $i \in \{p^\lambda, 2p^\lambda\}$. Однако, поскольку $\Delta^j \binom{x}{\nu} = \binom{x}{\nu - j}$ при $\nu \geqslant j$ и $\Delta^j \binom{x}{\nu} = 0$ при $\nu < j$, то для всех $j \in \mathbb{N}$ выполняется равенство

$$\Delta^j f(x) = \sum_{\nu=j}^{\infty} b_\nu p^{\lfloor \log_p \nu \rfloor} \binom{x}{\nu - j}. \tag{3}$$

Следовательно, если $j \in \{p^\lambda, 2p^\lambda\}$, то

$$\frac{\Delta^{j+kp^{\lambda-1}} f(x)}{kp^{\lambda-1}} \equiv 0 \pmod{p}. \tag{4}$$

при $k \in \{1, 2, \ldots, p-1\}$. Далее, если $j \in \{p^\lambda, 2p^\lambda\}$, то из равенства (3) ввиду 4.3 следует, что

$$\frac{\Delta^{j+kp^{\lambda-1}+p^\lambda} f(x)}{kp^\lambda} \equiv 0 \pmod{p}, \tag{5}$$

$$\frac{\Delta^{j+2p^\lambda} f(x)}{2p^\lambda} \equiv 0 \pmod{p}. \tag{6}$$

Теперь, по определению функции θ, комбинируя (4), (5) и (6), мы заключаем, что $\frac{\Delta^i \theta(x)}{\hat{\imath}} \equiv 0 \pmod{p}$ при $i \in \{p^\lambda, 2p^\lambda\}$ и, таким образом,

$$h^2 p^{\lambda+1-\operatorname{ord}_p i} \frac{\Delta^i \theta(x)}{\hat{\imath}} \equiv 0 \pmod{p^2} \tag{7}$$

для всех $i = 1, 2, \ldots, 2p^\lambda$.

Член порядка 1 относительно h в (2) не обращается в 0 по модулю p^2 лишь, может быть, при $i \in \{1, 2, \ldots, 2p^\lambda\}$ таких, что $\operatorname{ord}_p i \geqslant \lambda - 1$, т.е., при

$$i \in \{p^\lambda, 2p^\lambda, kp^{\lambda-1}, kp^{\lambda-1} + p^\lambda : k = 1, 2, \ldots, p-1\}.$$

Комбинируя 4.3, 4.4 и уже цитированное утверждение 3.4 из [11] (см. рассуждение, следующее за (8) в доказательстве 4.5), получаем, что

$$f_2'(x) \equiv \frac{\Delta^{p^\lambda} f(x)}{p^\lambda} + \sum_{t=0}^{\lambda-1} \sum_{\tau=1}^{p-1} (-1)^{\tau-1} \frac{\Delta^{\tau p^t} f(x)}{\tau p^t} \pmod{p}, \tag{8}$$

и, следовательно,

$$\Delta^i f_2'(x) \equiv \frac{\Delta^{i+p^\lambda} f(x)}{p^\lambda} + \sum_{t=0}^{\lambda-1} \sum_{\tau=1}^{p-1} (-1)^{\tau-1} \frac{\Delta^{i+\tau p^t} f(x)}{\tau p^t} \pmod{p}. \tag{9}$$

Последнее при $i \in \{kp^{\lambda-1} + p^\lambda : k = 1, 2, \ldots, p-1\}$ ввиду (3) и 4.2 означает, что $\Delta^i f_2'(x) \equiv 0 \pmod{p}$, и, следовательно,

$$hp \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f_2'(x)}{k+p} \equiv 0 \pmod{p^2} \tag{10}$$

при $k = 1, 2, \ldots, p-1$ (поскольку тогда мультипликативный обратный $\frac{1}{k+p}$ к $k+p$ лежит в $\mathbb{Z}_p$).

Если $i \in \{kp^{\lambda-1} : k = 1, 2, \dots, p-1\}$, то ввиду 4.2, (3) и (9) имеем:

$$\Delta^{kp^{\lambda-1}} f_2'(x) \equiv \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{p^\lambda} + \sum_{\tau=1}^{p-k-1} (-1)^{\tau-1} \frac{\Delta^{(\tau+k)p^{\lambda-1}} f(x)}{\tau p^{\lambda-1}} \pmod{p}. \quad (11)$$

Если $i = 2p^\lambda$, то из 4.4 следует, что

$$\Delta^{2p^\lambda} f_2'(x) \equiv \sum_{j=1}^{2p^\lambda} (-1)^{j-1} \frac{\Delta^{j+2p^\lambda} f(x)}{j} \pmod{p^2}.$$

Последнее ввиду (3) и 4.2 означает, что

$$\Delta^{2p^\lambda} f_2'(x) \equiv 0 \pmod{p^2}. \quad (12)$$

Рассмотрим теперь случай $i = p^\lambda$. Из предложения 4.4 вытекает, что

$$\Delta^{p^\lambda} f_2'(x) \equiv \sum_{j=1}^{1+p^\lambda} (-1)^{j-1} \frac{\Delta^{j+p^\lambda} f(x)}{j} \pmod{p^2}, \quad (13)$$

поскольку, комбинируя (3) с 4.2, заключаем, что при $j = p^\lambda + 1, \dots, 2p^\lambda$ справедливы сравнения

$$\frac{\Delta^{j+p^\lambda} f(x)}{j} \equiv 0 \pmod{p^2}.$$

Более того, из (3) следует, что последнее сравнение справедливо также для всех $j \leqslant p^\lambda - 1$ таких, что $j \neq kp^{\lambda-1}$ $(k = 1, 2, \dots, p-1)$. Таким образом, из (13) следует, что

$$\Delta^{p^\lambda} f_2'(x) \equiv \frac{\Delta^{2p^\lambda} f(x)}{p^\lambda} + \sum_{k=1}^{p-1} (-1)^{k-1} \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1}} \pmod{p^2}. \quad (14)$$

Теперь, подставляя (7), (10), (11), (12), (14) в (2) и суммируя все полученные таким образом сравнения по i от 1 до $2p^\lambda$, ввиду (1) и 4.4 заключаем, что

$$\begin{aligned} f_2'(x + p^\lambda h) \equiv f_2'(x) + hp \Bigg(& \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \sum_{\tau=1}^{p-k-1} (-1)^{\tau-1} \frac{\Delta^{(\tau+k)p^{\lambda-1}} f(x)}{\tau p^{\lambda-1}} + \\ & + \sum_{k=1}^{p-1} (-1)^{k-1} \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^\lambda} \Bigg) + \\ & + h \sum_{k=1}^{p-1} (-1)^{k-1} \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1}} + h \frac{\Delta^{2p^\lambda} f(x)}{p^\lambda} \pmod{p^2}. \quad (15) \end{aligned}$$

Напомним, что здесь и далее все вычисления проводятся в поле $\mathbb{Q}_p$, а сравнение $\xi \equiv 0 \pmod{p^k}$ для $\xi \in \mathbb{Q}_p$ и положительного рационального целого k означает,

что $\|\xi\|_p = p^{-k}$ (и потому ξ есть p-адическое целое). Ввиду этого замечания заключаем, что

$$\sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \sum_{\tau=1}^{p-k-1} (-1)^{\tau-1} \frac{\Delta^{(\tau+k)p^{\lambda-1}} f(x)}{\tau p^{\lambda-1}} =$$

$$= \sum_{m=1}^{p-1} (-1)^m \sum_{k+\tau=m} \frac{1}{k\tau} \cdot \frac{\Delta^{mp^{\lambda-1}} f(x)}{p^{\lambda-1}} = 2 \sum_{m=1}^{p-1} (-1)^m \sum_{\tau=1}^{m-1} \frac{1}{\tau} \cdot \frac{\Delta^{mp^{\lambda-1}} f(x)}{mp^{\lambda-1}}, \quad (16)$$

поскольку при $k, \tau \in \{1, 2, \dots, p-1\}$ справедливы очевидные равенства

$$\sum_{k+\tau=m} \frac{1}{k\tau} = \sum_{k+\tau=m} \frac{1}{(m-\tau)\tau} = \frac{1}{m} \sum_{k+\tau=m} \left(\frac{1}{\tau} + \frac{1}{m-\tau} \right) = \frac{2}{m} \sum_{\tau=1}^{m-1} \frac{1}{\tau}.$$

Кроме того, как было показано при доказательстве леммы 4.5, $\alpha(x)$ и $\beta_k(x)$ являются p-адическими целыми при $k = 1, 2, \dots, p-1$ и $x \in \mathbb{Z}_p$; таким образом,

$$2hp\alpha(x) = h \frac{\Delta^{2p^\lambda} f(x)}{p^\lambda}; \quad hp\beta_k(x) = h \frac{\Delta^{kp^{\lambda-1}+p^\lambda} f(x)}{kp^{\lambda-1}}, \quad (17)$$

где все сомножители есть p-адические целые. Теперь утверждение леммы следует из (15), (16), (17) и определения функции θ. $\square$

Доказательство теоремы 4.1. Приступая к доказательству теоремы 4.1, отметим вначале, что согласно 4.4 справедливо неравенство $N_2(f) \leqslant \lambda+1$. Таким образом, ввиду 3.14 достаточно показать лишь, что если $p \neq 3$ и функция f транзитивна по модулю $p^{\lambda+1}$, то тогда f транзитивна и по модулю $p^{\lambda+2}$. В свою очередь, в силу 3.15 для этого достаточно проверить лишь, что

$$f^{p^{\lambda+1}}(x) \not\equiv x \pmod{p^{\lambda+2}} \quad (1)$$

для хотя бы одного $x \in \mathbb{Z}_p$. Далее будем вычислять $f^{p^{\lambda+1}}(x) \bmod p^{\lambda+2}$.

Так как f совместима, то она в силу сделанных выше предположений транзитивна по модулю p^λ; поэтому ввиду 3.15 заключаем, что найдется определенная всюду на $\mathbb{Z}_p$ функция $\xi\colon \mathbb{Z}_p \to \mathbb{Z}_p$ такая, что для всех $x \in \mathbb{Z}_p$ справедливо следующее

$$f^{p^\lambda}(x) = x + p^\lambda \xi(x), \quad \xi(x) \not\equiv 0 \pmod{p}. \quad (2)$$

Далее, утверждается, что для каждого $i = 0, 1, 2, \dots$ выполняется сравнение:

$$f^{p^\lambda+i}(x) \equiv f^i(x) + p^\lambda \xi(x) (f^i(x))_2' + \\ + p^{\lambda+1} \xi(x)^2 (f^i(x))_2' \sum_{k=0}^{i-1} \frac{(f^k(x))_2'}{f_2'(f^k(x))} \theta(f^k(x)) \pmod{p^{\lambda+2}}. \quad (3)$$

Здесь и далее мы, как обычно, полагаем, что если множество значений индексов пусто, то соответствующая сумма (произведение) равна 0 (соответственно, 1). Заметим также, что поскольку f транзитивна по модулю $p^{\lambda+1}$, то

она биективна по модулю $p^{\lambda+1}$, а значит, f биективна и по каждому модулю $p^\lambda, \dots, p^2, p$ в силу совместимости f. Следовательно, $f_1'(x) \not\equiv 0 \pmod p$ для всех $x \in \mathbb{Z}_p$ (см. доказательство теоремы 3.9), а значит, и $f_2'(x) \not\equiv 0 \pmod p$ (так как $f_2'(x) \equiv f_1'(x) \pmod p$). Таким образом, все знаменатели в (3) имеют мультипликативные обратные в кольце $\mathbb{Z}_p$; в силу этого, при доказательстве справедливости сравнения (3) и далее в подобных случаях мы можем считать, что все вычисления проводятся в $\mathbb{Z}_p$.

Справедливость сравнения (3) легко доказать индукцией по i. Если $i = 0$, то (3) есть тривиальное следствие (2). Пусть (3) выполняется при $i = m - 1$. Так как

$$f^{p^\lambda+m}(x) = f(f^{p^\lambda+m-1}(x)), \tag{4}$$

то, положив в (3) параметр i равным $m-1$, затем подставив (3) в (4) и применив лемму 4.5, ввиду совместимости функции f и справедливости сравнения $(f^k(x))_2' \equiv \prod_{j=0}^{k-1} f_2'(f^j(x)) \pmod{p^2}$ мы сможем доказать справедливость сравнения (3) при $i = m$ прямыми вычислениями, детали которых опустим.

Теперь применим (3) для вычисления $f^{p^{\lambda+1}}(x) \pmod{p^{\lambda+2}}$. Положим

$$A_i(x) = (f^i(x))_2' = \prod_{j=0}^{i-1} f_2'(f^j(x));$$

$$B_i(x) = (f^i(x))_2' \sum_{k=0}^{i-1} \frac{(f^k(x))_2'}{f_2'(f^k(x))}\theta(f^k(x)) =$$

$$= \left(\prod_{j=0}^{i-1} f_2'(f^j(x))\right)\cdot\left(\sum_{k=0}^{i-1} \frac{\theta(f^k(x))}{f_2'(f^k(x))^2} \prod_{\tau=0}^{k} f_2'(f^\tau(x))\right).$$

Из леммы 4.6 следует, что

$$f_2'(c + p^\lambda h) \equiv \begin{cases} f_2'(c) \pmod{p^2}, & \text{если } h = 0; \\ f_2'(c) \pmod p, & \text{если } h \neq 0. \end{cases} \tag{5}$$

Поскольку f транзитивна по модулю p^λ, то сравнение (5) влечет $f_2'(f^k(x)) \equiv f_2'(f^r(x)) \pmod p$ как только $k \equiv r \pmod{p^\lambda}$. Кроме того, ввиду 4.5 из последнего условия следует также, что $\theta(f^k(x)) \equiv \theta(f^r(x)) \pmod p$.

Далее,

$$\prod_{\tau=0}^{p^\lambda-1} f_2'(f^\tau(x)) \equiv 1 \pmod p. \tag{6}$$

что, фактически, было уже установлено при доказательстве леммы 3.15 (см. там вывод равенства (6)), поскольку $N_1(f) \leqslant \lambda$ ввиду 4.5. Следовательно, $\prod_{\tau=0}^{k} f_2'(f^\tau(x)) \equiv \prod_{\tau=0}^{r} f_2'(f^\tau(x)) \pmod p$ как только $k \equiv r \pmod{p^\lambda}$. Окончательно заключаем, что

$$B_{tp^\lambda}(x) \equiv t \sum_{\tau=0}^{p^\lambda-1} \frac{\theta(f^\tau(x))}{f_2'(f^\tau(x))^2} \prod_{\nu=0}^{\tau} f_2'(f^\nu(x)) \equiv tB_{p^\lambda}(x) \pmod p \tag{7}$$

для всех $t \in \mathbb{N}$.

Вычислим теперь $A_{tp^\lambda}(x) \bmod p^2$ для $t \in \mathbb{N}$. Сравнение (3) ввиду сравнений (6) и $(f^k(x))'_2 \equiv \prod_{j=0}^{k-1} f'_2(f^j(x)) \pmod{p^2}$ означает, что

$$f^{kp^\lambda+\tau}(x) \equiv f^\tau(x) + kp^\lambda \xi(x) \prod_{j=0}^{\tau-1} f'_2(f^j(x)) \pmod{p^{\lambda+1}} \tag{8}$$

при всех $k \in \mathbb{N}$ и всех $\tau \in \{0, 1, \dots, p^\lambda - 1\}$. Но, поскольку

$$A_{tp^\lambda}(x) = \prod_{k=0}^{t-1} \prod_{\tau=0}^{p^\lambda-1} f'_2(f^{kp^\lambda+\tau}(x)),$$

то ввиду (5) и 4.6 из сравнения (8) получаем, что

$$A_{tp^\lambda}(x) = \prod_{k=0}^{t-1} \prod_{\tau=0}^{p^\lambda-1} f'_2\left(f^\tau(x) + kp^\lambda \xi(x) \prod_{j=0}^{\tau-1} f'_2(f^j(x))\right) \pmod{p^2},$$

откуда в силу 4.6 следует, что

$$A_{tp^\lambda}(x) = \prod_{k=0}^{t-1} \prod_{\tau=0}^{p^\lambda-1} \left(f'_2(f^\tau(x)) + 2kp\xi(x)\theta(f^\tau(x)) \prod_{j=0}^{\tau-1} f'_2(f^j(x))\right) \equiv$$

$$\equiv \prod_{k=0}^{t-1} \left(\prod_{\tau=0}^{p^\lambda-1} f'_2(f^\tau(x)) + \right.$$

$$\left. + 2kp\xi(x) \sum_{s=0}^{p^\lambda-1} \theta(f^s(x)) \frac{\prod_{j=0}^{p^\lambda-1} f'_2(f^j(x))}{f'_2(f^s(x))} \prod_{j=0}^{s-1} f'_2(f^j(x))\right) \pmod{p^2}. \tag{9}$$

Однако, из (6) вытекает, что $\prod_{j=0}^{p^\lambda-1} f'_2(f^j(x)) = 1 + p\varepsilon$ для подходящего $\varepsilon \in \mathbb{Z}_p$; следовательно, в силу (9) имеем:

$$A_{tp^\lambda}(x) \equiv \prod_{k=0}^{t-1} \left(1 + p\varepsilon + 2kp\xi(x) \sum_{s=0}^{p^\lambda-1} \theta(f^s(x)) \frac{\prod_{j=0}^{s-1} f'_2(f^j(x))}{f'_2(f^s(x))}\right) \equiv$$

$$\equiv 1 + tp\varepsilon + 2p\xi(x) \left(\sum_{k=0}^{t-1} k\right) \cdot \left(\sum_{s=0}^{p^\lambda-1} \theta(f^s(x)) \frac{\prod_{j=0}^{s-1} f'_2(f^j(x))}{f'_2(f^s(x))^2}\right) \equiv$$

$$\equiv 1 + tp\varepsilon + pt(t-1)\xi(x) \sum_{s=0}^{p^\lambda-1} \theta(f^s(x)) \frac{\prod_{j=0}^{s-1} f'_2(f^j(x))}{f'_2(f^s(x))^2} \pmod{p^2}. \tag{10}$$

Теперь, ввиду (2), (3), (7) и (10), заключаем, что

$$f^{(t+1)p^\lambda}(x) \equiv f^{tp^\lambda+p^\lambda}(x) \equiv$$

$$\equiv f^{tp^\lambda}(x) + p^\lambda \xi(x) + \varepsilon tp^{\lambda+1}\xi(x) + p^{\lambda+1}t^2\xi(x)^2 B_{p^\lambda}(x) \pmod{p^{\lambda+2}}. \tag{11}$$

Наконец, комбинируя (11) и (2) с очевидной индукцией по n, мы окончательно получаем, что

$$f^{np^\lambda}(x) \equiv x + np^\lambda\xi(x) + \varepsilon p^{\lambda+1}\xi(x)\frac{n(n-1)}{2} + \\ + p^{\lambda+1}\xi(x)^2 B_{p^\lambda}(x)\frac{n(n-1)(2n-1)}{6} \pmod{p^{\lambda+2}}.$$

В частности,

$$f^{p^{\lambda+1}}(x) \equiv x + p^{\lambda+1}\xi(x) \pmod{p^{\lambda+2}},$$

поскольку $p \neq 2, 3$. Однако ввиду (2) из последнего сравнения вытекает справедливость сравнения (1), что доказывает теорему 4.1. $\square$

Замечание. С помощью теоремы 4.1 можно проверить, является ли данный целозначный и совместимый полином $f(x) \in \mathbb{Q}_p[x]$ эргодическим. Представим $f(x)$ в виде $f(x) = \frac{g(x)}{r}$, где $r \in \mathbb{Z}_p$ и $g(x) \in \mathbb{Z}_p[x]$, причем по крайней мере один из коэффициентов полинома $g(x)$ не делится на p. На самом деле в качестве r можно взять общий знаменатель всех коэффициентов полинома $f(x)$, представленных в виде несократимых дробей. Здесь мы предполагаем, что полином $f(x)$ представлен в базисе из убывающих факториальных степеней $(x)_0 = 1, (x)_1 = x, (x)_2 = x(x-1), \ldots$ или в стандартном степенном базисе $1, x, x^2, \ldots$. Тогда $\rho(f) = \operatorname{ord}_p r$, причем $\rho(f)$ не зависит от выбора конкретного базиса. Теперь мы легко находим $\lambda(f)$ и определяем, является ли полином f транзитивным на $\mathbb{Z}/p^{\lambda(f)+1}$ (например, прямой проверкой). В силу теоремы 4.1 при $p \neq 2, 3$ это эквивалентно эргодичности полинома $f(x)$ (при $p = 3$ нужно исследовать транзитивность f на кольце $\mathbb{Z}/p^{\lambda(f)+2}$).

Более того, оказывается, что полученные результаты дают возможность при любом простом p проверить, является ли данный полином $f(x) \in \mathbb{Q}_p[x]$ целозначным, совместимым и эргодическим, подсчитав его значения в $O(\deg f)$ точках. Именно, справедливо следующее

4.7 Предложение. *Полином $f(x) \in \mathbb{Q}_p[x]$ является целозначным, совместимым и эргодическим тогда и только тогда, когда отображение*

$$z \mapsto f(z) \bmod p^{\lfloor \log_p(\deg f)\rfloor + 3},$$

где z пробегает значения $0, 1, \ldots, p^{\lfloor \log_p(\deg f)\rfloor+3} - 1$, задает совместимую и транзитивную функцию на кольце вычетов $\mathbb{Z}/p^{\lfloor \log_p(\deg f)\rfloor+3}$.

Доказательство. Коэффициенты $a_i \in \mathbb{Q}_p$ $(i = 0, 1, \ldots, d)$ полинома $f(x)$ степени d, представленного в виде $f(x) = \sum_{i=0}^{d} a_i \binom{x}{i}$ (см. $(\diamondsuit)$ из раздела 2), определяются его значениями в точках $0, 1, \ldots, d$. Другими словами, все значения $f(0), f(1), \ldots, f(d)$ являются p-адическими целыми числами тогда и только тогда, когда все коэффициенты $a_i \in \mathbb{Q}_p$ $(i = 0, 1, \ldots, d)$ есть p-адические целые, т.е. тогда и только тогда, когда полином $f(x)$ целозначен (см. начало раздела 2). По аналогичным соображениям, ввиду теоремы 2.1 полином $f(x)$ сохраняет все конгруэнции кольца $\mathbb{Z}/p^{\lfloor \log_p d\rfloor+1}$ тогда и только тогда, когда $\|a_i\| \leqslant p^{-\lfloor \log_p i\rfloor}$ для всех $i = 1, 2, \ldots, d$, т.е. тогда и только тогда, когда $f(x)$

совместим на $\mathbb{Z}_p$. Другими словами, для проверки целозначности и совместимости полинома $f(x)$ достаточно (и необходимо) ограничиться проверкой того, что он индуцирует совместимую функцию на кольце $\mathbb{Z}/p^k$ при некотором произвольным образом фиксированном $k \geqslant \lfloor \log_p d \rfloor + 1$.

В силу теоремы 4.1, при $p \neq 2$ целозначный совместимый полином $f(x)$ эргодичен тогда и только тогда, когда он транзитивен по модулю p^k для некоторого произвольно фиксированного $k \geqslant \lambda(f) + 2$. Представив $f(x)$ в виде $f(x) = b_0 + \sum_{i=1}^{d} b_i p^{\lfloor \log_p i \rfloor} \binom{x}{i}$, где $b_j \in \mathbb{Z}_p$ для $j = 0, 1, 2, \ldots$, заключаем, что $\rho(f)$ есть наименьшее неотрицательное рациональное целое число, не меньшее каждого из чисел $\operatorname{ord}_p i! - \lfloor \log_p i \rfloor - \operatorname{ord}_p b_i$ $(i = 1, 2, \ldots, d)$, а поскольку функция $\operatorname{ord}_p i! - \lfloor \log_p i \rfloor$ неубывающая (см. доказательство леммы 4.2), то любое $k \in \mathbb{N}$, удовлетворяющее неравенству $2\frac{p^k - 1}{p-1} - k > \operatorname{ord}_p d! - \lfloor \log_p d \rfloor$, удовлетворяет и неравенству $k \geqslant \lambda(f)$. Но поскольку $\operatorname{ord}_p d! = \frac{1}{p-1}(d - \operatorname{wt}_p d)$, где $\operatorname{wt}_p d$ есть сумма всех цифр в p-ичном представлении числа d, то выбрав любое $k \in \mathbb{N}$, удовлетворяющее неравенству

$$2\frac{p^k - 1}{p-1} - k > \frac{d}{p-1}, \tag{1}$$

получим, что $k \geqslant \lambda(f)$. Элементарные рассуждения показывают, однако, что $k = \lfloor \log_p d \rfloor + 1$ удовлетворяет неравенству (1), тем самым доказывая предложение при $p \neq 2$.

В случае $p = 2$ полином $f(x) \in \mathbb{Q}_2[x]$ степени d целозначен, совместим и эргодичен тогда и только тогда, когда он имеет вид

$$f(x) = 1 + x + \sum_{i=0}^{d} b_i \, 2^{\lfloor \log_2 (i+1) \rfloor + 1} \binom{x}{i}, \tag{2}$$

где $b_i \in \mathbb{Z}_2$, $i = 0, 1, 2, \ldots, d$ (см. теорему 2.3). Так как коэффициенты полинома $f(x)$, представленного в базисе $\binom{x}{i}$, $i = 0, 1, 2, \ldots$, однозначно определяются значениями $f(z)$ в точках $z = 0, 1, \ldots, d$, то проверить выполнимость условия (2) для полинома $f(x)$ можно, подсчитав его значения в точках $z = 0, 1, \ldots, 2^r - 1$, где $r \in \mathbb{N}$ произвольно фиксированное число, удовлетворяющее условию $d \leqslant 2^r - 1$. Поэтому можно взять, например, $r = \lfloor \log_2 (d+1) \rfloor + 1$, или $r = \lfloor \log_2 d \rfloor + 3$. Это завершает доказательство предложения 4.7. $\square$

Замечание. Предложение 4.4 показывает, что при $p \neq 2$ функция $f \in \mathcal{A}$ удовлетворяет условиям предложения 3.9; значит, поскольку $N_1(f) \leqslant N_2(f)$, функция f сохраняет меру тогда и только тогда, когда она биективна по модулю $p^{\lambda(f)+2}$. Рассуждениями, аналогичными проведенным при доказательстве предложения 4.7, можно тогда доказать

4.8 Предложение. *Полином $f(x) \in \mathbb{Q}_p[x]$ целозначен, совместим и сохраняет меру тогда и только тогда, когда отображение $z \mapsto f(z) \bmod p^{K_f}$, где $K_f = \lfloor \log_p (\deg f) \rfloor + 3$, а z пробегает значения $0, 1, \ldots, p^{K_f} - 1$, задает совместимую и биективную функцию на кольце вычетов $\mathbb{Z}/p^{K_f}$.* $\square$

И вновь оценки величин $\zeta(f)$ и $\eta(f)$, о которых шла речь в начале данного раздела, могут быть значительно уточнены для различных подклассов из $\mathcal{A}$ по

сравнению с теми, которые дают теорема 4.1 и предложения 4.7 и 4.8. Важным, например, представляется случай функций, аналитических всюду на $\mathbb{Z}_p$, т.е. функций, представимых в виде сумм сходящихся всюду на $\mathbb{Z}_p$ степенных рядов.

Хорошо известно (см., например, [3, гл. 14. раздел 4]), что степенной ряд $\sum_{i=0}^{\infty} c_i x^i$ $(c_i \in \mathbb{Q}_p,\ i = 0, 1, 2 \dots)$ сходится всюду на $\mathbb{Z}_p$ тогда и только тогда, когда $\lim\limits_{i\to\infty}\limits^{p} c_i = 0$; при выполнении последнего условия ряд задает непрерывную на $\mathbb{Z}_p$ функцию. Разумеется, в общем случае эта функция не является даже целозначной, не говоря уже о совместимости. Рассмотрим, однако, частный случай, когда все коэффициенты c_i есть p-адические целые. Именно, в кольце $\mathbb{Z}_p[[x]]$ формальных степенных рядов от переменной x над кольцом $\mathbb{Z}_p$ обозначим через $\mathcal{C}(x)$ подмножество всех рядов

$$s(x) = \sum_{i=0}^{\infty} c_i x^i \quad (c_i \in \mathbb{Z}_p,\ i = 0, 1, 2 \dots),$$

сходящихся всюду на $\mathbb{Z}_p$. Другими словами, $s(x) \in \mathcal{C}(x)$ тогда и только тогда, когда $\lim\limits_{i\to\infty}\limits^{p} c_i = 0$. При выполнении этих условий ряд $s(x) \in \mathcal{C}(x)$ задает определенную всюду на $\mathbb{Z}_p$ целозначную функцию $s : \mathbb{Z}_p \to \mathbb{Z}_p$. Оказывается, эта функция s равномерно дифференцируема и имеет целозначную производную всюду на $\mathbb{Z}_p$.

Действительно, рассмотрим формальную производную $s'(x) \in \mathbb{Z}_p[[x]]$ ряда $s(x)$:

$$s'(x) = \sum_{i=1}^{\infty} i c_i x^{i-1}.$$

Поскольку $0 \leqslant \|ic_i\|_p = \|i\|_p \|c_i\|_p \leqslant \|c_i\|_p$, а $\lim\limits_{i\to\infty}\limits^{p} c_i = 0$, то $\lim\limits_{i\to\infty}\limits^{p} ic_i = 0$ и, значит, $s'(x) \in \mathcal{C}(x)$. Мы утверждаем, что функция $s' : \mathbb{Z}_p \to \mathbb{Z}_p$ есть производная функции $s : \mathbb{Z}_p \to \mathbb{Z}_p$ по p-адической метрике.

В самом деле, известно, что в кольце $\mathbb{Z}_p[[x, y]]$ всех формальных степенных рядов от переменных x, y над $\mathbb{Z}_p$ справедливо равенство

$$s(x + y) = \sum_{i=0}^{\infty} \frac{s^{(i)}(x)}{i!} y^i,$$

где $s^{(i)}(x) \in \mathbb{Z}_p[[x]]$ $(i = 1, 2, \dots)$ есть i-я формальная производная ряда $s(x)$, а $s^{(0)}(x) = s(x)$. По доказанному выше, $s^{(i)}(x) \in \mathcal{C}(x)$ для всех $i = 0, 1, 2, \dots$. Стало быть,

$$\frac{s^{(i)}(u)}{i!} = \sum_{j=i}^{\infty} c_j \binom{j}{i} u^{j-i} \in \mathbb{Z}_p$$

для каждого $u \in \mathbb{Z}_p$. Но

$$\left\| \frac{s^{(i)}(u)}{i!} \right\|_p = \left\| \sum_{j=i}^{\infty} c_j \binom{j}{i} u^{j-i} \right\|_p \leqslant \max\{\|c_j\|_p : j = i, i+1, \dots\},$$

а значит,

$$\lim_{i\to\infty}^{p} \frac{s^{(i)}(u)}{i!} = 0,$$

поскольку $\lim\limits_{i\to\infty}^{p} c_i = 0$. Таким образом, для любого $u \in \mathbb{Z}_p$

$$s(u+y) = \sum_{i=0}^{\infty} \frac{s^{(i)}(u)}{i!} y^i \in \mathcal{C}(y). \qquad (\spadesuit)$$

Итак, если $s(x) \in \mathcal{C}(x)$, то ряд Тейлора ($\spadesuit$) в точке $u \in \mathbb{Z}_p$ сходится к s всюду на $\mathbb{Z}_p$. В частности, при $h \in \mathbb{Z}_p$ имеем

$$s(u+h) = s(u) + s'(u)h + \alpha(u,h),$$

причем $\lim\limits_{h\to 0}^{p} \dfrac{\alpha(u,h)}{h} = \lim\limits_{h\to 0}^{p} h \sum_{i=2}^{\infty} \frac{s^{(i)}(u)}{i!} h^{i-2} = 0$, поскольку $\sum_{i=2}^{\infty} \frac{s^{(i)}(u)}{i!} h^{i-2} \in \mathbb{Z}_p$, ввиду того, что $\lim\limits_{i\to\infty}^{p} \frac{s^{(i)}(u)}{i!} = 0$, что показано выше. Итак, $s'(u)$ есть производная функции s в точке u. Таким образом, множество $\mathcal{C}(x)$ замкнуто относительно дифференцирований, и все функции, задаваемые рядами из $\mathcal{C}(x)$, дифференцируемы неограниченное число раз.

Далее, пусть

$$s(x) = \sum_{i=0}^{\infty} s_i \binom{x}{i}$$

есть интерполяционный ряд для функции $s(x) \in \mathcal{C}(x)$. Утверждается, что тогда $\dfrac{s_i}{i!}$ есть целое p-адическое число при всех $i = 0, 1, 2, \ldots$. Действительно,

$$s(x) = \sum_{k=0}^{\infty} c_k x^k = \sum_{k=0}^{\infty} c_k \sum_{i=0}^{k} S_2(k,i) i! \binom{x}{i} = \sum_{i=0}^{\infty} i! \binom{x}{i} \sum_{k=i}^{\infty} S_2(k,i) c_k,$$

где $S_2(k,i)$ – число Стирлинга. Так как $\lim\limits_{i\to\infty}^{p} c_i = 0$, то $\lim\limits_{k\to\infty}^{p} S_2(k,i) c_k = 0$, поскольку все числа Стирлинга $S_2(k,i)$ являются рациональными целыми, т.е. $\|S_2(k,i)\|_p \leqslant 1$. Следовательно, ряд $\sum_{k=i}^{\infty} S_2(k,i) c_k$ сходится к некоторому $A_i \in \mathbb{Z}_p$ при всех $i = 0, 1, 2, \ldots$. Это доказывает утверждение, поскольку

$$s_i = i! A_i \quad (i = 0, 1, 2, \ldots). \qquad (\bigstar)$$

Положим

$$\mathcal{B}(x) = \left\{ f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i} : \frac{a_i}{i!} \in \mathbb{Z}_p, \quad i = 0, 1, 2, \ldots \right\}.$$

Другими словами, $\mathcal{B}(x)$ есть кольцо формальных степенных рядов с целыми p-адическими коэффициентами относительно убывающих факториальных степеней. Каждый ряд $f(x) \in \mathcal{B}(x)$ корректно задает целозначную и равномерно

непрерывную на $\mathbb{Z}_p$ функцию $f : \mathbb{Z}_p \to \mathbb{Z}_p$ (см. начало раздела 2). Эта функция f совместима ввиду 2.1, поскольку, как показано при доказательстве леммы 4.2, функция $\operatorname{ord}_p(i!) - \lfloor \log_p i \rfloor$ неотрицательная и неубывающая. Обозначим через $\mathcal{B}$ (соответственно, через $\mathcal{C}$) совокупность всех функций на $\mathbb{Z}_p$, задаваемых рядами из $\mathcal{B}(x)$ (соответственно, из $\mathcal{C}(x)$). Очевидно, что $\mathcal{B}(x)$, $\mathcal{B}$, $\mathcal{C}(x)$, $\mathcal{C}$ – кольца.

Заметим, что если два ряда различны как элементы из $\mathcal{B}(x)$ (соответственно, из $\mathcal{C}(x)$), то и задаваемые ими функции на $\mathbb{Z}_p$ различны. Для рядов из $\mathcal{B}(x)$ см. по этому поводу начало раздела 2. Что же касается рядов из $\mathcal{C}(x)$, то утверждение следует из того, что, поскольку выписанный выше интерполяционный ряд для $s(x) \in \mathcal{C}(x)$ задает функцию, тождественно равную нулю, тогда и только тогда, когда все его коэффициенты s_i равны 0, то и $A_i = 0$, $i = 0, 1, 2, \ldots$, (см. (★)); но $A_i = \sum_{k=i}^{\infty} S_2(k,i)c_k$, поэтому по формулам обращения $c_i = \sum_{k=i}^{\infty} S_1(k,i)A_k = 0$, где $S_1(k,i), S_2(k,i)$ есть числа Стирлинга, соответственно, первого и второго родов.

Итак, кольца $\mathcal{B}(x)$ и $\mathcal{B}$ (соответственно, $\mathcal{C}(x)$ и $\mathcal{C}$) изоморфны, и мы в дальнейшем можем не различать ряды и задаваемые ими функции.

Отметим, далее, что установленное выше (см. (★)) включение $\mathcal{B} \supset \mathcal{C}$ строгое. Очевидно, что $f(x) = \sum_{i=0}^{\infty}(x)_i \in \mathcal{B}$, поскольку $f(x) = \sum_{i=0}^{\infty} i!\binom{x}{i}$. Однако $f(x) \notin \mathcal{C}$, поскольку функция f не является даже аналитической на $\mathbb{Z}_p$: согласно [3, гл. 14, теорема 4] функция, представленная интерполяционным рядом (♢) (см. раздел 2) аналитична на $\mathbb{Z}_p$ тогда и только тогда, когда $\lim\limits_{i\to\infty}{}^{p} \frac{a_i}{i!} = 0$.

Таким образом, функция из $\mathcal{B}$ (в отличие от функций из $\mathcal{C}$), вообще говоря, не может быть представлена в виде сходящегося всюду на $\mathbb{Z}_p$ ряда Тейлора. Тем не менее, все функции из $\mathcal{B}$ дифференцируемы во всех точках из $\mathbb{Z}_p$, причем $\mathcal{B}$ замкнуто относительно дифференцирований: если $f \in \mathcal{B}$, то $f' \in \mathcal{B}$.

Действительно, согласно [3, гл. 13, теорема 2], равномерно непрерывная на $\mathbb{Z}_p$ функция f, представленная своим интерполяционным рядом (♢), дифференцируема всюду на $\mathbb{Z}_p$ тогда и только тогда, когда

$$\lim_{i\to\infty}{}^{p} \frac{a_{i+n}}{i} = 0 \qquad (\blacklozenge)$$

для всех $n \in \mathbb{N}_0$. Это условие, очевидно, выполнено для функции $f \in \mathcal{B}$, поскольку $\operatorname{ord}_p a_i \geqslant \operatorname{ord}_p(i!) = \frac{1}{p-1}(i - \operatorname{wt}_p i)$, а $\lfloor \log_p i \rfloor \geqslant \operatorname{ord}_p i$ для всех $i = 0, 1, 2, \ldots$. Таким образом, производная f' определена всюду на $\mathbb{Z}_p$, причем

$$f'(x) = \sum_{i=1}^{\infty}(-1)^{i+1}\frac{\Delta^i f(x)}{i},$$

если этот ряд сходится. Но $\frac{\Delta^i f(x)}{i} = \frac{1}{i}\sum_{j=i}^{\infty} a_j\binom{x}{j-i}$, следовательно

$$\sum_{i=1}^{\infty}(-1)^{i+1}\frac{\Delta^i f(x)}{i} = \sum_{k=0}^{\infty}\binom{x}{k}\sum_{i=1}^{\infty}(-1)^{i+1}\frac{a_{k+i}}{i}.$$

Но ряд $\sum_{i=1}^{\infty}(-1)^{i+1}\frac{a_{k+i}}{i}$ ввиду (♦) сходится при каждом $k \in \mathbb{N}_0$ к некоторому $S_k \in \mathbb{Q}_p$, причем $\operatorname{ord}_p \frac{a_{k+i}}{i} = \operatorname{ord}_p a_{k+i} - \operatorname{ord}_p i \geqslant \operatorname{ord}_p((k+i)!) - \lfloor \log_p i \rfloor =$

$\frac{1}{p-1}(i+k-\mathrm{wt}_p\,(i+k))-\lfloor\log_p i\rfloor=\frac{1}{p-1}(i-\mathrm{wt}_p\,i)-\lfloor\log_p i\rfloor+\frac{1}{p-1}(k-\mathrm{wt}_p\,k)+\frac{1}{p-1}(\mathrm{wt}_p\,k-\mathrm{wt}_p\,(i+k)+\mathrm{wt}_p\,i)\geqslant\frac{1}{p-1}(k-\mathrm{wt}_p\,k)=\mathrm{ord}_p\,(k!)$ (последнее из неравенств справедливо в силу того, что $\frac{1}{p-1}(i-\mathrm{wt}_p\,i)\geqslant\lfloor\log_p i\rfloor$ и $\frac{1}{p-1}(\mathrm{wt}_p\,k-\mathrm{wt}_p\,(i+k)+\mathrm{wt}_p\,i)=\mathrm{ord}_p\binom{i+k}{i}\geqslant 0$). Таким образом, $\dfrac{S_k}{k!}\in\mathbb{Z}_p$ для всех $k\in\mathbb{N}_0$; значит, $f'\in\mathcal{B}$.

С помощью полученных результатов теперь может быть доказана следующая

4.9 Теорема. *Функция $f\in\mathcal{B}$ сохраняет меру тогда и только тогда, когда она биективна по модулю p^2. Функция f эргодична тогда и только тогда, когда она транзитивна либо по модулю p^2, если $p\neq 2,3$, либо по модулю p^3, если $p\in\{2,3\}$.*

Доказательство. Из определения множества $\mathcal{B}$ сразу вытекает, что $\rho(f)=0$ для любой $f\in\mathcal{B}$, а потому $\lambda(f)=1$; значит, при $p\neq 2$ вторая часть утверждения следует из 4.1.

Для доказательства первой части утверждения теоремы в силу 3.9, достаточно показать, что функция f равномерно дифференцируема по модулю p и $N_1(f)\leqslant 1$, т.е. что

$$f(z+p^k r)\equiv f(z)+p^k r f'(z)\pmod{p^{k+1}}\tag{1}$$

для всех $z,r\in\mathbb{Z}_p$ и $k=1,2,\ldots$. Поскольку $f,f'\in\mathcal{B}$, то они обе совместимы, а значит достаточно доказать справедливость (1) при условии $z,r\in\mathbb{N}_0$. Так как при $r=0$ сравнение (1) тривиально, то можно считать, что $p^k r=n\in\mathbb{N}$. Далее, ввиду того, что $\frac{f(z+n)-f(z)}{n}=\sum_{i=1}^{\infty}\binom{n-1}{i-1}\frac{\Delta^i f(x)}{i}$, а $f'(z)=\sum_{i=1}^{\infty}(-1)^{i+1}\frac{\Delta^i f(z)}{i}$, то для доказательства справедливости (1) достаточно установить, что

$$\sum_{i=1}^{\infty}\left(\binom{n-1}{i-1}-(-1)^{i+1}\right)\frac{\Delta^i f(z)}{i}\equiv 0\pmod p.\tag{2}$$

Но $\frac{\Delta^i f(x)}{i}=\frac{1}{i}\sum_{j=i}^{\infty}a_j\binom{x}{j-i}$, поэтому, ввиду 4.2, при $p\neq 2$ имеет место $\frac{\Delta^i f(x)}{i}\equiv 0\pmod p$ для всех $i\geqslant 2p$; значит, в этом случае (2) эквивалентно сравнению

$$\sum_{i=1}^{2p-1}\left(\binom{n-1}{i-1}-(-1)^{i+1}\right)\frac{\Delta^i f(z)}{i}\equiv 0\pmod p.\tag{3}$$

Однако, поскольку f совместима, то $\frac{\Delta^i f(x)}{i}\not\equiv 0\pmod p$ лишь, может быть, при $i=sp^m$, где $m\in\mathbb{N}_0$, $s\in\{1,2,\ldots,p-1\}$ (см. [11, лемма 3.4]); но тогда, поскольку $n=p^k r$, справедливость сравнения (3) немедленно следует из уже упоминавшейся теоремы Люка, доказывая тем самым первую часть утверждения теоремы 4.9 при $p\neq 2$. Если же $p=2$, то (2) эквивалентно сравнению

$$\sum_{i=0}^{\infty}\left(\binom{2^k r-1}{2^i-1}+1\right)\frac{\Delta^{2^i} f(z)}{2^i}\equiv 0\pmod 2.\tag{4}$$

Но, поскольку $\frac{a_j}{j!} \in \mathbb{Z}_2$ для всех $j = 0, 1, 2, \ldots$, то $\operatorname{ord}_2 a_{2^i+m} \geqslant \operatorname{ord}_2 (2^i)! = 2^i - 1$ для всех $m = 0, 1, 2, \ldots$; значит $\frac{\Delta^{2^i} f(z)}{2^i} \not\equiv 0 \pmod 2$ лишь, может быть, при $i = 0$, что означает справедливость (4).

Наконец, вторая часть утверждения теоремы 4.9 при $p = 2$ следует из 2.3: поскольку $\operatorname{ord}_2 i! \leqslant \operatorname{ord}_2 a_i$ для всех $i = 0, 1, 2, \ldots$, и $\operatorname{ord}_2 i! = i - \operatorname{wt}_2(i)$, элементарными рассуждениями несложно показать, что $\lfloor \log_2(i+1) \rfloor + 1 \leqslant i - \operatorname{wt}_2(i) \leqslant \operatorname{ord}_2 a_i$ при $i \geqslant 4$; при этом $\operatorname{ord}_2 a_i \geqslant 3$. Но это означает, что необходимые и достаточные условия для эргодичности условия на коэффициенты интерполяционного ряда ($\diamondsuit$) (см. раздел 2) функции f заведомо выполнены для всех коэффициентов a_i при $i \geqslant 4$; при этом выполнимость этих условий для оставшихся коэффициентов эквивалентна транзитивности функции f по модулю 8, поскольку $a_i \equiv 0 \pmod 8$ при $i \geqslant 4$. $\square$

Замечание. Теорема 4.9 показывает, что необходимые и достаточные условия транзитивности по модулю p^n для полиномов с целыми рациональными коэффициентами, полученные М. В. Лариным в [15], остаются справедливыми для более широкого класса (именно, класса $\mathcal{B}$) функций. Оказывается, однако, что все эти функции по любому модулю p^n могут быть заданы полиномами с рациональными целыми коэффициентами.

Именно, из определения множества $\mathcal{B}$ легко следует, что каждая функция $f \in \mathcal{B}$ равномерно аппроксимируема полиномами над $\mathbb{Z}_p$: для любого $n \in \mathbb{N}$ найдется полином $f_n(x) \in \mathbb{Z}_p[x]$ такой, что $f(z) \equiv f_n(z) \pmod{p^n}$ для всех $z \in \mathbb{Z}_p$. В самом деле, поскольку ряд $\sum_{j=0}^{\infty} r_j \binom{x}{j}$ задает функцию, тождественно равную 0 по модулю p^n тогда и только тогда, когда все $r_j \equiv 0 \pmod{p^n}$ (см. [11, предложение 4.2]), то можно положить $f_n(x) = \sum_{i=0}^{\omega(n)} a_i \binom{x}{i}$, где $\omega(n) = \max\{j \in \mathbb{N}_0 : \frac{1}{p-1}(j - \operatorname{wt}_p j) < n\}$.

Оказывается, верно и обратное: если некоторая функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ равномерно аппроксимируема полиномами над $\mathbb{Z}_p$ в указанном выше смысле, то она лежит в $\mathcal{B}$. В самом деле, пусть $f(z) \equiv f_i(z) \pmod{p^i}$ для всех $z \in \mathbb{Z}_p$, где $f_i(x) \in \mathbb{Z}_p[x]$, $i = 1, 2, \ldots$. Каждый полином $f_i(x)$ степени d_i допускает одно и только одно представление в виде интерполяционного ряда ($\diamondsuit$) (см. раздел 2): $f_i(x) = \sum_{j=0}^{d_i} a_{ij} \binom{x}{j}$, где $a_{ij} \in \mathbb{Z}_p$ и $\operatorname{ord}_p a_{ij} \geqslant \operatorname{ord}_p (j!)$ в силу ($\bigstar$), поскольку, очевидно, $f_i \in \mathcal{C} \subset \mathcal{B}$. Для данной функции f каждый полином $f_i(x)$ определен однозначно с точностью до слагаемого, задающего функцию, тождественно равную 0 по модулю p^i, поэтому можно считать, что $d_i = \omega(i)$ (см. выше), а тогда коэффициенты полинома $f_i(x)$ определены однозначно с точностью до слагаемых с нормой, не превосходящей p^{-i}. Отсюда следует, что $a_{i+1,j} \equiv a_{ij} \pmod{p^i}$ (мы полагаем $a_{ij} = 0$ при $j > \omega(i)$). Это означает, что $\lim\limits_{i \to \infty}\limits^{p} a_{ij} = a_j \in \mathbb{Z}_p$, причем $\frac{a_j}{j!} \in \mathbb{Z}_p$. Следовательно, ряд $\sum_{i=0}^{\infty} a_i \binom{x}{i}$ задает равномерно непрерывную на $\mathbb{Z}_p$ функцию $\tilde{f} \in \mathcal{B}$, которая совпадает с f, поскольку $f(z) \equiv f_i(z) \equiv \tilde{f}(z) \pmod{p^i}$ для всех $z \in \mathbb{Z}_p$ и всех $i = 1, 2, \ldots$.

Итак, на кольце $\mathcal{B}$ можно задать неархимедову норму, положив ее равной $\max\{\|f(z)\|_p : z \in \mathbb{Z}_p\}$ для каждой функции $f \in \mathcal{B}$. Из доказанного легко следует, что относительно метрики D_p, индуцированной этой нормой, кольцо $\mathcal{B}$ является полным метрическим пространством: фактически, $\mathcal{B}$ есть пополне-

ние по метрике D_p пространства $\mathcal{P} \subset \mathcal{C}$ всех функций, индуцированных на $\mathbb{Z}_p$ всевозможными полиномами с рациональными целыми коэффициентами (в частности, пространство $\mathcal{B}$ сепарабельно).

В свою очередь, отсюда вытекает, что $\mathcal{B}$ (в отличие от $\mathcal{C}$) замкнуто относительно композиции функций: если $f, g \in \mathcal{B}$, то $f(g) \in \mathcal{B}$. В самом деле, пусть g равномерно аппроксимируется последовательностью $\{g_n(x) \in \mathbb{Z}_p[x] : n = 1, 2, \dots\}$, т.е. $g_n(z) \equiv g(z) \pmod{p^n}$ для всех $z \in \mathbb{Z}_p$. Из совместимости функции f следует тогда, что $D_p(f(g), f(g_n)) \leqslant p^{-n}$, т.е. последовательность $f(g_n)$ сходится к $f(g)$ относительно метрики D_p. Но $f(g_n) \in \mathcal{B}$ для любого $n = 1, 2, \dots$: если f равномерно аппроксимируется последовательностью $\{f_m(x) \in \mathbb{Z}_p[x] : m = 1, 2, \dots\}$, то $f_m(g_n(z)) \equiv f(g_n(z)) \pmod{p^m}$ для всех $z \in \mathbb{Z}_p$, т.е. последовательность $\{f_m(g_n(x)) \in \mathbb{Z}_p[x] : m = 1, 2, \dots\}$ сходится к функции $f(g_n)$ по метрике D_p, причем $f_m(g_n) \in \mathcal{B}$ как полином над $\mathbb{Z}_p$. Но тогда и $f(g) \in \mathcal{B}$ в силу полноты пространства $\mathcal{B}$.

Таким образом, доказано следующее

4.10 Предложение. *Кольцо $\mathcal{B}$ есть сепарабельное полное относительно метрики D_p пространство функций, дифференцируемых всюду на $\mathbb{Z}_p$, замкнутое относительно композиций и содержащее вместе с каждой функцией ее производную. Счетное множество $\mathcal{P}$ всех полиномиальных над $\mathbb{Z}$ функций всюду плотно в $\mathcal{B}$.* $\square$

С тем, чтобы пользоваться критерием 4.9 в прикладных целях для создания программно реализуемых генераторов псевдослучайных последовательностей, важно располагать запасом конкретных примеров функций из $\mathcal{B}$ и $\mathcal{C}$, которые могут быть реализованы программно. Как уже говорилось, все полиномиальные над $\mathbb{Z}_p$ функции, т.е. функции, задаваемые полиномами из $\mathbb{Z}_p[x]$, лежат в $\mathcal{C} \subset \mathcal{B}$.

Рациональные над $\mathbb{Z}_p$ функции, т.е. функции вида $f(x) = \frac{u(x)}{v(x)}$, где $u(x), v(x)$ полиномы над $\mathbb{Z}_p$, лежат в $\mathcal{B}$, если знаменатель не обращается в 0 по модулю p на $\mathbb{Z}_p$ (ввиду совместимости, последнее условие, очевидно, достаточно проверить лишь в точках $\{0, 1, \dots, p-1\}$). Действительно, так как при любом $z \in \mathbb{Z}_p$ элемент $v(z)$ имеет обратный в кольце вычетов $\mathbb{Z}/p^n$, то $\frac{u(z)}{v(z)} \equiv u(z)v(z)^{\varphi(p^n)-1} \pmod{p^n}$, где φ – функция Эйлера. Значит, функция f равномерно аппроксимируется полиномами $u(x)v(x)^{\varphi(p^n)-1} \in \mathbb{Z}_p[x]$, $n = 1, 2, \dots$; следовательно, она лежит в $\mathcal{B}$ в силу 4.10.

Еще один тип функций из $\mathcal{B}$ – экспоненциальные функции. Рассмотрим, например, функцию a^x, где $a \equiv 1 \pmod{p}$, т.е. $a = 1 + pr$ для подходящего $r \in \mathbb{Z}_p$. Тогда $a^x = \sum_{i=0}^{\infty} p^i r^i \binom{x}{i}$ и, как хорошо известно (см., например, [3, гл. 14, раздел 5]), если $p \neq 2$, то функция a^x является аналитической всюду на $\mathbb{Z}_p$ (и, значит, лежит в $\mathcal{C}$); если же $p = 2$ и r нечетно, то функция a^x не является аналитической на $\mathbb{Z}_2$ и, значит, не лежит в $\mathcal{C}$. Тем не менее, в последнем случае функция a^x лежит в $\mathcal{B}$, поскольку $(1 + 2r)^x = \sum_{i=0}^{\infty} 2^i r^i \binom{x}{i} \in \mathcal{B}$ ввиду того, что $\operatorname{ord}_2 (i!) = i - wt_2\, i$. Несложно показать также, что функция $(1 + 4r)^x$ лежит в $\mathcal{C}$. Итак, если $a \in \mathbb{Z}_p$, $a \equiv 1 \pmod{p}$, то функция a^x лежит в $\mathcal{B}$.

Рассмотренный тип экспоненциальных функций представляет собой частный случай функций вида u^v, где $u(z) \equiv 1 \pmod{p}$ для всех $z \in \mathbb{Z}_p$.

4.11 Лемма. *Если $u, v\colon \mathbb{Z}_p \to \mathbb{Z}_p$ — совместимые функции, и $u(z) \equiv 1 \pmod p$ для всех $z \in \mathbb{Z}_p$* (выполнимость последнего условия достаточно проверить лишь при $z = 0, 1, \dots, p-1$), *то функция $f(z) = u(z)^{v(z)}$ корректно определена для всех $z \in \mathbb{Z}_p$, целозначна и совместима. Более того, если $w, v \in \mathcal{B}$, $u(z) = 1 + pw(z)$, то $f \in \mathcal{B}$.*

Доказательство. То, что функция f корректно определена на $\mathbb{Z}_p$ и целозначна, сразу следует из проведенных выше рассуждениий о функциях вида a^x, где $a \equiv 1 \pmod p$. Для доказательства совместимости заметим, что если $b, c, d \in \mathbb{Z}_p$, то для любого $n = 1, 2, \dots$ справедливо равенство $(a + p^n b)^{c+p^n d} = (a + p^n b)^c((a + p^n b)^{p^n})^d$ (элементарные правила обращения со степенями в p-адическом и действительном случаях совпадают, [3, гл. 14, раздел 5]). Но, поскольку ввиду совместимости функций u и v, для любых $z, r \in \mathbb{Z}_p$ найдутся $s, t \in \mathbb{Z}_p$ такие, что $(u(z + p^n r))^{v(z+p^n r)} = (u(z) + p^n t)^{v(z)+p^n s}$, то $(u(z+p^n r))^{v(z+p^n r)} = (u(z)+p^n t)^{v(z)}((u(z)+p^n t)^{p^n})^s \equiv (u(z)+p^n t)^{v(z)} \pmod{p^n}$, ввиду того, что $(u(z) + p^n t)^{p^n} \equiv 1 \pmod{p^n}$. Докажем последнее сравнение.

Имеем $u(z) + p^n t = 1 + pk$ для подходящего $k \in \mathbb{Z}_p$, так как $u(z) \equiv 1 \pmod p$. Но $(1+pk)^{p^n} = \sum_{i=0}^{p^n} k^i p^i \binom{p^n}{i} = \sum_{i=0}^{p^n} k^i \frac{p^i}{i!}(p^n)_i \equiv 1 \pmod{p^n}$, поскольку $\frac{p^i}{i!} \in \mathbb{Z}_p$. Итак, окончательно, обозначая через $\overline{v(z)} = v(z) \bmod p^n$ наименьший неотрицательный вычет числа $v(z)$ по модулю p^n, получаем для подходящего $h \in \mathbb{Z}_p$, что $f(z+p^n r) \equiv (u(z)+p^n t)^{v(z)} = (u(z)+p^n t)^{\overline{v(z)}}(u(z)+p^n t)^{p^n h} \equiv (u(z) + p^n t)^{\overline{v(z)}} = \sum_{i=0}^{\overline{v(z)}} u(z)^{\overline{v(z)}-i} p^{ni} t^i \binom{\overline{v(z)}}{i} = (u(z))^{\overline{v(z)}} \equiv (u(z))^{\overline{v(z)}}(u(z))^{p^n h} = (u(z))^{v(z)}$, где знак $\equiv$ обозначает сравнение по модулю p^n. Стало быть, функция f совместима.

Для доказательства последнего утверждения леммы заметим, что для любого $z \in \mathbb{Z}_p$ и любого $n = 1, 2, \dots$ выполняется сравнение $(u(z))^{v(z)} \equiv \sum_{i=0}^{n}(u(z) - 1)^i \binom{v(z)}{i} \pmod{p^n}$, поскольку $\|u(z) - 1\|_p \leqslant \frac{1}{p}$. Отсюда следует, что все функции $f_n = \sum_{i=0}^{n} \frac{p^i}{i!}(v)_i w^i$ лежат в кольце $\mathcal{B}$, поскольку все $\frac{p^i}{i!}$ – целые p-адические числа (см. выше), и что последовательность $\{f_n : n = 1, 2, \dots\}$ сходится к f по метрике D_p. Стало быть, $f \in \mathcal{B}$ ввиду 4.10. $\square$

Полученные результаты позволяют в явном виде строить различные эргодические функции с целью их программной реализации. Например, справедливо следующее

4.12 Предложение. *Если $g \in \mathcal{B}$, то функция $f(x) = 1 + x + p^2 g(x)$ эргодична.*

Доказательство. При $p \notin \{2, 3\}$ утверждение тривиально следует из 4.9. Если же $p \in \{2, 3\}$, то в силу 4.9 достаточно доказать, что функция f транзитивна по модулю p^3. В свою очередь, для этого достаточно показать лишь, что $f^{kp^2}(0) \not\equiv 0 \pmod{p^3}$ при $k = 1, 2, \dots, p-1$, поскольку функция f индуцирует на $\mathbb{Z}/p^3$ подстановку, длина каждого цикла которой (в силу совместимости функции f и ее транзитивности по модулю p^2) кратна p^2. Однако, так как при всех $i = 0, 1, 2 \dots$ ввиду совместимости функции g справедливо сравнение $f^i(0) \equiv i + p^2 \sum_{j=0}^{i-1} g(j) \pmod{p^3}$, то $f^{kp^2}(0) \equiv kp^2 + p^2 \sum_{j=0}^{kp^2-1} g(j) \equiv kp^2 + p^2 \sum_{z=0}^{p-1} g(z)pk \equiv kp^2 \pmod{p^3}$, поскольку, опять-таки ввиду совмести-

мости функции g, при любых $s \equiv r \pmod p$ справедливо $p^2 g(r) \equiv p^2 g(s) \pmod{p^3}$. $\square$

5. Приложения и их обсуждение

Полученные результаты могут иметь приложения к синтезу псевдослучайных генераторов, допускающих относительно простую программную реализацию, вырабатывающих строго периодические последовательности чисел из множества $\{0, 1, \dots, m-1\}$, и обеспечивающих при этом ряд гарантированных характеристик качества вырабатываемых последовательностей, в первую очередь, равномерное распределение. Говоря об относительной простоте программной реализации, мы имеем ввиду то, что рассматриваемые псевдослучайные генераторы имеют ряд параметров, определяющих быстродействие соответствующих программ. Эти параметры можно варьировать, достигая нужной скорости, но не изменяя при этом вышеупомянутых характеристик качества вырабытываемой последовательности.

В случае, когда $m = p^k$ есть степень простого числа p, такие последовательности могут быть реализованы как рекуррентные последовательности первого порядка с законом рекурсии $x_{n+1} \equiv f(x_n) \pmod m$, где $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ — любая совместимая эргодическая функция из описанных в данной работе. В этом случае для каждого $k = 1, 2, \dots$ мы получим строго периодическую последовательность с периодом длины p^k, причем каждый элемент из множества $\{0, 1, \dots, p^k - 1\}$ встретится на периоде в точности один раз; в частности, полученная последовательность равномерно распределена.

Важным показателем качества вырабатываемой последовательности является распределение последовательности $(r+1)$-грамм $\{(x_n, x_{n+1}, \dots, x_{n+r}) : n = 0, 1, 2, \dots\}$. В идеальном случае последовательность $\{\mathbf{u}_n = (\frac{x_n}{p^k}, \frac{x_{n+1}}{p^k}, \dots, \frac{x_{n+r}}{p^k}) : n = 0, 1, 2, \dots\}$ точек $(r+1)$-мерного евклидова пространства должна быть равномерно распределена в единичном гиперкубе при всех r. Разумеется, для периодических последовательностей это заведомо недостижимо, и на подсчете характеристик семейства параллельных друг другу гиперплоскостей, содержащего все точки, соответствующие исследуемой последовательности $(r+1)$-грамм, основан ряд статистических тестов качества псевдослучайных генераторов (см.[2, п. 3.3.4]).

Если при некоторых $c, c_0, \dots, c_r \in \mathbb{Z}$ выполняются сравнения

$$c + \sum_{i=0}^{r} c_i x_{n+i} \equiv 0 \pmod{p^k}, \qquad (n = 0, 1, 2, \dots) \qquad (\blacktriangle)$$

то это означает, что все точки $\mathbf{u}_n$ попали на параллельные друг другу гиперплоскости $h + \sum_{i=0}^{r} c_i X_i = 0$. Для линейных конгруэнтных генераторов такие семейства параллельных друг другу гиперплоскостей существуют уже при $r = 2$, каково бы ни было k (см. введение).

Отметим, что если соотношение $(\blacktriangle)$ выполнено для некоторого k, то для всех $j = 1, 2, \dots$ выполнены и соотношения $p^j c + \sum_{i=0}^{r} p^j c_i x_{n+i} \equiv 0 \pmod{p^{k+j}}$. Соотношения последнего типа будем временно называть тривиальными. Тривиальные соотношения существуют всегда: например, зафиксировав некоторое

$K \in \mathbb{N}$, в силу эргодичности f для всех $k \geqslant K$ получаем тривиальные соотношения $p^{k-K} x_{n+p^K} \equiv p^{k-K} x_n \pmod{p^k}$. Говоря несколько неформально, тривиальность соотношения означает, что коэффициенты его при неограниченном росте k стремятся относительно p-адической метрики к 0, т.е. соотношение (▲) при $k \to \infty$ вырождается в соотношение $0 = 0$ в $\mathbb{Z}_p$.

Для одного важного и обширного класса нелинейных конгруэнтных генераторов мы покажем, что если размерность параллельных друг другу гиперплоскостей, составляющих семейство, содержащее все точки $\mathbf{u}_n$, $(n = 0, 1, 2, \dots)$, не растет неограниченно вместе с k, то это семейство определяется тривиальным соотношением. Дадим точные формулировки.

5.1 Предложение. *Если $f \in \mathbb{Q}_p[x]$ есть целозначный совместимый эргодический полином степени d над полем $\mathbb{Q}_p$ p-адических чисел* (все такие полиномы полностью описываются теоремой 2.3 при $p = 2$, при $p \neq 2$ см. утверждения 2.4 и 4.7 и замечание, предшествующее 4.7)*, и если существует натуральное r такое, что для любого $k \in \mathbb{N}$ найдутся $c, c_0, \dots, c_r \in \mathbb{Z}_p$, не все кратные p, при которых выполняются сравнения* (▲)*, то $d = 1$.*

Нам понадобится следующая

5.2 Лемма. *В условиях предложения 5.1 допустим, что $c, c_0, \dots, c_r \in \mathbb{Z}_p$ можно выбрать не зависящими от k, т.е. пусть существуют $c, c_0, \dots, c_r \in \mathbb{Z}_p$ такие, что сравнения* (▲) *выполняются для всех $k \in \mathbb{N}$. Тогда $d = 1$.*

Доказательство леммы 5.2. Ввиду эргодичности f, заведомо $d \neq 0$. Пусть $d > 1$. Положим $w(x) = c + \sum_{i=0}^{r} c_i f^i(x)$. Тогда $w(x)$ есть целозначный совместимый полином из $\mathbb{Q}_p[x]$, как композиция целозначных совместимых полиномов. Но каждый $f^i(x)$ есть совместимый полином над $\mathbb{Q}_p$ степени d^i; поэтому, так как $d > 1$, то $w(x)$ — полином ненулевой степени (как сумма полиномов попарно различных степеней). Однако, поскольку $x_{n+i} \equiv f^i(f^n(x_0)) \pmod{p^k}$, из условий леммы следует, что $w(x_n) \equiv 0 \pmod{p^k}$ для всех $n = 0, 1, 2, \dots$. Другими словами, $w(z) \equiv 0 \pmod{p^k}$ для всех $z \in \mathbb{Z}_p$, поскольку x_n пробегает все множество $\{0, 1, \dots, p^k - 1\}$ ввиду эргодичности f, а $w(x)$ совместим. Условия леммы теперь означают, что $w(z) \equiv 0 \pmod{p^k}$ для всех $z \in \mathbb{Z}_p$ и всех $k = 1, 2, \dots$; следовательно $w(z) = 0$ для всех $z \in \mathbb{Z}_p$, а значит, $w(x) = 0$ как элемент кольца $\mathbb{Q}_p[x]$. Противоречие, доказывающее лемму. □

Доказательство предложения 5.1. По условию, существует r такое, что для каждого $k \in \mathbb{N}$ множество $\mathcal{L}_k$ всех $\mathbf{c} = (c, c_0, \dots, c_r) \in \mathbb{Z}_p^{r+2}$, $\|\mathbf{c}\|_p = 1$, удовлетворяющих системе сравнений (▲), непусто. Очевидно, что $\mathcal{L}_1 \supset \mathcal{L}_2 \supset \dots$, так как f совместим.

Далее, каждое множество $\mathcal{L}_k$ замкнуто в топологии метрического пространства $\mathbb{Z}_p^{r+2}$. Действительно, если $\mathbf{c} \in \mathcal{L}_k$, $\mathbf{c}' \in \mathbb{Z}_p^{r+2}$, $\|\mathbf{c} - \mathbf{c}'\|_p \leqslant p^{-s}$, $s \geqslant k$, то $\mathbf{c}' = \mathbf{c} + p^s \mathbf{z}$ для подходящего $\mathbf{z} \in \mathbb{Z}_p^{r+2}$, а значит, $\|\mathbf{c}'\|_p = 1$ и $\mathbf{c}'$ удовлетворяет (▲); следовательно $\mathbf{c}' \in \mathcal{L}_k$. Применяя теперь к последовательности $\mathcal{L}_1 \supset \mathcal{L}_2 \supset \dots$ непустых замкнутых множеств аналог теоремы о вложенных отрезках (справедливость его вытекает из, например, [16, гл. 3, п. 34]), заключаем, что эта последовательность имеет непустое пересечение, т.е. существует $\mathbf{c}'' \in \mathbb{Z}_p^{r+2}$, удовлетворяющий условиям леммы 5.2. Но тогда $d = 1$. □

Отсюда вытекает следующая

5.3 Теорема. *Пусть $f \in \mathbb{Q}_p[x]$ — целозначный совместимый эргодический полином,* $\deg f > 1$, *и пусть существует такое r, что при каждом $k \in \mathbb{N}$ последовательность $\{x_n\}$ с законом рекурсии $x_{n+1} \equiv f(x_n) \pmod{p^k}$ имеет над $\mathbb{Z}/p^k$ линейную сложность $\leqslant r$, т.е. найдутся $c^{(k)}, c_0^{(k)}, \dots, c_r^{(k)} \in \mathbb{Z}_p$ такие, что*

$$c^{(k)} + \sum_{i=0}^{r} c_i^{(k)} x_{n+i} \equiv 0 \pmod{p^k} \qquad (n = 0, 1, 2, \dots). \tag{◀}$$

Тогда $\lim\limits_{k\to\infty}{}^{p} c^{(k)} = \lim\limits_{k\to\infty}{}^{p} c_1^{(k)} = \ldots = \lim\limits_{k\to\infty}{}^{p} c_r^{(k)} = 0.$

Доказательство. Отметим, что, как следует из доказательств соответствующих утверждений, и лемма 5.2, и предложение 5.1 остаются справедливыми, если считать, что k пробегает произвольное бесконечное подмножество из $\mathbb{N}$. Для каждого $k \in \mathbb{N}$ зафиксируем набор $c^{(k)}, c_0^{(k)}, c_1^{(k)}, \dots, c_r^{(k)} \in \mathbb{Z}_p^{(r+2)}$ коэффициентов, при которых выполняется (◀). Положим $\mathbf{c}_k = (c^{(k)}, c_0^{(k)}, c_1^{(k)}, \dots, c_r^{(k)}) \in \mathbb{Z}_p^{(r+2)}$. Ввиду 5.1 тогда $\|\mathbf{c}_k\|_p < 1$ для всех $k \in \mathbb{N}$. Обозначим $\mathcal{N} = \{k \in \mathbb{N} : \|\mathbf{c}_k\|_p > p^{-k}\}$. Другими словами, $k \notin \mathcal{N}$ тогда и только тогда, когда соотношение (◀) равносильно сравнению $0 \equiv 0 \pmod{p^k}$. Очевидно, что если множество $\mathcal{N}$ конечно или пусто, то утверждение теоремы справедливо.

Пусть $\mathcal{N}$ бесконечно. Для $k \in \mathcal{N}$ положим $\hat{\mathbf{c}}_k = \|\mathbf{c}_k\|_p \mathbf{c}_k$ и обозначим $\hat{\mathcal{N}}$ множество всех $m \in \mathbb{N}$ таких, что $p^k \|\mathbf{c}_k\|_p = p^m$ для подходящего $k \in \mathcal{N}$. Другими словами, мы каждое соотношение (◀) заменяем равносильным ему соотношением

$$\hat{c}^{(k)} + \sum_{i=0}^{r} \hat{c}_i^{(k)} x_{n+i} \equiv 0 \pmod{p^m} \qquad (n = 0, 1, 2, \dots),$$

где $(\hat{c}^{(k)}, \hat{c}_0^{(k)}, \hat{c}_1^{(k)}, \dots, \hat{c}_r^{(k)}) = \hat{\mathbf{c}}_k$, $p^m = p^k \|\mathbf{c}_k\|_p$.

Если множество $\hat{\mathcal{N}}$ конечно, то, очевидно, утверждение теоремы справедливо. Если же $\hat{\mathcal{N}}$ бесконечно, то, поскольку $\|\hat{\mathbf{c}}_k\|_p = 1$, в силу предложения 5.1 необходимо $\deg f = 1$, вопреки условию теоремы. □

В формулировке теоремы 5.3 мы упомянули понятие линейной сложности последовательности над кольцом. Это часто используемая (особенно в криптографии) характеристика качества последовательности. Лемма 5.2 в этих терминах означает, что последовательность $\{x_i = f(x_{i-1}) : i \in \mathbb{N}\}$ имеет бесконечную линейную сложность над кольцом $\mathbb{Z}_p$, если $f \in \mathbb{Q}_p[x]$ — целозначный совместимый эргодический полином степени $d > 1$. Это утверждение можно несколько усилить:

5.4 Следствие. *Если $f \in \mathbb{Q}_p[x]$ — целозначный совместимый эргодический полином степени $d > 1$, то последовательность $\{x_n\}$ с законом рекурсии $x_{n+1} = f(x_n)$ имеет бесконечную линейную сложность над полем $\mathbb{Q}_p$.*

Доказательство. Если для подходящих $c, c_0, \dots, c_r \in \mathbb{Q}_p$, не равных одновременно 0, соотношение $c + \sum_{j=0}^{r} c_j x_{n+j} = 0$ выполняется при всех $n =$

$0, 1, 2, \dots$, то выполняется и соотношение $hc + \sum_{j=0}^{r} hc_j x_{n+j} = 0$, где $h = 1$, если $c, c_0, \dots, c_r \in \mathbb{Z}_p$, и $h = \|(c, c_0, \dots, c_r)\|_p$ в противном случае. Ввиду совместимости f утверждение теперь следует из 5.2. $\square$

Замечание. Условие $f \in \mathbb{Q}_p[x]$ в условиях 5.1–5.4 не может быть отброшено. Например, при $p = 2$ положим

$$f(x) = 1 + x + 4(-1)^{1+x} = 1 + x + \sum_{j=0}^{\infty} (-1)^j 2^{j+2} \binom{x}{j}.$$

По теореме 2.3 эта функция совместима и эргодична. Однако легко видеть, что последовательность $\{x_n \in \mathbb{Z}_2\}$ с законом рекурсии $x_{n+1} = f(x_n)$ удовлетворяет соотношению $x_{n+2} = x_n + 2$, т.е. имеет линейную сложность 2 над кольцом $\mathbb{Z}_2$.

Отметим, что в этом разделе мы употребляем понятие линейной сложности последовательности над кольцом в несколько более широком смысле, чем обычно принято: чаще линейной сложностью последовательности $\{x_n\}$ элементов коммутативного кольца R называют наименьшее $r > 0$ такое, что существуют $c_0, \dots, c_{r-1} \in R$, удовлетворяющие одновременно всем равенствам $x_{n+r} = \sum_{j=0}^{r-1} c_j x_{n+j}$, $(n = 0, 1, 2, \dots)$. Мы же допускаем и наличие свободного члена, и то, что все коэффициенты одновременно могут быть делителями нуля (но не равными 0 одновременно; в формулировке теоремы 5.3 последнее, впрочем, несущественно). Если R поле, то оба понятия, по существу, совпадают: если последовательность удовлетворяет соотношению $c + \sum_{i=0}^{r} c_i x_{n+i} = 0$, где $c_r \neq 0$, то она удовлетворяет и сотношению $x_{n+r+1} = c_r^{-1} c_0 x_n - \sum_{j=0}^{r-1} c_r^{-1}(c_j - c_{j+1}) x_{n+j+1}$. Наше определение кажется нам чуть более удобным с точки зрения геометрической интерпретации, см. выше.

Другими словами, мы показали, что, выражаясь неформально, нелинейные эргодические полиномиальные генераторы совершенно нелинейны: генерируемые ими последовательности не могут быть реализованы как линейные рекуррентные последовательности над $\mathbb{Q}_p$. Мы не обсуждаем здесь эти результаты в связи с поведением этих последовательностей относительно упомянутых выше статистических тестов — это предмет следующей статьи. Отметим лишь, что они дают определенные основания считать, что соответствующие генераторы на практике будут успешно проходить эти тесты.

Должным образом переформулированные аналоги утверждений 5.1–5.4 справедливы и для составного $m = p_1^{k_1} \cdots p_s^{k_s}$, являющегося произведением степеней различных простых чисел $p_1, \dots, p_s$, если только преобразование f сохраняет все конгруэнции кольца $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$. В связи с конгруэнтными генераторами по составному модулю m отметим, что в качестве f можно взять функцию, определенную на множестве $\mathbb{N}_0$ всех неотрицательных рациональных целых чисел, принимающую значения в кольце $\mathbb{Z}$ всех рациональных целых чисел, сохраняющую все конгруэнции этого кольца и эргодическую как функция целого p-адического аргумента при всех $p \in \{p_1, \dots, p_s\}$. Такие функции также могут быть построены с помощью полученных в работе результатов.

Например, такие функции можно найти в классе

$$\mathcal{B}_0 = \left\{ \sum_{i=0}^{\infty} a_i \, (x)_i : a_i \in \mathbb{Z}; i = 0, 1, 2, \dots \right\},$$

где, напоминаем, $(x)_i$ есть i-я убывающая факториальная степень x: $(x)_0 = 1$, $(x)_i = x(x-1)\cdots(x-i+1)$ при всех $i = 1, 2, \ldots$. Ясно, что $\mathcal{B}_0$ есть собственный подкласс рассмотренного в разделе 4 класса $\mathcal{B}$ при любом простом p (определение последнего из классов зависит от p). Поскольку класс $\mathcal{B}$ состоит из функций, сохраняющих все конгруэнции кольца $\mathbb{Z}_p$, то каждая функция g из $\mathcal{B}_0$ сохраняет все конгруэнции кольца $\mathbb{Z}$, т.е. для любых $a, b \in \mathbb{N}_0$ и любого натурального $N > 1$ выполняется сравнение $g(a) \equiv g(b) \pmod N$ как только $a \equiv b \pmod N$. Таким образом, в законе рекурсии псевдослучайного генератора можно положить

$$f(x) = 1 + x + p_1^2 \cdots p_s^2 g(x) \qquad (g \in \mathcal{B}_0);$$

в силу 4.12 тогда функция f будет эргодична как функция целого p_j-адического аргумента при всех $j = 1, 2, \ldots, s$, т.е. будет транзитивна по каждому модулю p_j^k для всех $k = 1, 2, \ldots$ и всех $j = 1, 2, \ldots, s$. Стало быть, f будет тогда транзитивна по каждому модулю $p_1^{t_1} \cdots p_s^{t_s}$ при любых натуральных $t_1, \ldots, t_s \in \mathbb{N}$. В частности, функция f будет транзитивна и по модулю m, т.е. псевдослучайный генератор с законом рекурсии $x_{n+1} \equiv f(x_n) \pmod m$ при любом начальном состоянии $x_0 \in \{0, 1, \ldots, m-1\}$ будет вырабатывать строго периодическую последовательность элементов из $\{0, 1, \ldots, m-1\}$ с периодом длины m, причем каждый элемент из $\{0, 1, \ldots, m-1\}$ встретится на периоде этой последовательности в точности один раз.

Ясно, что класс $\mathcal{B}_0$ содержит все функции, задаваемые полиномами с рациональными целыми коэффициентами, поэтому в случае, когда полином $g(x)$ из кольца $\mathbb{Z}[x]$ всех полиномов от одной переменной x над кольцом $\mathbb{Z}$ имеет степень $d \geqslant 1$, то сложность программной реализации соответствующего псевдослучайного генератора эквивалентна d сложениям и d умножениям целых чисел по модулю m. Ясно также, что класс $\mathcal{B}_0$ не исчерпывается полиномиальными над $\mathbb{Z}$ функциями. Неясно, однако, содержит ли он наряду с этими функциями иные «естественные» функции, допускающие относительно простую программную реализацию.

Вообще, при произвольном m не очень понятно, какие функции считать «естественными», а какие нет. Если под «естественностью» понимать возможность задания функции с помощью арифметических операций (сложения, вычитания, умножения, деления, возведения в степень с натуральным показателем, экспоненцирования), то такого рода функции могут быть построены, например, с помощью утверждений 2.3, 2.4, и 4.9 совместно с 4.11 и 4.12. Так, из теорем 2.3 и 2.4 следует, что полином $f(x)$ над полем $\mathbb{Q}$ рациональных чисел, имеющий вид

$$f(x) = 1 + x + \sum_{i=0}^{d} c_i \, p_1^{\lfloor \log_{p_1}(i+1) \rfloor + 1} \cdots p_s^{\lfloor \log_{p_s}(i+1) \rfloor + 1} \binom{x}{i},$$

при любых $c_0, c_1, c_2 \ldots \in \mathbb{Z}$ транзитивен по модулю любого натурального числа $M > 1$, которое может быть представлено в виде произведения степеней простых чисел из $\{p_1, \ldots, p_s\}$; в частности, он транзитивен по модулю m. Следовательно, сложность программной реализации соответствующего псевдослучайного генератора эквивалентна d умножениям, d сложениям, $d+1$ приведениями по некоторым модулям и одному делению рациональных целых чисел.

Из вышеприведенной формулы вытекает, например, что полином $f(x) = 1 + x + \frac{5}{18}(x)_6$ транзитивен по модулю 10^k для всех $k = 1, 2, \ldots$. Аналогичным образом, с помощью утверждений 2.5 и 4.11 (или 4.9 совместно с 4.11) могут быть построены генераторы с использованием экспоненцирования: например, функция $f(x) = 1 + x + 201^x$ (или, более общо, $f(x) = 1 + x + (1 + 200u(x))^{w(x)}$, где $u(x), v(x) \in \mathbb{Z}[x]$), а также функция $f(x) = 1 + x + 201^{201^x}$ транзитивны по модулю 10^k для всех $k = 1, 2, \ldots$ (в силу 4.9 и 4.11); то же верно и для функции $f(x) = 1 + x + 100 \cdot 11^x$ (в силу 2.5 и 4.11). Если судить по количеству публикаций, посвященных инверсивным генераторам, то к «естественным» функциям следует отнести и взятие мультипликативного обратного по модулю m (или, более общо, возведение в отрицательные степени). Генераторы такого типа тоже могут быть построены при помощи полученных в работе результатов: например, при $w(x) = -1, v(x) = x$ приведенный выше пример дает функцию $f(x) = 1 + x + (1 + 200x)^{-1}$, транзитивную по модулю 10^k для всех $k = 1, 2, \ldots$.

Отметим, что в течение последнего десятилетия интенсивно исследовались свойства степенного ($f(x) = x^r, r \in \mathbb{N}$), экспоненциального ($f(x) = a^x$), дважды экспоненциального ($f(x) = a^{b^x}$) и инверсивного ($f(x) = a + bx^{-1}$ или $f(x) = (a + bx)^{-1}$) генераторов. Приведеные выше примеры генераторов, построенных на основе композиции арифметических операций, включая экспоненцирование и возведение в степень с отрицательным показателем, как мы видим, несколько отличаются от изучаемых в литературе, в первую очередь, наличием слагаемого $1 + x$. Эти отличия практически не увеличивают ни сложности программной реализации, ни уменьшают ее быстродействия, но обеспечивают максимальность периода выходной последовательности и тем самым ее равномерное распределение. Однако эти отличия не позволяют (по крайней мере, немедленно) перенести все полученные для уже изученных в литературе типов генераторов результаты на рассмотренные в данной работе генераторы. Изучение возможности такого переноса было бы, по мнению автора, чрезвычайно полезным, поскольку в этой области различными авторами получен ряд важных результатов, даже краткий обзор которых невозможно привести здесь по причине их значительного количества.

Вместе с тем, поскольку все рассмотренные в данной работе генераторы могут быть при данном m реализованы как генераторы с законом рекурсии $x_{n+1} \equiv f_m(x_n) \pmod m$, где $f_m(x) \in \mathbb{Q}[x]$ (что немедленно следует из p-адической теоремы Вейерштрасса, см. [3, гл. 10, теорема 1]), то все результаты, полученные в литературе для т.н. полиномиальных конгруэнтных генераторов, немедленно переносятся на рассмотренные в данной работе, по крайней мере, при дополнительном условии $f_m(x) \in \mathbb{Z}[x]$.

Следует отметить, что ряд изучаемых в литературе генераторов относится к случаю, когда m есть произведение двух различных больших простых чисел. Результаты данной работы применительно к этой ситуации мало интересны, ибо, как правило, позволяют строить генераторы, которые либо эквивалентны по модулю простого делителя p числа m линейному конгруэнтному генератору, либо требующие для своего задания изначального знания транзитивного по модулю p полинома степени > 1, который потом нужно «подправить», обеспечив его транзитивность по модулю p^s, где s удовлетворяет условиям теорем 3.14, 4.1 или 4.9. Методы, позволяющие должным образом

«подправлять» полиномы, автор надеется опубликовать в одной из следующих статей, здесь же мы ограничимся примером. Например, упомянутым способом на основе полинома $1 + 3x^3$, транзитивного по модулю 5, можно построить полином $1 - 127x - 152x^3 + 152x^5$, который транзитивен по любому модулю 10^k, $k = 1, 2, \ldots$.

В свете сказанного, методы построения псевдослучайных генераторов, основанные на представленных в данной работе результатах, имеют наибольший интерес применительно к случаю, когда m разлагается в произведение сравнительно небольшого числа степеней относительно небольших простых чисел с достаточно большими показателями. Здесь естественным образом выделяется подслучай $m = 2^s$, как наиболее простой в программной реализации, ибо приведение натурального числа по модулю 2^s состоит просто в отбрасывании в его двоичной записи всех старших разрядов с номерами $\geqslant s$ (наша нумерация разрядов начинается с 0). Именно в этом случае возникают наиболее естественные (с точки зрения их программной реализации) операции, отличные от упомянутых выше арифметических — $\mathrm{XOR}, \mathrm{OR}, \mathrm{AND}$ и другие операции с неотрицательными целыми числами, осуществляемые поразрядно над записями этих чисел в двоичной системе счисления. И именно в этом случае, к счастью, удается получить полное описание совместимых эргодических (или сохраняющих меру) функций — см. раздел 2.

Полученные результаты позволяют строить псевдослучайные генераторы, удовлетворяющие ряду требований к быстродействию, статистическим и/или криптографическим характеристикам. Эта тема подробно будет рассмотрена в последующих статях. Здесь же мы бегло отметим лишь, что применение описанных в данной работе равновероятных функций к выходным последовательностям конгруэнтных генераторов, построенных на основе эргодических функций на $\mathbb{Z}_2$, позволяет, сохранив равномерность распределения, ликвидировать еще один известный недостаток, т.н. «эффект младших разрядов», который состоит в том, что последовательность, составленная из всех разрядов с номером j членов последовательности $\{x_n\}$, удовлетворяющей рекуррентному соотношению $x_{n+1} \equiv f(x_n) \pmod{2^k}$, где $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ — совместимая функция, имеет период длины не более чем 2^{j+1}. Методы исправления этого недостатка подробно будут рассмотрены в одной из последующих статей.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. *Кейперс Л., Нидеррейтер Г.,* Равномерное распределение последовательностей. М.: Наука, 1985.
2. *Кнут Д.* Искусство программирования. Т. 2. М.–СПб–Киев: «Вильямс», 2000.
3. *Mahler K.* p-adic numbers and their functions. (2nd edition). Cambridge Univ. Press, 1981.
4. *Alperin R. C.* p-adic binomial coefficients mod P //The Amer. Math. Month. 1985. V. 92. № 8. P. 576–578.
5. *Hall R. R.* On pseudo-polynomials //Arch. Math. 1971. V. 18. P. 71–77.
6. *Коблиц Н.* p-адические числа, p-адический анализ и дзета-функции. М.: Мир, 1982.

7. *Marsaglia G.* Random numbers fall mainly in the planes //Proc. Nat. Ac. Sci. USA. 1968. T. 61. C. 25–28.
8. *Lausch H., Nöbauer W.* Algebra of polynomials. Amsterdam: North-Holl. Publ. Co, 1973.
9. *Kaiser H. K., Nöbauer W.* Permutation polynomials in several variables over residue class rings //J. Austral. Math. Soc. 1987. V. A43. P. 171–175.
10. *Юров И. А.* О p-адических функциях, сохраняющих меру Хаара //Матем. заметки. 1998. Т. 63. № 6. С. 935–950.
11. *Анашин В. С.* Равномерно распределенные последовательности целых p-адических чисел //Матем. заметки. 1994. Т. 55. № 2. С. 3–46.
12. *Anashin V. S.* Uniformly distributed sequences over p-adic integers. In: Number theoretic and algebraic methods in computer science (A. J. van der Poorten, I. Shparlinsky and H. G. Zimmer, eds.). Proceedings of the Int'l Conference (Moscow, June–July, 1993). World Scientific, 1995. P. 1–18.
13. *Rivest R.* Permutation polynomials modulo 2^w //Finite fields and appl. 2001. V. 7. № 2. P. 287–292.
14. *Anashin V. S.* Uniformly distributed sequences over p-adic integers ... In: Number theoretic and algebraic methods in computer science. (Conference abstracts. Moscow, 29 June–2 July, 1993). Moscow: Int'l Centre for Sci. and Tech. Information, 1993. P. 6 – 8.
15. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов //Дискретная математика (в печати).
16. *Куратовский К.* Топология. Т. 1. М.: Мир, 1966.
17. *Anashin V. S.* Uniformly distributed sequences in computer algebra, or how to construct program generators of random numbers //J. Math. Sci. 1998. V. 89. № 4. New York: Plenum Publishing Corp., P. 1355 – 1390.

Российский государственный гуманитарный университет
E-mail: vladimir@anashin.msk.su, anashin@rsuh.ru

Аннотация. В статье описаны эргодические относительно меры Хаара функции на кольце $\mathbb{Z}_p$ целых p-адических чисел, принимающие значения в $\mathbb{Z}_p$ и удовлетворяющие (по крайней мере, локально) условию Липшица с коэффициентом 1. Также описаны равновероятные (в частности, сохраняющие меру Хаара) функции из указанного класса. В некоторых случаях (особенно при $p = 2$) описание дается в виде явных формул. Некотрые результаты могут быть интерпретированы как описание эргодических изометричных динамических систем на p-адическом единичном диске. Исследование мотивировано задачей построения псевдослучайных генераторов для компьютерного моделирования и криптографии. С этой точки зрения результаты статьи могут рассматриваться как описания нелинейных конгруэнтных генераторов по модулю m, генерирующих строго периодические равномерно распределенные по модулю m последовательности максимально возможного (т.е. равного m) периода. В качестве функций выхода и перехода таких генераторов можно выбирать, например, мероморфные на $\mathbb{Z}_p$ функции (в частности, полиномы с рациональными, но не обязательно целыми коэффициентами), или композиции арифметических операций (сложения, умножения, экспоненцирования, возведения в степень с целым, в том числе отрицательным показателем) и стандартных компьютерных команд, типа поразрядных логических операций (например, XOR, OR, AND, NEG, и т.п.). Изуается и линейная сложность таких последовательностей.

Ключевые слова: равномерно распределенная последовательность – uniformly distributed sequence; p-адическое целое число – p-adic integer; неархимедовы динамические системы – non-Archimedean dynamical systems; эргодическая функция – ergodic function; равновероятная функция – equiprobable function; функция, сохраняющая меру – measure preserving function; транзитивный полином – transitive polynomial; биективный полином – bijective polynomial; подстановочный полином – permutation polynomial; псевдослучайный генератор – pseudorandom number generator; нелинейный конгруэнтный генератор – nonlinear congruential generator; линейная сложность – linear complexity.