ВВЕДЕНИЕ В ПРИКЛАДНОЙ p-АДИЧЕСКИЙ АНАЛИЗ

В.С.АНАШИН

1. Понятие p-адического числа

1.1. **Приготовления.** Мы можем вычислить сумму двух неотрицательных целых чисел, представленных в двоичной системе счисления, с помощью школьного алгоритма сложения «в столбик». Отметим, что слагаемые при этом представляются в виде конечных строчек из нулей и единиц (или, лучше сказать, в виде бесконечных строчек из нулей и единиц, но которые содержат не более конечного числа единиц). Посмотрим, что произойдет, если мы применим этот алгоритм к произвольным бесконечным строчкам из нулей и единиц.

Начнем с примера:

$$\begin{array}{cccccc} & \ldots 1 & 1 & 1 & 1 \\ + & & & & \\ & \ldots 0 & 0 & 0 & 1 \\ \hline & \ldots 0 & 0 & 0 & 0 \end{array}$$

Ясно, что строчка $\ldots 000$ — это просто 0, а строчка $\ldots 001$ есть 1. Но тогда мы *вынуждены* заключить, что $\ldots 111 = -1$; т.е., что бесконечная строка $\ldots 111$ есть ни что иное как представление *отрицательного* числа -1 в двоичной системе счисления! Запомним это и продолжим наши исследования. Рассмотрим пример на умножение:

$$\begin{array}{cccccccc} & \ldots 0 & 1 & 0 & 1 & 0 & 1 \\ \times & & & & & & \\ & \ldots 0 & 0 & 0 & 0 & 1 & 1 \\ \hline & \ldots 0 & 1 & 0 & 1 & 0 & 1 \\ + & & & & & & \\ & \ldots 1 & 0 & 1 & 0 & 1 & \\ \hline & \ldots 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

Поскольку, как мы знаем, $\ldots 0011 = 3$, и поскольку мы согласились с тем, что $\ldots 111 = -1$, мы обязаны сделать вывод, что $\ldots 01010101 = -\frac{1}{3}$. Это выглядит немного странным для нас, но вполне нормальным для компьютера: все вышеприведенные выкладки могут быть проделаны,

например, на стандартном встроенном в Windows калькуляторе с максимальной точностью, которую он допускает, 64 бита.[1]

Теперь обозначим через $\mathbb{Z}_2$ множество всех двоичных строк и зададим на этом множестве операции сложения и умножения с помощью вышеупомянутых алгоритмов «в столбик», превратив тем самым $\mathbb{Z}_2$ в коммутативное кольцо с единицей.

Важно отметить, что

> *Все «поразрядные» (т.е. без переноса единицы) команды процессора, такие как* XOR *(«исключительное или»),* OR *(«или»),* AND *(«и»),* NOT *(отрицание) являются корректно определенными функциями, определенными на множестве $\mathbb{Z}_2$ всех бесконечных двоичных последовательностей, принимающими значения в этом же множестве $\mathbb{Z}_2$.*

Фактически, все эти функции оказываются *непрерывными* в некотором точно определенном смысле функциями, а некоторые из них даже и *дифференцируемыми*, и мы сможем использовать некоторое дифференциальное исчисление, чтобы изучать важные для криптографии свойства этих функций.

Но сначала давайте задумываемся над тем, что первое приходит на ум, когда мы говорим о дифференциальном исчислении. Ну конечно, это понятие производной. А на каком понятии базируется понятие производной? Очевидно, на понятии предела. Но, говоря о том, что a есть предел последовательности $\{a_i\}_{i=0}^{\infty}$ при i стремящемся к бесконечности, мы на самом деле утверждаем, что все эти a_i суть *приближения* a, причем мы можем обеспечить *любую сколь угодно высокую* точность приближения, беря члены с *достаточно большими* i.

Теперь мы должны понять, что же означает термин «приближение», или, точнее, с какими «приближениями» работает компьютер. Процессор компьютера работает с двоичными словами некоторой фиксированной длины, которая называется *разрядностью* процессора. Обычные значения разрядности современных процессоров — это числа 8,16,32, 64.

Возьмем некоторую конечную двоичную строчку, например строчку $\underbrace{1\ldots111}_{\text{64 единицы}}$. Эта строчка есть двоичное представление числа $2^{64}-1 = 18446744073709551615$. Но 8-разрядный процессор может работать только с 8-битными строчками, поэтому при попытке загрузить это число в регистр 8-битного процессора, в регистре окажутся только 8 младших разрядов этого числа (для остальных там попросту нет места!), т.е., процессор запомнит число $2^8-1 = 255$. А 16-битный процессор запомнит лишь младшие 16 бит, т.е. число $2^{16}-1 = 65535$, соответственно, 32-битный процессор запомнит эту строчку как число $2^{32}-1 = 4294967295$, и т.д. Поэтому разумно считать, что число 255 есть приближение с 8-битной точностью числа $2^{64}-1$, число 65535 — это приближение с 16-битной точностью, и т.д.

---

[1] Не забудьте переключить калькулятор в `scientific mode` и установить режим двоичных вычислений `bin`.

Следуя этой логике, мы заключаем, что последовательность

$$255, 65535, 4294967295, \ldots, 2^{2^n} - 1, \ldots$$

стремится к $-1 = \ldots 111$ при k стремящимся к бесконечности. Такой же вывод мы должны сделать и для последовательности чисел $2^n - 1$: именно, $\lim\limits_{n\to\infty}^{2}(2^n - 1) = -1$, где $\lim\limits^{2}$ есть нечто, похожее на «предел» в привычном нам смысле, но относительно n-битной точности. Впрочем, глядя на нижеследующую картинку, интуитивно становится понятным, почему последовательность $\ldots 0001$, $\ldots 0011$, $\ldots 0111$, $\ldots$ двоичных представлений чисел $1, 3, 7, 15, \ldots$ «стремится» к $\ldots 1111 = -1$:

$$\begin{array}{cccccccc}
\ldots & 0 & 0 & 0 & 0 & 1 & = 1 \\
\ldots & 0 & 0 & 0 & 1 & 1 & = 3 \\
\ldots & 0 & 0 & 1 & 1 & 1 & = 7 \\
\ldots & 0 & 1 & 1 & 1 & 1 & = 15 \\
\ldots & . & . & . & . & . & . \\
\ldots & 1 & 1 & 1 & 1 & 1 & = -1
\end{array}$$

Чтобы понять скрывающуюся за этими непривычными утверждениями суть, мы должны разобраться, на каком понятии базируется классическое определение предела числовой последовательности. Вспомнив это определение, мы, допуская некоторую вольность речи, можем сказать, что оно сформулировано в терминах «близости» членов последовательности к числу, являющемуся ее пределом. Другими словами, *определение предела базируется на понятии расстояния* между числами.

Приведенные выше примеры призваны продемонстрировать тот факт, что для человека интуитивно ясное понятие расстояния отличается от «естественного с точки зрения компьютера», а лучше сказать, что компьютер и человек измеряют расстояния по-разному! Например, с нашей людской точки зрения естественно считать, что число $2^{32} = 4294967296$ лежит дальше от 0, чем число $2^8 = 256$. Напротив, «с точки зрения компьютера» число 2^{32} расположено ближе к 0, чем число 2^8. Какое же «расстояние» можно считать естественным для компьютера?

1.2. **Понятие расстояния.** Фактически, когда мы измеряем расстояние между двумя точками, мы сопоставляем паре точек некоторое неотрицательное действительное число. Разумно считать, что это число равно 0 тогда и только тогда, когда точки совпадают, и что расстояние, измеренное в направление от первой точки ко второй должно совпадать с расстоянием, измеренным в направлении от второй точки к первой. Так же естественен и «принцип треугольника»; именно, расстояние от точки A до точки B не превосходит суммы двух расстояний: от точки A до некоторой произвольно выбранной точки C, и от этой точки C до точки B. Эти соображения суммируются в понятии *метрики*:

Определение 1.1. Пусть M — некоторое непустое множество, и пусть $d\colon M \times M \to \mathbb{R}_{\geq 0}$ — функция двух переменных, определенная на этом множестве и принимающая значения во множестве действительных неотрицательных чисел. Функция d называется *метрикой* (а множество M — *метрическим пространством*), если d удовлетворяет трем условиям:

(1) Для каждой пары $a, b \in M$ справедливо: $d(a,b) = 0$ тогда и только тогда, когда $a = b$.
(2) Для каждой пары $a, b \in M$ справедливо равенство $d(a,b) = d(b,a)$.
(3) Для каждой тройки $a, b, c \in M$ справедливо неравенство $d(a,b) \leq d(a,c) + d(c,b)$.

Например, множество $\mathbb{R}$ всех действительных чисел есть метрическое пространство с метрикой $d(a,b) = |a-b|$, где $|\cdot|$ есть абсолютная величина. Последнее понятие может быть сформулировано для произвольного коммутативного кольца R.

Определение 1.2. Функция $\|\cdot\|$, определенная на R и принимающая значения в $\mathbb{R}_{\geq 0}$ называется *нормой* (также, *абсолютной величиной*), если она удовлетворяет следующим условиям:

(1) Для любого $a \in R$ справедливо, что $\|a\| = 0$ тогда и только тогда, когда $a = 0$.
(2) Для каждой пары $a, b \in R$ справедливо равенство $\|a \cdot b\| = \|a\| \cdot \|b\|$.
(3) Для каждой пары $a, b \in R$ справедливо неравенство $\|a + b\| \leq \|a\| + \|b\|$.

Легко проверить, что полагая $d(a,b) = \|a - b\|$, мы задаем метрику d на кольце R. Эта метрика d называется метрикой, индуцированной нормой $\|\cdot\|$.

Отметим, что как только мы определили норму (а значит, и метрику) на кольце R, мы тем самым определили и понятие сходящейся последовательности элементов из R, и понятие предела, и понятие непрерывной функции на R, принимающей значения в R, и понятие производной, и т.п. Например, элемент $a \in R$ есть производная функции $f\colon R \to R$ в точке $x \in R$ тогда и только тогда, когда для всех *достаточно малых* $h \in R$, $h \neq 0$, (т.е., для $\|h\| < \delta$ для некоторого действительного $\delta > 0$) справедливо равенство

$$f(x+h) = f(x) + a \cdot h + \lambda(h),$$

где $\frac{\|\lambda(h)\|}{\|h\|}$ стремится 0 при $\|h\|$ стремящемся к 0. Говоря неформально, каждая новая норма задает свое дифференциальное исчисление.

1.3. **Нормы на $\mathbb{Z}$.** Мы знаем пока только, что абсолютная величина $|\cdot|$ — это норма на кольце $\mathbb{Z}$ всех целых чисел. Возникает вопрос, а существуют ли другие нормы на $\mathbb{Z}$? Ответ — *да*!

Пусть p — некоторое простое число. С помощью этого числа p мы сейчас зададим норму $\|\cdot\|_p$ на $\mathbb{Z}$. Очевидно, что поскольку $\|-a\| = \|a\|$ для каждого $a \in R$ (что немедленно вытекает из определения 1.2), то достаточно задать $\|\cdot\|_p$ на множестве $\mathbb{N}_0$ всех неотрицательных целых чисел.

Положим $\|0\|_p = 0$. Далее, если $n > 0$ есть некоторое натуральное число, его можно представить в виде произведения степеней простых чисел. Обозначим через $\operatorname{ord}_p n$ показатель степени, в которой p входит в это произведение и положим $\|n\|_p = p^{-\operatorname{ord}_p n}$. Нетрудно показать, что $\|\cdot\|_p$ есть норма.

В самом деле, свойства (1) и (2) из определения 1.2, очевидно, выполняются. Более того, выполняется более сильное свойство, чем (3):

(3′) Для любых $a, b \in \mathbb{Z}$ верно, что $\|a+b\|_p \le \max\{\|a\|_p, \|b\|_p\}$.

Отсюда сразу следует, что для метрики d_p, индуцированной нормой $\|\cdot\|_p$ также выполняется условие более сильное, чем условие (3) из определения 1.1:

(3′) Для любых $a, b, c \in \mathbb{Z}$ верно, что $d_p(a,b) \le \max\{d_p(a,c), d_p(c,b)\}$.

Последнее свойство называется *сильным неравенством треугольника*, а метрика, удовлетворяющая ему, называется *неархимедовой метрикой*, или *ультраметрикой*. Соответствующее метрическое пространство называется наархимедовым, или ультраметрическим.

1.4. **p-адические целые числа.** Ясно, что для натурального $n \in \mathbb{N}$ найти $\operatorname{ord}_p n$ мжно по следующему правилу: представим n в системе счисления с основанием p, найдем номер самого младшего ненулевого разряда в этом представлении (пусть это номер i, нумерация начинается с нуля); тогда $\operatorname{ord}_p n = i$. Другими словами,

$$\text{если } n = \dots a_{i+1} a_i \underbrace{0 \dots 0}_{i \text{ нулей}}; a_i \neq 0, \text{ то } \|n\|_p = \frac{1}{p^i}.$$

Определение нормы в таком виде может быть распространено на все множество $\mathbb{Z}_p$ бесконечных строчек с элементами из множества $0, 1, \dots, p-1$. Можно показать, что множество $\mathbb{Z}_p$ есть коммутативное кольцо по отношению к операциям сложения и умножения, определенным с помощью алгоритмов «в столбик» для чисел, представленных в системе счисления с основанием p, и что функция $\|\cdot\|_p$ есть норма на этом кольце. Элементы кольца $\mathbb{Z}_p$ называются *целыми p-адическими числами*. На самом деле мы рассматриваем бесконечную строчку $\dots a_i a_{i-1} \dots a_0$ над алфавитом $\{0, 1, \dots, p-1\}$ как «представление в системе с основанием p» целого p-адического числа a:

$$a = \dots a_i a_{i-1} \dots a_0 = \sum_{i=0}^{\infty} a_i \cdot p^i \tag{1.2.1}$$

Это представление называется *каноническим*.

Отметим, что для $a, b \in \mathbb{Z}_p$ всегда $d_p(a,b) = \frac{1}{p^i}$ для подходящего $i = 0, 1, 2, \dots, \infty$ (случай $i = \infty$ означает просто, что $d_p(a,b) = 0$, т.е., что $a = b$). Более того, $d_p(a,b) = \frac{1}{p^i}$ тогда и только тогда, когда

$$a = \dots a_{i+1} a_i c_{i-1} \dots c_0;$$
$$b = \dots b_{i+1} b_i c_{i-1} \dots c_0,$$

и $a_i \neq b_i$. Используя очевидную аналогию с неотрицательными рациональными целыми числами, мы будем писать в этом случае, что $a \equiv b \pmod{p^i}$, или, более формально, что $a \bmod p^i = b \bmod p^i$, где $\bmod p^i$ —

эпиморфизм кольца $\mathbb{Z}_p$ на кольцо вычетов $\mathbb{Z}/p^i\mathbb{Z}$: мы полагаем, естественно, что

$$\left(\sum_{j=0}^{\infty} a_j \cdot p^j\right) \bmod p^i = \sum_{j=0}^{i-1} a_j \cdot p^j.$$

Заметим, что $d_p(a,b) = \frac{1}{p^i}$, если i есть наибольшее положительное рациональное целое число, такое что $a \equiv b \pmod{p^i}$ и $a \not\equiv b \pmod{p^{i+1}}$. Далее мы будем обозначать i-й разряд ($i = 0, 1, 2, \ldots$) в каноническом представлении целого p-адического числа $a \in \mathbb{Z}_p$ через $\delta_i^p(a)$; т.е., $\delta_i^p(a) = a_i$, см. (1.2.1). Мы будем опускать верхний индекс (особенно для $p = 2$) в тех случаях, когда это не ведет к недоразумениям.

Упомянутое ранее множество $\mathbb{Z}_2$ всех бесконечных двоичных строк соответствут случаю $p = 2$, т.е. $\mathbb{Z}_2$ есть ультраметрическое пространство по отношению к метрике d_2, индуцированной нормой $\|\cdot\|_2$. Ну и, действительно, по отношению к этой метрике d_2 последовательность $1, 2, 4, \ldots, 2^n, \ldots$ стремится к 0 при n стремящимся к бесконечности, а значит, последовательность $1, 3, 7, \ldots, 2^n - 1, \ldots$ сходится к -1.

Поскольку кольцо (метрическое пространство) $\mathbb{Z}_2$ играет в приложениях к криптографии особо важную роль, мы рассмотрим сейчас несколько иллюстраций наших основных понятий на примере кольца $\mathbb{Z}_2$.

Последовательностям, которые содержат лишь конечное число единиц, соответствуют неотрицательные рациональные целые числа, представленные в двоичной системе счисления, например

$$\ldots 00011 = 3$$

Последовательности, содержащие лишь конечное число нулей, представляют собой отрицательные рациональные целые числа, например

$$\ldots 111100 = -4$$

Периодические (с некоторого места) последовательности — это рациональные числа, которые могут быть записаны в виде несократимых дробей с нечетными знаменателями, например

$$\ldots 1010101 = -\frac{1}{3}$$

Последовательностям, не являющимся периодическими, не соответствует ни одно рациональное число.

Пример на измерение расстояний в $\mathbb{Z}_2$:

$$\left.\begin{aligned} \ldots 10101\underbrace{0101} &= -\frac{1}{3} \\ \ldots 00000\underbrace{0101} &= 5 \end{aligned}\right\} \Longrightarrow d_2\left(-\frac{1}{3}, 5\right) = \frac{1}{2^4} = \frac{1}{16}$$

Таким образом, $-\frac{1}{3} \equiv 5 \pmod{16}$; $-\frac{1}{3} \not\equiv 5 \pmod{32}$.

1.5. **Поле p-адических чисел.** Задав метрику d_p на кольце целых чисел $\mathbb{Z}$, мы можем распространить ее на все поле рациональных чисел $\mathbb{Q}$ очевидным образом: поскольку любое рациональное число $r \in \mathbb{Q}$ может быть представлено в виде дроби $r = \frac{m}{n}$, где $m, n \in \mathbb{Z}$, то мы полагаем, что

$$\|r\|_p = p^{\operatorname{ord}_p n - \operatorname{ord}_p m}.$$

Таким образом, поле рациональных чисел $\mathbb{Q}$ является метрическим пространством относительно метрики d_p, индуцированной нормой $\|\cdot\|_p$. Это пространство не является полным: не всякая последовательность рациональных чисел, удовлетворяющая условию Коши относительно метрики d_p, имеет своим пределом рациональное число. По теореме о пополнении метрических пространств, поле $\mathbb{Q}$ рациональных чисел можно пополнить до полного метрического пространства $\mathbb{Q}_p$, в котором поле $\mathbb{Q}$ будет всюду плотным подмножеством. Полученное полное относительно d_p метрическое пространство $\mathbb{Q}_p$ является полем, которое называется *полем p-адических чисел*. Кольцо $\mathbb{Z}_p$ целых p-адических чисел является кольцом целых элементов поля $\mathbb{Q}_p$ (и поле $\mathbb{Q}_p$ является полем частных кольца $\mathbb{Z}_p$). Каждый элемент s поля $\mathbb{Q}_p$ допускает одно и только одно *каноническое* представление в виде

$$s = \sum_{j=t}^{\infty} \sigma_j \cdot p^j,$$

где $t \in \mathbb{Z}$ — некоторое рациональное целое число, а $\sigma_j \in \{0, 1. \ldots, p-1\}$, $j = t, t+1, t+2, \ldots$.

Таким образом, мы видим, что пополняя множество рациональных чисел до полных метрических пространств, можно построить много различных числовых полей, среди которых только одно поле, поле действительных чисел $\mathbb{R}$ является архимедовым метрическим пространством, а все другие поля $\mathbb{Q}_p$, где p пробегает множество всех простых чисел, уже не являются архимедовыми.

В связи со сказанным возникает естественный вопрос, существуют ли еще какие-то поля, являющиеся пополнениями поля рациональных чисел $\mathbb{Q}$ относительно метрики, индуцированной некоторой нормой на $\mathbb{Q}$. Отрицательный ответ на этот вопрос дает *теорема Островского*, которая гласит, что с точностью до эквивалентности метрик, других пополнений, кроме поля действительных чисел $\mathbb{R}$ и полей p-адических чисел $\mathbb{Q}_p$, поле рациональных чисел не имеет. Напомним, что метрики d и d', заданные на пространстве M, называются эквивалентными, если каждая последовательность элементов множества M, являющаяся фундаментальной относительно метрики d (т.е. удовлетворяющая условию Коши относительно метрики d) является фундаментальной и относительно метрики d', и обратно, каждая фундаментальная относительно метрики d' последовательность, фундаментальна и относительно метрики d.

1.6. **Особенности неархимедова мира.** В этом разделе мы упомянем некоторые непривычные свойства неархимедова мира чтобы сделать его чуть более понятным.

Привычный нам мир, мир действительных чисел $\mathbb{R}$, архимедов. Это означает, что в нем выполняется аксиома Архимеда, которая гласит:

> Для данного отрезка S длины s и другого (меньшего) отрезка L длины ℓ, $\ell < s$, можно указать такое натуральное число n, что $n \cdot \ell > s$. (Другими словами, если мы приложим короткий отрезок сам к себе достаточное число раз,

мы получим отрезок, длиннее наперед заданного отрезка).

Эта аксиома *не выполняется* в p-адическом мире $\mathbb{Z}_p$: прикладывая отрезок сам к себе мы можем получить отрезок *короче*, чем исходный. Например, пусть $p = 2$, и пусть L — это некоторый «отрезок длины» $\frac{1}{2}$. Тогда удвоение этого отрезка (прикладывание к самому себе) дает «отрезок», который имеет длину $\|4\|_2 = \frac{1}{4}$. Удвоенный отрезок оказался *вдвое короче* исходного. Именно, возьмем точки $0, 2, 4$; тогда $d_2(0,2) = \|2\|_2 = \frac{1}{2}$, $d_2(2,4) = \|4-2\|_2 = \frac{1}{2}$, но $d_2(0,4) = \|4\|_2 = \frac{1}{4}$.

Вот еще несколько удивительных фактов, вытекающих из сильного неравенства треугольника ($3'$), которое отличает неархимедов мир от архимедова.

- Все треугольники — равнобедренные.
- Каждая точка внутри шара является центром этого шара.
- Ряд $\sum_{i=0}^{\infty} z_i$ целых p-адических чисел сходится *тогда и только тогда*, когда $\lim\limits_{i\to\infty}^{p} z_i = 0$, где $\lim\limits_{i\to\infty}^{p}$ — это предел относительно p-адической нормы $\|\cdot\|_p$.

Кстати, из последнего факта следует, например, что $\ln(-1) = \ln(1 + (-2)) = \sum_{i=1}^{\infty}(-1)^{i+1}\frac{(-2)^i}{i} = -\sum_{i=1}^{\infty}\frac{4^i}{i}$ есть целое 2-адическое число. Но поскольку из равенств $0 = \ln(1) = \ln((-1)(-1)) = \ln(-1) + \ln(-1) = 2\cdot\ln(-1)$ следует, что $\ln(-1) = 0$ в $\mathbb{Z}_2$, то, например, $\ln(-z) = \ln(z)$: в частности, $\ln(-5) = \ln(5) = \sum_{i=1}^{\infty}(-1)^{i+1}\frac{4^i}{i}$ есть некоторое целое 2-адическое число. И вообще, в $\mathbb{Z}_p$ функция $\ln$ определена на всем множестве $1 + p\mathbb{Z}_p$.

Заметим, что каждый шар $B_{p^{-1}}(a)$ в $\mathbb{Z}_p$ радиуса $\frac{1}{p^k}$ с центром в точке a имеет вид $B_{p^{-k}}(a) = a + p^k\cdot\mathbb{Z}_p = \{a + p^k\cdot z\colon z\in\mathbb{Z}_p\}$. Кстати, отсюда следует, что граница этого замкнутого шара (сфера радиуса $\frac{1}{p^k}$) есть объединение $p-1$ непересекающихся шаров радиуса $\frac{1}{p^{k+1}}$ каждый; следовательно, граница замкнутого шара замкнута, т.е. *замкнутый шар открыт*! Но поскольку открытый шар радиуса $\frac{1}{p^k}$ с центром в точке $a\in\mathbb{Z}_p$ есть множество

$$\left\{z\in\mathbb{Z}_p\colon \|z-a\|_p < \frac{1}{p^k}\right\} = \left\{z\in\mathbb{Z}_p\colon \|z-a\|_p \leqslant \frac{1}{p^{k+1}}\right\} = a+p^{k+1}\mathbb{Z}_p = B_{p^{-k-1}}(a),$$

то *открытый шар замкнут*. Таким образом, в p-адической топологии шары и сферы есть множества, который открыты и замкнуты одновременно. Например, граница шара радиуса $\frac{1}{2^k}$ есть шар радиуса $\frac{1}{2^{k+1}}$: т.е. сфера радиуса $\frac{1}{2}$ — это шар радиуса $\frac{1}{4}$. Все пространство $\mathbb{Z}_p$ — это шар радиуса 1, который является p-адическим аналогом единичного отрезка действительной прямой. Несложно показать, что два p-адических шара либо не пресекаются, либо один из них содержится в другом.

Все пространство $\mathbb{Z}_p$ тоже есть p-адический шар (радиуса 1; оно *полно* относительно метрики d_p и *компактно*.

1.6.1. *p-адические единицы.* Поскольку $\mathbb{Z}_p$ — коммутативное кольцо с единицей, то понятие обратимого элемента определяется стандартным

образом. Именно, говорят, что целое p-адическое число $x \in \mathbb{Z}_p$ *обратимо* в $\mathbb{Z}_p$, если для него существует *мультипликативный обратный* $x^{-1} \in \mathbb{Z}_p$: $x^{-1} \cdot x = 1$. Разумеется, если мультипликативный обратный существует, то он только один. Обратимые p-адические целые иногда называются также *p-адическими единицами*.

Несложно доказать следующие утверждения:

Предложение 1.3. *Целое p-адическое число $z \in \mathbb{Z}_p$ обратимо тогда и только тогда, когда $\delta_0(x) \neq 0$; т.е., тогда и только тогда, когда x* обратимо по модулю p, *что значит что наименьший неотрицательный вычет $x \bmod p$ является обратимым элементом поля $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Предложение 1.4. *Для любого $x \in \mathbb{Q}_p \setminus \{0\}$ найдется единственная p-адическая единица $\bar{x} \in \mathbb{Z}_p$ такая, что $x = p^{\operatorname{ord}_p x}\bar{x}$.*

Предложение 1.5.

$$(1+pz)^{-1} = 1 - pz + p^2z^2 - p^3z^3 + \cdots + (-1)^j p^j z^j + \cdots$$

Множество $\mathbb{Z}_p^*$ всех p-адических единиц из $\mathbb{Z}_p$ образует группу относительно умножения, которая называется *группой единиц* или *мультипликативной подгруппой* в $\mathbb{Z}_p$. Эта группа является *p-адической сферой* радиуса 1 с центром в точке 0:

$$\mathbb{Z}_p^* = \{z \in \mathbb{Z}_p \colon |z|_p = 1\} = \mathbb{Z}_p \setminus p\mathbb{Z}_p = B_1(0) \setminus B_{p^{-1}}(0) = S_1(0).$$

2. Элементы прикладного p-адического анализа

Основная задача этого раздела — изложить основы анализа и дифференциального исчисления в $\mathbb{Z}_p$. Мы не собираемся делать это слишком уж формально, поскольку есть много хороших книжек, посвященных p-адическому анализу в целом (см., например [2, 1, 3]), а сосредоточимся в основном на тех методах и идеях, которые используются в криптографических приложениях.

2.1. Предел и непрерывность в $\mathbb{Z}_p$.

Компакт $\mathbb{Z}_p$ есть пополнение множества $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ по метрике $d_p(x, y) = \|x - y\|_p$. Стало быть, любое число из $\mathbb{Z}_p$ есть предел последовательности чисел из $\mathbb{N}_0$ (эквивалентно, из $-\mathbb{N}_0 = \{0, -1, -2, \ldots\}$).

Стандартная формулировка p-адического предела выглядит следующим образом:

Определение 2.1 (p-адический предел)**.** p-адическое целое z является пределом последовательности $\{z_i\}_{i=0}^{\infty}$, если для любого $\varepsilon > 0$ найдется N такое, что $\|z_i - z\|_p < \varepsilon$ как только $i > N$.

Однако, согласно определению p-адической метрики, величина $\|z_i - z\|_p$ может принимать только значения вида $p^{-\ell}$ для подходящих $\ell = 0, 1, 2, \ldots$; поэтому можно считать, что $\varepsilon = p^{-r}$, где $r = 0, 1, 2, \ldots$ и переписать определение в эквивалентном виде:

Определение 2.2 (p-адический предел, эквивалентная формулировка)**.** p-адическое целое z есть предел последовательности $\{z_i\}_{i=0}^{\infty}$ если для любого (достаточно большого) положительного рационального целого K найдется N такое, что $z_i \equiv z \pmod{p^K}$ при всех $i > N$.

Замечание 2.3. По определению p-адической метрики,

$$\|z_i - z\|_p \le p^{-K} \text{ тогда и только тогда, когда } z_i \equiv z \pmod{p^K}.$$

Теперь мы можем сформулировать определение p-адической непрерывной функции:

Определение 2.4 (p-адическая непрерывная функция, эквивалентная формулировка)**.** Функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ называется непрерывной в точке $z \in \mathbb{Z}_p$, если для любого (достаточно большого) положительного рационального целого M найдется положительное рациональное целое L такое, что $f(x) \equiv f(z) \pmod{p^M}$ как только $x \equiv z \pmod{p^L}$.

Функция f называется *равномерно* непрерывной на $\mathbb{Z}_p$, если f непрерывна в каждой точке $z \in \mathbb{Z}_p$, и L зависит только от M и не зависит от z.

2.2. **T-функции.** Мы начнем с очень важных для криптографии примеров, с 2-адических продолжений тех функций, которые мы называем элементарными командами процессора. Это, в первую очередь, арифметические операции (сложение, вычитание, умножение), а также поразрядные логические операции. Эти операции не являются независимым: некоторые из них могут быть выражены через другие. Например, для всех $u, v \in \mathbb{Z}_2$ выполняются следующие тождества:

$$\begin{aligned}
&\mathsf{NOT}(u) = u \,\mathsf{XOR}(-1);\\
&\mathsf{NOT}(u) + u = -1;\\
&u \,\mathsf{XOR}\, v = u + v - 2(u \,\mathsf{AND}\, v);\\
&u \,\mathsf{OR}\, v = u + v - (u \,\mathsf{AND}\, v);\\
&u \,\mathsf{OR}\, v = (u \,\mathsf{XOR}\, v) + (u \,\mathsf{AND}\, v).
\end{aligned} \tag{2.4.1}$$

Отметим, что мы часто пишем $\oplus$ вместо XOR, $\odot$, $\&$ или $\wedge$ вместо AND, и $\vee$ вместо OR. Все эти операции (за исключением NOT) суть функции двух 2-адических переменных. Чтобы работать с такими функциями, нам нужно сначала задать 2-адическую метрику на декартово квадрате $\mathbb{Z}_2^2$. Поскольку метрика на $\mathbb{Z}_2$ уже задана, метрика на декартовом произведении

$$\mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n \text{ раз}}$$

задается стандартным способом: для $\mathbf{a} = (a^{(1)}, \ldots, a^{(n)}), \mathbf{b} = (b^{(1)}, \ldots, b^{(n)}) \in \mathbb{Z}_2^n$ мы полагаем $\|\mathbf{a}\|_2 = \max\{\|a^{(1)}\|_2, \ldots, \|a^{(n)}\|_2\}$ и, соответственно,

$$d_2(\mathbf{a}, \mathbf{b}) = \max\{d_2(a^{(1)}, b^{(1)}), \ldots, d_2(a^{(n)}, b^{(n)})\}.$$

Мы также будем писать $\mathbf{a} \equiv \mathbf{b} \pmod{2^i}$, если $a^{(j)} \equiv b^{(j)} \pmod{2^i}$ для всех $j = 1, 2, \ldots, n$.

Вышеприведенные операции являются примерами так называемых *T-функций*, преобразований, играющих в криптографии очень важную роль.

Определение 2.5. T-функция (от m переменных) — это любое отображение

$$F\colon (\ldots, \alpha_2^{\downarrow}, \alpha_1^{\downarrow}, \alpha_0^{\downarrow}) \mapsto (\ldots, \Phi_2(\alpha_0^{\downarrow}, \alpha_1^{\downarrow}, \alpha_2^{\downarrow}), \Phi_1(\alpha_0^{\downarrow}, \alpha_1^{\downarrow}), \Phi_0(\alpha_0^{\downarrow}))$$

где $\alpha_i^{\downarrow} \in \mathbb{F}_2^m$ — m-мерный булев вектор-столбец; $\mathbb{F}_2 = \{0,1\}$; отображение $\Phi_i\colon (\mathbb{F}_2^m)^{(i+1)} \to \mathbb{F}_2^n$ сопоставляет $(i+1)$-у m-мерным булевым вектор-столбцам $\alpha_i^{\downarrow}, \ldots, \alpha_0^{\downarrow}$ соответствующий n-мерный булев вектор-столбец $\Phi_i(\alpha_0^{\downarrow}, \ldots, \alpha_i^{\downarrow})$.

Например, T-функция $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ одной переменной —

$$(\ldots, \chi_2, \chi_1, \chi_0) \overset{F}{\mapsto} (\ldots; \psi_2(\chi_0, \chi_1, \chi_2); \psi_1(\chi_0, \chi_1); \psi_0(\chi_0)),$$

где $\chi_j \in \{0,1\}$, и каждая $\psi_j(\chi_0, \ldots, \chi_j)$ есть булева функция от булевых переменных $\chi_0, \ldots, \chi_j$.

T-функции естественным образом можно рассматривать как непрерывные 2-адические отображения. Фактически (см. определение 2.5) мы определяли T-функцию как отображение специального вида, сопоставляющее каждой последовательности m-мерных булевых векторов-столбцов некоторую последовательность n-мерных булевых векторов-столбцов. Мы можем рассмотреть каждую такую последовательность не как последовательность столбцов, а как m (соответственно, n) бесконечных строк, если начнем считывать строку за строкой, начиная с верхней строки. Каждая такая строка есть бесконечная последовательность нулей и единиц, т.е. целое 2-адическое число. Таким образом, мы заключаем:

> *Каждая T-функция F из определения 2.5 есть отображение $\mathbb{Z}_2^m$ в $\mathbb{Z}_2^n$ такое, что $F(\mathbf{a}) \equiv F(\mathbf{b}) \pmod{2^i}$ как только $\mathbf{a} \equiv \mathbf{b} \pmod{2^i}$.*

Из этого наблюдения сразу вытекает следующая важная теорема:

Теорема 2.6. *Все T-функции суть отображения $\mathbb{Z}_2^m$ в $\mathbb{Z}_2^n$, удовлетворяющие 2-адическому условию Липшица с константой 1:*

$$\|F(\mathbf{a}) - F(\mathbf{b})\|_2 \leq \|\mathbf{a} - \mathbf{b}\|_2$$

Обратно, все отображения, удовлетворяющие этому условию, суть T-функции.

Следствие 2.7. *Все T-функции являются непрерывными 2-адическими функциями* (поскольку любая функция, удовлетворяющая условию Липшица относительно некоторой метрики, непрерывна в этой метрике).

Эти довольно несложные для доказательства утверждения дают основания считать, что 2-адический анализ может оказаться полезным при изучении свойств T-функций (разумеется, если речь идет об «аналитических» свойствах, которые могут быть сформулированы в терминах математического анализа в виде сходимостей, производных, рядов и т.п.). Мы пока еще не сформулировали, какие именно свойства T-функций важны для криптографии. Но, когда мы сформулируем эти свойства чуть позже, мы убедимся в том, что они «аналитические».

2.3. **Совместимые функции.** Вышеприведенное наблюдение отражает еще одно очень специфическое *алгебраическое* свойство T-функций. В общей алгебре *конгруэнция* алгебраической системы есть, по определению, отношение эквивалентности, сохраняющееся относительно всех операций этой системы; т.е., заменяя элементы под знаком операции

на эквивалентные, мы получим в результате операции элемент, эквивалентный первоначальному. Функция, определенная и принимающая значения на элементах алгебраической системы, называется *совместимой*, если она сохраняет все конгруэнции этой системы. Поскольку все конгруэнции кольца $\mathbb{Z}_p$ суть отношения сравнимости по модулю p^k при $k = 1, 2, \ldots$, то мы приходим к выводу, что *T-функции суть совместимые функции на кольце $\mathbb{Z}_2$ и обратно*. Поэтому мы будем использовать термин «совместимая функция», наряду (или вместо) термина «T-функция». Фактически, термин «T-функция» означает просто «совместимая функция на кольце $\mathbb{Z}_2$». Многие результаты, сформулированные для T-функций, остаются справедливыми для совместимых функций на кольце $\mathbb{Z}_p$, p простое. Например, p-адическая совместимая функция удовлетворяет p-адическому условию Липшица с константой 1, и обратно.

Мы уже знаем, что арифметические операции (сложение, вычитание, умножение) и поразрядные логические операции (XOR, AND, и т.п.) суть T-функции, т.е. совместимые 2-адические функции. Очевидно, что *композиция совместимых функций есть совместимая функция*. Значит, естественными примерами совместимых функций являются *полиномы* с целыми p-адическими коэффициентами. В частности, все полиномы с целыми коэффициентами суть T-функции.

При некоторых дополнительных усилиях можно показать, что некоторые другие «естественные» функции тоже являются T-функциями:

$$\begin{aligned}
&-\textit{экспоненцирование, } \uparrow\colon\ (u, v) \mapsto u \uparrow v = (1 + 2 \cdot u)^v;\ \text{в частности,}\\
&-\textit{возведение в отрицательную степень, } u \uparrow (-r) = (1 + 2 \cdot u)^{-r}, r \in \mathbb{N};\\
&-\textit{деление } /\ : u/v = u \cdot (v \uparrow (-1)) = \frac{u}{1 + 2 \cdot v}.
\end{aligned} \tag{2.7.1}$$

Именно, все эти функции корректно определены на $\mathbb{Z}_2$ и удовлетворяют 2-адическому условию Липшица с константой 1. Использование этих функций в композиции с поразрядными логическими операциями позволяет строить совместимые функции совсем уж «дикие» на вид, как, например, эта:

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

Между прочим, значения этой функции несложно сосчитать на любом компьютере, поскольку эта функция непрерывна относительно 2-адической метрики.

Аналоги вышеприведенных функций для нечетного простого p определяются естественным образом. Также уместно отметить, что $(1 + p \cdot v)^{-1} = \sum_{i=0}^{\infty} (-1)^{i+1} p^i v^i$, причем ряд в правой части этого равенства сходится при всех $v \in \mathbb{Z}_p$.

Кроме T-функций, важным примером совместимых функций являются *детерминированные функции*, т.е. функции, задаваемые автоматами.

По определению, (инициальный) автомат есть кортеж $\mathfrak{A}(s_0) = \langle \mathcal{I}, \mathcal{S}, \mathcal{O}, S, O, s_0 \rangle$, где $\mathcal{I}$ — входной алфавит, $\mathcal{S}$ — множество состояний, $\mathcal{O}$ — выходной алфавит, $S\colon \mathcal{I}\times\mathcal{S} \to \mathcal{S}$ — функция перехода, $O\colon \mathcal{I}\times\mathcal{S} \to \mathcal{O}$ — функция выхода, $s_0 \in \mathcal{S}$ — начальное состояние. Автомат $\mathfrak{A}(s_0)$ преобразует входное слово $w = \chi_{n-1}\cdots\chi_1\chi_0$ над входным алфавитом $\mathcal{I} = \mathbb{F}_p = \{0, 1, \ldots, p-1\}$ преобразует в выходное слово $w' = \xi_{n-1}\cdots\xi_1\xi_0$ над выходным алфавитом $\mathcal{O} = \mathbb{F}_p$ в соответствии с алгоритмом, блок-схема которого изображена на рис. 1): В начальный момент времени автомат $\mathfrak{A}(s_0)$ находится в состоянии s_0 и принимает входной символ $\chi_0 \in \mathcal{I}$, подавая на выход выходной символ $\xi_0 = O(\chi_0, s_o) \in \mathcal{O}$ и переходя в состояние $s_1 = S(\chi_0, s_0) \in \mathcal{S}$. Затем автомат принимает следующий входной символ $\chi_1 \in \mathcal{I}$, переходит в состояние $s_2 = S(\chi_1, s_1) \in \mathcal{S}$ и подает на выход символ $\xi_1 = O(\chi_1, s_1) \in \mathcal{O}$, и т.д. Таким образом автомат $\mathfrak{A}(s_0)$ корректно задает отображение $f_{\mathfrak{A}(s_0)}$ из $\mathbb{Z}_p$ в $\mathbb{Z}_p$, если трактовать элементы из $\mathbb{Z}_p$ как бесконечные слова над алфавитом $\mathbb{F}_p$. Это отображение $f_{\mathfrak{A}(s_0)}$ и называется детерминированной функцией, задаваемой автоматом $\mathfrak{A}(s_0)$.

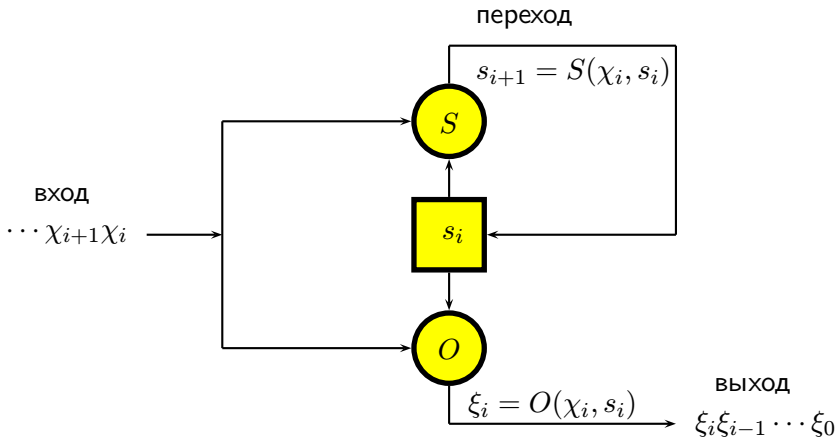

Рис. 1. Инициальный автомат

Как мы видим, выходной символ ξ_i автомата в i-ом такте зависит только от входных символов $\chi_0, \ldots, \chi_i$ в тактах $0, 1, \ldots, i$; следовательно, всякая детерминированная функция над алфавитом из p символов совместима, т.е. удовлетворяет p-адическому условию Липшица с константой 1. Можно показать, что верно и обратное: каждая функция, удовлетворяющая p-адическому условию Липшица с константой 1, может быть задана с помощью некоторого автомата (не обязательно имеющего конечное число состояний).

Теорема 2.8. *Детерминированная функция $f_{\mathfrak{A}(s_0)}\colon \mathbb{Z}_p \to \mathbb{Z}_p$, соответствующая автомату $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0 \rangle$, совместима, т.е. удовлетворяет p-адическому условию Липшица с константой 1. Обратно, для каждой совместимой функции $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ существует автомат $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0 \rangle$ такой, что $f = f_{\mathfrak{A}(s_0)}$.*

Доказательство. Действительно, поскольку каждый i-й выходной символ $\psi_i = O(s_i, \chi_i)$ автомата зависит только от i-го состояния s_i и от i-го

входного символа χ_i, и поскольку состояние $s_i = S(s_{i-1}, \chi_{i-1})$ зависит только от s_{i-1} и от χ_{i-1}, и т.д. Таким образом, каждый выходной символ $\xi_i = \psi_i(\chi_0, \ldots, \chi_i) \in \mathbb{F}_p$, $i = 0, 1, 2, \ldots$, зависит только от входных символов $\chi_0, \ldots, \chi_i \in \mathbb{F}_p$ и не зависит от символов $\chi_{i+1}, \chi_{i+2}, \ldots$. Следовательно, детерминированная функция $f = f_{\mathfrak{A}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ имеет вид

$$f \colon x = \sum_{i=0}^{\infty} \chi_i p^i \mapsto f(x) = \sum_{i=0}^{\infty} \psi_i(\chi_0, \ldots, \chi_i) p^i. \tag{2.8.1}$$

Другими словами, каждой детерминированной функции f соответствует единственная последовательность отображений $\psi_i \colon \mathbb{F}_p^n \to \mathbb{F}_p$. Однако каждая функция $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$, имеющая вид (2.8.1), очевидно совместима, т.е. удовлетворяет p-адическому условию Липшица с константой 1, ср. определение 2.5 и подраздел 2.3.

Обратно, пусть дана совместимая функция $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$; тогда ее можно представить в виде (2.8.1). Построим автомат $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0 \rangle$ такой что $f_{\mathfrak{A}(s_0)} = f$. Возьмем множество $\mathbb{F}_p^\star$ всех непустых конечных слов над алфавитом $\mathbb{F}_p$, рассмотрим эти слова как представления натуральных чисел $\mathbb{N} = \{1, 2, 3, \ldots\}$ в системе счисления с основанием p и перенумеруем слова в лексикографическом порядке в соответствии с естественным порядком на $\mathbb{N}$. Таким образом мы установим взаимнооднозначное соответствие между всеми непустыми словами w над алфавитом $\mathbb{F}_p$ и числами $i = 1, 2, 3, \ldots$: $w \leftrightarrow \nu(w)$, $i \leftrightarrow \omega(i)$ ($\nu(w) \in \mathbb{N}$, $\omega(i) \in \mathbb{F}_p^\star$). Заметим, что $\nu(\omega(i)) = i$, $\omega(\nu(w)) = w$ для всех $i \in \mathbb{N}$ и всех непустых слов $w \in \mathbb{F}_p^\star$. Будем считать, что $\omega(0)$ есть пустое слово.

В качестве множества $\mathcal{S}$ всех состояний автомата $\mathfrak{A}$ возьмем множество $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$, и возьмем $s_0 = 0$ в качестве начального состояния. Зададим функцию перехода S следующим образом: $S(i, r) = \nu(r\omega(i))$, где $i = 0, 1, 2, \ldots$ $r \in \mathbb{F}_p$; т.е. $S(i, r)$ равна номеру слова $r\omega(i)$, которое есть результат конкатенации слова $\omega(i)$ (с номером i) в качестве *префикса* (начала) с однобуквенным словом r в качестве *суффикса* (окончания). Зададим функция выхода следующим образом: $O(i, r) = \psi_{|\omega(i)|}(r\omega(i))$; здесь и далее в доказательстве теоремы символом $|w|$ обозначается длина слова w (длина пустого слова равна 0). Отображение $\psi_i \colon F_p^{i+1} \to \mathbb{F}_p$ может рассматриваться как отображение множества всех слов длины $i + 1$ над алфавитом $\mathbb{F}_p$ во множество всех однобуквенных слов $\mathbb{F}_p$, $i = 0, 1, 2, \ldots$. Отметим, что при необходимости здесь и далее мы будем использовать без дополнительных оговорок естественное соответствие между словами длины n и элементами кольца вычетов m $\mathbb{Z}/p^n\mathbb{Z}$, также как и соответствие между множеством всех бесконечных слов $\mathbb{F}_p^\infty$ и кольцом $\mathbb{Z}_p$.

Поскольку f удовлетворяет p-адическому условию Липшица с константой 1, она непрерывна относительно p-адической метрики, а потому чтобы доказать, что $f = f_{\mathfrak{A}(s_0)}$ достаточно показать, что $f_{\mathfrak{A}(s_0)}(w) \equiv f(w) \pmod{p^{\lambda(w)}}$ для всех непустых слов $w \in \mathbb{F}_p^\star$: действительно, если это так, то если дано бесконечное слово $w \in \mathbb{F}_p^\infty$, то последовательность $w \bmod p^n$, $n = 1, 2, 3, \ldots$, состоящая из конечных слов, сходится p-адически к w, т.е. $f(w) \bmod p^n$ сходится p-адически к $f(w)$ при n стремящимся к бесконечности.

Индукцией по n докажем, что если входное слова w имеет длину $n > 0$, то $f_{\mathfrak{A}(s_0)}(w) \equiv f(w) \pmod{p^n}$. Если $n = 1$, то $w \in \mathbb{F}_p$, и после того, как w подано на вход, автомат $\mathfrak{A}$ перейдет в состояние $S(0, w) = \nu(w)$ и подаст на выход символ $O(0, w) = \psi_0(w) = f(w) \bmod p$, см. (2.8.1).

Предположим, что утверждение верно для всех $n < k$ и докажем, что оно верно и при $n = k$. Рассмотрим слово w длины n; тогда $w = rv$, где $r \in \mathbb{F}_p$, $|v| = n-1$ (т.е. w состоит из префикса v и суффикса r). По предположению индукции, после того как слово v будет подано на вход, автомат перейдет в состояние $\nu(v)$ и подаст на выход слово $v' = f(v) \bmod p^{n-1}$. Следовательно, после того как на вход будет подан символ r, автомат подаст на выход символ $O(\nu(v), r) = \psi_{|\omega(\nu(v))|}(r\omega(\nu(v))) = \psi_{|v|}(rv)$. Стало быть, если подать на вход слово w, то автомат подаст на выход слово $v'' = (\psi_{|v|}(rv))v'$, которое есть результат конкатенации слова $v' = f(v) \bmod p^{n-1}$ в качестве префикса с однобуквенным словом $\psi_{|v|}(rv) \in \mathbb{F}_p$ в качестве суффикса. Однако $v'' = f(w) \bmod p^n$, см. (2.8.1). Этим завершается доказательство утверждения и теоремы в целом. □

Итак, класс всех p-адических функций, удовлетворяющих p-адическому условию Липшица с константой 1, совпадает с классом всех детерминированных функций над алфавитом из p символов, а тот в свою очередь совпадает с классом всех совместимых функций на $\mathbb{Z}_p$.

Можно дать и еще одну (эквивалентную) характеризацию совместимых функций: именно, функция совместима тогда и только тогда, когда она каждый p-адический шар отображает в p-адический шар. Доказательство этой эквивалентности немедленно следует из того, что совместимость функции f означает, что $f(a) \bmod p^n = f(b) \bmod p^n$ как только $a \bmod p^n = b \bmod p^n$.

2.4. **p-адическая дифференцируемость.** В p-адическом анализе дифференцируемость функции определяется так же, как и в действительном анализе, с той лишь разницей, что в определении фигурирует p-адическая абсолютная величина:

Определение 2.9. Функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ называется *дифференцируемой в точке* $x \in \mathbb{Z}_p$, если существует p-адическое число $f'(x) \in \mathbb{Q}_p$ такое, что для любого $M \in \mathbb{N}$

$$\left\| \frac{f(x+h) - f(x)}{h} - f'(x) \right\|_p \leqslant \frac{1}{p^M}, \tag{2.9.1}$$

если h достаточно мало, т.е. когда $\|h\|_p \leqslant p^{-K}$, где $K = K(M)$ достаточно велико.

Функция f называется *равномерно дифференцируемой* (на $\mathbb{Z}_p$), если неравенство (2.9.1) выполняется одновременно для всех $x \in \mathbb{Z}_p$ как только h достаточно мало.

Можно показать, что если функция f совместимой(т.е. удовлетворяет p-адическому условию Липшица с константой 1), то из ее дифференцируемости в точке x с необходимостью следует, что $\|f'(x)\|_p \leqslant 1$, а следовательно, $f'(x) \in \mathbb{Z}_p$.

Предложение 2.10. *Если совместимая функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ дифференцируема в точке $x \in \mathbb{Z}_p$, то $f'(x) \in \mathbb{Z}_p$.*

Доказательство. Если $f'(x) = 0$, то предложение доказано. Пусть $f'(x) \neq 0$; тогда $f'(x) = p^m s$, где $s \in \mathbb{Z}_p$, $s \not\equiv 0 \pmod p$, $m = \operatorname{ord}_p f'(x)$ (см. предложения 1.4 и 1.3). В силу дифференцируемости, $f(x+p^n) \equiv f(x)+p^m s\cdot p^n \pmod{p^{n+1}}$ для всех достаточно больших n; поэтому $f(x+p^n) - f(x) \equiv p^{m+n}s \pmod{p^{n+1}}$.

С другой стороны, $\|f(x+p^n) - f(x)\|_p \leqslant p^{-n}$, поскольку f совместима; стало быть, $f(x+p^n t) - f(x) = p^n a$ для подходящего $a \in \mathbb{Z}_p$. Следовательно, $p^n a \equiv p^{m+n}s \pmod{p^{n+1}}$; значит, $a \equiv p^m s \pmod p$. Из последнего сравнения вытекает, что $m \geqslant 0$ так как $a, s \in \mathbb{Z}_p$ и $s \not\equiv 0 \pmod p$. Значит, $\operatorname{ord}_p f'(x) \geq 0$; т.е., $f'(x) \in \mathbb{Z}_p$.

□

Итак, *значение производной совместимой функции является целым p-адическим числом*, а потому определение 2.9 можно в силу замечания 2.3 переписать в эквивалентной форме, в терминах сравнений, а не неравенств:

Определение 2.11. Функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ называется *дифференцируемой в точке $x \in \mathbb{Z}_p$*, если существует p-адическое число $f'(x)\mathbb{Q}_p$ такое, что для любого $M \in \mathbb{N}$

$$f(x+h) \equiv f(x) + h\cdot f'(x) \pmod{p^{M+\operatorname{ord}_p h}}. \tag{2.11.1}$$

Функция f называется *равномерно дифференцируемой* (на $\mathbb{Z}_p$), если неравенство (2.11.1) выполняется одновременно для всех $x \in \mathbb{Z}_p$ как только h достаточно мало, т.е. когда $\operatorname{ord}_p h \geqslant K = K(M)$ для достаточно большого $K \in \mathbb{N}$.

Иными словами, равномерная дифференцируемость означает, что для любого (достаточно большого) $M \in \mathbb{N}$ найдется $N = N_M(f) \in \mathbb{N}$ такое, что

$$f(x+h) \equiv f(x) + h\cdot f'(x) \pmod{p^{M+K}} \tag{2.11.2}$$

как только $h \equiv 0 \pmod{p^K}$ и $K \geqslant N_M(f)$.

Пример 2.12. Функция $f(x) = x \operatorname{AND} C$ равномерно дифференцируема на $\mathbb{Z}_2$ при любом $C \in \mathbb{Z}$, причем

$$f'(x) = \begin{cases} 0, & \text{если } C \geqslant 0, \\ 1, & \text{если } C < 0. \end{cases}$$

Действительно, пусть $n \geq \ell(|C|)$, где $\ell(|C|)$ — число разрядов, необходимых для двоичной записи $|C|$; тогда $f(x+2^n s) = f(x)$ при $C \geq 0$, и $f(x+2^n s) = f(x) + 2^n s$ при $C < 0$. Напомним, что в младших разрядах 2-адического представления отрицательного числа $-R$ находится двоичное представления числа $2^{\ell(R)} - R$, а все остальные разряды равны 1. Например, $-1 = \ldots 111$, $-3 = \ldots 11101$, и т.п.

Аналогичным образом можно показать, что

- Функция $f(x) = x \operatorname{XOR} C$ равномерно дифференцируема на $\mathbb{Z}_2$ при любом $C \in \mathbb{Z}$; $f'(x) = 1$, если $C \geq 0$, и $f'(x) = -1$, если $C < 0$.

- Функции $x \bmod 2^n$ (наименьший неотрицательный вычет x по модулю 2^n), $\mathsf{NOT}(x)$ и $x \mathbin{\mathsf{OR}} C$, где $C \in \mathbb{Z}$, равномерно дифференцируемы на $\mathbb{Z}_2$, и $(x \bmod 2^n)' = 0$, $(\mathsf{NOT}\, x)' = -1$, $(x \mathbin{\mathsf{OR}} c)' = 1$, если $C \geqslant 0$, $(x \mathbin{\mathsf{OR}} C)' = 0$ если $C < 0$.

Отметим, что правила дифференцирования не зависят от метрики: для вычисления производных суммы, частного и сложной функции в p-адическом анализе используются те же формулы, что и в действительном.

Пример 2.13. Для любого $m \in \mathbb{N}$ степенная функция $f(x) = x^m$ равномерно дифференцируема на $\mathbb{Z}_p$ и $f'(x) = mx^{m-1}$.

В самом деле, по биному Ньютона,

$$(x + p^n z)^m = \sum_{i=0}^{m} \binom{m}{i} x^{m-i} p^{ni} z^i;$$

значит $(x + p^n z)^m \equiv x^m + mx^{m-1} \cdot p^n z \pmod{p^{n+k}}$, если $n \geqslant k$. Стало быть, $(x + h)^m \equiv x^m + mx^{m-1} \cdot h \pmod{p^{\operatorname{ord}_p h + k}}$ как только $h \equiv 0 \pmod{p^k}$. Другими словами, мы можем положить $N_k(f) = k$, см. определение 2.11.

Отсюда следует, например, что функция $f(x) = x^2 \mathbin{\mathsf{OR}} 4$ равномерно дифференцируема на $\mathbb{Z}_2$ и ее производная равна $2x$.

Не упускать из виду и некоторые резкие различия между p-адическим анализом и действительным: например, и в том, и в другом случае производная константы равна 0, однако в p-адическом анализе в отличие от действительного равенство нулю производной некоторой функции не означает, что эта функция — константа! Например, функция $\delta_0(x)$, которая также является совместимой, равномерно дифференцируема на $\mathbb{Z}_p$, но ее производная равна 0 во всех точках из $\mathbb{Z}_p$.

2.5. **Лемма Гензеля и ее следствия.** Следующий результат — это знаменитая Лемма Гензеля, которая и положила начало p-адическому анализу. Курт Гензель — немецкий математик, открывший p-адические числа на рубеже XIX–XX веков.

Лемма 2.14 (Классическая лемма Гензеля)**.** *Если многочлен $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ над кольцом целых чисел $\mathbb{Z}$ имеет корень z по модулю p* (т.е., если $f(z) \equiv 0 \pmod p$) *такой, что $f'(z) \not\equiv 0 \pmod p$, то f имеет корень $\hat{z}$ в $\mathbb{Z}_p$ и $z \equiv \hat{z} \pmod p$.*

Доказательство. Положим $z_0 = z$; покажем, что для $z_n \in \mathbb{Z}_p$ такого, что $f(z_n) \equiv 0 \pmod{p^n}$, найдется $z_{n+1} \in \mathbb{Z}_p$ такое, что

$$f(z_{n+1}) \equiv 0 \pmod{p^{n+1}}; \tag{2.14.1}$$

$$z_{n+1} \equiv z_n \pmod{p^n}. \tag{2.14.2}$$

Положим $z_{n+1} = z_n + p^n t$; найдем $t \in \mathbb{Z}_p$ такое, чтобы вышеприведенные условия были выполнены.

В силу примера 2.13, для $n \geq 1$ мы имеем, что $f(z_n + p^n t) \equiv f(z_n) + f'(x) \cdot p^n t \pmod{p^{n+1}}$; следовательно, достаточно найти t такое, что

$$0 \equiv p^n s + f'(x) \cdot p^n t \pmod{p^{n+1}} \tag{2.14.3}$$

где $p^n s \equiv f(z_n) \pmod{p^{n+1}}$. Напомним, что из сравнения $f(z_n) \equiv 0 \pmod{p^n}$ следует, что $f(z_n) = p^n s$ для подходящего $s \in \mathbb{Z}_p$.

Сравнение (2.14.3) эквивалентно сравнению $0 \equiv s + f'(x) \cdot t \pmod{p}$, которое имеет решение относительно неизвестного t, поскольку $f'(x) \not\equiv 0 \pmod{p}$ и, стало быть, $f'(x)$ обратим в $\mathbb{Z}_p$ в силу предложения 1.3.

Система сравнений (2.14.2) означает, что последовательность $(z_j)_{j=0}^{\infty} = z_0, z_1, z_2, \ldots$ фундаментальна по отношению к p-адической метрике. Стало быть, эта последовательность имеет своим пределом целое p-адическое число $\hat{z}$ так как $\mathbb{Z}_p$ замкнуто в p-адической топологии. Однако $f(\hat{z}) = \lim\limits_{n\to\infty}^{p} f(z_n) = 0$ в силу (2.14.1), поскольку f непрерывна относительно p-адической метрики. □

Замечание. Из доказательства леммы Гензеля немедленно следует, что она справедлива и для многочленов над $\mathbb{Z}_p$.

В качестве приложения мы собираемся получить необходимые и достаточные условия обратимости некоторых автоматов, используя идеи из доказательства леммы Гензеля, а попутно установим целый ряд других фактов, имеющих важные приложения к криптографии.

Мы имеем целью показать, что если детерминированная функция, соответствующая автомату с входным и выходным алфавитом $0, 1, \ldots, p-1$, является равномерно дифференцируемой на $\mathbb{Z}_p$, то автомат обратим на множестве всех слов любой фиксированной длины тогда и только тогда, когда он обратим на множестве всех слов некоторой (достаточно большой) фиксированной длины. Напомним, что автомат $\mathfrak{A}(s_0)$ называется обратимым, если существует автомат $\mathfrak{B}(t_0)$, который задает детерминированную функцию, обратную к той, которую задает автомат $\mathfrak{A}(s_0)$; другими словами, если последовательное соединение автоматов $\mathfrak{A}(s_0)$ и $\mathfrak{B}(t_0)$ осуществляет тождественное преобразование слов над алфавитом $\mathbb{F}_p$.

Определение 2.15. Совместимая функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ называется биективной по модулю p^n, если отображение $f \bmod p^n\colon z \mapsto f(z) \bmod p^n$ кольца вычетов $\mathbb{Z}/p^n\mathbb{Z} = \{0, 1, \ldots, p^n - 1\}$ в себя взаимно-однозначно.

Отметим, что в данном определении мы трактуем элементы кольца $\mathbb{Z}/p^n\mathbb{Z}$ вычетов по модулю p^n как числа $0, 1, \ldots, p^n - 1$. Таким образом, отображение $f \bmod p^n$ ставит в соответствие числу $z \in \{0, 1, \ldots, p^n - 1\}$ число $f(z) \bmod p^n \in \{0, 1, \ldots, p^n - 1\}$, которое является наименьшим неотрицательным вычетом (по модулю p^n) p-адического целого $f(z)$. Заметим также, что в силу совместимости функции f отображение $f \bmod p^n$ определено корректно в том смысле, что не зависит от выбора конкретных представителей в классах p-адических целых чисел, имеющих одинаковые вычеты по модулю p^n.

Теорема 2.16. *Пусть совместимая функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ равномерно дифференцируема на $\mathbb{Z}_p$. Функция f является биективной на $\mathbb{Z}_p$ тогда и только тогда, когда функция f биективна по модулю p^n для какого-нибудь $n \geqslant N_1(f) + 1$* (см. определение 2.11).

Для доказательства этой теоремы нам понадобятся три леммы, каждая из которых представляет самостоятельный интерес.

Лемма 2.17. *Если совместимая* (не обязательно дифференцируемая!) *функция* $g\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *биективна по модулю* p^{n+1} *для некоторого* $n \in \mathbb{N}$, *то она биективна и по модулю* p^n.

Доказательство леммы 2.17. Поскольку g сюръективна по модулю p^{n+1}, то для любого $a \in \{0, 1, \ldots, p^{n+1}-1\}$ найдется $b \in \{0, 1, \ldots, p^{n+1}-1\}$ такое, что $g(b) \equiv a \pmod{p^{n+1}}$. Но тогда тем более $g(b) \equiv a \pmod{p^n}$. Отсюда следует сюръективность (а значит, и биективность) функции g по модулю p^n, поскольку любое число из $\{0, 1, \ldots, p^n-1\}$ есть вычет по модулю p^n некоторого числа из $\{0, 1, \ldots, p^{n+1}-1\}$: для $\bar{a} \in \{0, 1, \ldots, p^n-1\}$ берем $a \in \{0, 1, \ldots, p^{n+1}-1\}$ такое, что $a \equiv \bar{a} \pmod{p^n}$; тогда $g(\bar{b}) \equiv \bar{a} \pmod{p^n}$, где $\bar{b} = b \bmod p^n$. □

Лемма 2.18. *Совместимая* (не обязательно дифференцируемая!) *функция* $g\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *есть биекция* $\mathbb{Z}_p$ *на* $\mathbb{Z}_p$ *тогда и только тогда, когда она биективна по модулю* p^n *для каждого* $n = 1, 2, 3, \ldots$.

Доказательство леммы 2.18. Если отображение $g \bmod p^n$ не сюръективно для некоторого $n \in \mathbb{N}$, т.е. если существует $c \in \mathbb{Z}/p^n\mathbb{Z}$ такое, что $g(z) \not\equiv c \pmod{p^n}$ для всех $z \in \mathbb{Z}_p$, то это значит, что шар $c + p^n\mathbb{Z}_p$ не лежит в $g(\mathbb{Z}_p)$[2], и, следовательно, g не является биекцией $\mathbb{Z}_p$ на $\mathbb{Z}_p$ вопреки условию леммы. Следовательно, если g — биекция, то каждое отображение $g \bmod p^n$ сюръективно, а значит, и биективно, т.к. $g \bmod p^n$ есть отображение конечного множества в себя.

Обратно, предположим, что все отображения $g \bmod p^n$ биективны. Докажем, что тогда функция g инъективна и сюръективна.

Действительно, если бы g не была инъективной, то нашлись бы $a, b \in \mathbb{Z}_p$, $a \neq b$, такие, что $f(a) = f(b) = z$; но тогда бы $f(a) \bmod p^n = f(b) \bmod p^n = z \bmod p^n$ для всех $n \in \mathbb{N}$. Однако $a \bmod p^n \neq b \bmod p^n$ для всех достаточно больших n, т.к. последовательности $(a \bmod p^n)_{n=1}^{\infty}$ $(b \bmod p^n)_{n=1}^{\infty}$ сходятся к a и b соответственно, но $a \neq b$. Противоречие.

Теперь докажем, что функция g сюръективна. Возьмем произвольное $z \in \mathbb{Z}_p$ и рассмотрим последовательность $(z_n = z \bmod p^n)_{n=1}^{\infty}$. Эта последовательность сходится к z относительно p-адической метрики. Поскольку каждое отображение $g \bmod p^n$ биективно, для каждого $n \in \mathbb{N}$ найдется единственное $\tilde{z}_n \in \{0, 1, \ldots, p^n - 1\}$ такое, что $g(\tilde{z}_n) \bmod p^n = z_n$.

Докажем, что последовательность $(\tilde{z}_n)_{n=1}^{\infty}$ фундаментальна относительно p-адической метрики. Действительно, возьмем $m, n \in \mathbb{N}$, $m > n$; тогда $\tilde{z}_m \equiv \tilde{z}_n \pmod{p^n}$, ибо в противном случае нашлось бы как минимум два различных элемента в $\mathbb{Z}/p^n\mathbb{Z}$ (именно, $\tilde{z}_n$ и $\tilde{z}_m \bmod p^n$), образы которых при действии $g \bmod p^n$ совпадают. Но это противоречит биективности отображения $g \bmod p^n$. Стало быть, $\tilde{z}_m \equiv \tilde{z}_n \pmod{p^n}$ для всех $m, n \in \mathbb{N}$, $m > n$, что означает фундаментальность последовательности $(\tilde{z}_n)_{n=1}^{\infty}$.

Фундаментальность последовательности $(\tilde{z}_n)_{n=1}^{\infty}$ означает, что, поскольку $\mathbb{Z}_p$ полно относительно p-адической метрики, то существует $\tilde{z} \in \mathbb{Z}_p$ такое, что $\tilde{z} \bmod p^n = \tilde{z}_n$ для всех $n \in \mathbb{N}$. Но тогда $g(\tilde{z}) \bmod p^n =$

[2]Отметим, что здесь мы используем тот факт, что функция совместима тогда и только тогда, когда она каждый p-адический шар отображает в p-адический шар

$g(\tilde{z}_n) \bmod p^n = z_n$.[3] Стало быть, последовательность $(g(\tilde{z}) \bmod p^n)_{n=1}^{\infty}$ сходится p-адически к z. Но это означает, что $g(\tilde{z}) = z$. □

Лемма 2.19. *В условиях теоремы 2.16, функция f является биективной на $\mathbb{Z}_p$ тогда и только тогда, когда одновременно выполняются два условия:*

(1) *функция f биективна по модулю $p^{N_1(f)}$* (см. определение 2.11), *и*
(2) *производная f' функции f не обращается в 0 по модулю p нигде на $\mathbb{Z}_p$.*

Доказательство леммы 2.19. Докажем по индукции, что при выполнении условий (1)–(2) функция $f \bmod p^n$ биективна для всех $n \geqslant N_1(f)$. Основание индукции — условие (1). Предположим, что функция $f \bmod p^n$ биективна на $\mathbb{Z}/p^n\mathbb{Z}$ и докажем, что функция $f \bmod p^{n+1}$ биективна на $\mathbb{Z}/p^{n+1}\mathbb{Z}$.

Предположим, что найдутся $x, y \in \{0, 1, \ldots, p^{n+1}-1\}$ такие, что $f(x) \equiv f(y) \pmod{p}^{n+1}$. Тогда тем более $f(x) \equiv f(y) \pmod{p}^n$, а стало быть, $x \equiv y \pmod{p^n}$ по предположению индукции. Следовательно, $y = x + p^n t$ для подходящего целого t. Но тогда в виду сравнения (2.11.2) получаем, что

$$f(y) = f(x + p^n t) \equiv f(x) + p^n t \cdot f'(x) \pmod{p^{n+1}},$$

откуда следует, что $0 \equiv t \cdot f'(x) \pmod{p}$. Однако поскольку $f'(x) \not\equiv 0 \pmod{p}$ по условию (2), то необходимо чтобы $t \equiv 0 \pmod{p}$. Однако это означает, что $y = x + p^n t \equiv x \pmod{p^{n+1}}$, т.е. что $x = y$, поскольку $x, y \in \{0, 1, \ldots, p^{n+1} - 1\}$. Но это и означает, что f биективна по модулю p^{n+1}.

Итак, мы доказали, что при выполнении условий (1)–(2) функция f биективна по модулю p^n для всех $n \geqslant N_1(f)$. Но тогда по лемме 2.17 она биективна по модулю p^n для всех $n \in \mathbb{N}$, а значит, биективна на $\mathbb{Z}_p$ по лемме 2.18.

Обратно, если функция f биективна на $\mathbb{Z}_p$, то по лемме 2.18 биективна по модулю p^n для всех $n \in \mathbb{N}$. Значит, она биективна и по модулю $p^{N_1(f)}$, что доказывает необходимость условия (1). Для доказательства необходимости условия (2) заметим, что если бы $f'(a) \equiv 0 \pmod{p}$ для некоторого $a \in \mathbb{Z}_p$, то тогда

$$f(a + p^n t) \equiv f(a) + p^n t \cdot f'(a) \equiv f(a) \pmod{p^{n+1}} \tag{2.19.1}$$

для всех $n \geqslant N_1(f)$ и всех $t \in \mathbb{Z}_p$, см. (2.11.2). Пусть $a = \sum_{i=0}^{\infty} \alpha_i p^i$ — каноническое представление $a \in \mathbb{Z}_p$, т.е. $\alpha_j \in \{0, 1, \ldots, p-1\}$ для всех $j = 0, 1, 2, \ldots$. Зафиксируем $n \geqslant N_1(f)$ и возьмем $b \in \mathbb{Z}_p$, имеющее каноническое представление $b = \sum_{i=0}^{\infty} \beta_i p^i$, где $\beta_j = \alpha_j$ для $j = 0, 1, \ldots, n-1$ и $\beta_n \neq \alpha_n$. Тогда $\bar{a} = a \bmod p^{n+1} \neq b \bmod p^{n+1} = \bar{b}$, но из (2.19.1) при $t = \beta_n - \alpha_n$ следует, что $f(\bar{b}) \equiv f(\bar{a}) \pmod{p^{n+1}}$. Это противоречит биективности функции f по модулю p^{n+1}. □

Теперь все готово для доказательства теоремы 2.16:

[3] Здесь мы использовали тот факт, что поскольку g совместима, значение $g(r) \bmod p^n$ не зависит от выбора представителя r в смежном классе $r + p^n\mathbb{Z}_p$!

Доказательство теоремы 2.16. Необходимость условий уже доказана леммой 2.18. Докажем достаточность. Заметим вначале, что в при доказательстве необходимости условия (2) леммы 2.19 мы, фактически, доказали следующее: если производная функции f обращается в 0 по модулю p в какой-то точке, то функция f не может быть биективной ни по какому модулю p^{n+1} для $n \geqslant N_1(f)$. В силу этого, если функция f биективна по модулю p^m для какого-то $m \geqslant N_1(f)+1$, то ее производная не обращается в 0 по модулю p ни в одной точке из $\mathbb{Z}_p$. Но по лемме 2.17, если функция f биективна по модулю p^m для какого-то $m \geqslant N_1(f)+1$, то она биективна и по модулю $p^{N_1(f)+1}$, и по модулю $p^{N_1(f)}$, а значит, в силу сказанного, ее производная не обращается в 0 по модулю p ни в одной точке. Стало быть, по лемме 2.19 функция f биективна на $\mathbb{Z}_p$. □

Следствие 2.20. *Многочлен с коэффициентами из $\mathbb{Z}_p$ биективен на $\mathbb{Z}_p$ тогда и только тогда, когда он биективен по модулю p^2.*

Доказательство. Действительно, как было показано в примере 2.13, $N_1(f) = 1$ если f — полином над $\mathbb{Z}_p$. □

Теорема 2.21. *Если детерминированная функция некоторого автомата* (входной и выходной алфавиты которого состоят из p символов) *равномерно дифференцируема, то этот автомат обратим тогда и только тогда, когда он обратим на множестве всех слов некоторой (достаточно большой) конечной длины.*

Доказательство. Необходимость немедленно следует из определения обратимости автомата. Докажем достаточность.

Поскольку детерминированная функция $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ равномерно дифференцируема на $\mathbb{Z}_p$, то по теореме 2.16 она биективна тогда и только тогда, когда она биективна по модулю p^m для какого-нибудь $m \geqslant N_1(f)$. Последнее условие эквивалентно обратимости автомата на множестве всех слов длины m. Значит, если автомат обратим на множестве всех слова длины $m \geqslant N_1(f)$, то задаваемая им детерминированная функция биективна на $\mathbb{Z}_p$, и, стало быть, для нее существует обратная функция $f^{-1}\colon \mathbb{Z}_p \to \mathbb{Z}_p$. Теперь для завершения доказательства достаточно показать, что функция f^{-1} также совместима: тогда по теореме 2.8 ей соответствует некоторый автомат, который, очевидно, является обратным к данному автомату.

Докажем, что f^{-1} совместима. Допустим, что нашлись $a, b \in \mathbb{Z}_p$ такие, что $a \equiv b \pmod{p^k}$ и $f^{-1}(a) \not\equiv f^{-1}(b) \pmod{p^k}$; тогда $a = f(u)$, $b = f(v)$ для единственным образом определенных $u, v \in \mathbb{Z}_p$. Имеем $f(u) \equiv f(v) \pmod{p^k}$ и $f^{-1}(f(u)) \not\equiv f^{-1}(f(v)) \pmod{p^k}$; т.е., $f(u) \equiv f(v) \pmod{p^k}$ и $u \not\equiv v \pmod{p^k}$. Ввиду леммы 2.18, последние два сравнения противоречат биективности функции f на $\mathbb{Z}_p$. □

Список литературы

[1] С. Б. Каток. *p-адический анализ в сравнении с вещественным*. МЦНМО, Москва, 2004. 9

[2] Н. Коблиц. *p-адические числа, p-адический анализ и дзета-функции*. Мир, Москва, 1982. 9

[3] А. Ю. Хренников. *Неархимедов анализ и его приложения*. Физматлит, Москва, 2003. 9