УДК 621.391

И. Д. ГОРБЕНКО, д-р техн. наук, *В. И. БАРСОВ*,
Р. П. ЛЫСАК

УЛУЧШЕННЫЙ АЛГОРИТМ ПРЕДСТАВЛЕНИЯ ЦЕЛЫХ ЧИСЕЛ В p-АДИЧЕСКОМ КОДЕ

В работе [1] рассмотрены теоретические основы преобразований, подобных теоретико-числовым, в конечно-сегментированном p-адическом поле Q_p и предложено использовать p-адическую арифметику в цифровой обработке сигналов (ЦОС), в частности для описания матричного процессора. Известно, что решение матричных задач связано с необходимостью выполнения различных вычислений, повышением скорости решения задач и обеспечением требуемых точностей вычислений.

Перспективным направлением достижения указанной цели, на наш взгляд, является реализация матричных вычислений в поле p-адических преобразований, что позволит уменьшить вычислительную сложность решения матричных задач и вычисления цифровой свертки. В свою очередь, необходима оптимизация и самих p-адических преобразований, одним из этапов которой является упрощение алгоритмов прямого и обратного представления целых чисел p-адическим кодом, называемым кодом Хенселя.

Фактически вычисление значений p-адических цифр кода Хенселя a_i для любого нулевого рационального числа α может быть сделано последовательными операциями по простому модулю p, так в работе [2] описывается метод, разработанный Башманом, алгоритм которого состоит в следующем.

Шаг 1. $\beta=\alpha$. Определяем значение n, такое, чтобы α можно было представить в виде $\alpha=(a/b)p^n$.

Если $n\geqslant 0$, то $a_0, a_1, \ldots, a_{n-1}:=0$.

Делаем переход к шагу 3.

Шаг 2. Определяем значение n, такое, что $\beta=(a/b)p^n$.

Шаг 3. Решается сравнение $b\cdot x\equiv 1 \pmod p$, если x_n — решение, то $a_n=a\cdot x \pmod p$.

Шаг 4. $\gamma:=\beta-a_np^n$, если $\gamma=0$, то $a_i:=0$ для $i>n$ и следует переход к шагу 5. Если $\gamma\neq 0$, то $\beta:=\gamma$ и следует переход к шагу 2.

Шаг 5. Поставить p-адическую точку между a_{-1} и a_0 членами бесконечного ряда $\alpha=\sum_{n}^{\infty} a_i p^i$, где $0\leqslant a_i<p$, который сходится к рациональному числу α по p-адической норме.

Пример 1. $\alpha=\frac{1}{15}$, $p=5$, $r=5$ — длина кода Хенселя.

Шаг 1. $\beta:=\frac{1}{15}$ и определяем n, преобразуя α к виду $\alpha=\left(\frac{1}{3}\right)\cdot 5^{-1}$.

Шаг 3. $3\cdot x\equiv 1 \pmod 5$, $\Rightarrow x=2$, $a_n=a_{-1}=1\cdot 2 \pmod 5=2$.

Шаг 4. $\gamma:=\frac{1}{15}-2\cdot 5^{-1}=\left(-\frac{1}{3}\right)\cdot 5^0>0$, $\Rightarrow \beta:=\gamma$ и переход к шагу 2.

Шаг 2. $\beta:=\left(-\frac{1}{3}\right)\cdot 5^0$, $\Rightarrow n=0$,

Шаг 3. $3\cdot x\equiv 1 \pmod 5$, $\Rightarrow x=2$, $a_n=a_0=(-1)\cdot 2 \pmod 5=$ $=-2+5=3$.

Шаг. 4. $\gamma:=\left(-\frac{1}{3}\right)\cdot 5^0-3\cdot 5^0=\left(-\frac{2}{3}\right)\cdot 5^1>0$, $\Rightarrow \beta:=\gamma$ и переход к шагу 2.

Шаг 2. $\beta:=\left(-\frac{2}{3}\right)\cdot 5^1$, $\Rightarrow n=1$.

Шаг 3. $3\cdot x\equiv 1 \pmod 5$, $\Rightarrow x=2$, $a_n=a_1=(-2)\cdot 2 \pmod 5=1$

Шаг 4. $\gamma:=\left(-\frac{2}{3}\right)\cdot 5^0-1\cdot 5^0=\left(-\frac{1}{3}\right)\cdot 5^2>0$, $\Rightarrow \beta:=\gamma$ и переход к шагу 2.

Вычисления продолжаем до получения r p-адических цифр.

Шаг 5. Ставим p-адическую точку между a_{-1} и a_0 членами p-адического ряда 2.313...

Пример 2. $\alpha=17$, $p=7$, $r=3$.

Шаг 1. $\beta:=17$ и определяем n, преобразуя α к виду $\alpha=(17)\cdot 7^0$, $=>n=0$, переход к шагу 3.

Шаг. 3. $1\cdot x\equiv 1 \pmod 7$, $\Rightarrow x=1$, $a_n=a_0=17\cdot 1 \pmod 7=3$.

Шаг 4. $\gamma:=17-3\cdot 7^0=14>0\Rightarrow \beta:=\gamma$ и переход к шагу 2.

Шаг 2. $\beta:=(2)\cdot 7^1$, $\Rightarrow n=1$.

Шаг 3. $x=1$, $a_n=a_1=2$.

Шаг 4. $\gamma = 14 - 2 \cdot 7^1 = 0$, $\Rightarrow$ переход к шагу 5.

Шаг 5. Ставим p-адическую точку: 0.32.

Проведенные расчеты и анализ алгоритма Башмана позволили сделать выводы о его оптимальности для представления p-адическим кодом рациональных чисел и громоздкости для целых чисел. Кроме того, этот алгоритм сложен для восприятия и трудно программно реализуется на ЭВМ.

В настоящее время в связи с широким использованием в ЦОС абстрактных алгебраических систем большой интерес представляют вычисления в конечных полях и кольцах целых чисел. В связи с этим ниже предлагается модификация алгоритма Башмана для представления целых чисел в p-адическом коде. Этот алгоритм характеризуется меньшей вычислительной сложностью, в частности содержит меньшее количество операций умножения и приведения по модулю p, легко реализуется программно и прост для восприятия.

Пусть даны значения α, p и r. Тогда существует алгоритм p-адического преобразования вида.

Шаг 1. Если $p > \alpha$, то $a_0 = \alpha$ и переход к шагу 4, в противном случае — к шагу 2.

Шаг 2. Определяем значение $a_n = \alpha / p^n \pmod p$, где $n = \overline{0, r}$.

Шаг 3. $\gamma := \alpha - a_n \cdot p^n$.

Если $\gamma = 0$, то переход к шагу 4, в противном случае $\alpha := \gamma$ и переход к шагу 2.

Шаг 4. $a_i := 0$ для $n < i \leqslant r$. Строим p-адический код для значений $\alpha = \sum_{i=0}^{r} a_i p^i$, где $0 \leqslant a_i < p$.

Пример 3. $\alpha = 17$, $p = 7$, $r = 3$.

Шаг 1. $p < \alpha$, то переход к шагу 2.

Шаг 2. $a_n = a_0 = 17/7^0 \pmod 7 = 3$.

Шаг 3. $\gamma := 17 - 3 \cdot 7^0 = 14 > 0 \Rightarrow \alpha := 14$, переход к шагу 2.

Шаг 2. $a_n = a_1 = 14/7^1 \pmod 7 = 2$.

Шаг 3. $\gamma: 14 - 2 \cdot 7^1 = 0$, $\Rightarrow$, переход к шагу 4.

Шаг 4. Строим p-адический код 320.

Сравнительный анализ показал, что затраты на вычисление каждой из n p-адических цифр кода Хенселя при использовании улучшенного алгоритма уменьшаются на пять операций. При использовании улучшенного алгоритма количество умножений составляет 1, а алгоритма Башмана — 4. Количество вычитаний по mod$p$ составляет 1 и 2 соответственно, а вычитаний-сравнений — 0 и 1.

Суммарный выигрыш V при вычислении n p-адических цифр составляет $V = 5n$.

В таблице приведены результаты вычисления кодов Хенселя для различных значений α и p с использованием улучшенного ал-

Значения	Алгоритм	Количество							Выигрыш УА по сравнению с АБ, операций
		умножений	возведений в степень	делений	вычитаний по mod	операций присвоения	выполнения логических условий	вычитаний-сравнений	
$a=17$	УА	2	2	2	2	5	3	0	10
$p=7$	АБ	8	2	2	4	6	2	2	
$a=301$	УА	4	4	4	4	11	5	0	20
$p=5$	АБ	16	4	4	8	12	4	4	
$a=200$	УА	3	3	3	3	8	4	0	15
$p=13$	АБ	12	3	3	6	9	3	3	

горитма и алгоритма Башмана. В примечании указан выигрыш УА по сравнению с АБ в количестве операций.

Обратное восстановление целого числа a из его кода Хенселя можно выполнить вычислением выражения для p-адического разложения

$$a = \sum_{i=0}^{r} a_i p^i. \qquad (1)$$

Пример 4. Для значения кода Хенселя 320 по модулю 7, используя выражение (1), вычисляем

$$a = 3 \cdot 7^0 + 2 \cdot 7^1 + 0 \cdot 7^2 = 17,$$

что совпадает с расчетами, приведенными в примере 3.

Среди известных методов обращения кода Хенселя в рациональное число, прежде всего метода просмотра таблиц [3], метода приближения рациональностями Фарея [4], метода расширенного алгоритма Евклида [5], минимальную вычислительную сложность имеет алгоритм обращения p-адического кода в целое число.

Поэтому использование алгоритма p-адического преобразования над конечными полями и кольцами позволит уменьшить объем вычислений на этапах прямого и обратного вычислений кода Хенселя, а следовательно, уменьшить объем вычислений при решении матричных задач и вычислений свертки.

Список литературы: 1. *Nasrabadi N. M., King R. A.* The fast digital convolution using p-adic transforms//Electron. lett. 1983. N 1. P. 111—113. 2. *Bachmann G.* Introduction to p-adic numbers and valuation theory. New York, 1964. 200 p. 3. *Manadeva Rao T.* Conversion of hensel codes to rational numbers//Computers & matematics. 1984. N 2. P. 200—225. 4. *Krishnamurhy E. D.* On the conversion of hensel sodes to farey rationals//IEEE trans, on computers. 1983. N 4. P. 130—150. 5. *Miola A.* Algebraic approach to p-adic conversion of rational numbers//Information processing letters. 1984. N 3. P. 180—200.

Поступила в редколлегию 27.07.89