УДК 621.391.26

Я.Е. ВИЗОР

ОДИН ИЗ МЕТОДОВ ВЫЧИСЛЕНИЯ ПЕРВООБРАЗНЫХ КОРНЕЙ В ОСТАТОЧНЫХ КЛАССАХ

Abstract: *With the purpose of constructing optimal on speed and the equipment of arithmetic devices of computer facilities, the analysis of two number systems, item and number systems in residual classes is carried out(spent). The method of an evaluation of primitive roots for the units represented as the sum of geometrical progression is offered, permitting without superfluous temporary expenditures to calculate not only primitive roots, but also numbers from the carried out(spent) system of residues with orders of dividers* $\varphi(p)$.

Key words: *primitive roots, system of residual classes, residue system.*

Анотація: *З метою побудови оптимальних по швидкодії та обладнанню арифметичних пристроїв обчислювальної техніки проведено аналіз двох систем числення: позиційної і системи числення в залишкових класах. Запропоновано метод обчислення первісних коренів для модулів, представлених у вигляді суми геометричної прогресії, який дозволяє без зайвих, часових витрат обчислювати не тільки первісні корені, але й числа з проведеної системи лишків даного модуля з порядками дільників* $\varphi(p)$.

Ключові слова: *первісні корні, система залишкових класів, приведення, система лишку.*

Аннотация: *С целью построения оптимальных по быстродействию и оборудованию арифметических устройств вычислительной техники проведен анализ двух систем счисления: позиционной и системы счисления в остаточных классах. Предложен метод вычисления первообразных корней для модулей, представленных в виде суммы геометрической прогрессии, позволяющий без лишних временных затрат вычислять не только первообразные корни, но и числа из проведённой системы вычетов с порядками делителей* $\varphi(p)$.

Ключевые слова: *первообразные корни, система остаточных классов, приведения, система вычетов.*

1. Введение

Изучение любых алгебр, в том числе и машинной, сводится не только к изучению набора операций и множеств, на которых они заданы, но и представлению этих алгебр, заключающихся в отображении одной алгебры в другую. Такое отображение, если оно сохраняет операции, т.е. имеет место морфизм, называется представлением [1−8]. Для машинной алгебры одним из таких представлений являются системы счисления.

Главные требования к любой предназначенной для практического применения системы следующие:

− возможность представления в данной системе любой величины в рассматриваемом, заранее назначенном диапазоне;

− возможность представления – любая кодовая комбинация соответствует одному и только одному числу в заданном диапазоне;

− простота оперирования с числами в данной системе счисления.

Диапазон, т.е. количество различных чисел, которые могут быть представлены в данной кодовой системе, очевидно, определяется количеством различных возможностей кодовых комбинаций.

Поскольку позиционная система счисления достаточно хорошо изучена, отметим лишь только её основной недостаток – наличие межразрядных связей, которые накладывают свой отпечаток на способы реализации арифметических операций, усложняют аппаратуру и ограничивают быстродействие. Поэтому как альтернатива возникли методы вычислений на основе

непозиционных систем счисления, в частности, на основе системы счисления в остаточных классах.

В системе остаточных классов, восходящей своими идейными корнями к классическим трудам Эйлера, Гаусса, Чебышева по теории сравнений, числа представляются своими остатками от деления на выбранную систему оснований. Все рациональные операции могут выполняться параллельно над цифрами каждого разряда в отдельности.

Охарактеризуем в общих чертах достоинства и недостатки системы счисления в остаточных классах.

К достоинствам следует отнести:

− независимость образования чисел, в силу чего каждый разряд несет информацию обо всем исходном числе, а не о промежуточном числе, получающемся в результате образования младших разрядов (как это имеет место в позиционной системе). Отсюда вытекает независимость разрядов числа друг от друга и возможность их независимой параллельной обработки;

− малоразрядность остатков, представляющих число. Ввиду малого количества вложенных кодовых комбинаций открывается возможность построения табличной арифметики, благодаря чему большинство операций, выполняемых арифметическими устройствами, превращается в однотактные, выполняемые простой выборкой из таблицы.

К основным недостаткам системы счисления в остаточных классах следует отнести:

− невозможность визуального сопоставления чисел, так как внешняя запись чисел не дает представления о его величине;

− отсутствие простых признаков выхода результатов операций за пределы диапазона;

− ограниченность действия системы сферой целых положительных чисел;

− получение во всех случаях точного результата операции, что исключает возможность непосредственного приближенного выполнения операций, округления результата и т.п;

− трудоемкое вычисление первообразных корней, что ведет к определенным трудностям при создании таблиц индексов и антииндексов [9].

В настоящее время система счисления в остаточных классах не нашла широкого распространения в современной вычислительной технике в силу своих недостатков, но способ представления чисел и методы выполнения арифметических операций позволит в дальнейшем уменьшить влияние основного недостатка позиционной системы счисления на быстродействие вычислительной системы в целом.

2. Постановка задачи

Для получения быстрых методов выполнения арифметических операций необходимо, с учётом выбранной машинной алгебры, проанализировать реализацию этих методов в системе счисления остаточных классов. В этой системе счисления некоторые арифметические операции, например, операцию умножения, можно выполнять над двоичными малоразрядными остатками чисел по определенному простому модулю, но для этого требуются определенные затраты (времени, оборудования) на вычисление этих же остатков и модуля их произведения. В теории индексов эта же операция умножения представлена как сумма индексов множителей по инкрементированному

простому модулю. В этом методе используются простые модули, которые имеют первообразные корни, о трудоемкости, вычисление которых было отмечено выше.

3. Методы вычисления первообразных корней

Отметим некоторые известные теоремы, касающиеся порядка числа, которые необходимы для дальнейших исследований.

Пусть a – число взаимно простое с m. Порядком (показателем) числа a по модулю m называется наименьшее целое положительное число d, такое, что $a^d \equiv 1(\mathrm{mod}\, m)$. Если $b \equiv 1(\mod m)$ и если $b \equiv a(\mathrm{mod}\, m)$, то b имеет тот же порядок по модулю m, что и a. Таким образом, все элементы класса вычетов $a \bmod m$ имеют порядок d; число d называется порядком класса вычетов $a \bmod m$ и обозначается через $G(a \bmod m)$.

Теорема 1. Пусть a, b – числа взаимно простые с m. Если числа $G(a \bmod m)$ и $G(b \bmod m)$ взаимно простые, то

$$G(ab \bmod m) = G(a \bmod m) G(b \bmod m).$$

Теорема 2. Если $G(a \bmod \cdot\, m) = n$ и $(k, n) = d$, то $G(a^k \bmod m) = n/d$. Отсюда, если $d = 1$, то $G(a^k \bmod m) = n.$

Для мультипликативной группы вычетов по простому модулю необходимо изучить числа, имеющие наибольший порядок по этому модулю.

В теории сравнений доказано, что если p – простое число и d – натуральный делитель числа $p-1$, то в приведенной системе вычетов по модулю p существует точно $\varphi(d)$ чисел, имеющих порядок d. Функция $\varphi(n))$ называется функцией Эйлера. Она обозначает число положительных целых чисел, не превосходящих n и взаимно простых с n, причем эта числовая функция определена на множестве всех целых положительных чисел. Отсюда, если вычет a по модулю m имеет порядок $\varphi(m))$, то a называется первообразным корнем по модулю m. Тогда, анализируя вышесказанное, заключаем, что число первообразных корней по модулю m равно $\varphi(m-1)$.

Далеко не всякое число p имеет первообразный корень. Точно так же нет каких-либо формул (за исключением некоторых p специального вида, представлены в работах П.Л.Чебышева), которые выражали бы величину первообразного корня в случае, когда он существует в зависимости от p. Нахождение первообразного корня проводится в подавляющем большинстве случаев простым перебором чисел, входящих в приведенную систему вычетов по некоторому модулю, что требует больших временных затрат особенно для больших модулей.

К более эффективному алгоритму определения первообразных корней, чем испытание всех возможных оснований, может привести известная теорема [10, 11].

Теорема 3. Пусть $\pi_1, \pi_2, ...\pi_r$ – простые делители числа $p-1$. Тогда необходимым и достаточным условием того, что g есть первообразный корень простого числа p, является невыполненное ни одно из сравнений:

$$g^{\frac{p-1}{\pi_1}} \equiv 1(\mathrm{mod}\, p), g^{\frac{p-1}{\pi_2}} \equiv 1(\mathrm{mod}\, p), g^{\frac{p-1}{\pi_{3r}}} \equiv 1(\mathrm{mod}\, p). \quad (1)$$

Из этой теоремы вытекает, что для вычисления первообразных корней надо испытывать основание только на невыполнение условий (1).

Этот метод также малоэффективен особенно для больших модулей, когда приходится проверять на невыполнение условий (1) большое количество чисел из проведенной системы вычетов по данному модулю, и, кроме того, количество таких проверок возрастает в r раз, (где r – количество делителей $p-1$), так как общее количество проверок определяется как $(p-1)\cdot r$.

4. Вычисление первообразных корней модуля $p = \sum_{L=1}^{N-1} A^j$

Некоторые простые числа p можно представить суммой членов геометрической прогрессии:

$$A_j = A_0 g^j, \quad j \in \{ 0,1,... \}.$$

Если $A_0 = 1$, то $A_j = g^j$, а сумма S_N равна

$$S_N = \sum_{l=0}^{N-1} A_l = \frac{g^N - 1}{g - 1},$$

где g – знаменатель прогрессии.

Далее, если $g = A$, то $S_N = \frac{A^N - 1}{A - 1}$.

Рассмотрим вычисление первообразных корней в случае, если $p = S_N$. Запишем уравнение для простого p:

$$p = A^0 + A^1 + A^2 + ... + A^{N-1} = \frac{A^N - 1}{A - 1}, \quad (2)$$

где $A^j (j = 0,1...N)$ – член геометрической прогрессии, A – знаменатель прогрессии. Имеет место сравнение

$$p \equiv 0(\mathrm{mod}\, p).$$

Подставив значение p из (2), получим

$$\frac{A^N - 1}{A - 1} \equiv 0(\mathrm{mod}\, p)$$

или, с учётом свойств сравнений

$$A^N - 1 \equiv 0(\mathrm{mod}\, p).$$

Отсюда

$$A^N \equiv 1(\mathrm{mod}\, p). \quad (3)$$

Теорема 4. Пусть $p = A^0 + A^1 ... A^{N-1}$ – простое число, A – знаменатель геометрической прогрессии, тогда N – число членов геометрической прогрессии, удовлетворяющее сравнению $A^N \equiv 1(\mathrm{mod}\, p)$, является порядком числа A по модулю p.

Доказательство. Известно, что порядки, которым числа принадлежат по модулю p, суть делители $\varphi(p)$. По условию p – простое число, то $\varphi = (p) + p - 1$. Покажем, что N делит $p-1$. Допустим, что число A имеет порядок d, тогда N делится на d согласно [12] или

$$N = kd. \tag{4}$$

Запишем систему сравнений:

$$\begin{cases} A^N \equiv 1(\mathrm{mod}\, p) \\ A^{p-1} \equiv 1(\mathrm{mod}\, p) \end{cases}.$$

Отсюда

$$A^{p-1} \equiv A^N (\mathrm{mod}\, p). \tag{5}$$

Сравнение (5) имеет место тогда и только тогда, когда

$$p - 1 \equiv N(\mathrm{mod}\, d). \tag{6}$$

Переходя к уравнению, получим

$$(p-1) - N = md.$$

Поставив вместо d его значение N/k, получим следующее уравнение:

$$(p-1) - N = \frac{m \cdot N}{k}.$$

Тогда

$$\frac{k(p-1)}{N} = m + k. \tag{7}$$

Из (7) видно, что, поскольку $N > k$, нацело на N должен делиться только множитель $p-1$. Отсюда делаем вывод, что N является делителем числа $p-1$. Далее, поскольку d – порядок числа A, то оно может принимать любое из значений $d = 0,1,2,...N-1$, при этом должно иметь место сравнение

$$A^d \equiv 1(\mathrm{mod}\, p). \tag{8}$$

Но любое число A^d является элементом суммы (2), которая равна p. Поскольку в нашем случае $A^d < p$, то и $A^d - 1 < p$. Отсюда делаем вывод, что сравнение (8) может существовать при $d = N$, т.е. число N является порядком числа A по модулю p.

Рассмотрим случай, когда $N = 3$. Тогда формулу (2) можно переписать в виде

$$A^0 + A^1 + A^2 = p, \tag{9}$$

Или, поскольку $A^0 = 1$, то

$$A(A+1) = p - 1. \tag{10}$$

Иначе говоря, в данном случае мы будем иметь дело с такими знаменателями A геометрической прогрессии, которые при умножении на стоящее рядом в натуральном ряду число $A+1$ даст $\varphi(p))$ или $p-1$. Формула (9) представляет собой квадратное уравнение, корнями которого будут положительные A:

$$A=\frac{-1+\sqrt{4p-3}}{2}.$$

Сделав замену $d^2=4p-3$, получим

$$A=\frac{d-1}{2}; \tag{11}$$

$$p=\frac{d^2+3}{4}. \tag{12}$$

Из формул (11) и (12) видно, что d – нечетное простое число и больше 3, т.е. $d=5,7...$, так как необходимо, чтобы получаемое p из (12) было простым числом. Например, если принять $d=11$, то получим $A=5$, $p=31$, что удовлетворяет уравнению (10).

Подставляя значение $d_i(i=1,2.3.4....)$ в формулы (11), (12), можно получить бесконечную систему уравнений:

$$\begin{cases} A_1(A_1+1)=p_1-1; \\ A_2(A_2+1)=p_2-1; \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ A_i(A_i+1)=p_i-1. \end{cases} \tag{13}$$

Анализ системы уравнения (13) и сравнения (3) показывает, что знаменатель геометрической прогрессии A_{i-1} и $p_{i-1}-1$ является первообразными корнями модуля p_i, т.е. эти числа имеют порядок p_i-1. Для примера подставим четыре значения d_i в формулы (11) и (12) и запишем систему сравнений:

$$\begin{cases} 2^3\equiv 1 \pmod 7 \\ 3^3\equiv 1 \pmod{13} \\ 5^3\equiv 1 \pmod{31} \\ 6^3\equiv 1 \pmod{43} \end{cases}.$$

Числа $A_1=2$ и $p_1-1=6$ из первого сравнения будут первообразными корнями модуля $p_2=13$, числа $A_2=2$ и $p_2-1=12$ – модуля $p_3=31$ и т. д.

Основным достоинством предложенного метода вычисления первообразных корней является то, что вычисления производятся без проверок оснований из проведенной системы вычетов для заданного p, что является более эффективным с точки зрения временных затрат. Кроме того, предложенный метод позволяет, на основании выведенной теоремы 4 и известных

теорем 1 и 2, вычислять числа из проведенной системы вычетов, имеющих порядки делителей числа $p-1$, а также их количество. Например, пусть $p=13$. Число p можно записать в виде

$$p=(p-1)^0+(p-1)^1=\frac{(p-1)^2-1}{(p-1)-1}.$$

Отсюда число $p-1=12$ на основании теоремы 4 имеет порядок 2. Кроме того, для данного p существует (2) $A=3$, имеющее порядок 3. С учетом теоремы 1, остаток от $\frac{(p-1)\cdot a}{p}$ есть число 10, имеющее порядок 6. Вычислив, все первообразные корни, получим четыре числа с порядком $p-1=12$. Число с порядком 4 вычисляем на основании предложения 5,7 из [12], т.е. остаток от $\frac{x_m^3}{p}=\frac{6^3}{13}$ есть число 8, имеющее порядок 4. Число $p-1=12$ имеет 6 натуральных делителей: 1,2,3,4,6,12. Количество чисел с соответствующими порядками определяем на основании теоремы 5,9 [12]:

$$\varphi(1)=1;\ \varphi(2)=1;\ \varphi(3)=2;\ \varphi(4)=2;\ \varphi(6)=2;\ \varphi(12)=4.$$

Вычисляем по одному представителю приведенной системы вычетов модуля $p=13$ с порядками делителей $p-1$, остальные числа, имеющие такие же порядки, вычисляем на основании теоремы 2. В итоге получаем следующий результат: числа 2,6,7,11 имеют порядок 12 (первообразные корни); число 12 – порядок 2; число 3 – порядок 3; числа 5, 8 – порядок 4, число 1 – порядок 1.

Таким образом получен новый метод для вычисления первообразных корней (для $p=\sum_{i=1}^{N-1}A^i$), позволяющий без лишних временных затрат вычислять не только первообразные корни, но и числа из проведённой системы вычетов с порядками делителей $\varphi(p)$.

5. Применение индексов для выполнения арифметических операций

Вычисление первообразных корней являлось основой для использования теории индексов в арифметических операциях.

Из теории индексов известно, что если g – первообразный корень p, то сравнение

$$g^x\equiv(\mathrm{mod}\ p),$$

где A, не кратное p, имеет одно и только одно решение, которое называется индексом I числа A и обозначается $I=indA$. Первообразный корень g называется основанием индекса.

Известно, что если $A_1,A_2,...,A_k$ суть целые положительные числа, индексы которых по модулю p при первообразном корне g соответственно равны $i_1,i_2,...,i_k$, и если через I обозначен индекс произведения этих чисел $A_1,A_2,...,A_k$ по модулю p при том же первообразном корне, то индекс произведения равен сумме индексов сомножителей, взятой по модулю $p-1$, т.е.

$$I = \sum_{j-1}^{k} i_j (\mathrm{mod}\, p-1). \qquad (14)$$

Соотношение (14) применяется и для выполнения деления по модулю. Под делением по модулю $\frac{a}{b}(\mathrm{mod}\, p)$ понимается частное $\frac{a+kp}{b}$, где k – наименьшее из возможных чисел, превращающих $a+rp$ в число, кратное b. В данном случае, если $\frac{a}{b}(\mathrm{mod}\, p) = c$, то

$$(\mathrm{ind\ a} - \mathrm{ind\ b}) \bmod (\mathrm{p}-1) = \mathrm{ind\ c}.$$

Эта особенность индексов роднит их с логарифмами и позволяет заменять умножение и деление чисел соответственно сложением и вычитанием их индексов с последующим переходом от произведения и деление индексов к самому произведению и делению. Для перехода от индексов к фактическому числу применяются антииндексы. Антииндексом числа I называется число A такое, что

$$I = inda \text{ или } a = ind^{-1} I. \qquad (15)$$

Если антииндекс обозначить через $N(I)$, то из (15) следует

$$N(inda) = a. \qquad (16)$$

Для того чтобы иметь возможность использовать для целей умножение соотношение (14), надо вычислить антииндексы чисел. Поскольку имеется таблица вычисленных индексов чисел, то соответствующим обращением этой таблицы можно получить все значения *a* из выражения (16).

6. Выводы

В работе предложен метод вычисления первообразных корней для модулей, представленных в виде суммы геометрической прогрессии, которые являются основой для использования теории индексов в арифметических операциях. Данный метод позволяет без лишних временных затрат вычислять не только первообразные корни, но и числа из проведённой системы вычетов с порядками делителей $\varphi(p)$.

В системе остаточных классов предполагается применять индексы для получения цифр произведения чисел по каждому из оснований в отдельности. Теория индексов может быть применена и для сложных модулей, а формула (14), при надлежащем выборе сложного модуля, обеспечивающего наличие первообразного корня, может иметь место для перемножаемых чисел в целом. Однако для сформулированной цели достаточно рассматривать индексы отдельно по модулям – основанием выбранной системы. В этом случае не трудно выбрать эти основания такими, чтобы для них можно было вычислить первообразные корни и, следовательно, могли бы быть построены таблицы индексов. Для любого простого модуля первообразный корень всегда существует и поэтому, если в качестве оснований системы использовать простые числа (что совпадает с условием при выборе машинной алгебры), то удовлетворяются как основное требование однозначности представления чисел – взаимная простота оснований системы, так и условие существования первообразный корней. Следовательно, имеется возможность построения

соответствующих таблиц индексов, что позволит увеличить быстродействие арифметического блока.

СПИСОК ЛИТЕРАТУРЫ

1. Ленг С. Алгебра. – М.: Мир, 1968. – 564 с.
2. Калужнин Л.А. Введение в общую алгебру. – М.: Наука, 1973. – 239 с.
3. Фрид Э. Элементарное введение в абстрактную алгебру. – М.: Мир, 1972. – 260 с.
4. Курош А.Г. Курс высшей алгебры. – М.: Наука, 1976. – 431 с.
5. Воеводин В.В. Линейная алгебра. – М.: Наука, 1980. – 400 с.
6. Кострикин А.И. Введение в алгебру. – М.: Наука, 1979. – 495 с.
7. Ван Дер Варден Б.Л. Алгебра. – М.: Наука, 1986. – 624 с.
8. Скорняков Л.А. Элементы алгебры. – М.: Наука, 1986. – 239 с.
9. Акушинский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 429 с.
10. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. – 379 с.
11. Виноградов И.М. Основы теории чисел. – М.: Наука, 1972. – 167 с.
12. Куликов В.В. Алгебра и теория чисел. – М.: Наука, 1980. – 400 с.