УДК 621.391.26

Визор Я. Е., канд. техн. наук

МЕТОДЫ ВЫЧИСЛЕНИЯ ПЕРВООБРАЗНЫХ КОРНЕЙ В ОСТАТОЧНЫХ КЛАССАХ

Институт кибернетики им. В. М. Глушкова НАН Украины

С целью построения оптимальных по быстродействию и оборудованию арифметических устройств вычислительной техники, проведен анализ двух систем счисления, позиционной и системы счисления в остаточных классах. Предложены методы вычисления первообразных корней, в виде $\phi(p-1)$ решений сравнений степени $\phi(p-1)$ для простых чисел с законами распределения $p=2^m+1$ и $p=2^m \cdot 3^n+1$ с минимальным количеством испытаний чисел из приведенной системы вычетов данного модуля.

Введение

Изучение любых алгебр, в том числе и машинной, сводится не только к изучению набора операций и множеств, на которых они заданы, но и представлений 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 суть следующее:

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

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

в) 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 ее 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 выполнять 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 более 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;

• получения 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.

Постановка задачи

Для получения быстрых методов выполнения арифметических операций, необходимо, с учетом 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 требуется 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 вычисления которых было отмечено выше.

Методы вычисления первообразных корней

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 $b \equiv 1(\mathrm{mod}\, m)$ 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 $G(a \bmod m)$.

Отметим некоторые известные теоремы, касающихся порядка числа, необходимые для дальнейших исследований.

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 $G(a \bmod m) = n$ 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, имеющий 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 $\phi(d)$ чисел, имеющих порядок d. Функция $\phi(n)$ называется функцией Эйлера. Она обозначает число положительных целых чисел, не превосходящих n и взаимно простых с n, при чем эта числовая функция определена на множестве всех целых положительных чисел. Отсюда, если вычет a по модулю m имеет порядок $\phi(m)$, то a называется первообразным корнем по модулю m. Тогда анализируя

вышесказанное, заключаем, что число первообразных корней по модулю m равно $\phi(m-1)$.

Далеко не всякое число p имеет первообразный корень. Точно так же нет каких-либо формул (за исключением некоторых p специального вида, для которых такого рода формулы установлены в работах П. Л. Чебышева), которые выражали бы величину первообразного корня в случае, когда он существует в зависимости от p. Нахождение первообразного корня проводятся 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, нежели 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 невыполненные ни одного из сравнений

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

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 $(p-1)\cdot r$.

Вычисление первообразных корней для модулей $p = 2^m + 1$

Пусть d – любой делитель $p-1$, $p-1 = k-1$. тогда сравнение

$$x^{p-1} - 1 \equiv 0(\mathrm{mod}\, p), \qquad (2)$$

можно записать в виде

$$(x^d - 1)\,(x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1) = 0(\mathrm{mod}\, p). \qquad (3)$$

Из теоремы Ферма известно, что если p – простое число, то сравнение $x^{p-1} - 1 \equiv 0(\mathrm{mod}\, p)$ имеет точно $p-1$ решений, т.е. сравнению удовлетворяют любые числа, не делящиеся на p; решениями являются числа $1, 2, \ldots, p-1$. Каждое решение сравнения (2) должно удовлетворять одному из сравнений:

$$(x^d - 1) \equiv 0(\mathrm{mod}\, p); \qquad (4)$$
$$x^{d(k-1)} + \ldots + x^d + 1 \equiv 0(\mathrm{mod}\, p). \qquad (5)$$

Известно, что сравнение (5) имеет не более $d(k-1)=p-1-d$ решений. Поэтому сравнение (4) должно иметь не менее d решений. Следовательно, ввиду вышесказанного предложения из теоремы Ферма, сравнение (4) имеет точно d решений. Тогда можно сформулировать теорему.

Теорема 4. Если p – простое число и d – натуральный делитель числа $p-1$, то сравнение $x^d - 1 \equiv 0(\mathrm{mod}\, p)$ имеет точно d решений.

Рассмотрим следующую теорему.

Теорема 5. Если n целое число и $n>2$, то функция Эйлера $\phi(n)$ – четное число.

Доказательство. Если n – простое число и >1, то известно, что $\phi(n)=n-1$ есть число четное. Рассмотрим случай, когда n – составное число. Из [12] известно, что если $n = \prod_{p \perp n} p_p^{\alpha}$ – каноническое разложение натурального числа n, то

$$\varphi(n) = n\prod_{p\perp n}\left(1-\frac{1}{p}\right). \qquad (6)$$

Выражение $\left(1-\frac{1}{p}\right)$ можно преобразовать:

$$1-\frac{1}{p} = \frac{1}{p}(p-1),$$

где p – простое число, так как каноническое разложение составного числа, есть разложение на простые множители. Поскольку в этом выражении p–1 – четное число, то и $\phi(n)$ будет четным числом, так как при умножение любого целого числа на число четное, результатом будет четное число.

Известно, что если целое число x взаимно простое с p, то (теорема Эйлера):

$$x^{\varphi(p)} \equiv 1(\mathrm{mod}\, p), \qquad (7)$$

в частности, если p – простое число и $\varphi(p) = p-1$, то (малая теорема Ферма):

$$x^{p-1} \equiv 1(\mathrm{mod}\, p). \qquad (8)$$

Выше мы доказали, что $\phi(p)$ при p>2 есть число четное. Значит формулу (7) можно переписать в следующем виде:

$$x^{\varphi(p)} - 1 = \left(x^{\frac{\varphi(p)}{2}} + 1\right)\left(x^{\frac{\varphi(p)}{2}} - 1\right) \equiv \equiv 0(\mathrm{mod}\, p). \qquad (9)$$

Поскольку в нашем случае p – простое число, то

$$x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} + 1\right)\left(x^{\frac{p-1}{2}} - 1\right) \equiv \equiv 0(\mathrm{mod}\, p). \qquad (10)$$

В множество p–1 решений уравнения (10) входит и подмножество $n(p$–1) первообразных корней для данного модуля. Каждый из сомножителей сравнения (10) имеет $\frac{p-1}{2}$ решений, так как, согласно теоремы 6., сравнение $x^{\frac{p-1}{2}} - 1 \equiv 0(\mathrm{mod}\, p)$ имеет $\frac{p-1}{2}$ решений, а общее число решений сравнения (10) равно *p-1*. Отсюда, сравнение $x^{\frac{p-1}{2}} + 1 \equiv 0(\mathrm{mod}\, p)$ имеет также $\frac{p-1}{2}$ решений.

Будем считать, что x - представитель подмножества первообразных корней, тогда если x какой-либо первообразный корень с порядком $G(x \bmod p) = p-1$, то множитель $x^{\frac{p-1}{2}} - 1$, не может делится на p, или:

$$x^{\frac{p-1}{2}} - 1 \neq 0(\mathrm{mod}\, p).$$

Из теории чисел известно, что если произведение двух целых чисел делится без остатка на простое число p, то по меньшей мере один из сомножителей делится на p. Отсюда мы делаем выводы, что если x – первообразный корень, то

$$x^{\frac{p-1}{2}} + 1 \equiv 0(\mathrm{mod}\, p). \qquad (11)$$

Другими словами $\frac{p-1}{2}$ решений сравнения (11) определяют некоторое множество, подмножеством которого являются все первообразные корни сравнения (8). Для вычисления первообразных корней сравнений (8) или (10), условие записанное в виде сравнения (11), является необходимым но не всегда достаточным, поскольку число решений сравнения (11) равно $\frac{p-1}{2}$, а число первообразных корней $\phi(p$–1). Для определения достаточности условия, рассмотрим связь между $\frac{p-1}{2}$ и $\phi(p$–1). Запишем для $\phi(p$–1):

$$\varphi(p-1) = (p-1)\prod_{a|p-1}(1-\frac{1}{a}),$$

где a – простые множители из канонического разложения составного числа p–1.

Отсюда:

$$p-1 = \frac{\varphi(p-1)}{\prod_{a|p-1}(1-\frac{1}{a})}.$$

Разделив обе части уравнения на 2, получим:

$$\frac{p-1}{2} = \frac{\varphi(p-1)}{2\cdot\prod_{a|3-1}(1-\frac{1}{a})}. \qquad (12)$$

Достаточность условия (11) определяется равенством

$$\frac{p-1}{2} = \varphi(p-1), \qquad (13)$$

т.е. число решений сравнения (11) равно числу первообразных корней. Из (12) видно, что в случае если знаменатель

$$2\cdot\prod_{a|p-1}(1-\frac{1}{a}) = 1,$$

то получим выражения 13. Но тогда из

$$\prod_{a|p-1}(1-\frac{1}{a}) = \frac{1}{2}$$

следует, что $a=2^m$ (где m=1,2,…..), p–1=2^m или $p=2^m+1$. Из анализа вышесказанного, следует, что первообразные корни можно вычислить непосредственно из сравнения (11) только в случае, если простое $p=2^m+1$. В остальных случаях, число решений сравнения (11) $\frac{p-1}{2}$ будет больше числа первообразных корней $\varphi(\rho-1)$. Действительно, если p – простое число, то p–1 – четное число, т.е. в каноническом разложении одно из простых множителей a=2. Преобразуя равенство (12), получим:

$$\frac{\frac{p-1}{2}}{\varphi(p-1)} = \frac{1}{2\cdot\prod_{a|p-1}(1-\frac{1}{a})}. \qquad (14)$$

Рассмотрим знаменатель в правой части уравнения (14). Его можно записать в виде:

$$2\cdot\prod_{a|p-1}(1-\frac{1}{a}) = 2(1-\frac{1}{a_1})\ (1-\frac{1}{a_2})$$

$$(1-\frac{1}{a_3})\text{.....}$$

Поскольку одно из a_i равно 2, например, a_1=2, тогда

$$2\cdot\prod_{a|p-1}(1-\frac{1}{a}) = (1-\frac{1}{a_2})\ (1-\frac{1}{a_3}), \qquad (15)$$

Очевидно, что число, получаемое в (15) будет всегда меньше 1.

Из этого вытекает, что число в отношении (14) будет всегда больше 1, тогда $\frac{p-1}{2} \rangle\ \varphi\ (p-1)$, т.е. число решений сравнения (11) будет больше числа первообразных корней.

Отсюда делаем вывод, что не всякое решение сравнения (11) может быть первообразным корнем, кроме случая, когда $p=2^m+1$.

Вычисление первообразных корней для модулей $p = 2^m 3^m + 1$

Выражение $x^{\frac{p-1}{2}}+1$ разложим на сомножители, если это возможно, и формулу (11) перепишем в виде:

$$x^{\frac{3-1}{2}}+1 = (x^k+1)(x^{\varphi(p-1)} - x^{\frac{\varphi(p-1)}{2}}+1)\ .(16)$$

Это разложение возможно не для всякого простого p. Из возможности су-

ществования (16) запишем систему уравнений:

$$\begin{cases} k = \dfrac{\varphi(p-1)}{2} \\ \dfrac{p-1}{2} = k + \varphi(p-1). \end{cases}$$

Далее

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

Отсюда:

$$\varphi(p-1) = \frac{p-1}{3}, \qquad (17)$$

а формулу (12), с учетом (11), запишем в виде:

$$x^{\frac{p-1}{2}} + 1 = (x^{\frac{\varphi(p-1)}{2}} + 1) \times \\ \times (x^{\varphi(p-1)} - x^{\frac{\varphi(p-1)}{2}} + 1) \equiv 0 (\mathrm{mod}\, p). \qquad (18)$$

Рассмотрим сомножители в уравнении (18). Первый множитель не определяет множество первообразных корней, так как если записать сравнение вида

$$x^{\varphi(p-1)} - 1 = (x^{\frac{\varphi(p-1}{2}} + 1) \times \\ \times (x^{\frac{\varphi(p-1)}{2}} - 1) \equiv 0 (\mathrm{mod}\, p),$$

то можно заметить, что сравнение $x^{\varphi(p-1)} - 1 \equiv 0 (\mathrm{mod}\, p)$ не имеет решений, если x - первообразный корень, поскольку $\phi(p-1) < p-1$.

Отсюда сравнение

$$x^{\frac{\varphi(p-1)}{2}} + 1 \equiv 0 (\mathrm{mod}\, p), \qquad (19)$$

также не может иметь решений, если x – первообразный корень. Значит сравнение (19) определяет подмножество не первообразных корней в сравнении (18), число элементов которого равняется $\dfrac{\varphi(p-1)}{2}$. Отсюда делаем вывод, что подмножество первообразных корней определяет второй множитель сравнения (18):

$$x^{\varphi(p-1)} - x^{\frac{\varphi(p-1)}{2}} + 1 \equiv 0 (\mathrm{mod}\, p). \qquad (20)$$

Действительно, в теории сравнений доказано, что сравнение

$$a_n x^n + \dots a_1 x + a_0 \equiv 0 \ (\mathrm{mod}\, p)$$

степени n по простому модулю p имеет не более n решений. Тогда сравнение (20) имеет $\phi(p-1)$ решений, что соответствует числу первообразных корней по модулю n. Перейдем от сравнений к уравнениям, тогда (20) будет иметь вид:

$$x^{\varphi(p-1)} - x^{\frac{\varphi(p-1)}{2}} + 1 = K_l P \ , \qquad (21)$$

где K_l =1,3 …. Очевидно, мы получили уравнения, корнями которого будут первообразные корни сравнения (18), причем это уравнения всегда можно свести к квадратному, поскольку $\phi(p-1)$ – четное число. Далее необходимо знать для каких p можно получить уравнение (21). Ответ на этот вопрос дает анализ уравнения (17). Доказано, что одно из a (например a_1) в каноническом разложении составного $p-1$, равно 2. Отсюда можно записать:

$$a(p-1) = (p-1) \cdot (1 - \frac{1}{2}) \times \\ \times (1 - \frac{1}{a_2})(1 - \frac{1}{a_3}) \dots \qquad (22)$$

Подставив $a(p-1)$ из (17) в (12) и разделив обе части на $p-1$, получим:

$$\frac{1}{3} = (1 - \frac{1}{2}) \cdot (1 - \frac{1}{a_2})(1 - \frac{1}{a_3}) \dots = \\ = \frac{1}{2} \cdot (1 - \frac{1}{a_2})(1 - \frac{1}{a_3}) \qquad ,$$

или

$$\frac{1}{3} = \frac{1}{2} [\ \frac{a_2 - 1}{a_2}\ ] \times \\ \times [\ \frac{a_3 - 1}{a_3}\ ] \dots = \frac{m}{d} \qquad . \qquad (23)$$

В уравнении (23) (в скобках) все a_i (2,3,5,) простые нечетные числа, а их разница с единицей – четные. Так как произведение всех четных чисел равно четному числу, то сократив это число на 2, получим четное число m. Произведение нечетных a_i равно нечетному числу d. Чтобы равенство (23) имело смысл, необходимо, чтобы четное m делило без остатка нечетное d, что невозможно. Значит m должно быть нечетным числом, что возможно, лишь после сокращения произведения четных числителей на 2, т.е. когда это произведение будет равно 2. Это возможно тогда, когда в произведении участвуют два числа 1 и 2, что влечет существование такого из a_i (например a_2), что $a_2-1=2$.

Отсюда $a_2=3$, что и подтверждает уравнение (23). Мы определили, что для данного случая, в каноническом разложении числа $p-1$ существуют только два простых множителей 2 и 3, тогда можно записать

$$p-1=2^m\cdot 3^n\,(m=1,2,:....,n=1,2,3....)$$

$$p=2^m\cdot 3^n+1. \qquad (24)$$

Теорема 6. Если p – простое число, подчиняется закону распределения вида $p=2^m 3^n+1$ (m=1,2,3,4…, n=1,2,3,4……), то существует сравнение:

$$x^{\varphi(p-1)}-x^{\frac{\varphi(p-1)}{2}}+1\equiv 0(\mathrm{mod}\,p)$$

степени $\phi(p-1)$ по модулю p, в котором все $\phi(p-1)$ решений будут первообразными корнями числа p.

В уравнении (21) сделаем замену $x^{\frac{\varphi(p-1)}{2}}=y$, тогда получим

$y^2-y+1=\kappa p$

или

$$y^2-y-(\kappa p-1)=0. \qquad (25)$$

Как видно из (25), мы получили квадратное уравнение. Корни этого уравнения будут иметь вид:

$$y_{1,2}=\frac{1}{2}\pm\sqrt{\frac{1}{4}+kp-1}=\frac{1\pm\sqrt{4kp-3}}{2};$$

Поскольку мы рассматриваем положительные числа, первообразные корни X_β с учетом (17) можно вычислить из формулы:

$$X_\beta=\sqrt[\frac{\phi(p-1)}{2}]{y}=\sqrt[\frac{p-1}{6}]{\frac{1+\sqrt{4K_\beta p-3}}{2}}, \qquad (26)$$

где β=1,2,3,…,$\phi(p-1)$. Индекс при X и K, указывает на порядковый номер вычисляемого первообразного корня и соответствующего ему выбранного K. Исходя из (25), определим какие значения может принимать K_β и предел их изменения для данного модуля p. Для этой цели запишем формулу (25) в виде: $y(y-1)+1=K_\beta p$.

Очевидно, что для любых положительных целых y, произведение $y(y-1)$ – число четное, а выражение $y(y-1)+1$ – нечетное. Тогда K_β должно быть также нечетным числом, так как модуль p – простое число. Кроме того, анализ формулы (26) показывает, что число K_β – простое число. Диапазон изменения K_β можно вывести из формулы (21), с учетом того, что в приведенной системе вычетов наименьшее значение первообразных корней соответственно равно $X_{\min}=2$ и $X_{\max}=p-1$. Подставив в формулу (21) вместо $\phi(p-1)$ его значение из (17), запишем неравенства:

$$\frac{2^{\frac{p-1}{3}}-2^{\frac{p-1}{6}}+1}{p}\le K_\beta;$$

$$K_\beta\le\frac{(p-1)^{\frac{p-1}{3}}-(p-1)^{\frac{p-1}{6}}+1}{p}.$$

Выбирая из заданного диапазона все подходящие для (26) простые K_β, можно вычислить все первообразные корни для заданного модуля. Недостатком, в предлагаемом методе, этого способа вычисления корней является то, что для больших модулей количество проверочных выборок K_β будет больше, чем в методе испытания всех возможных оснований, где число проверок равно $(p-1)^2$, или, чем в методе испытания оснований на невы-

полнение условий (1), где число проверок равно $(p-1)r$. Значительно эффективнее в предлагаемом методе испытывать основания, используя формулу (21), поскольку только первообразные корни могут удовлетворить равенство:

$$K_\beta = \frac{X^{\frac{p-1}{3}} - X^{\frac{p-1}{6}} + 1}{p},$$

т.е., подставляя вместо X все $p-1$ значений вычетов из приведенной системы вычетов данного модуля p, выделяем только те вычеты, которые превращают числитель данного равенства в число, которое нацело делится на p, такие вычеты и будут первообразными корнями данного модуля p, причем количество проверок равно $p-1$, что в $p-1$ раз меньше, чем число проверок оснований по формуле Ферма и в r раз меньше, чем число проверок оснований на невыполнение условий (1).

Выводы

При вычислении первообразных корней методами, описанными выше, нет необходимости проверять все основания из приведенной системы вычетов. Достаточно найти один первообразный корень из множества корней данного модуля, а затем, используя тот факт, что все первообразные корни имеют один и тот же порядок $p-1$, применив теорему 2, вычислить все остальные первообразные корни. Таким образом, количество ненужных проверок значительно сокращается.

Предложенный новый метод позволяет вычислять первообразные корни для модулей, подчиняющихся законам распределения $p=2^m+1$ и $p=2^m\cdot 3^n+1$, непосредственно из формул (11) или (21) с минимальным, среди известных методов, количеством испытаний чисел из приведенной системы вычетов данного модуля. Другими словами, из бесконечного множества простых модулей, выделено два подмножества модулей, причем каждый из модулей, имеет свое множество первообразных корней, являющихся $\phi(p-1)$ решениями сравнений (11) или (20).

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. *Акушский И. Я., Юдицкий Д. И.* Машинная арифметика в остаточных классах. – М.: Сов. 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.