УДК 681.142

В.А. Краснобаев[1], А.С. Янко[1], С.А. Кошман[2]

[1] *Полтавский национальный технический университет имени Юрия Кондратюка, Полтава*
[2] *Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков*

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И АЛГОРИТМЫ ВОЗВЕДЕНИЯ ЦЕЛЫХ ЧИСЕЛ В КВАДРАТ ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ КЛАССА ВЫЧЕТОВ

В статье разработаны математические модели и алгоритмы возведения целых чисел в квадрат по произвольному модулю класса вычетов (КВ). Данные алгоритмы основываются на доказанных в статье аналитических соотношениях. Предложенные алгоритмы возведения целых чисел в квадрат по произвольному модулю могут быть использованы в компьютерных вычислительных устройствах функционирующих как в обычной позиционной двоичной системе счисления, так и в непозиционной системе счисления КВ.

Ключевые слова: *возведения целых чисел в квадрат по произвольному модулю, позиционная двоичная система счисления, непозиционная система счисления в классе вычетов.*

Введение

При аппаратной реализации компьютерными вычислительными устройствами некоторых вычислительных алгоритмов, представленных последовательностью целочисленных операций (арифметические операции над целыми числами и полиномами, целочисленное линейное программирование, операции над множествами, решение многомерных NP-полных задач, реализация алгоритмов маршрутизации, задачи о путях и умножение матриц, задачи быстрого преобразование Фурье и его приложения, обработка сейсмологических и метеорологических данных, создание систем искусственного интеллекта, решение задач аэродинамики, ядерной физики и задач военного назначения, цифровая обработка сигналов, цифровая обработка изображений, криптографические преобразования, целочисленная арифметика высокой точности, решение задач, связанных с исследованием космического пространства, высокоточные цифро-аналоговые и аналого-цифровые преобразования и пр.), часто возникает задача возведения целого числа A в квадрат по модулю m натурального числа, т. е. задача определения аналитического выражения $A^2 \pmod m$. Так, на пример, при криптографических преобразованиях для базиса расширенного поля (нормального базиса) необходимо производить операцию возведения в квадрат элемента A. При построении эллиптической кривой над простым полем Галуа и при ее описании требуется введение в теорию модулярных форм и функций, квадратичных полей и функций Вейерштрасса. При решении уравнения Фробениуса для подгруппы значительная часть вычислений состоит в расчете значений $x^m, x^m, x^{m^2}, y^{m^2}$ в заданном кольце. Отметим, что особенно важна техническая реализация операции определения значения $A^2 \pmod m$ в непозиционной системе счисления класса вычетов (КВ).

Таким образом актуальны и важны исследования, посвященные разработке алгоритма реализации операции $A^2 \pmod m$. Цель статьи – построение математической модели процесса реализации аналитического соотношения $A^2 \pmod m$ и на ее основе провести синтез алгоритма реализации операции возведения чисел A в квадрат по произвольному модулю m КВ.

Обзор литературных источников. Существуют алгоритмы реализации модульной операции возведения целых чисел A в квадрат по модулю m КВ [1, 2]. Однако данные алгоритмы не всегда применимы для всех возможных значений A и m. В этом случае не все технические устройства, реализующие алгоритм $A^2 \pmod m$, обеспечивают достоверный результат вычисления [3 – 12].

Основная часть

Пусть необходимо определить значение $A^2 \pmod m$, где: A, m – натуральные числа и $0 \le A \le m-1$. Вначале покажем, что выполняется следующее математическое соотношение

$$A^2 \pmod m = (m - A)^2 \bmod m. \qquad (1)$$

Действительно, A^2 представим в виде $A^2 = k + \alpha$ $(0 \le \alpha \le m-1)$, т.е. $A^2 \equiv \alpha \pmod m$. Тогда $(m-A)^2 = m^2 - 2mA + A^2 = m^2 - 2mA + k m + \alpha$. В этом случае $(m^2 - 2mA + k m + \alpha) \equiv \alpha \pmod m$. Равенство (1) справедливо как для четного, так и для и нечетного значения m.

Аналитическое соотношение (1) является математической моделью процесса реализации аналитического соотношения $A^2 \pmod m$ для первого алгоритма.

В случае технической реализации операции $A^2 \pmod m$ целесообразно рассмотреть три возможных варианта значения m.

Первый алгоритм. Для значений m=2n+1 нечетного (n=0, 1, 2, ...). Для этого случая схема процесса реализации операции $A^2(\text{mod m})$ представлена на рис. 1. Данная схема представлена в общем виде и реализует алгоритм, представленный выражением (1). Устройство работает следующим образом. По входу устройства во входной регистр в двоичном коде записывается число A. С выхода дешифратора число A, в унитарном ходе, через соответствующий логический элемент ИЛИ (в соответствии с алгоритмом (1)) поступает на вход шифратора, который соответствует значению $A^2(\text{mod m})$. С выхода шифратора значение $A^2(\text{mod m})$ в двоичном коде поступает в выходной регистр. Очевидно, что основным звеном в технической реализации операции $A^2(\text{mod m})$ является нужная кодировка шин между дешифратором и шифратором. Алгоритм реализации величины $A^2(\text{mod m})$ для m=11 представлен в табл. 1.

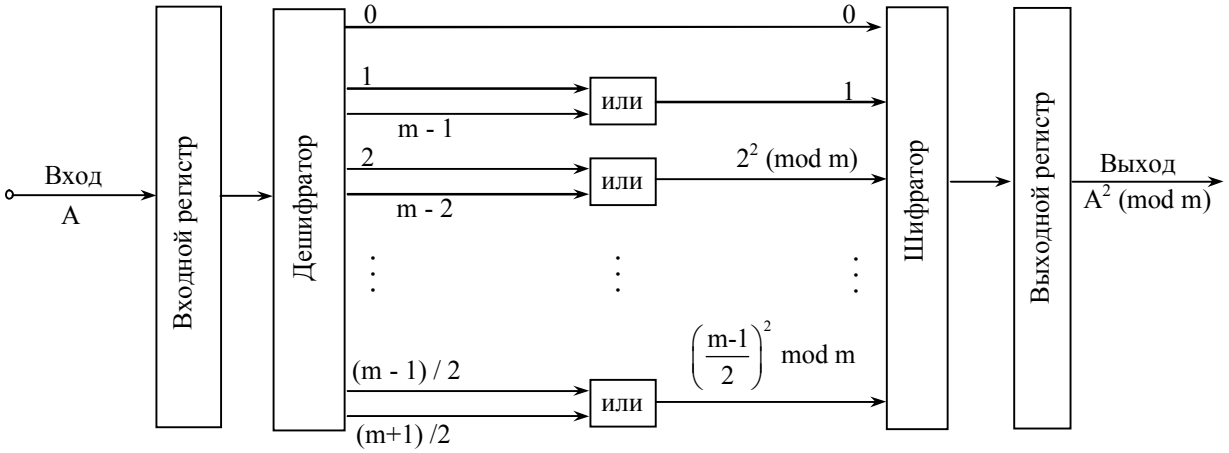

Рис. 1. Первый вариант схемы, реализующей операцию A^2 (mod m)

Таблица 1

Первый алгоритм вычисления значения A^2 (mod m)

Номер пары выходных шин дешифратора	Значения, присваиваемые паре выходных шин дешифратора	Значения A^2 (mod 11), которые присваиваются входным шинам шифратора	Значения выходных шин шифратора
0	0	0	0000
1	1,10	1	0001
2	2,9	4	0100
3	3,8	9	1001
4	4,7	5	0101
5	5,6	3	0011

Второй алгоритм. Для значений m=2n четного и m/2 также четного чисел. В этом случае значение $\frac{m}{2}$ является целым числом и, следовательно, $\left(\frac{m}{2}\right)^2 = \frac{m}{4}\cdot m \equiv 0(\text{mod m})$. Тогда выходная шина дешифратора, соответствующая значению $\frac{m}{2}$, одновременно с нулевой шиной, через нулевой элемент ИЛИ подключена к нулевому входу шифратора. Алгоритм функционирования устройства, в соответствии со вторым вариантом, определяется следующим следующей математической моделью (2)

$$\left(\frac{m}{2}\right)^2 = 0\,(\text{mod m})\,. \qquad (2)$$

Схема организации процесса реализации операции A^2 (mod m) представлена на рис. 2. В табл. 2 представлен алгоритм образования численного значения A^2 (mod m) для m = 12 (m/2 = 6).

Третий алгоритм. Для значений m = 2 n четного и m/2 нечетного чисел. Предлагаемый алгоритм основывается на использовании следующей математической модели (3)

$$\left(\frac{m}{2}\right)^2 \equiv \frac{m}{2}\,(\text{mod m})\,. \qquad (3)$$

Действительно выражение (3) легко представить в виде

$$\frac{m}{2}\cdot\left(\frac{m}{2}-1\right) = 0\,(\text{mod}\,\frac{m}{2}\cdot 2).\ . \qquad (4)$$

Из теории чисел известно, что сравнимость A≡B (mod m) двух чисел A и B по модулю m равносильна делимости числа A – B на модуль m. Из выражения (4) следует, что число $\frac{m}{2}\cdot\left(\frac{m}{2}-1\right)$ делится

на модуль $m=\frac{m}{2}\cdot 2$. Действительно, первое слагаемое $m/2$ произведения (4) делится на $m/2$, а второе $m/2-1$ слагаемое – делится на два, так как по условию $\frac{m}{2}$ нечетное число.

Таким образом, показана справедливость сравнения (3).

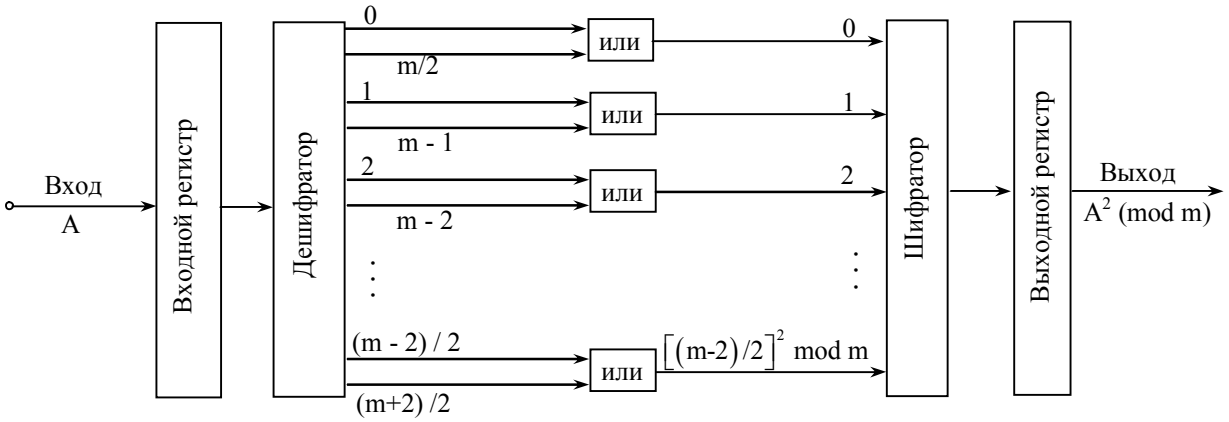

Рис. 2. Второй вариант схемы, реализующей операцию A^2 (mod m)

Таблица 2

Второй алгоритм вычисления значения A^2 (mod m)

Номер пары выходных шин дешифратора	Значения, присваиваемые паре выходных шин дешифратора	Значения A^2 (mod 12), которые присваиваются входным шинам шифратора	Значения выходных шин шифратора
0	0,6	0	0000
1	1,11	1	0001
2	2,10	4	0100
3	3,9	9	1001
4	4,8	4	0100
5	5,7	1	0001

Схема организации процесса реализации операции возведения чисел A в квадрат по модулю m представлена на рис. 3. В табл. 3 представлен алгоритм образования значения A^2 (mod m) для модуля m = 14 (m/2 = 7).

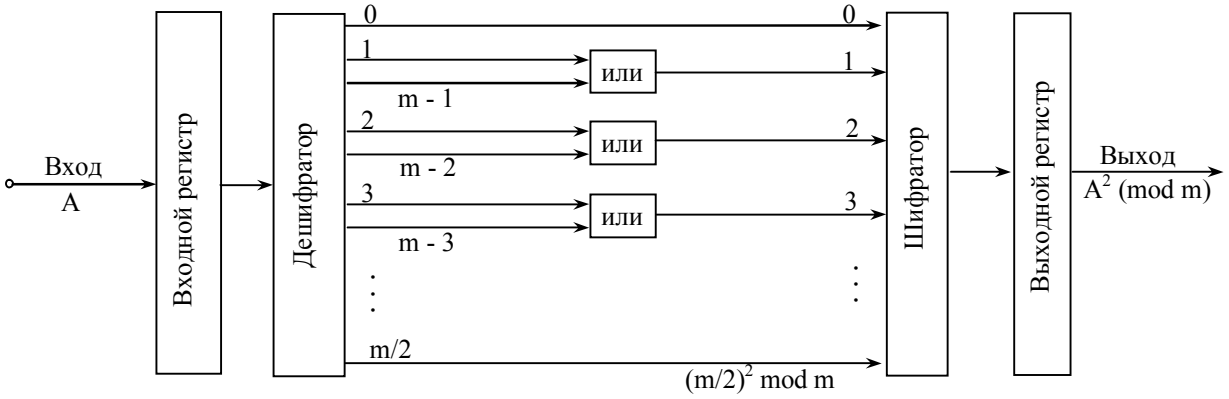

Рис. 3. Третий вариант схемы, реализующей операцию A^2 (mod m)

На рис. 4 представлены общие схемы объединения выходных шин дешифратора для первого ($ДШ_1$), второго ($ДШ_2$) и третьего ($ДШ_3$) вариантов для одновременной реализации рассматриваемой операции A^2 (mod m).

На рис. 5 представлен пример схемы объединения выходных шин дешифратора для первого (m_1=11), второго (m_2=12) и третьего (m_3=14) вариантов.

В этом случае устройство для реализации операции возведения чисел в квадрат по модулю m КВ для произвольного значения модуля будет содержать три дешифратора, четыре группы элементов ИЛИ и три шифратора (рис. 6) [13].

Таблица 3

Третий алгоритм вычисления значения A^2(mod m)

Номер пары выходных шин дешифратора	Значения, присваиваемые паре выходных шин дешифратора	Значения A^2(mod 14), которые присваиваются входным шинам шифратора	Значения выходных шин шифратора
0	0,6	0	0000
1	1,13	1	0001
2	2,12	4	0100
3	3,11	9	1001
4	4,10	2	0010
5	5,9	11	1011
6	6,8	8	1000
7	7	7	0111

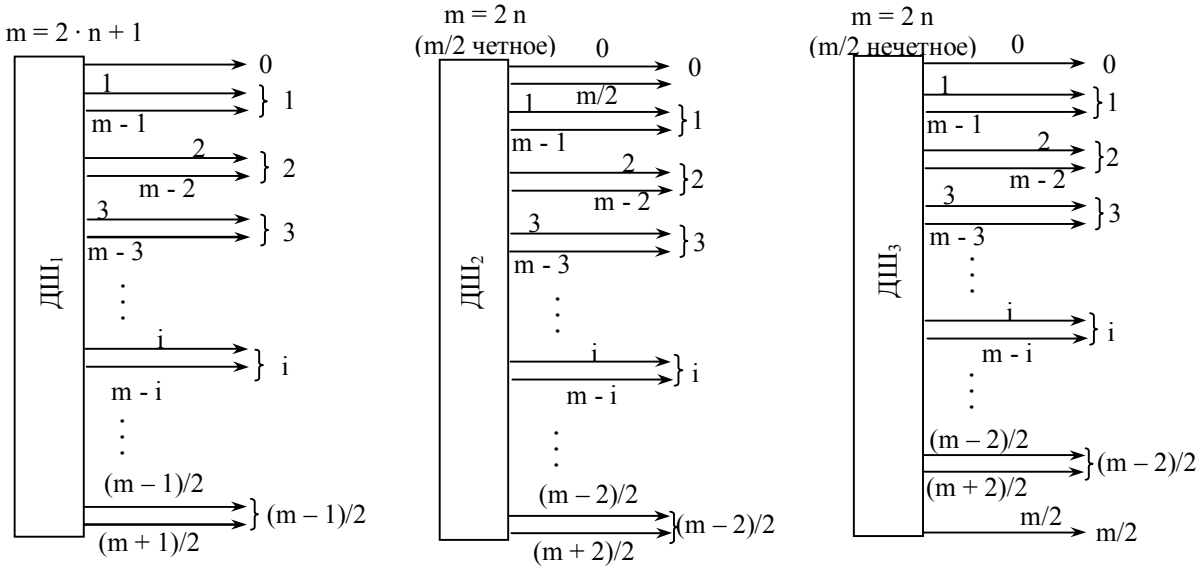

Рис. 4. Схемы объединения выходных шин дешифраторов для различных значений m

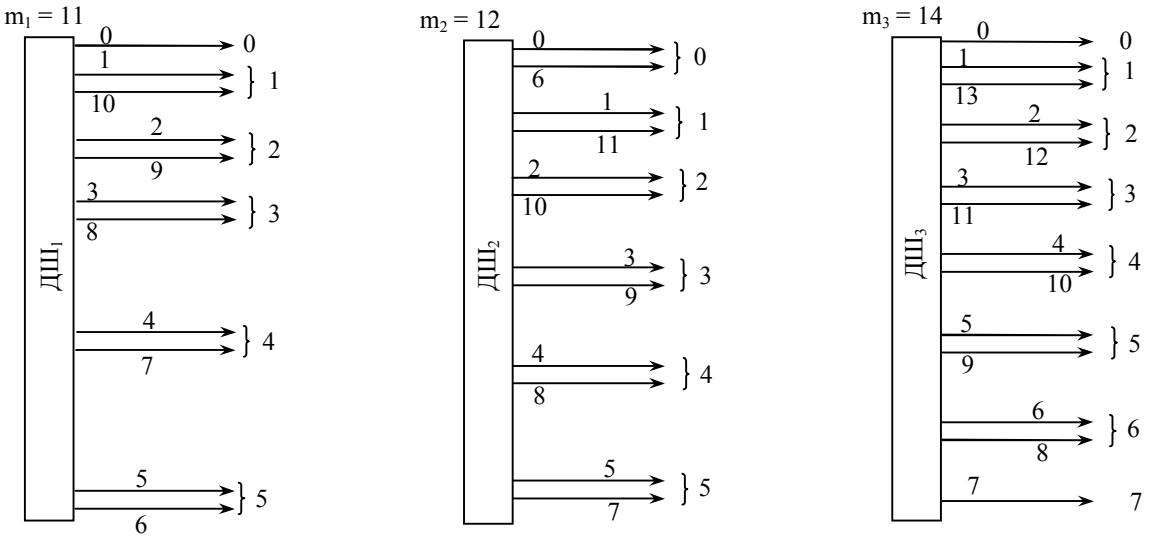

Рис. 5. Примеры схем объединений выходных шин дешифраторов для $m_1 = 11$, $m_2 = 12$ и $m_3 = 14$

Один из недостатков данной схемы – большое количество элементов ИЛИ, непосредственно участвующих в образовании результата A^2 (mod m) операции (первая, вторая и третья группы элементов ИЛИ). Общее количество $N_{ИЛИ}$ х элементов ИЛИ трех групп ($ИЛИ_1$, $ИЛИ_2$ и $ИЛИ_3$) примерно равно $N_{ИЛИ}=N_{ИЛИ_1}+N_{ИЛИ_2}+N_{ИЛИ_3}$. При реализации операции A^2 (mod m) возведения чисел А в квадрат по одному из модулей m_i $(i=\overline{1,3})$, выбирается нужная схема соединения входов-выходов дешифратор-шифратор.

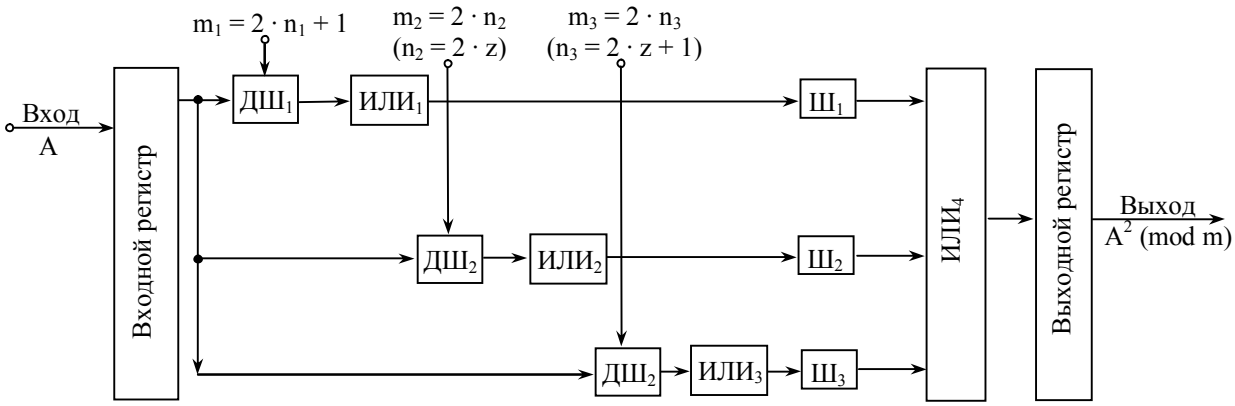

Рис. 6. Общая схема реализации операции A^2 (mod m) для производного модуля m

Проведем расчет и сравнительный анализ количества элементов ИЛИ в трех группах. Пусть для определенности $m_1 < m_2 < m_3$ (три возможных варианта). Тогда можно считать, что $N_{\substack{ИЛИ \\ \Sigma}} \approx 3 \cdot N_{ИЛИ_3}$.

Если считать, что количество элементов ИЛИ в одной группе равно $\left[\frac{m_3}{2}\right]$, тогда $N_{\substack{ИЛИ \\ \Sigma}} \approx \left[\frac{3}{2} \cdot m_3\right]$, где $[x]$ – целая часть числа x, его не превосходящая. Учитывая, что $m_3 > m_2 > m_1$, то в качестве одной из трех групп элементов $ИЛИ_i$ $\left(i = \overline{1,3}\right)$ необходимо синтезировать схему для наибольшей $ИЛИ_3$ по количеству элементов ИЛИ группу. Такая схема представлена на рис. 7, где обозначения "m_i" означают сигнал подачи признака модуля m_i, по которому работает схема [14].

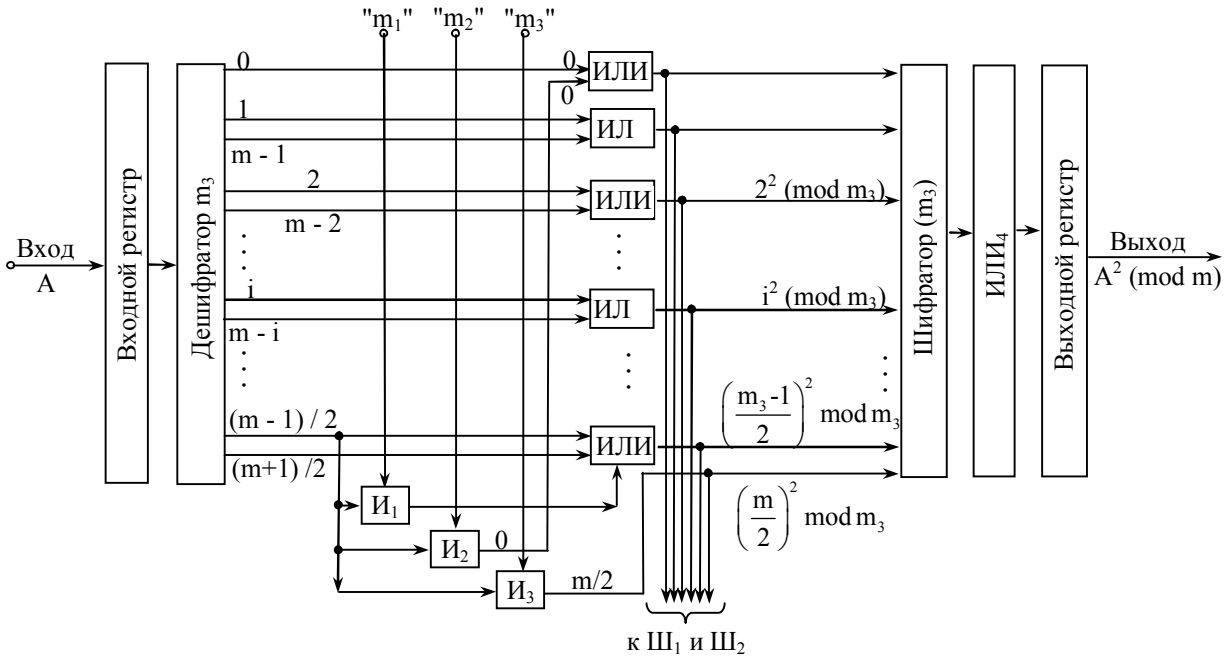

Рис. 7. Обобщенная схема реализации операции A^2(mod m)

Пусть $m_1 = 11$, $m_2 = 12$ и $m_3 = 14$ ($m_3 > m_2 > m_1$). В этом случае для общей схемы (рис. 6) количество $N_{\substack{ИЛИ \\ \Sigma}}$ элементов приблизительно равно

$$N_{\substack{ИЛИ \\ \Sigma}} \approx \left[\frac{m_1}{2}\right] + \left[\frac{m_2}{2}\right] + \left[\frac{m_3}{2}\right] = 5 + 6 + 7 = 18,$$

а для упрощенной схемы (рис. 7) имеем, что

$$N_{\substack{ИЛИ \\ \Sigma}} \approx \left[\frac{m_3}{2}\right] + N_и = 7 + 3 = 10.$$

Для данного набора модулей m_i $\left(i = \overline{1,3}\right)$ имеем выигрыш в уменьшении количества $N_{\substack{ИЛИ \\ \Sigma}}$ элементов И на ≈ 55 % при сохранении всех функциональных возможностей устройства для определения величины A^2 (mod m).

Заключение

В данной статье предложено три математические модели для реализации аналитического соот-

ношения $A^2(\mathrm{mod}\ m)$. На основании этих моделей разработаны соответствующие алгоритмы возведения целых чисел в квадрат по произвольному модулю m КВ. На основании разработанных алгоритмов, в зависимости от численного значения модуля m, синтезировано три группы устройств для реализации соотношения $A^2(\mathrm{mod}\ m)$.

Отметим, что полученные результаты важны и могут быть использованы для реализации модульной операции $A^2(\mathrm{mod}\ m)$ компьютерными вычислительными устройствами, функционирующими как в непозиционной системе счисления КВ, так и в обычной позиционной двоичной системе счисления.

Список литературы

1. Краснобаев В.А. Методы и алгоритмы возведения чисел в произвольную степень по модулю системы остаточных классов / В.А. Краснобаев // АСУ и приборы автоматики. – 1986. – Вып. 80. – С. 101-103.

2. Мартыненко С.О. Метод возведення чисел в квадрат по модулю М модулярной системы счисления / С.О. Мартыненко, В.А. Краснобаєв // Радіоелектронні і комп'ютерні системи. – 2010. – № 5 (46). – С. 165-171.

3. А.с. № 1034036 СССР. Устройство для возведения чисел в квадрат по модулю / В.А. Краснобаев, Е.И. Бороденко. – Опубл. в БИ. 1983. № 29.

4. А.с. № 1096641 СССР. Устройство для возведения чисел в квадрат по модулю / В.А. Краснобаев, Е.И. Бороденко, А.Ю. Семенов и др. – Опубл. в БИ. 1984. № 21.

5. А. с. № 1095172 СССР. Устройство для возведения чисел в квадрат по модулю / В.А. Краснобаев, Е.И. Бороденко, В.И. Стеценко. – Опубл. в БИ. 1984. № 20.

6. А.с. № 1160397 СССР. Устройство для возведения чисел в степень по модулю / В.А. Краснобаев, А.Ю. Семенов. – Опубл. в БИ. 1985. № 21.

7. А.с. № 1233154 СССР. Устройство для возведения чисел в квадрат по модулю / В.А. Краснобаев, О.Н. Фоменко и др. – Опубл. в БИ. 1986. № 20.

8. А.с. № 1683014 СССР. Устройство для возведения чисел в степень по модулю три / В.А. Краснобаев, О.Н. Фоменко, В.П.Ирхин и др. – Опубл. в БИ. 1991. № 30.

9. Д.П. на корисну модель № 39493 України, МПК G 06 F 7/60 (2009) / В.А. Краснобаєв, О.А. Сіора, С.О. Кошман, К.В. Яськова, В.І. Барсов. Пристрій для піднесення чисел до квадрата за модулем т. № и 2008 15512. Заявл. 24.10.2008. – Опубл. 25.12.2009, Бюл. № 4. – 4 с.

10. Д.П. на корисну модель № 40905 України, МПК G 06 F 7/00 (2009) / С.О. Кошман, В.І. Барсов, О.А. Сіора, В.А. Краснобаєв Пристрій для піднесення комплексних чисел в квадрат за комплексним модулем у модулярній системі числення. № и 2008 14308. Заявл. 12.12.2008. Опубл. 27.04.2009, Бюл. № 8.-5с.

11. ДП на корисну модель № 41267 України, МПК (2009) G 06 F 7/60 / С.О. Кошман, В.І. Барсов, О.А. Сіора, В.А. Краснобаєв / Пристрій для піднесення чисел до довільного степеня за модулем три модулярної системи числення. № и 2008 15194. Заявл. 24.03.2009. Опубл. 12.05.2009, Бюл. № 9. – 4 с.

12. Д.П. на корисну модель № 51512 України, МПК G 06 F 7/74 (2009) / В.І. Барсов, С.О. Мартиненко, В.А. Краснобаєв. Пристрій для піднесення чисел до квадрата за модулем т модулярної системи числення. № и 2009 12508. Заявл. 03.12.2009. Опубл. 26.07.2010, Бюл. № 14. – 6 с.

13. Д.П. на корисну модель № 61798 України, МПК G 06 F 7/60 (2006.01) / І.Д. Горбенко, К.В. Загумена, В.А. Краснобаєв, О.А. Замула, Ю.І. Горбенко. Пристрій для піднесення чисел до квадрата за модулем т класу лишків. № и 201101245. Заявл. 04.02.2011. – Опубл. 25.07.2011, Бюл. № 14. – 6 с.

14. Д.П. на корисну модель № 66645 України, МПК G 06 F 7/74 (2006.01) / В.І. Барсов, М.В. Дугін, Л.С. Сорока, В.А. Краснобаєв, К.В. Загуменна. Пристрій для піднесення чисел до квадрата за модулями ті класу лишків. № и 2011 07927. Заявл. 23.06.2011. Опубл. 10.01.2012, Бюл. № 1. – 12 с.

Поступила в редколлегию 13.11.2013

Рецензент: д-р техн. наук, проф. В. М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.

МАТЕМАТИЧНІ МОДЕЛІ ТА АЛГОРИТМИ ПІДНЕСЕННЯ ЦІЛИХ ЧИСЕЛ ДО КВАДРАТУ ЗА ДОВІЛЬНИМ МОДУЛЕМ КЛАСУ ЛИШКІВ

В.А. Краснобаєв, А.С. Янко, С.О. Кошман

В статі розроблено математичні моделі та алгоритми піднесення цілих чисел до квадрату за довільним модулем класу лишків (КЛ). Дані алгоритми базуються на доказаних у статі аналітичних співвідношеннях. Запропоновані алгоритми піднесення цілих чисел до квадрату за довільним модулем можуть використовуватися у комп'ютерних обчислювальних пристроях, що функціонують як у звичайній позиційній двійковій системі числення, так і у непозиційній системі числення КЛ.

Ключові слова: *піднесення цілих чисел до квадрату за довільним модулем, позиційна двійкова система числення, непозиційна система числення у класі лишків.*

THE MATHEMATICAL MODELS AND ALGORITHMS FOR THE SQUARING OF INTEGERS BY AN ARBITRARY MODULE OF RESIDUE CLASS

V.A. Krasnobaeyv, A.S. Yanko, S.A. Koshman

The mathematical models and algorithms for the squaring of integers by an arbitrary module of residue class are developed in this paper. These algorithms are based on analytical ratios that are proven in this article. The proposed algorithms for the squaring of integers by an arbitrary module of residue class can be used in computer devices that function as in positional number systems, and in no positional binary system of residue class.

Keywords: *squaring of integers by an arbitrary module, positional binary system, no positional binary system of residue class.*