УКРАЇНА

# ПАТЕНТ

## НА КОРИСНУ МОДЕЛЬ

## № 95060

**ПРИСТРІЙ ДЛЯ ПІДНЕСЕННЯ ЦІЛИХ ЧИСЕЛ, ЩО ПРЕДСТАВЛЕНІ У КЛАСІ ЛИШКІВ, ДО СТЕПЕНЯ НАТУРАЛЬНОГО ЧИСЛА**

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі **10.12.2014.**

Голова Державної служби
інтелектуальної власності України А.Г. Жарінова

Державна служба інтелектуальної власності України
Ідентифікаційний код 37552556
№1

(11) **95060**

(19) **UA**

(51) **МПК**
***G06F 7/60*** **(2006.01)**

(21) Номер заявки: **u 2014 06854**

(22) Дата подання заявки: **18.06.2014**

(24) Дата, з якої є чинними права на корисну модель: **10.12.2014**

(46) Дата публікації відомостей про видачу патенту та номер бюлетеня: **10.12.2014, Бюл. № 23**

(72) Винахідники:
**Краснобаєв Віктор Анатолійович, UA,**
**Янко Аліна Сергіївна, UA,**
**Кошман Сергій Олександрович, UA**

(73) Власники:
**Краснобаєв Віктор Анатолійович,**
вул. Енгельса, 19, к. 407, м. Харків-12, 61012, UA,
**Янко Аліна Сергіївна,**
вул. Великотирнівська, 36, корп. 3, к. 122, м. Полтава, 36014, UA,
**Кошман Сергій Олександрович,**
вул. Енгельса, 19, к. 409, м. Харків-12, 61012, UA

(54) Назва корисної моделі:

# ПРИСТРІЙ ДЛЯ ПІДНЕСЕННЯ ЦІЛИХ ЧИСЕЛ, ЩО ПРЕДСТАВЛЕНІ У КЛАСІ ЛИШКІВ, ДО СТЕПЕНЯ НАТУРАЛЬНОГО ЧИСЛА

(57) Формула корисної моделі:

Пристрій для піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа, що містить вхідний і вихідний регістри, групу елементів АБО, першу та другу групи елементів І, при цьому вхід пристрою підключено до входу вхідного регістра, а вихід вихідного регістра якого є виходом пристрою, який **відрізняється** тим, що введено третю, четверту та п'яту групи елементів І, перший і другий прийомні регістри, регістр пам'яті, групу з n множників за модулями $m_i (i = \overline{1,n})$, при цьому, вихід вхідного регістра підключено до перших входів елементів І першої та другої груп, шина додатної ознаки підключена до других входів елементів І першої групи, а шина від'ємної ознаки підключена до других входів елементів І другої групи, виходи елементів І першої та другої груп підключено до перших входів відповідно першого та другого суматорів, виходи яких через перший та другий входи елементів АБО групи підключено до входу першого прийомного регістра та до входу регістра пам'яті, виходи підрегістрів яких підключено до перших входів елементів І відповідно третьої та четвертої груп, до других входів яких підключена перша шина керування пристрою, до других входів першого та другого суматорів підключена шина подачі значення $\frac{M}{2}(M = \prod_{i=1}^{n} m_i)$, виходи елементів І відповідно третьої та четвертої груп підключено до перших і других входів множників за модулями $m_i$ групи, виходи яких підключено до відповідних підрегістрів другого прийомного регістра, вихід якого підключено до третього входу елементів АБО групи та до перших входів елементів І п'ятої групи, виходи яких підключено до входу вихідного регістра, до других входів елементів І п'ятої групи підключена друга шина керування пристрою.

Пронумеровано, прошито металевими
люверсами та скріплено печаткою
2 арк.
10.12.2014

Уповноважена особа

Державна служба інтелектуальної власності України
Ідентифікаційний код 37552556
№1

(підпис)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

**УКРАЇНА** (19) **UA** (11) **95060** (13) **U**

(51) МПК
***G06F 7/60*** (2006.01)

## (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2014 06854**

(22) Дата подання заявки: **18.06.2014**

(24) Дата, з якої є чинними права на корисну модель: **10.12.2014**

(46) Публікація відомостей про видачу патенту: **10.12.2014, Бюл.№ 23**

(72) Винахідник(и):
**Краснобаєв Віктор Анатолійович (UA),**
**Янко Аліна Сергіївна (UA),**
**Кошман Сергій Олександрович (UA)**

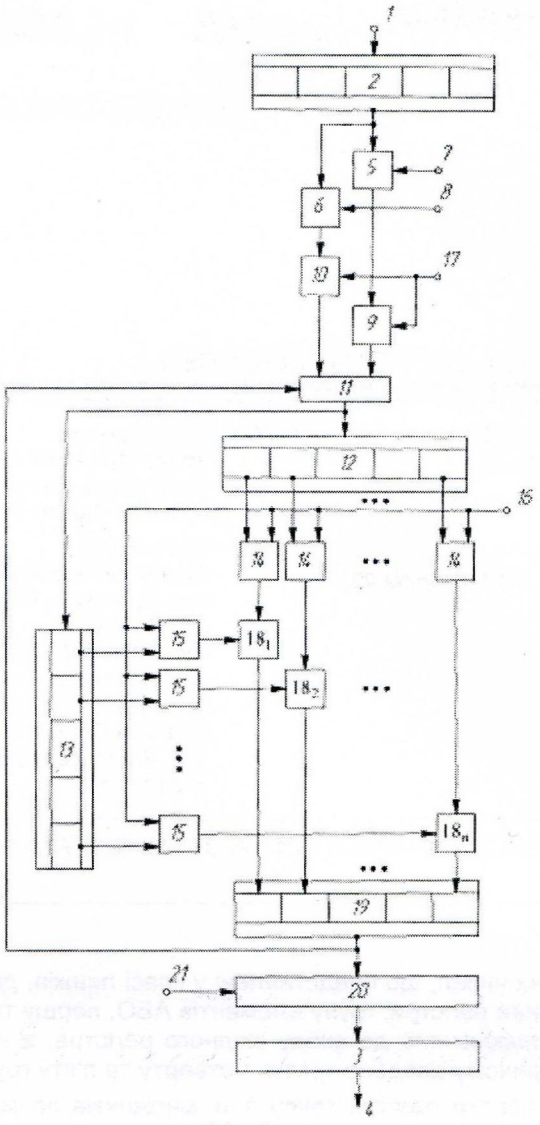
(73) Власник(и):
**Краснобаєв Віктор Анатолійович,**
вул. Енгельса, 19, к. 407, м. Харків-12, 61012 (UA),
**Янко Аліна Сергіївна,**
вул. Великотирнівська, 36, корп. 3, к. 122, м. Полтава, 36014 (UA),
**Кошман Сергій Олександрович,**
вул. Енгельса, 19, к. 409, м. Харків-12, 61012 (UA)

### (54) ПРИСТРІЙ ДЛЯ ПІДНЕСЕННЯ ЦІЛИХ ЧИСЕЛ, ЩО ПРЕДСТАВЛЕНІ У КЛАСІ ЛИШКІВ, ДО СТЕПЕНЯ НАТУРАЛЬНОГО ЧИСЛА

(57) Реферат:

Пристрій для піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа містить вхідний і вихідний регістри, групу елементів АБО, першу та другу групи елементів І, при цьому вхід пристрою підключено до входу вхідного регістра, а вихід вихідного регістра якого є виходом пристрою, причому введено третю, четверту та п'яту групи елементів І, перший і другий прийомні регістри, регістр пам'яті, групу з $n$ множників за модулями $m_i (i = \overline{1,n})$, при цьому вихід вхідного регістра підключено до перших входів елементів І першої та другої груп. Шина додатної ознаки підключена до других входів елементів І першої групи, а шина від'ємної ознаки підключена до других входів елементів І другої групи, виходи елементів І першої та другої груп підключено до перших входів відповідно першого та другого суматорів, виходи яких через перший та другий входи елементів АБО групи підключено до входу першого прийомного регістра та до входу регістра пам'яті, виходи підрегістрів яких підключено до перших входів елементів І відповідно третьої та четвертої груп, до других входів яких підключена перша шина керування пристрою, до других входів першого та другого суматорів підключена шина подачі значення $\frac{M}{2} (M = \prod_{i=1}^{n} m_i)$, виходи елементів І відповідно третьої та четвертої груп підключено до перших і других входів множників за модулями $m_i$ групи, виходи яких підключено до відповідних підрегістрів другого прийомного регістра, вихід якого підключено до третього входу елементів АБО групи та до перших входів елементів І п'ятої групи, виходи яких підключено до входу вихідного регістра, до других входів елементів І п'ятої групи підключена друга шина керування пристрою.

UA 95060 U




Фіг. 1

Корисна модель належить до області обчислювальної техніки і призначена для піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа.

Відомий пристрій (аналог), що містить елементи І та АБО, вхідний та вихідний регістри, групи елементів І та АБО. При цьому вхід пристрою підключено до входу вхідного регістра, вихід якого підключено до входу дешифратора. Виходи дешифратора попарно підключені до входів елементів АБО. Вихід вихідного регістра підключено до виходу пристрою (А. с. СРСР № 1095172, кл. G06F 7/72,1984р.).

Недоліком відомого пристрою (аналога) є низькі функціональні можливості, що обумовлено неможливістю піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа.

Відомий пристрій (аналог) для піднесення чисел до квадрату за модулем, що Містить вхідний та вихідний регістри, першу групу елементів АБО, першу групу елементів І, дешифратор, шифратор та ін. При цьому вхід пристрою підключено до входу вхідного регістра, вихід якого підключено до входу дешифратора, вихідні шини якого попарно підключено до входів елементів АБО першої групи, виходи яких підключено до входу шифратора (А. с. СРСР № 1034036, кл. G06F 7/72, 1982р.).

Недоліком відомого пристрою (аналога) - низькі функціональні можливості, що обумовлено неможливістю піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа.

Відомий пристрій (прототип) для піднесення чисел до квадрату за модулем m містить вхідний та вихідний регістри, першу групу елементів АБО, першу групу елементів І, дешифратор і шифратор. При цьому вхід пристрою підключено до входу вхідного регістра, вихід якого піднесено до входу дешифратора, вихідні шини якого попарно (сума чисел, що присвоєна кожній парі чисел дорівнює значенню модулю т) підключено до входів елементів АБО першої групи, виходи яких підключено до входу шифратора. В пристрій додатково введено в другу групу елементів І, суматор за модулем т, другу групу елементів АБО. При цьому вихід шифратора підключено до перших входів елементів І першої та другої груп. До других входів елементів І першої та другої груп підключено відповідно шини ознаки числового діапазону реалізації операції піднесення чисел до квадрату за модулем для додатного (+) та від'ємного (-). Виходи елементів І другої групи підключено до перших входів суматора за модулем т, до других входів якого підключено шини подачі значення т/2. Виходи елементів І першої групи та суматора за модулем т через другу групу елементів АБО підключено до входу вихідного регістра, вихід якого є виходом пристрою (Патент на корисну модель № 39493, Україна, МКП G06F 7/60. Бюл. № 4,2009р.).

Недолік прототипу - низькі функціональні можливості, що обумовлено неможливістю піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа. Прототип може виконувати операцію піднесення цілих чисел до квадрату за лише за одним модулем, а не за всіма модулями КЛ.

Задача корисної моделі - розширення функціональних можливостей пристрою за рахунок піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа.

Поставлена задача вирішується тим, що пристрій для піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа, що містить вхідний і вихідний регістри, групу елементів АБО, першу та другу групи елементів І, при цьому вхід пристрою підключено до входу вхідного регістра, а вихід вихідного регістра якого є виходом пристрою, що введено третю, четверту та п'яту групи елементів І, перший і другий прийомні регістри, регістр пам'яті, групу з n множників за модулями $m_i(i=\overline{1,n})$, при цьому вихід вхідного регістра підключено до перших входів елементів І першої та другої груп, шина додатної ознаки підключена до других входів елементів І першої групи, а шина від'ємної ознаки підключена до других входів елементів І другої групи, виходи елементів І першої та другої груп підключено до перших входів відповідно першого та другого суматорів, виходи яких через перший та другий входи елементів АБО групи підключено до входу першого прийомного регістра та до входу регістра пам'яті, виходи підрегістрів яких підключено до перших входів елементів І відповідно третьої та четвертої груп, до других входів яких підключена перша шина керування пристрою, до других входів першого та другого суматорів підключена шина подачі значення $\frac{M}{2}(M=\prod_{i=1}^{n} m_i)$, виходи елементів І відповідно третьої та четвертої груп підключено до перших і других входів множників за модулями $m_i$ групи, виходи яких підключено до відповідних підрегістрів другого прийомного регістра, вихід якого підключено до третього входу елементів АБО групи та до

Корисна модель належить до області обчислювальної техніки і призначена для піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа.

Відомий пристрій (аналог), що містить елементи І та АБО, вхідний та вихідний регістри, групи елементів І та АБО. При цьому вхід пристрою підключено до входу вхідного регістра, вихід якого підключено до входу дешифратора. Виходи дешифратора попарно підключені до входів елементів АБО. Вихід вихідного регістра підключено до виходу пристрою (А. с. СРСР № 1095172, кл. G06F 7/72,1984р.).

Недоліком відомого пристрою (аналога) є низькі функціональні можливості, що обумовлено неможливістю піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа.

Відомий пристрій (аналог) для піднесення чисел до квадрату за модулем, що Містить вхідний та вихідний регістри, першу групу елементів АБО, першу групу елементів І, дешифратор, шифратор та ін. При цьому вхід пристрою підключено до входу вхідного регістра, вихід якого підключено до входу дешифратора, вихідні шини якого попарно підключено до входів елементів АБО першої групи, виходи яких підключено до входу шифратора (А. с. СРСР № 1034036, кл. G06F 7/72, 1982р.).

Недоліком відомого пристрою (аналога) - низькі функціональні можливості, що обумовлено неможливістю піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа.

Відомий пристрій (прототип) для піднесення чисел до квадрату за модулем m містить вхідний та вихідний регістри, першу групу елементів АБО, першу групу елементів І, дешифратор і шифратор. При цьому вхід пристрою підключено до входу вхідного регістра, вихід якого піднесено до входу дешифратора, вихідні шини якого попарно (сума чисел, що присвоєна кожній парі чисел дорівнює значенню модулю т) підключено до входів елементів АБО першої групи, виходи яких підключено до входу шифратора. В пристрій додатково введено в другу групу елементів І, суматор за модулем т, другу групу елементів АБО. При цьому вихід шифратора підключено до перших входів елементів І першої та другої груп. До других входів елементів І першої та другої груп підключено відповідно шини ознаки числового діапазону реалізації операції піднесення чисел до квадрату за модулем для додатного (+) та від'ємного (-). Виходи елементів І другої групи підключено до перших входів суматора за модулем т, до других входів якого підключено шини подачі значення т/2. Виходи елементів І першої групи та суматора за модулем т через другу групу елементів АБО підключено до входу вихідного регістра, вихід якого є виходом пристрою (Патент на корисну модель № 39493, Україна, МКП G06F 7/60. Бюл. № 4,2009р.).

Недолік прототипу - низькі функціональні можливості, що обумовлено неможливістю піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа. Прототип може виконувати операцію піднесення цілих чисел до квадрату за лише за одним модулем, а не за всіма модулями КЛ.

Задача корисної моделі - розширення функціональних можливостей пристрою за рахунок піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа.

Поставлена задача вирішується тим, що пристрій для піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа, що містить вхідний і вихідний регістри, групу елементів АБО, першу та другу групи елементів І, при цьому вхід пристрою підключено до входу вхідного регістра, а вихід вихідного регістра якого є виходом пристрою, що введено третю, четверту та п'яту групи елементів І, перший і другий прийомні регістри, регістр пам'яті, групу з n множників за модулями $m_i(i=\overline{1,n})$, при цьому вихід вхідного регістра підключено до перших входів елементів І першої та другої груп, шина додатної ознаки підключена до других входів елементів І першої групи, а шина від'ємної ознаки підключена до других входів елементів І другої групи, виходи елементів І першої та другої груп підключено до перших входів відповідно першого та другого суматорів, виходи яких через перший та другий входи елементів АБО групи підключено до входу першого прийомного регістра та до входу регістра пам'яті, виходи підрегістрів яких підключено до перших входів елементів І відповідно третьої та четвертої груп, до других входів яких підключена перша шина керування пристрою, до других входів першого та другого суматорів підключена шина подачі значення $\frac{M}{2}(M=\prod_{i=1}^{n} m_i)$, виходи елементів І відповідно третьої та четвертої груп підключено до перших і других входів множників за модулями $m_i$ групи, виходи яких підключено до відповідних підрегістрів другого прийомного регістра, вихід якого підключено до третього входу елементів АБО групи та до

перших входів елементів І п'ятої групи, виходи яких підключено до входу вихідного регістра, до других входів елементів І п'ятої групи підключена друга шина керування пристрою.

Даний ефект досягається за рахунок представлення чисел А у КЛ для піднесення до степеня k натурального числа у штучній А' формі (ШФ).

При цьому маємо, що

$$\begin{cases} A' = \frac{M}{2} + |A|, \text{якщо } A \geq 0, \\ A' = \frac{M}{2} - |A|, \text{якщо } A < 0 \end{cases}$$

тобто, для додатних чисел маємо $A' = \frac{M}{2} + |A|$, а для від'ємних - $A' = \frac{M}{2} - |A|$. В цьому випадку маємо

$$\begin{cases} -\frac{M}{2} \leq A \leq \frac{M}{2} - 1, \\ 0 \leq A' \leq M - 1. \end{cases}$$

На кресленні (фіг. 1) представлена блок-схема корисної моделі, де: 1 - вхід пристрою; 2 - вхідний регістр; 3 - вихідний регістр; 4 - вихід пристрою; 5, 6 - перша та друга групи елементів І; 7, 8 - шини додатної та від'ємної ознак; 9, 10 - перший та другий суматори; 11 - елементи АБО групи; 12 - перший прийомний регістр; 13 - регістр пам'яті, у якому постійно зберігається значення А'; 14, 15 - третя та четверта групи елементів І; 16 - М перша шина керування пристрою; 17 - шина подачі значення $\frac{M}{2}$; $18_1 \div 18_n$ - множники $(a_i' \cdot a_i')\text{mod}m_i = (a_i')^2 \text{mod}m_i$ за модулями $m_i$ групи 18; 19 - другий прийомний регістр; 20 - п'ята група елементів І; 21 - друга шина керування пристрою.

На кресленні (фіг. 2) представлена блок-схема корисної моделі, для КЛ, що задано основами $m_1 = 2,\ m_2 = 5, m_3 = 7$.

Вхід 1 пристрою підключено до входу вхідного 2 регістра. Вихід вихідного регістра 3 є виходом 4 пристрою. Вихід вхідного 2 регістра підключено до перших входів елементів І першої 5 та другої 6 груп. Шина 7 додатної ознаки підключена до других входів елементів І першої 5 групи, а шина 8 від'ємної ознаки підключена до других входів елементів І другої 6 групи. Виходи елементів І першої 5 та другої 6 груп підключено до перших входів відповідно першого 9 та другого 10 суматорів, виходи яких через перший та другий входи елементів АБО групи 11 підключено до входу першого 12 прийомного регістра та до входу регістра 13 пам'яті, виходи підрегістрів яких підключено до перших входів елементів І відповідно третьої 14 та четвертої 15 груп, до других входів яких підключена перша 16 шина керування пристрою. До других входів першого 9 та другого 10 суматорів підключена шина 17 подачі значення $\frac{M}{2}(M = \prod_{i=1}^{n} m_i)$. Виходи елементів І відповідно третьої 14 та четвертої 15 груп підключено до перших і других входів множників $18_1 - 18_n$ за модулями $m_i (i = \overline{1,n})$ групи 18, виходи яких підключено до відповідних підрегістрів другого 19 прийомного регістра, вихід якого підключено до третього входу елементів АБО групи 11 та до перших входів елементів І п'ятої 20 групи, виходи яких підключено до входу вихідного регістра 3. До других входів елементів І п'ятої 20 групи підключена друга 21 шина керування пристрою.

Пристрій функціонує наступним чином (фіг. 1). За шиною 1 в регістр 2 надходить число $A = (a_1 \| a_2 \| .. \| a_i \| .. \| a_n)$, (де - $\|$ математичний знак, що визначає операцію сполучення (склеювання)), що представлено у КЛ. В залежності від наявності сигналу шин 7 або 8 значення А через відповідні елементи І першої 5 або другої 6 групи надходить до входів першого 9 або другого 10 суматорів, з виходів яких значення $A' = \frac{M}{2} + |A|$ або $A' = \frac{M}{2} - |A|$ через елементи АБО 11 групи одночасно надходять до входів першого 12 прийомного регістра та регістра 13 пам'яті. Сигнал першої 16 керуючої шини одночасно відкриває всі елементи І третьої 14 і четвертої 15 груп. В цьому випадку з виходів підрегістрів регістрів 12 і 13 значення лишків $a_i'$ через відкриті елементи І третьої 14 і четвертої 15 груп надходять до першого та другого входів відповідних і-х

множників $18_i$ $(i=\overline{1,n})$ за модулями $m_i$ групи 18, з виходів яких значення $(a_i')^2 \bmod m_i$ надходять до входів відповідних підрегістрів другого 19 прийомного регістра, з виходу якого значення $(A')^2$ через елементи АБО групи 11 надходить до входу регістра 12 і до перших (інформаційних) входів елементів І п'ятої 20 групи. Якщо $k=2$, тоді присутній сигнал другої 21 шини керування, що відкриває елементи І п'ятої 20 групи. Тоді значення $(A')^2$ надходить до входу регістра 3. Якщо $k>2$, тоді сигнал другої 21 шини керування відсутній і елементи І п'ятої 20 групи закриті. В цьому випадку з виходів підрегістрів регістра 12 значення лишків $(a_i')^2 \bmod m_i$ через відкриті елементи І третьої 14 групи надходять до перших входів відповідних і-х множників $18_i$ за модулями $m_i$ групи 18, до других входів яких з виходів підрегістрів регістра 13 значення лишків $a_i'$ через відкриті елементи І четвертої 15 групи надходять до других входів відповідних і-х множників $18_i$ за модулями $m_i$ групи 18, з виходів яких значення $(a_i')^3 \bmod m_i$ надходять до входів відповідних підрегістрів другого 19 прийомного регістра, з виходу якого значення $(A')^3$ через елементи АБО групи 11 надходить до входу регістра 12 і до перших (інформаційних) входів елементів І п'ятої 20 групи. У подальшому сигнал шини 21 буде присутній тільки тоді, коли значення $k$ буде остаточним. В цьому випадку на виході 4 пристрою буде значення $A^k$, що визначається.

Розглянемо приклади конкретної реалізації операції $A^k$ піднесення цілих чисел А, що представлені у КЛ основами $m_1=2$, $m_2=5$, $m_3=7$, до степеня к натурального числа. При цьому $M=70$, $\frac{M}{2}=35=(1\|0\|0)$. В таблиці представлено кодові слова А і А′ у КВ.

Таблиця

Кодові слова А та А′ у КЛ

| А | А′ | А | А′ | А | А′ | А | А′ | А | А′ |
|---|---|---|---|---|---|---|---|---|---|
| -35 | 0 | -20 | 15 | -5 | 30 | 10 | 45 | 25 | 60 |
| -34 | 1 | -19 | 16 | -4 | 31 | 11 | 46 | 26 | 61 |
| -33 | 2 | -18 | 17 | -3 | 32 | 12 | 47 | 27 | 62 |
| -32 | 3 | -17 | 18 | -2 | 33 | 13 | 48 | 28 | 63 |
| -31 | 4 | -16 | 19 | -1 | 34 | 14 | 49 | 29 | 64 |
| -30 | 5 | -15 | 20 | 0 | 35 | 15 | 50 | 30 | 65 |
| -29 | 6 | -14 | 21 | 1 | 36 | 16 | 51 | 31 | 66 |
| -28 | 7 | -13 | 22 | 2 | 37 | 17 | 52 | 32 | 67 |
| -27 | 8 | -12 | 23 | 3 | 38 | 18 | 53 | 33 | 68 |
| -26 | 9 | -11 | 24 | 4 | 39 | 19 | 54 | 34 | 69 |
| -25 | 10 | -10 | 25 | 5 | 40 | 20 | 55 | - | - |
| -24 | 11 | -9 | 26 | 6 | 41 | 21 | 56 | - | - |
| -23 | 12 | -8 | 27 | 7 | 42 | 22 | 57 | - | - |
| -22 | 13 | -7 | 28 | 8 | 43 | 23 | 58 | - | - |
| -21 | 14 | -6 | 29 | 9 | 44 | 24 | 59 | - | - |

Приклади визначення величини $A^k$ (табл.).

Приклад 1.

Нехай $A=2=(0\|2\|2)$ і $k=2$. Визначити $A^k=2^2$. По шині 1 значення $A=2=(0\|2\|2)$ у КЛ надходить до входу регістра 2. Так, як $A=2>0$, тоді присутній сигнал шини 7. У цьому випадку з виходу суматора 9, через елементи АБО 11 значення $A'=\frac{M}{2}=+A=35+2=(1\|0\|0)+(0\|2\|2)=(1\|2\|2)=37$ у КЛ надходить до входів регістра 12 і 13, з виходів яких через відкриті елементи І груп 14 і 15 значення лишків числа $A'=(1\|2\|2)$ надходять на входи відповідних множників 18. З виходів множників $18_1 \div 18_3$ значення $(1\cdot 1)\bmod 2$,

$(1\cdot 1)\bmod 5$ та $(1\cdot 1)\bmod 7$ надходять на входи відповідних підрегістрів регістра 19. За умовою $k=2$, тоді присутній сигнал шини 21, який відчиняє елементи I групи 20, і значення результату операції $(A')^2=(1\|4\|4)$ надходить до входу регістра 3.

Перевірка:

$(A')^2=37^2=37\times 37=1369=39(\bmod 70)=(1\|2\|2)\times(1\|2\|2)=(1\|4\|4)=39$;

$(A')^2=\frac{M}{2}+A^2$,

$A^2=(A^2)'-\frac{M}{2}$,

$2^2=39-35$,

$2^2=4$.

Приклад 2.

Нехай $A=-2$ $(2=(0\|2\|2))$ і $k=2$. У цьому випадку присутній сигнал шини 8 $(A=-2<0)$. З виходу суматора 10 значення $A'=\frac{M}{2}-A=35-2=(1\|0\|0)-(0\|2\|2)=(1\|3\|5)=33$ надходить у КЛ до входів регістра 12 і 13. З виходів множників $18_1\div 18_3$ значення $1\cdot 1=1(\bmod 2)$, $3\cdot 3=4(\bmod 5)$ та $5\cdot 5=4(\bmod 7)$ надходять на входи відповідних підрегістрів регістра 19. За умовою $k=2$, тоді присутній сигнал шини 21, який відчиняє елементи I групи 20, і значення результату операції $(A')^2=(1\|4\|4)$ надходить до входу регістра 3.

Перевірка:

$(A')^2=33^2=33\times 33=1089=39(\bmod 70)=(1\|3\|5)\times(1\|3\|5)=(1\|4\|4)=39$;

$A^2=(A^2)'-\frac{M}{2}$,

$(-2^2)=39-35$,

$(-2^2)=4$.

Приклад 3.

Нехай $A=2$ $(0\|2\|2)$ і $k=3$. Якщо $A=2>0$, тоді присутній сигнал шини 7. В цьому випадку з виходу суматора 9, значення $A'=\frac{M}{2}+A=35+2=37=(1\|0\|0)+(0\|2\|2)=(1\|2\|2)=37$ надходить до регістрів 12 і 13. З виходів множників $18_1\div 18_3$ значення $1\cdot 1=1(\bmod 2)$, $2\cdot 2=4(\bmod 5)$ та $2\cdot 2=4(\bmod 7)$ надходять на входи відповідних підрегістрів регістра 19. За умовою $k=3$, тоді сигнал шини 21 відсутній, і значення $(A')^2=(1\|4\|4)$ надходить до входу регістра 12. У цьому випадку з виходів множників $18_1\div 18_3$ значення $1\cdot 1=1(\bmod 2)$, $4\cdot 2=3(\bmod 5)$ та $4\cdot 2=1(\bmod 7)$, надходять на входи відповідних підрегістрів регістра 19. Так, як $k=3$, то після третього множення $(A')\times(A')\times(A')$ числа $A'$ сигнал шини 21 присутній, і результат операції $A^k=2^3$ (значення $(A')^3=(1\|3\|1)$) надходить до входу під регістра 3.

Перевірка:

$(A')^3=37^3=50653=43(\bmod 70)=(1\|2\|2)\times(1\|2\|2)\times(1\|2\|2)=(1\|3\|1)=43$;

$A^3=(A^3)'-\frac{M}{2}$,

$2^3=43-35$,

$2^3=8$.

Приклад 4.

Нехай $A=-2$ $(2=(0\|2\|2))$, $k=3$. Якщо $A=-2<0$, тоді присутній сигнал шини 8. З виходу суматора 10, значення $A'=\frac{M}{2}-A=35-2=(1\|0\|0)-(0\|2\|2)=(1\|3\|5)=33$ надходить до входів регістрів 12 і 13. З виходів множників $18_1 \div 18_3$ за першою ітерацією множення $A'\times A'=(A')^2$ отримаємо наступні значення $1\cdot 1=1(\mathrm{mod}2)$, $3\cdot 3=4(\mathrm{mod}5)$ та $5\cdot 5=4(\mathrm{mod}7)$. Так, як $k=3$ проведемо другу ітерацію множення $(A')^2\times A'$. У цьому разі з виходів множників $18_1 \div 18_3$ отримуємо результат операції у вигляді $(A')^3=(A')^2\times A'=(1\|4\|4)\times(1\|3\|5)=(1\|2\|6)=27$.

Перевірка:

$(A')^3=33^3=35937=27(\mathrm{mod}\,70)=A'\times A'\times A'=(1\|3\|5)\times(1\|3\|5)\times(1\|3\|5)=(1\|2\|6)=27$;

$A^3=(A^3)'-\frac{M}{2}$,

$(-2)^3=27-35$,

$(-2)^3=-8$.

Приклад 5.

Нехай $A=-3$ $(3=(1\|3\|3))$, $k=3$. Якщо $A=-3<0$, тоді присутній сигнал шини 8. З виходу суматора 10, значення $A'=\frac{M}{2}-A=35-2=(1\|0\|0)-(1\|3\|3)=(0\|2\|4)=32$ надходить до входів регістрів 12 і 13. З виходів множників $18_1 \div 18_3$ за першою ітерацією $A'\times A'=(A')^2=(0\|2\|4)\times(0\|2\|4)=(0\|4\|2)$ отримаємо, що у регістрі 19 значення $(A')^2=(0\|4\|2)$. Так, як $k=3$ проводимо другу ітерацію множення $(A')^2\times A'=(A')^3=(0\|4\|2)\times(0\|2\|4)=(0\|3\|1)$. Таким чином на виході 4 маємо результат операції $A^k=(-3)^3=(0\|3\|1)$.

Перевірка:

$(A')^3=32^3=32768=8(\mathrm{mod}\,70)=A'\times A'\times A'=(0\|2\|4)\times(0\|2\|4)\times(0\|2\|4)=(0\|2\|4)=(0\|3\|1)=8$;

$A^3=(A^3)'-\frac{M}{2}$,

$(-3)^3=8-35$,

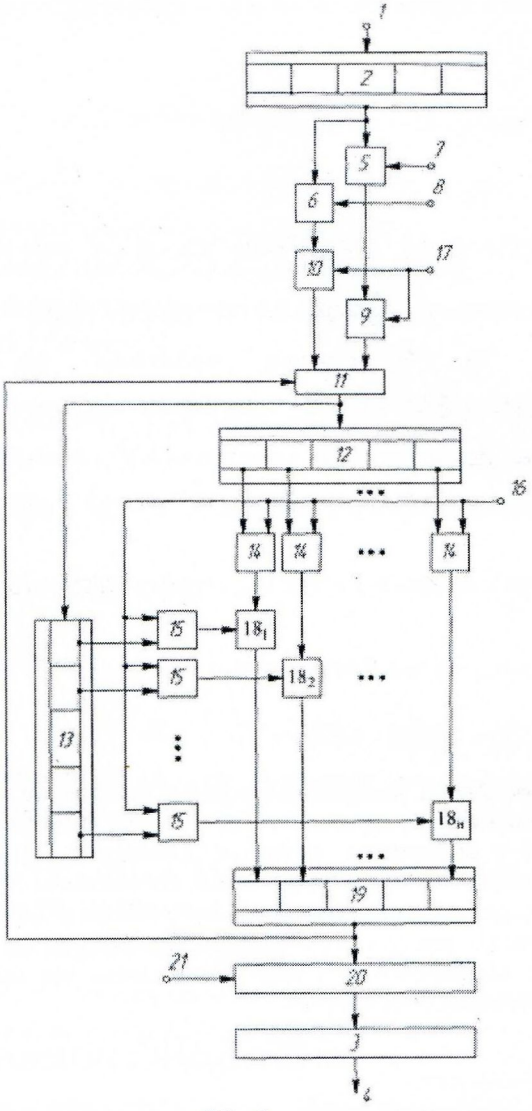
$(-3)^3=-27$.

Технічний результат від використання даної корисної моделі, полягає в реалізації операції для піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа, як у додатному так і у від'ємному числових діапазонах. Це значно розширює функціональні можливості пристрою-прототипу. Даний ефект досягається за рахунок представлення чисел A у КЛ для піднесення до степеня $k$ натурального числа у ШФ $A'$. Приклади реалізації операції піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа, як у додатному так і у від'ємному числових діапазонах, що приведено у опису, підтверджують практичну доцільність корисної моделі.

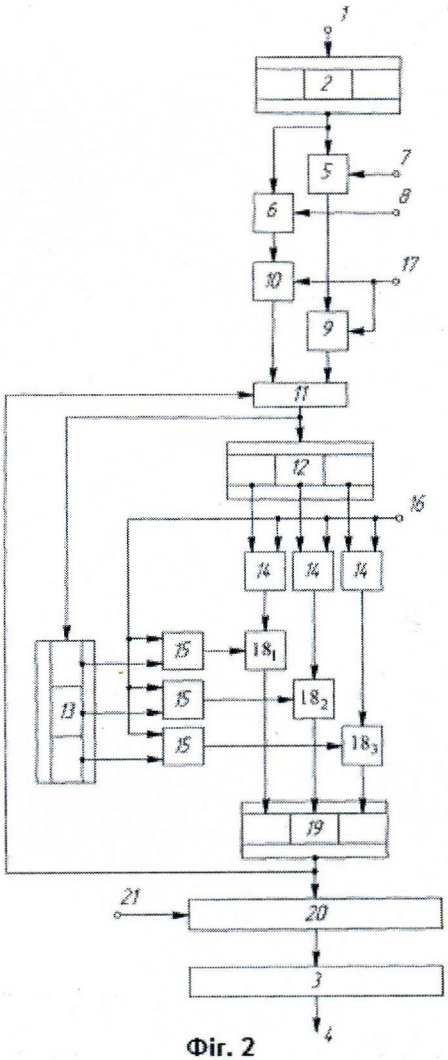
## ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій для піднесення цілих чисел, що представлені у класі лишків, до степеня натурального числа, що містить вхідний і вихідний регістри, групу елементів АБО, першу та другу групи елементів І, при цьому вхід пристрою підключено до входу вхідного регістра, а вихід вихідного регістра якого є виходом пристрою, який **відрізняється** тим, що введено третю, четверту та п'яту групи елементів І, перший і другий прийомні регістри, регістр пам'яті, групу з $n$ множників за модулями $m_i(i=\overline{1,n})$, при цьому, вихід вхідного регістра підключено до перших входів елементів І першої та другої груп, шина додатної ознаки підключена до других входів елементів І першої групи, а шина від'ємної ознаки підключена до других входів елементів І другої групи, виходи елементів І першої та другої груп підключено до перших входів відповідно першого та другого суматорів, виходи яких через перший та другий входи елементів АБО групи підключено до входу першого прийомного регістра та до входу регістра пам'яті, виходи підрегістрів яких

підключено до перших входів елементів І відповідно третьої та четвертої груп, до других входів яких підключена перша шина керування пристрою, до других входів першого та другого суматорів підключена шина подачі значення $\frac{M}{2}(M=\prod_{i=1}^{n} m_i)$, виходи елементів І відповідно третьої та четвертої груп підключено до перших і других входів множників за модулями $m_i$ групи, виходи яких підключено до відповідних підрегістрів другого прийомного регістра, вихід якого підключено до третього входу елементів АБО групи та до перших входів елементів І п'ятої групи, виходи яких підключено до входу вихідного регістра, до других входів елементів І п'ятої групи підключена друга шина керування пристрою.




**Фіг. 1**




**Фіг. 2**

Комп'ютерна верстка І. Мироненко

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601