УДК 531.38

©2012. **А. Г. Матюхіна, Л. Л. Оридорога**

ПОДІЛЬНІСТЬ ЕЛЕМЕНТІВ ЗВОРОТНИХ ПОСЛІДОВНОСТЕЙ

Нехай u_n – n-е число Фібоначчі, p – просте число. Тоді, якщо 5-квадратичний лишок у полі лишків за модулем p, то $u_{n(p-1)} \equiv 0(\mathrm{mod} p)$, якщо 5-квадратичний нелишок, то $u_{n(p+1)} \equiv 0(\mathrm{mod} p)$. Дається узагальнення цього результату на довільні зворотні послідовності другого порядку.

Ключові слова: *подільність, послідовність, лишок, поле, число Фібоначчі, формула Біне.*

1. Вступ. У даній роботі досліджено різні задачі на подільність чисел, що задаються арифметичними виразами від кореня з цілого числа D – дискримінанта характеристичного рівняння зворотних послідовностей II-го порядку. В залежності від того, чи є D квадратичним лишком за даним простим модулем p, застосовується один з двох методів. Якщо D є квадратичним лишком за модулем p, то цей вираз сам є елементом поля лишків за модулем p. Інакше він є елементом розширення даного поля другого порядку, побудованого за допомогою елемента $\sqrt{D}$. В першому випадку для дослідження подільності застосовується мала теорема Ферма, в другому – її аналог для скінченних полів.

Отримані результати застосовуються для дослідження подільності спочатку чисел Фібоначчі, а потім елементів довільних зворотних послідовностей на прості числа p. При цьому відповідь суттєво відрізняється, в залежності від того, чи є дискримінант характеристичного рівняння послідовності квадратичним лишком за модулем p.

Подільність елементів зворотних послідовностей вивчалася багатьма авторами (див., наприклад, роботи [5]-[7]). У роботі [5] доведено, якщо просте число має вигляд $5t+1$ або $5t+1$, то $p-1$ елемент послідовності ділиться на p. Це доведено завдяки тому, що біноміальний коефіцієнт із p по k ділиться на p, де p – просте [5]. У даній роботі результат про подільність чисел Фібоначчі отримується завдяки розгляданню розширення поля лишків, побудованого за допомогою елемента $\sqrt{D}$,та застосуванню аналога малої теореми Ферма для скінченних полів.

2. Додаткові позначення.

Z_p – поле лишків за модулем p. Порядок Z_p дорівнює p.

Z_p^* – мультиплікативна група скінченного поля Z_p. Порядок Z_p^* дорівнює $p-1$.

$Z_p[\xi]$ – множина, яка вийшла розширенням поля Z_p за допомогою ξ-кореня незвідного рівняння II-го ступеня, а саме $\xi^2 - D = 0$. Множина $Z_p[\xi]$ є полем, так як виконуються всі властивості поля. Порядок поля $Z_p[\xi]$ дорівнює p^2.

$a+b\xi$ та $c+d\xi$ та $e+f\xi$ – елементи поля $Z_p[\xi]$ $(a,b,c,d,e,f \in Z_p)$.

$Z[\xi]^*$ – мультиплікативна група скінченного поля $Z[\xi]$. Порядок $Z[\xi]^*$ дорівнює p^2-1.

This work was awarded the Gold Medal from Yale Science & Engineering Association for Most Outstanding Eleventh Grade Exhibit in Mathematics at the Intel Isef 2011 Science Fair

3. Випадок, коли дискримінант характеристичного рівняння є квадратичним лишком у полі лишків за простим модулем p.

$a_i = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^i - \left(\frac{1-\sqrt{5}}{2}\right)^i\right)$ – формула Біне для обчислення і-го члена послідовності Фібоначчі.

При $i = n(p-1)$, $n \in Z$, p – просте, формула Біне має вигляд:

$$a_{n(p-1)} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n(p-1)} - \left(\frac{1-\sqrt{5}}{2}\right)^{n(p-1)}\right).$$

Якщо 5-квадратичний лишок за модулем p (у полі Z_p), то $\frac{1+\sqrt{5}}{2} \equiv x(\mathrm{mod}p)$ та $\frac{1-\sqrt{5}}{2} \equiv y(\mathrm{mod}p)$, тоді формула Біне перетворюється у такий вигляд:

$$a_{n(p-1)} = \frac{1}{\sqrt{5}}(x^{n(p-1)} - y^{n(p-1)}) \quad x, y \in Z_p,$$

($p \neq 2$ та $p \neq 5$ – так як формула Біне у Z_2 та у Z_5 має ділення на нуль).

По малій теоремі Ферма – при p простому і m, яке не ділиться на p, маємо:

$$m^{p-1} \equiv 1(\mathrm{mod}p).$$

Якщо $m = x^n$ та $x \neq 0(\mathrm{mod}p)$, тоді $x^{n(p-1)} \equiv 1(\mathrm{mod}p)$.
Якщо $m = y^n$ та $y \neq 0(\mathrm{mod}p)$, тоді $y^{n(p-1)} \equiv 1(\mathrm{mod}p)$.
У результаті отримаємо:

$$a_{n(p-1)} \equiv \frac{1}{\sqrt{5}}(1-1)(\mathrm{mod}p);$$

$$a_{n(p-1)} \equiv 0(\mathrm{mod}p).$$

Теорема про подільність елементів послідовності Фібоначчі. *Якщо 5-квадратичний лишок у полі лишків за модулем p, у $Z_p, p \neq 2$ та $p \neq 5$, то $a_{n(p-1)}$ член послідовності Фібоначчі $\{a_i\}$ націло ділиться на p, $a_{n(p-1)} \equiv 0(mod p)$ $n \in Z, p$ – просте.*

Узагальнюючи висновок про подільність елементів послідовності Фібоначчі $\{a_i\}$ до будь-якої зворотної послідовності $\{u_i\}$, маємо:

нехай $u_0 = 0$ – виконується для будь-якої зворотної послідовності $\{u_i\}$, тоді вираз для обчислення $n(p-1)$ члена послідовності $\{u_i\}$ має вигляд:

$$u_{n(p-1)} = \frac{\gamma}{\sqrt{D}}\left(\left(\frac{a_0+\sqrt{D}}{2}\right)^{n(p-1)} - \left(\frac{a_0-\sqrt{D}}{2}\right)^{n(p-1)}\right), \quad \gamma \in R, \qquad (1)$$

D – дискримінант характеристичного рівняння $q^2 = a_0 q + b_0$, зворотної послідовності $u_{i+2} = a_0 u_{i+1} + b_0 u_i$ $(a_0, b_0 \in Z)$, $\frac{a_0+\sqrt{D}}{2}$ та $\frac{a_0-\sqrt{D}}{2}$ – корені характеристичного рівняння.

Розглядаючи D, як квадратичний лишок у Z_p, та застосовуючи до виразу (1) малу теорему Ферма, маємо:

$$u_{n(p-1)} \equiv 0(\mathrm{mod}p),$$

$p \neq 2$ та $D \neq 0(\mathrm{mod}p)$ – так як у виразі (1) є ділення на ці числа, $b_0 \neq 0(\mathrm{mod}p)$ – так як один із коренів характеристичного рівняння при $b_0 \equiv 0(\mathrm{mod}p)$ дорівнює нулю.

Теорема про подільність елементів зворотних послідовностей II-го порядку. *Якщо дискримінант характеристичного рівняння зворотної послідовності II-го порядку $\{u_i\}$ є квадратичним лишком за даним простим модулем p, то $u_{n(p-1)}$ член $\{u_i\}$ націло ділиться на p, $u_{n(p-1)} \equiv 0(modp)$, $n \in Z$, p – просте.*

4. Випадок, коли дискримінант характеристичного рівняння є квадратичним нелишком у полі лишків за простим модулем p. Так як порядок елемента – це ступінь, в який потрібно звести елемент, щоб отримати 1 [3]. Порядок елемента дорівнює порядку циклічної підгрупи, яка містить цей елемент (це випливає через обмеженість підгрупи) [3]. У всякої скінченної групи порядок будь-якої підгрупи є дільником порядку самої групи (теорема Лагранжа). Із цього випливає, що будь-який елемент групи скінченного поля, зведений у порядок цієї групи, дорівнює 1.

Застосовуючи дану теорему до груп $Z_p[\xi]^*$ та Z_p^*, маємо:

– будь-який елемент із $Z_p[\xi]^*$, зведений до p^2-1, дорівнює 1, тому $(a+b\xi)^{p^2-1} = 1$;

– будь-який елемент із Z_p^*, зведений до $p-1$ дорівнює 1, тому $c^{p-1} = 1, c \in Z_p^*$.

У множині $Z_p[\xi]^*$ рівняння $c^{p-1} = 1$ має не більше, ніж $p-1$ коренів. Це випливає із того, що елементів у множині $Z_p^* : p-1$, і кожен із них є коренем цього рівняння, тому інших коренів у цьому рівнянні у полі $Z_p[\xi]^*$ не існує.

А так як $(a+b\xi)^{p^2-1} = ((a+b\xi)^{p+1})^{p-1} = 1$ – за раніше доведеним, тому $(a+b\xi)^{p+1} = c$.

Із цього випливає, що при зведенні будь-якого елемента із $Z_p[\xi]^*$ до степеня $p+1$ ув результаті завжди отримаємо певний елемент, який входить у Z_p^*:

$$(a+b\xi)^{p+1} = a_1, \quad a_1 \in Z_p^*.$$

За допомогою математичної індукції доводиться: якщо спряжені числа із $Z_p[\xi]^*$ звести до степеня n, то отримаємо також спряжені числа, які належать $Z_p[\xi]^*$, тобто

$$\begin{aligned} (a+b\xi)^n &= a_1 + b_1\xi \\ (a-b\xi)^n &= a_1 - b_1\xi \end{aligned} \tag{2}$$

При $n = p+1$ та використовуючи, те що $(a+b\xi)^{p+1} = a_1, a_1 \in Z_p^*$, маємо:

$$\begin{aligned} (a+b\xi)^{p+1} &= a_1, \quad a_1 \in Z_p^* \\ (a-b\xi)^{p+1} &= a_1, \quad a_1 \in Z_p^*. \end{aligned}$$

І тому

$$(a+b\xi)^{p+1} = (a-b\xi)^{p+1} = a_1.$$

Якщо піднести обидві частини рівнянь (2) до степеня $p+1$, отримаємо

$$((a+b\xi)^n)^{p+1} = (a_1+b_1\xi)^{p+1} = a_2$$

$$((a-b\xi)^n)^{p+1} = (a_1-b_1\xi)^{p+1} = a_2.$$

Тому $(a+b\xi)^{n(p+1)} = (a-b\xi)^{n(p+1)}$. Тому у загальному випадку спряжені числа із Z_p^* : $a+b\xi$ та $a-b\xi$, зведені у степінь $n(p+1)$, де $n \in Z$, p – просте, дорівнюють один одному, тобто виконується $(a+b\xi)^{n(p+1)} = (a-b\xi)^{n(p+1)}$.

Застосуємо дані доведення до формули Біне послідовності Фібоначчі $\{a_i\}$:

$$a_i = \frac{1}{\sqrt{5}}\left(\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)^i - \left(\frac{1}{2}-\frac{1}{2}\sqrt{5}\right)^i\right).$$

Якщо $\frac{1}{2} = a$, $\frac{1}{2} = b$, $\sqrt{5} = \xi$, тобто 5-є квадратичним нелишком у Z_p, $i = n(p+1)$, то

$$a_{n(p+1)} = \frac{1}{\sqrt{5}}((a+b\xi)^{n(p+1)} - (a-b\xi)^{n(p+1)}).$$

За раніше доведеним $(a+b\xi)^{n(p+1)} = (a-b\xi)^{n(p+1)}$ маємо:

$$a_{n(p+1)} \equiv 0(\mathrm{mod}p).$$

Теорема про подільність елементів послідовності Фібоначчі. *Якщо 5-квадратичний нелишок у полі лишків за модулем p у $Z_p, p \neq 2$ та $p \neq 5$, то $a_{n(p+1)}$ член послідовності Фібоначчі $\{a_i\}$ націло ділиться на p, $a_{n(p+1)} \equiv 0(mod p), n \in Z, p$ – просте.*

Узагальнюючи висновок про подільність елементів послідовності Фібоначчі $\{a_i\}$ до будь-якої зворотної послідовності $\{u_i\}$, маємо:

$$u_{n(p+1)} = \frac{\gamma}{\sqrt{D}}\left(\left(\frac{a_0}{2}+\frac{1}{2}\sqrt{D}\right)^{n(p+1)} - \left(\frac{a_0}{2}-\frac{1}{2}\sqrt{D}\right)^{n(p+1)}\right), \quad \gamma \in R.$$

При $a = \frac{a_0}{2}$, $b = \frac{1}{2}$, $\xi = \sqrt{D}$, D – квадратичний нелишок у Z_p, тому вираз для знаходження $n(p+1)$ члена послідовності $\{u_i\}$ перетворюється у такий вигляд:

$$u_{n(p+1)} = \frac{\gamma}{\xi}((a+b\xi)^{n(p+1)} - \frac{\gamma}{\xi}((a-b\xi)^{n(p+1)}).$$

А так як $(a+b\xi)^{n(p+1)} = (a-b\xi)^{n(p+1)}$ за раніше доведеним, то

$$u_{n(p+1)} \equiv 0(\mathrm{mod}p).$$

Із цього випливає:

Теорема про подільність елементів зворотних послідовностей II-го порядку. *Якщо дискримінант характеристичного рівняння зворотної послідовності II-го порядку є квадратичним нелишком за даним простим модулем p, то $u_{n(p+1)}$ член довільної зворотної послідовності $\{u_i\}$ націло ділиться на p, $u_{n(p+1)} \equiv 0(mod p)$, $n \in Z$, p – просте.*

1. *Маркушевич А.И.* Возвратные последовательности. – М.: Государственное издательство технико-теоретической литературы, 1950. – 47 с.
2. *Виноградов И.М.* Основы теории чисел. – 9-е изд. – М.: Наука, 1981. – 176 с.
3. *Курош А.Г.* Курс высшей алгебры. — 11-е изд. – М.: Наука, 1975. – 432 с.
4. *Кострикин А.И.* Введение в алгебру. – М.: Просвещение, 2000. – 493 с.
5. *Воробьев Н.Н.* Числа Фибоначчи. – 4-е изд. – М.: Наука, 1978. – 144 с.
6. *Laslo Geroecs* Some properties of divisibility of higher-order linear recursive sequences – Fibonacci Quarterly, 20, 1982. – P. 354-359.
7. *Joseph H. Silverman* Divisibility sequences and powers of algebraic integers.Documenta Math. – Extra Volume Coates, 2006. – P. 711-727.

A. G. Matyukhina, L. L. Oridoroga

Divisibility of recursive sequence elements.

Let u_n be the n-th Fibonacci number and let p be a prime number. We prove that $u_{n(p-1)} \equiv 0(\mathrm{mod}p)$ if 5 is a quadratic residue in Z_p and that $u_{n(p+1)} \equiv 0(\mathrm{mod}p)$ if 5 is the quadratic nonresidue in Z_p. A generalization of this result is also obtained for arbitrary recursive sequences of second order.

Keywords: *divisibility, sequence, residue, field, Fibonacci, Binet formula.*

А. Г. Матюхина, Л. Л. Оридорога

Делимость элементов возвратных последовательностей.

Пусть u_n – n-ое число Фибоначчи, p – простое число. Тогда, если 5-квадратичный вычет в поле вычетов по модулю p, то $u_{n(p-1)} \equiv 0(\mathrm{mod}p)$, если 5-квадратичный невычет, то $u_{n(p+1)} \equiv 0(\mathrm{mod}p)$. Дается обобщение этого результата на произвольные возвратные последовательности второго порядка.

Ключевые слова: *делимость, последовательность, вычет, поле, число Фибоначчи, формула Бине.*

Донецький національний ун-т
`a-l-i-n-a.matyukhina@yandex.ru`

Получено 08.06.12