1 Постановка задачи

На проекте была поставлена задача исследования чисел Фибоначчи, а точнее, их остатков по модулю n. Было известно, что эта последовательность состоит из повторяющейся подпоследовательности (в дальнейшем именуемой периодом или макропериодом). Верхняя оценка для длины периода n^2. Практика показывает, что это слишком грубая оценка. Обычно, для малых n, длина периода сравнима с n. Возник вопрос: нельзя ли получить более точную оценку длины периода.

2 Установленные факты

В процессе работы над проектом удалось установить следующие факты.

1. Макропериод существует.
2. Один макропериод состоит из одного, двух или четырёх микропериодов. (Микропериод - последовательность чисел между двумя нулями)
3. Если брать остатки по модулю p, то $p \pm 1 = 0\ (mod\ d)$. Причём, если p оканчивается на 1 или 9, то в формуле ставится знак - , а если на 3 или на 7 то $+$. (Здесь d - длина микропериода)

3 Доказательства

1. Утверждение. Макропериод существует.

   Доказательство. Так как остаток от деления не превосходит делителя, то остатков от деления на n максимум n. Следовательно, максимально возможное число всех пар чисел n^2. Вся последовательность задаётся одной парой подряд идущих чисел. Первая пара при любом n - 1,1. Следующая, пара - 1,(1+1). Она либо совпадает с первой (в этом случае и дальше будут наблюдаться повторения), либо не совпадает. В этом случае рассмотрим следующую пару. Если она тоже не совпадает ни с одной из предыдущих, то следующую. Поскольку всего пар ограниченное количество, то когда нибудь они закончатся и новая пара станет обязана совпасть с одной из предыдущих.

2. Утверждение. Один макропериод состоит из одного, двух или четырёх микропериодов. (Микропериод - последовательность чисел между двумя нулями)

   Доказательство. Доказано, что последовательность содержит периоды. Для определённости будем считать, что период начинается с первого числа после нуля. Тогда схема макропериода выглядит следующим образом:

   $$1, 1, ..., a, 0, a, a, ..., a^2, 0, a^2, a^2, ..., a^3, 0, a^3, a^3, ..., a^4, 0, ...$$

   Рассмотрим несколько случаев.

(a) a=1

В этом случае у нас всего один микропериод.

(b) $a \neq 1$

В этом случае, применяя формулу $u_n^2 = u_{n-1} \cdot u_{n+1} + (-1)^{n+1}$ для начала второго микропериода, получим, что $a^2 = (-1)^{n+1}$. Отсюда следует, что a^2 равняется либо 1, либо -1, следовательно, $a^4 = 1$, следовательно, больше четырёх микропериодов быть не может. Докажем, что не может быть трёх микропериодов. Рассмотрим два случая.

i. $a^2 = 1$ Это значит, что у нас всего два микропериода.

ii. $a^2 = -1 \Rightarrow a^3 = -a \neq 1$ В этом случае у нас четыре микропериода.

Таким образом, мы доказали, что бывает только один, два или четыре микропериода.

3. Утверждение. Если брать остатки по модулю p, то $p \pm 1 = 0 \ (mod\ d)$. Причём, если p оканчивается на 1 или 9, то в формуле ставится знак - , а если на 3 или на 7 то +. (Здесь d - длина микропериода)

Доказательство.

Лемма: $C_p^a \vdots p$, если p - простое(0<a<p). Доказательство леммы очевидно.

Воспользуемся формулой N-го члена последовательности, биномом Ньютона, малой теоремой Ферма и данной леммой, в результате получим, что

$$u_p = \frac{1}{(\sqrt{5})}\left(\left(\frac{(1+\sqrt{5})}{2}\right)^p - \left(\frac{(1-\sqrt{5})}{2}\right)^p\right) =$$
$$= \frac{1}{2^p\sqrt{5}}\left(C_p^0(\sqrt{5})^0 + C_p^1(\sqrt{5})^1 + \ldots + C_p^k(\sqrt{5})^k + \ldots + C_p^p(\sqrt{5})^p - \right.$$
$$\left. - \left(C_p^0(\sqrt{5})^0 - C_p^1(\sqrt{5})^1 + \ldots + C_p^k(-1)^k(\sqrt{5})^k + \ldots + C_p^p(-1)^p(\sqrt{5})^p\right) =\right.$$
$$= \frac{1}{2^{p-1}(\sqrt{5})}\left(C_p^1(\sqrt{5}) + C_p^3(\sqrt{5})^3 + \ldots + C_p^{2l-1}(\sqrt{5})^{2l-1} + \ldots + C_p^p(\sqrt{5})^p\right) =$$
$$= \frac{1}{2^{p-1}}\left(\sqrt{5}\right)^{p-1} = 5^{\frac{p-1}{2}} \ (mod\ p). \quad (1)$$

Аналогично для u_{p+1} получим, что

$$u_{p+1} = \frac{1}{2^p\sqrt{5}}\left(C_{p+1}^1\sqrt{5} + C_{p+1}^p(\sqrt{5})^p\right) =$$
$$= \frac{1}{2^p}(p+1+(p+1)(\sqrt{5})^{p-1}) = \frac{1+5^{\frac{p-1}{2}}}{2} \ (mod\ p). \quad (2)$$

Так как $5^{\frac{p-1}{2}}$ сравнимо с 1 или -1 в зависимости от p. Если оно равно 1, то $u_p = 1$ и $u_{p+1} = 1$, следовательно, $u_{p-1} = 0$, следовательно, микропериод является делителем p-1. Если оно равняется -1, то $u_{p+1} = 0$ и микропериод является делителем p+1. Докажем, что первый случай реализуется при $p\ mod\ 5$ равным 2 или 3, а второй - при 1 или 4. Чтобы понять, при каких p выражение $5^{\frac{p-1}{2}}$ сравним с 1 или -1, воспользуемся следующей теоремой

$\binom{p}{q} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\binom{q}{p}$, где $\binom{a}{b}$ обозначает символ Лежандра, который равен 1, если a является квадратичным вычетом по модулю b, и -1, если не является.

Отсюда следует, что $\binom{5}{p} = \binom{p}{5}$. Если $\binom{5}{p} = 1$, то p=1 или 4 по модулю 5, если $\binom{5}{p} = -1$, то p=2 или 3 по модулю 5.

Заметим, что в случае, когда $u_p = -1$, а $u_{p+1} = 0$, то есть, когда p даёт остатки 2 и 3 при делении на 5, количество микропериодов как минимум два, так как первый микропериод начинается с единицы, а следующий после u_{p+1} начинается, очевидно, с -1.

4 Картинки Неретина

Картинкой Неретина назовем квадрат n*n с отмеченными в нем точками с координатами вида (u_k,u_{k+1}), где u_k и u_{k+1}- члены исследуемой последовательности.

Было замечено, что некоторые картинки обладают явной симметрией. Например, картинки для многих n, кратных 5, обладают сдвиговой симметрией на вектор $(n/5, 3n/5)$. Есть гипотеза, что это верно для всех, кратных пяти, чисел кроме тех, в разложении которых на простые множители есть простое вида 5n+1.

Была доказана симметрия для простых чисел с микропериодом 2 или 4, которая является поворотной симметрией относительно центра.

Доказательство. В общем виде макропериод имеет следующий вид:

$$1, 1, ..., a, 0, a, a, ..., a^2, 0, a^2, a^2, ..., a^3, 0, a^3, a^3, ..., a^4, 0, ...$$

В случае двух микропериодов $a = -1$, следовательно период имеет следующий вид:

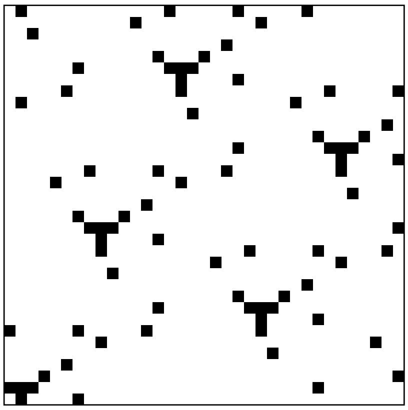
$$1, 1, 2, ..., -2, 1, -1, 0, -1, -1, -2, ..., 2, -1, 1, 0, 1, 1$$

или (то же самое)

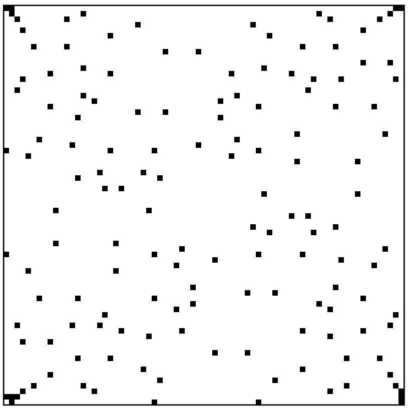
$$1, 1, 2, ..., p-2, 1, p-1, 0, p-1, \text{p}-1, \text{p}-2, ..., 2, p-1, 1, 0, ...$$

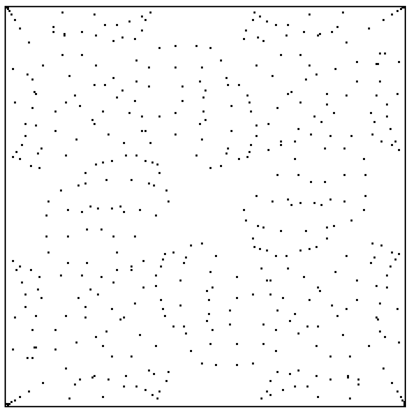
Как видим, для каждой пары имеется три симметричных, кроме пар (1,0),(0,1),(p-1,0),(0,p-1), которые являются исключениями и не имеют симметричных. В случае четырёх микропериодов доказательство аналогично($a^2 = -1$).

5 Примеры картинок Неретина



Пример сдвиговой симметрии. n=35





Просто красивая картинка. n=227.