

Tutorial 3

1. The Fibonacci sequence is defined by $F_0 = 0$, $F_1 = 1$ and $F_i = F_{i-2} + F_{i-1}$ for all $i \geq 2$. (In Question 3 last week we investigated the sequence (F_i) modulo a prime p .)

(i) Suppose that a Fibonacci number F_n is divisible by some positive integer d , and write $F_{n+1} = k$. Show that $F_n \equiv kF_0 \pmod{d}$ and $F_{n+1} \equiv kF_1 \pmod{d}$, and use induction on i to prove that $F_{n+i} \equiv kF_i \pmod{d}$ for all integers $i \geq 0$. [Hint: $kF_0 = k \cdot 0 = 0$; so the first statement you are asked to prove just says $F_n \equiv 0 \pmod{d}$. As for the second, in fact $F_{n+1} = kF_1 = k$.]

(ii) Use Part (i) and induction on j to prove that if $d|F_n$ then $d|F_{jn}$ for all natural numbers j .

Solution.

(i) Observe that $kF_0 = 0$. But $F_n \equiv 0 \pmod{d}$, since $d|F_n$ by hypothesis. Thus $kF_0 \equiv F_n \pmod{d}$. And $kF_1 = k = F_{n+1}$; so certainly $kF_1 \equiv F_{n+1} \pmod{d}$. This shows that the statement “ $kF_{i-1} \equiv F_{n+(i-1)}$ and $kF_i \equiv F_{n+i} \pmod{d}$ ” is true for $i = 1$. Assume now that $i > 1$, and the statement holds with $i - 1$ in place of i . Thus

$$kF_{i-2} \equiv F_{n+(i-2)} \pmod{d}$$

$$kF_{i-1} \equiv F_{n+(i-1)} \pmod{d}$$

and adding these congruences we deduce that

$$kF_i = k(F_{i-2} + F_{i-1}) = kF_{i-2} + kF_{i-1} \equiv F_{n+(i-2)} + F_{n+(i-1)} = F_{n+i}.$$

Since also $kF_{i-1} \equiv F_{n+(i-1)} \pmod{d}$ it follows that the statement holds for i , and hence for all positive integers, by induction. In particular $kF_i \equiv F_{n+i}$ for all natural numbers i , as required.

(ii) Since we are given that $d|F_n$, Part (i) tells us that $F_{n+i} \equiv kF_i \pmod{d}$ for all i , where $k = F_{n+1}$. In particular, if $F_i \equiv 0 \pmod{d}$ then $F_{n+i} \equiv k \cdot 0 \equiv 0 \pmod{d}$. That is, for all i , if $d|F_i$ then $d|F_{n+i}$.

Since $F_0 = 0$ we see that $d|F_{jn}$ is true when $j = 0$. This starts the induction. Now suppose that $j > 0$ and that $d|F_{(j-1)n}$. By what we have just shown, it follows that $d|F_{n+(j-1)n}$; that is, $d|F_{jn}$, as required.

2. Let F_n be as in Question 1. Check that the following matrix formula holds for $n = 1$, $n = 2$ and $n = 3$, and then try to prove it for all positive integers n , using induction:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}.$$

Use this formula, combined with the same formula with n replaced by $2n$, to show that $F_n(F_{n-1} + F_{n+1}) = F_{2n}$, and $F_n^2 + F_{n+1}^2 = F_{2n+1}$. Verify this for $n \leq 5$ by direct calculation.

Solution.

F_0, F_1, F_2, F_3, F_4 are 0, 1, 1, 2, 3. Thus $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} F_1 & F_2 \\ F_2 & F_3 \end{pmatrix}$, and $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} F_2 & F_3 \\ F_3 & F_4 \end{pmatrix}$. So the formula holds when $n = 2$ and $n = 3$.

It is also obviously true at $n = 1$, since

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} F_0 & F_1 \\ F_1 & F_2 \end{pmatrix}.$$

To complete a proof by induction, let $n > 1$ and assume that the formula holds when n is replaced by $n - 1$. That is, assume that

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-1} = \begin{pmatrix} F_{n-2} & F_{n-1} \\ F_{n-1} & F_n \end{pmatrix}.$$

Then it follows that

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} F_{n-2} & F_{n-1} \\ F_{n-1} & F_n \end{pmatrix} \\ &= \begin{pmatrix} F_{n-1} & F_n \\ F_{n-2} + F_{n-1} & F_{n-1} + F_n \end{pmatrix} \\ &= \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}, \end{aligned}$$

and so the formula holds for n , as required.

We have that

$$\begin{pmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{2n} = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix},$$

giving the desired relations when the product on the right hand side is expanded.

$$\begin{aligned} F_1(F_0 + F_2) &= 1 = F_2 & F_1^2 + F_2^2 &= 2 = F_3 \\ F_2(F_1 + F_3) &= 3 = F_4 & F_2^2 + F_3^2 &= 5 = F_5 \\ F_3(F_2 + F_4) &= 8 = F_6 & F_3^2 + F_4^2 &= 13 = F_7 \\ F_4(F_3 + F_5) &= 21 = F_8 & F_4^2 + F_5^2 &= 34 = F_9 \\ F_5(F_4 + F_6) &= 55 = F_{10} & F_5^2 + F_6^2 &= 89 = F_{11} \end{aligned}$$

3. For each prime p , define the *Fibonacci entry point* of p to be the least integer n such that $p|F_n$ (where F_n is as in Questions 1 and 2). The following table shows the Fibonacci entry points of all the primes up to 61.

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61
3	4	5	8	10	7	9	18	24	14	30	19	20	44	16	27	58	15

Use this table and Question 1 above to verify that for $p \leq 61$ the following is true: if $p \equiv \pm 1 \pmod{5}$ then $p|F_{p-1}$, and if $p \equiv \pm 2 \pmod{5}$ then $p|F_{p+1}$. Find all primes p for which $p \not\equiv \pm 1$ and $p \not\equiv \pm 2 \pmod{5}$, and find their Fibonacci entry points.

Solution.

The following table lists the primes p that are congruent to $\pm 2 \pmod{5}$, their Fibonacci entry points, and $p + 1$:

p	2	3	7	13	17	23	37	43	47	53
entry point	3	4	8	7	9	24	19	44	16	27
$p + 1$	3	4	8	14	18	24	38	44	48	54.

The crucial fact to observe is that each number n in the second row is a divisor of the number below it (namely, $p + 1$). By the definition of the Fibonacci entry point, $p|F_n$ in each case, by inspection of the table $n|p + 1$ in each case, and so by Question 1 it follows that $p|F_{p+1}$ in each case.

The next table gives the corresponding information for the primes congruent to $\pm 1 \pmod{5}$:

p	11	19	29	31	41	59	61
entry point	10	18	14	30	20	58	15
$p - 1$	10	18	28	30	40	58	60.

The same argument applies in this case.

Since $\{-2, -1, 0, 1, 2\}$ is a complete system modulo 5, any number that is not congruent to ± 1 or $\pm 2 \pmod{5}$ must be congruent to 0 – that is, divisible by 5. Obviously the only prime with this property is 5 itself. The Fibonacci entry point of 5 is easily checked to be 5.

4. (i) Let p be a prime number, and let $t_1 = 1$. Now define t_i recursively, for $i > 1$, as follows: if $t_i \neq 0$, choose a number s_i such that $s_i t_i \equiv 1 \pmod{p}$ and let t_{i+1} be the residue of $1 + s_i \pmod{p}$. That is to say, t_{i+1} is the unique integer satisfying $0 \leq t_{i+1} < p$ and $(t_{i+1} - 1)t_i \equiv 1 \pmod{p}$. The sequence (t_1, t_2, \dots) stops as soon as we find an integer ℓ such that $t_\ell = 0$. Work out the value of ℓ for the first few prime numbers p , and compare with the table in Question 3. What relationship do you observe? MATH2988 students: prove it.
- (ii) Assuming the relationship you observed persists, show that the Fibonacci entry point of a prime number p can never exceed $p + 1$. (Hint: Show that the sequence (t_i) in (i) cannot have any repeated terms, by considering the first repeated term.)

Solution.

- (i) Taking the primes in increasing order (starting at 2) we find that the sequences (t_i) are as follows.

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

In each case the length of the sequence is one less than the Fibonacci entry point as shown on the table. It is actually not hard to prove this; the key fact is that $F_i t_i \equiv F_{i+1} \pmod{p}$ for all i less than the entry point. When you find that $t_i = 0$, it means that F_{i+1} is divisible by p .

(ii) The sequence (t_i) cannot contain any repeated terms. To see this, let us first prove that $t_k = 1$ only when $k = 1$. Indeed, since $t_{i+1} \equiv 1 + s_i \pmod{p}$, $t_{i+1} = 1$ would mean that $s_i \equiv 0 \pmod{p}$, and this is impossible since $t_i s_i \equiv 1 \pmod{p}$. Now suppose that there are repeated terms, and let t_i be the first term that occurs again later. Then $i > 1$, since we know that 1 is never repeated. Now $t_i = t_j$ for some $j > i$, and the rule for calculating t_i and t_j tells us that $1 + s_{i-1} \equiv t_i = t_j \equiv 1 + s_{j-1}$. Thus $s_{i-1} \equiv s_{j-1}$. But this means that $t_{i-1} = t_{j-1}$, contradicting the fact that t_i is the first term to be later repeated. Since the sequence (t_i) has no repeated terms, its length is at most p . So the Fibonacci entry point is at most $p + 1$.