Algorithm for calculating the Jacobi symbol $(\frac{a}{m})$:

$a = a \bmod m$
$t = 1$
while $(a \neq 0)$
    while (a even)
        $a = a/2$;
        if $(m \equiv 3, 5 \pmod 8)$ then $t = -t$
    $(a, m) = (m, a)$
    if $(a \equiv m \equiv 3 \pmod 4)$ then $t = -t$
    $a = a \bmod m$
if $(m = 1)$ then return t
        else return 0

We see that this algorithm is very similar to Euclid's algorithm. The only significant difference is in the special treatment of factor 2, which we need to extract before we exchange the upper and lower parameter.

Example 4.13. *Calculate* $\left(\frac{105}{317}\right)$.

Solution: We have $\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right) = 1$. ♢

Example 4.14. *Calculate* $\left(\frac{-23}{83}\right)$.

Solution: We have:

$$\left(\frac{-23}{83}\right) = -\left(\frac{23}{83}\right) = \left(\frac{83}{23}\right) = \left(\frac{14}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = \left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right)$$
$$= -\left(\frac{2}{7}\right) = -1.$$ ♢

4.5 Divisibility of Fibonacci numbers

Let us recall that the Fibonacci numbers are defined by $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$, and that they satisfy Binet's formula

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n), \quad \alpha = \frac{1+\sqrt{5}}{2}, \ \beta = \frac{1-\sqrt{5}}{2}.$$

Example 4.15. *Prove that any two consecutive Fibonacci numbers are relatively prime.*

Solution: Let n be a positive integer and $d = \gcd(F_n, F_{n+1})$. Then d divides F_n and F_{n+1}, so it also divides $F_{n+1} - F_n = F_{n-1}$. We conclude that d also divides $F_n - F_{n-1} = F_{n-2}$, $F_{n-1} - F_{n-2} = F_{n-3}, \ldots$ Finally, we find that d divides $F_2 = 1$, so $d = 1$, which needed to be proved. $\diamondsuit$

Proposition 4.12. *Let m and n be positive integers. If n divides m, then F_n divides F_m.*

Proof: Let $m = n \cdot k$. We will prove the statement using the mathematical induction over k. For $k = 1$, the statement is evidently true since $F_n \mid F_n$. Assume that $F_n \mid F_{nk}$. Then, by (1.7),

$$F_{n(k+1)} = F_{nk+n} = F_{nk-1}F_n + F_{nk}F_{n+1}\,.$$

The first summand in this sum is obviously divisible by F_n, and the second is divisible by F_n by the inductive assumption. We conclude that $F_n \mid F_{n(k+1)}$, which needed to be proved. $\square$

Proposition 4.13. *Let n be a composite positive integer different from 4. Then the number F_n is also composite.*

Proof: If n is composite, then it can be written in the form $n = a \cdot b$, where $a, b > 1$. Since $n \neq 4$, at least one of the numbers a, b is greater than 2. Let us say that $a > 2$. Then $F_a \neq F_n$, $F_a \neq 1$, and by Example 4.12, we know that $F_a \mid F_n$. This means that F_n is composite. $\square$

Let us mention that the converse statement of Proposition 4.13 does not hold. Namely, it can happen that a number p is prime and the number F_p is composite. The smallest such number is $F_{19} = 4181 = 37 \cdot 113$. In this manner, we come to the following open problem: are there infinitely many Fibonacci numbers which are prime. The largest known prime Fibonacci number is F_{104911}, and it has $21\,925$ digits.

Proposition 4.14. *Let m and n be positive integers. Then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.*

Proof: Let $m > n$. We apply Euclid's algorithm to the numbers m and n:

$$\begin{aligned}
m &= nq_0 + r_1, \ \text{ where } \ 0 < r_1 < n \\
n &= r_1q_1 + r_2, \ \text{ where } \ 0 < r_2 < r_1 \\
r_1 &= r_2q_2 + r_3, \ \text{ where } \ 0 < r_3 < r_2 \\
&\vdots \\
r_{i-2} &= r_{i-1}q_{i-1} + r_i, \ \text{ where } \ 0 < r_i < r_{i-1} \\
r_{i-1} &= r_iq_i.
\end{aligned}$$

The greatest common divisor is equal to the last remainder of Euclid's algorithm, which is different from zero. Thus, $\gcd(m,n) = r_i$.

Let us now determine the greatest common divisor of the numbers F_m and F_n. From the first step of Euclid's algorithm, we have

$$\begin{aligned}\gcd(F_m, F_n) &= \gcd(F_{nq_0+r_1}, F_n) = \gcd(F_{nq_0-1}F_{r_1} + F_{nq_0}F_{r_1+1}, F_n)\\ &= \gcd(F_{nq_0-1}F_{r_1}, F_n)\,.\end{aligned}$$

By Example 4.15, we know that $\gcd(F_{nq_0-1}, F_{nq_0}) = 1$, so $\gcd(F_{nq_0-1}, F_n) = 1$. We conclude that $\gcd(F_m, F_n) = \gcd(F_{r_1}, F_n)$.

We obtained this from the first step of Euclid's algorithm. By application of the following steps, in the same manner we obtain

$$\gcd(F_{r_1}, F_n) = \gcd(F_{r_2}, F_{r_1}) = \cdots = \gcd(F_{r_i}, F_{r_{i-1}})\,.$$

Since $r_i \mid r_{i-1}$, we have $F_{r_i} \mid F_{r_{i-1}}$ and we conclude that $\gcd(F_{r_i}, F_{r_{i-1}}) = F_{r_i}$. Hence, we proved that $\gcd(F_m, F_n) = F_{r_i} = F_{\gcd(m,n)}$. ♢

Proposition 4.14 shows that if $n \neq 2$, then in Proposition 4.12 the opposite implication is also true, i.e. $F_n \mid F_m \;\Rightarrow\; n \mid m$. Indeed, for $n = 1$, the statement is trivially satisfied. Let $n \geq 3$. If $F_n \mid F_m$, then $\gcd(F_n, F_m) = F_n$. Now, from Proposition 4.14, it follows that $F_{\gcd(m,n)} = F_n$. Since the Fibonacci numbers are all different, except for $F_1 = F_2$, we conclude that $\gcd(m,n) = n$, which means that $n \mid m$. In that way, we proved the following theorem.

Theorem 4.15. *Let m, n be positive integers and $n \neq 2$. Then*

$$F_n \mid F_m \iff n \mid m\,.$$

Corollary 4.16.

(i) A Fibonacci number F_n is even if and only if n is divisible by 3.

(ii) A Fibonacci number F_n is divisible by 3 if and only if n is divisible by 4.

(iii) A Fibonacci number F_n is divisible by 5 if and only if n is divisible by 5.

Example 4.16. *Prove the statement: If $3 \mid n$, then $\gcd(F_n, L_n) = 2$, and if $3 \nmid n$, then $\gcd(F_n, L_n) = 1$.*

Solution: From formula (1.14), i.e. $L_n^2 - 5F_n^2 = 4\cdot(-1)^n$ it follows that the numbers F_n and L_n are either both even or both odd. Let $d = \gcd(F_n, L_n)$. Then $d^2 \mid 4$, so $d = 1$ or $d = 2$. Now, the statement follows from Corollary 4.16.(i). ♢

Example 4.17. *Prove the following statements:*

a) If p is a prime number of the form $10k \pm 1$, then $F_{p-1} \equiv 0 \pmod{p}$.

b) If p is a prime number of the form $10k \pm 3$, then $F_{p+1} \equiv 0 \pmod{p}$.

Solution:

a) From Binet's formula, we have

$$F_{p-1} = \frac{1}{2^{p-2}} \left(\binom{p-1}{1} + \binom{p-1}{3} \cdot 5 + \cdots + \binom{p-1}{p-2} \cdot 5^{(p-3)/2} \right).$$

For $0 < k < p$, $\binom{p-1}{k-1} + \binom{p-1}{k} = \binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!} \equiv 0 \pmod{p}$. Hence, $\binom{p-1}{0} \equiv -\binom{p-1}{1} \equiv \binom{p-1}{2} \equiv -\binom{p-1}{3} \equiv \cdots \equiv \binom{p-1}{p-1} \pmod{p}$, and from $\binom{p-1}{0} = 1$, we get $\binom{p-1}{1} \equiv \binom{p-1}{3} \equiv \cdots \equiv \binom{p-1}{p-2} \equiv -1 \pmod{p}$. By Euler's criterion for the Legendre symbol (Theorem 4.2) and Fermat's little theorem (Theorem 3.10), we have

$$\begin{aligned} 2^{p-1} F_{p-1} &\equiv -2(1 + 5 + \cdots + 5^{(p-3)/2}) \equiv -\frac{5^{(p-1)/2} - 1}{2} \\ &\equiv -\frac{1}{2}\left(\left(\frac{5}{p} \right) - 1 \right) \pmod{p}. \end{aligned}$$

Since $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, and the quadratic residues modulo 5 are 1 and 4, we conclude that $\left(\frac{5}{p}\right) = 1$ if $p \equiv \pm 1 \pmod{10}$, while $\left(\frac{5}{p}\right) = -1$ if $p \equiv \pm 3 \pmod{10}$. Hence, $F_{p-1} \equiv 0 \pmod{p}$ for $p = 10k \pm 1$.

b) We have

$$F_{p+1} = \frac{1}{2^p} \left(\binom{p+1}{1} + \binom{p+1}{3} \cdot 5 + \cdots + \binom{p+1}{p} \cdot 5^{(p-1)/2} \right).$$

From $\binom{p+1}{k} = \binom{p}{k} + \binom{p}{k-1}$, it follows that $\binom{p+1}{k} \equiv 0 \pmod{p}$ for $1 < k < p$. Hence,

$$2^p F_{p+1} \equiv 1 + 5^{(p-1)/2} \equiv 1 + \left(\frac{5}{p} \right) \equiv 0 \pmod{p},$$

so $F_{p+1} \equiv 0 \pmod{p}$ for $p = 10k \pm 3$. ♢

Remark 4.1. The property from Example 4.17 can be generalized and used for testing primality. Let α and β be roots of the polynomial $x^2 - ax + b = 0$, $a, b \in \mathbb{Z} \setminus \{0\}$. We define the sequences $U_k(a,b) = \frac{\alpha^k - \beta^k}{\alpha - \beta}$, $V_k(a,b) = \alpha^k + \beta^k$.

These sequences are called *Lucas sequences*. For $a = 1$, $b = -1$, U_k are Fibonacci numbers and V_k are (ordinary) Lucas numbers. It can be proved that for primes p, such that p does not divide $2bD$, where $D = a^2 - 4b$,

$$U_{\delta(p)} \equiv 0 \pmod{p}, \tag{4.4}$$

where $\delta(p) = p - (\frac{D}{p})$. (For Fibonacci numbers this means that $p \mid F_{p-1}$ if $p \equiv \pm 1 \pmod{10}$, while $p \mid F_{p+1}$ if $p \equiv \pm 3 \pmod{10}$.) Therefore, this property of prime numbers can be used for defining a new class of pseudoprimes and for constructing tests of primality based on them. If an odd composite number n satisfies $U_{\delta(n)} \equiv 0 \pmod{n}$, then we say that n is a *Lucas pseudoprime with parameters* a, b (n is a lpsp(a, b)). It is shown in practice that a combination of tests with strong pseudoprimes and Lucas pseudoprimes performs very well, and it is believed that a number which passes a test with spsp and a test with lpsp, with suitably chosen parameters, has to be prime (see [351, Chapter 4]).

Theorem 4.17. *Let m be a positive integer. The sequence of remainders of Fibonacci numbers in the division by m is periodic. Let $k = k(m)$ be the* fundamental period *of that sequence, i.e. the smallest positive integer such that $F_{n+k} \equiv F_n \pmod{m}$ for any $n \in \mathbb{N}$. Then $k \leq m^2$.*

Proof: Let $a \bmod m$ denote the remainder in the division of a by m. There are m such possible remainders: $0, 1, 2, \ldots, m-1$. Let us now consider a sequence of ordered pairs

$$(F_1 \bmod m, F_2 \bmod m), (F_2 \bmod m, F_3 \bmod m), (F_3 \bmod m, F_4 \bmod m), \ldots$$

In this sequence, there are at most m^2 different elements. Namely, on the first position in an ordered pair, one of the m remainders can appear, as well as on the second position. Now, by Dirichlet's box principle, we conclude that among the first $m^2 + 1$ elements of this sequence, there are at least two equal elements. Let

$$(F_t \bmod m, F_{t+1} \bmod m) = (F_s \bmod m, F_{s+1} \bmod m),$$

where $1 \leq s < t \leq m^2 + 1$. This means that $F_t \equiv F_s \pmod{m}$ and $F_{t+1} \equiv F_{s+1} \pmod{m}$. From $F_{t-1} = F_{t+1} - F_t$ and $F_{s-1} = F_{s+1} - F_s$, it follows that $F_{t-1} \equiv F_{s-1} \pmod{m}$. In the same manner, we obtain $F_{t-2} \equiv F_{s-2} \pmod{m}$, $\ldots$, $F_{t-s+2} \equiv F_2 \equiv 1$, $F_{t-s+1} \equiv F_1 \equiv 1 \pmod{m}$.

Hence, for the positive integer $l = t - s$ we have $F_{l+1} \equiv F_1 \pmod{m}$ and $F_{l+2} \equiv F_2 \pmod{m}$, so from the definition of Fibonacci numbers, it follows

by induction that $F_{n+l} \equiv F_n \pmod m$, which means that l is a period of the sequence $(F_n \bmod m)_{n\geq 1}$.

Finally, from $k \leq l = t - s$, it follows that $k \leq m^2$. □

Corollary 4.18. *For any positive integer m, among the first m^2 Fibonacci numbers, there is at least one divisible by m.*

Proof: By Theorem 4.17, the fundamental period k of the sequence of remainders of Fibonacci numbers divided by m satisfies $k \leq m^2$, and we have $F_{k+1} \equiv F_1 \pmod m$, $F_{k+2} \equiv F_2 \pmod m$. We conclude that $F_k \equiv F_2 - F_1 \equiv F_0 \equiv 0 \pmod m$, which means that F_k is divisible by m. □

It can be shown that $k(m) \leq 6m$, while the equality holds if and only if $m = 2 \cdot 5^n$. Similarly, the smallest index $z(m)$, such that $F_{z(m)}$ is divisible by m, satisfies $z(m) \leq 2m$, while the equality holds if and only if $m = 6 \cdot 5^n$. The paper [414] is devoted to the properties of the function $k(m)$.

Let us mention, without proof, another significant divisibility property of Fibonacci numbers. Let p be a prime number. If $p \mid F_n$, but $p \nmid F_m$ for $1 \leq m < n$, then we say that p is a *primitive prime divisor* of F_n. Carmichael's theorem on primitive prime divisors states that every Fibonacci number F_n, where $n \neq 1, 2, 6, 12$, has at least one primitive prime divisor (for the proof and generalizations see [100, Chapters 13.4 and 13.5]). Note that $F_{12} = 144 = 2^4 \cdot 3^2$ does not have a primitive prime divisor since $2 \mid F_3$ and $3 \mid F_4$.

4.6 Exercises

1. Determine all remainders which a perfect square can give in the division by 16.

2. Determine all quadratic residues

   a) modulo 17,

   b) modulo 19,

   c) modulo 24.

3. Let n be a positive integer. Prove that the greatest common divisor of the numbers $n^2 + 1$ and $(n + 1)^2 + 1$ is either 1 or 5. Prove that it is equal to 5 if and only if $n \equiv 2 \pmod 5$.

4. Let $\gcd(a, p) = 1$. Calculate $\displaystyle\sum_{x=1}^{p} \Big(\frac{ax + b}{p}\Big)$.