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 $\displaystyle\sum_{x=1}^{p} \Big(\frac{ax + b}{p}\Big)$.

5. Let p be an odd prime number and n a positive integer. How many quadratic residues modulo p^n are there?

6. Let $p > 3$ be a prime number. Prove that the sum of all quadratic residues r modulo p, such that $1 \leq r \leq p-1$, is divisible by p.

7. Determine all primes p such that $\left(\frac{10}{p}\right) = 1$.

8. Determine all primes p such that $\left(\frac{-3}{p}\right) = 1$. Prove that there are infinitely many primes of the form $6k+1$.

9. Prove that there are infinitely many primes whose decimal representation ends with the digit 9.

10. For which primes p does the congruence $x^4 \equiv -4 \pmod{p}$ have a solution?

11. Prove that for a positive integer m, the number $2^m + 1$ does not divide $5^m - 1$.

12. Let p be a prime number. Prove that there is a positive integer n such that the number $(n^2-3)(n^2-5)(n^2-15)$ is divisible by p.

13. Solve the congruence $x^2 \equiv 41 \pmod{43}$.

14. Let p be an odd prime number and g a primitive root modulo p. Prove that g is a quadratic nonresidue modulo p.

15. Find all positive integers $a \in \{1, \ldots, 34\}$ for which the Jacobi symbol $\left(\frac{a}{35}\right)$ is equal to 1, but the congruence $x^2 \equiv a \pmod{35}$ does not have a solution.

16. Compute the Legendre symbols:

    a) $\left(\frac{51}{71}\right)$,
    b) $\left(\frac{7}{227}\right)$,
    b) $\left(\frac{30}{571}\right)$.

17. How many solutions are there for the congruence $x^2 \equiv 19 \pmod{170}$?

18. Solve the congruence $x^2 \equiv 23 \pmod{77}$.

19. Prove that for any positive integer k there are k consecutive Fibonacci numbers which are all composite.

20. Determine the period of the sequence $(F_n \bmod m)$ if:

    a) $m = 7$,

    b) $m = 10$,

    c) $m = 11$.

21. Prove that no Lucas number L_n is divisible by 5.

22. Find relatively prime positive integers a and b such that sequence $c_n = an + b$ does not contain any Fibonacci number.

23. Let $k(m)$ denote the period length of the sequence $(F_n \bmod m)$. Prove the statement: If p is a prime number of the form $10l \pm 1$, then $k(p) \mid (p-1)$, and if p is a prime number of the form $10l \pm 3$, then $k(p) \mid (2p+2)$.

24. Let $F_{n(k)}$ be the smallest Fibonacci number ending with k zeros, i.e. $n(k) = z(10^k)$. Check that $n(1) = 15$, $n(2) = 150$ and $n(3) = 750$. Prove that

$$n(k) = \begin{cases} 15 \cdot 10^{k-1}, & \text{for } k \leq 2, \\ 75 \cdot 10^{k-2}, & \text{for } k \geq 3. \end{cases}$$

25. Prove that for all positive integers m and n,

    a) $F_{mn} \equiv mF_nF_{n+1}^m \pmod{F_n^2}$,

    b) $F_{mn+1} \equiv F_{n+1}^m \pmod{F_n^2}$.

26. Use the previous exercise to prove *Matiyasevich's lemma*, used in his famous solution of Hilbert's tenth problem of the non-existence of an algorithm for decidability whether arbitrary Diophantine equation has integer solutions:

$$F_{mn} \equiv 0 \pmod{F_n^2} \iff m \equiv 0 \pmod{F_n}.$$

27. Prove that for any prime number p, $L_p \equiv 1 \pmod{p}$.

28. Prove that for any positive integer n and any prime number p,

    a) $F_{(n+1)p} \equiv F_{np} + F_{(n-1)p} \pmod{p}$,

    b) $F_{np} \equiv F_nF_p \pmod{p}$.