probability that 500-bits number, which passed just one test, is composite, is less than $1/4^{28}$.

The complexity of one Miller-Rabin test is $O(\ln^3 n)$. Namely, $b^t \bmod n$ can be calculated in $O(\ln^3 n)$ bit operations, and then for calculating $b^{2t}, b^{4t}, \ldots, b^{2^{s-1}t}$ by iterative squaring, we need also $O(\ln^3 n)$ bit operations.

With the assumption that the extended Riemann hypothesis (ERH) holds, the Miller-Rabin test becomes a deterministic polynomial time algorithm for proving primality. Namely, it can be shown that if n is a composite, then, assuming the ERH, there is at least one base $b < 2\ln^2 n$ for which (3.11) does not hold (see [93, Chapter 3.5]) and [257, Chapter 2]). Therefore, assuming the ERH, the complexity of this algorithm is $O(\ln^5 n)$.

3.10 Exercises

1. Find two distinct complete residue systems modulo 5, $\{a_1, \ldots, a_5\}$ and $\{b_1, \ldots, b_5\}$, such that $\{a_1 + b_1, \ldots, a_5 + b_5\}$ is also a complete residue systems modulo 5.

2. For which positive integers m are there two distinct complete residue systems modulo m, $\{a_1, \ldots, a_m\}$ and $\{b_1, \ldots, b_m\}$, such that $\{a_1 + b_1, \ldots, a_m + b_m\}$ is also a complete residue systems modulo m?

3. Are there two distinct complete residue systems modulo 5, $\{a_1, \ldots, a_5\}$ and $\{b_1, \ldots, b_5\}$, such that $\{a_1 \cdot b_1, \ldots, a_5 \cdot b_5\}$ is also a complete residue system modulo 5?

4. What is the smallest positive integer n divisible by 15 that has the sum of digits equal to 15?

5. What is the smallest positive integer n divisible by 22 that has the sum of digits equal to 22?

6. Add a digit on the left and on the right side of the number 10 so that the new number is divisible by 36.

7. Write down all seven-digit numbers with digits 1 and 2 which are divisible by 36.

8. Determine all three-digit numbers $\overline{abc}$ divisible by 7, whose sum of digits is 8.

9. Determine all positive integers divisible by 792 whose decimal representation is of the form $\overline{13xy45z}$, where x, y, z are unknown digits.

10. Find two three-digit numbers whose quotient is equal to 7 and the sum is divisible by 336.

11. Solve the congruences

    a) $111x \equiv 186 \pmod{321}$,
    b) $589x \equiv 209 \pmod{817}$,
    c) $535x \equiv 145 \pmod{635}$.

12. Let a and m be coprime positive integers. Prove that there exist positive integers $x, y \le \sqrt{m}$ such that $ax \equiv \pm y \pmod{m}$ for a suitable choice of the sign (Thue's lemma, see [369, Chapter 1.13]).

13. Solve the system of congruences

$$x \equiv 5 \pmod{7}, \quad x \equiv 7 \pmod{11}, \quad x \equiv 3 \pmod{13}.$$

14. Solve the system of congruences

$$x \equiv 7 \pmod{14}, \quad x \equiv 13 \pmod{24}, \quad x \equiv 16 \pmod{27}.$$

15. Solve the system of congruences

$$7x \equiv 12 \pmod{39}, \quad 2x \equiv 7 \pmod{35}, \quad 21x \equiv 15 \pmod{22}.$$

16. Find an even positive integer k such that $p^2 + k$ is composite for each prime number p. Prove that there are infinitely many such numbers.

17. Determine the last two digits in the decimal representation of the numbers 11^{1000}, 12^{1000} and 15^{1000}.

18. Prove using the mathematical induction (over a) that for any prime number p and positive integer a, $a^p \equiv a \pmod{p}$.

19. Let a and n be relatively prime positive integers and $n \ge 2$. Calculate the sum $\displaystyle\sum_{\substack{1 \le x \le n \\ \gcd(x,n)=1}} \left\{\frac{ax}{n}\right\}$. Here $\{z\} = z - \lfloor z \rfloor$ is the fractional part of z, while x runs through the set of all reduced residues modulo n.

20. Find an even positive integer k such that the equation $\varphi(n) = k$ does not have a solution.

21. Find all solutions of the equation $\varphi(n) = 24$.

22. Solve the congruence $x^2 \equiv 1 \pmod{21}$.

23. Let p be a prime number and $d \mid p-1$. Prove that the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions modulo p.

24. Let m and n be positive integers and p a prime number. If $m = m_k p^k + \cdots + m_1 p + m_0$, $n = n_k p^k + \cdots + n_1 p + n_0$, where $m_i, n_i \in \{0, 1, \ldots, p-1\}$ for $i = 0, 1, \ldots, k$, prove that
$$\binom{m}{n} = \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}$$
(Lucas' theorem, see [198]).

25. Solve the congruence $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$.

26. Solve the congruence $x^3 - 2x + 4 \equiv 0 \pmod{13^3}$.

27. What is the remainder in the division of $\varphi(a^n - 1)$ by n?

28. Let a positive integer a belong to the exponent 3 modulo p, where p is a prime number. To which exponent modulo p does the number $1 + a$ belong?

29. Find the least primitive root:

    a) modulo 13,
    b) modulo 17,
    c) modulo 41.

30. Prove properties 1) – 3) from Theorem 3.22.

31. How many primitive roots modulo 31 are there? Find the smallest among them and solve the congruence $2x^{16} \equiv 5 \pmod{31}$.

32. Solve the congruences:

    a) $2x^8 \equiv 5 \pmod{13}$,
    b) $x^6 \equiv 5 \pmod{17}$,
    c) $x^{12} \equiv 37 \pmod{41}$.

33. Solve the congruences:

    a) $7^x \equiv 6 \pmod{17}$,
    b) $2^x \equiv 3 \pmod{23}$.

34. Let g be a primitive root modulo p. What is the remainder in the division of $g^{p(p-1)/2}$ by p?

35. Which condition has to be satisfied so that the numbers

$$1^k, 2^k, \dots, (p-1)^k$$

form a reduced residue system modulo p?

36. Let n be a positive integer for which there is a primitive root modulo n. Prove that there are exactly $\varphi(\varphi(n))$ primitive roots modulo n.

37. Determine the length of period in the decimal representation of rational numbers with denominator

    a) $q = 31$,
    b) $q = 37$,
    c) $q = 43$.

38. Determine the length of pre-period in the decimal representation of the number $\frac{1}{10!}$.

39. The number $157\,894\,736\,842\,105\,263$ has the property that when its last digit (digit of ones) is moved to the first position, we obtain the number $315\,789\,473\,684\,210\,526$ which is twice the initial number. Prove that there are infinitely many positive integers with this property.

40. Is 341:

    a) a pseudoprime to the base 2,
    b) a strong pseudoprime to the base 2?

41. Find a strong pseudoprime to the base $b = 211$.

42. Determine the smallest positive integer n which is a strong pseudoprime both to the base 3 and to the base 5.