Congruences

Exercises

Application of discrete models

Mathematical questions

1. Define congruence. Illustrate the definition for an example with the modulus $m = 8$.

2. Which of the following are true:
a) $1 \equiv 6 \pmod 3$, b) $3 \equiv 9 \pmod 6$, c) $10 \equiv 2 \pmod 4$, d) $2 \equiv -2 \pmod 5$?

3. Write down the congruence classes modulo 3.

4. What is a complete residue system? Give *two* examples modulo 6.

5. Solve the following linear congruences:
a) $3x \equiv 5\ (8)$; b) $6x \equiv 6\ (15)$; c) $12x \equiv 9\ (18)$; d) $21x \equiv 14\ (35)$; e) $100x \equiv 40\ (260)$.

6. Define modular inverse. Give an example for it with the modulus $m = 5$.

7. When does the modular inverse exist? Which numbers are invertible modulo 8?

8. Calculate the inverses of the following values modulo m (which method is easier?):
a) $a = 1, m = 3$; b) $a = 2, m = 3$; c) $a = 2, m = 5$; d) $a = 7, m = 10$; e) $a = 3, m = 6$;
f) $a = 2, m = 99$; g) $a = 17, m = 50$; h) $a = 27, m = 100$; i) $a = 34, m = 55$.

9. Solve the following simultaneous congruence systems:

a) $\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 5 \pmod 8; \end{cases}$ b) $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 5; \end{cases}$ c) $\begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 5 \pmod 6; \end{cases}$

d) $\begin{cases} x \equiv 8 \pmod{10} \\ x \equiv 4 \pmod{15}; \end{cases}$ e) $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 5. \end{cases}$

Programming exercises

10. How many prime numbers are there up to 2800000 which are congruent to 7 modulo 235?

11. Write a function that solves the linear congruence $ax \equiv b \pmod{m}$ for given $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}^+$ numbers

a) using brute force search; b) using the extended Euclidean algorithm.

The return value is the list of all solutions between 0 and $m-1$. The congruences from question 5 above can be used for testing. Also, solve the following congruence:

$$30517578125x \equiv 33729082272 \pmod{999999999999}.$$

12. Write a function that calculates the multiplicative inverse of $a \in \mathbb{Z}$ for a given $m \in \mathbb{N}^+$, using the methods below. If a is not invertible, return `None`.

a) Solve it using brute force search (but don't search longer than necessary).
b) Solve it using the extended Euclidean algorithm.
c) Test the solutions for all possible numbers for all moduli from $m = 2$ to 100.
d) Invert $a = 3$ for increasingly bigger moduli: $m = 10, 100, 1000, \ldots$. Which method can go further?

13. a) Write a function that checks whether a Hungarian bank account number is correct (according to the checksum). Which of the following numbers are correct:

- 10402196-50526765-81771006,
- 10700505-70347915-51300009?

b) Write a function that receives a (potentially incorrect) bank account number and the index of the single wrong digit between 1 and 24. You can assume that all other digits are correct. Return the corrected bank account number. Solve it in at least two fundamentally different ways. For testing, start from a known correct account number, and change each digit (one at a time) in each possible way.

14. Implement the Chinese remainder theorem for two congruences, i.e. write a function that finds the common solutions of the congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. It expects the same four parameters as `crt()`: a, b, m, n, but unlike that, the return value is the pair (x, r), where x is the smallest nonnegative solution, and r is the modulus of the solution. If there is no solution, return `None`. (Don't use `crt()` or Sage's other equation solving functions.) For testing, use the appropriate congruence systems from question 9 above, and check whether the solution really satisfies the original congruences.