Elementary Number Theory - Exercise 5a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Show that the linear congruence

$$ax \equiv b \pmod{m}$$

is solvable if and only if $\gcd(a, m)$ divides b, in which case there are precisely $\gcd(a, m)$ different solutions modulo m.

Problem 2. Determine all solutions of the following congruences (if there are any).

$$5x \equiv 9 \pmod{11}; \qquad 4x \equiv 8 \pmod{12}; \qquad 3x \equiv 7 \pmod{6}.$$

Problem 3. Compute $15^{10235} \pmod 7$, $120^{13} \pmod{11}$, $3^{2023} \pmod 7$, $3^{-1} \pmod{28}$, and $5^{12345678} \pmod{11}$.

Problem 4. Solve the following system of linear congruences.

$$\begin{aligned} x &\equiv 2 \pmod 3, \\ x &\equiv 4 \pmod 5, \\ x &\equiv 3 \pmod 7. \end{aligned}$$

Problem 5. Fermat's Little Theorem can be stated as

$$a^p \equiv a \pmod p$$

for every $a \in \mathbb{Z}$, and prime p. Show that $(a+1)^p \equiv a^p + 1 \pmod p$ for any $a \in \mathbb{Z}$ and use this to prove Fermat's Little Theorem by induction.

Problem 6 (Homework)**.** Let n be a natural number. Show that

1. n is divisible by 3 if and only if the sum of its digits is divisible by 3.
2. n is divisible by 7 if and only if twice the last digit of n minus the rest of n is divisible by 7.
3. n is divisible by 11 if the alternating sum of its digits is divisible by 11.

Check whether 27797 is divisible by $3, 7$, or 11.

Problem 7 (Homework)**.** In order to compute $a^n \pmod m$ for large exponents n, one can use the method of *repeated squaring*: For example, consider $3^{23} \pmod 7$. Write the exponent 23 to base 2, that is, $23 = 2^4 + 2^2 + 2^1 + 2^0$. Then

$$3^{23} = 3^{2^4} \cdot 3^{2^2} \cdot 3^2 \cdot 3 = (((3^2)^2)^2)^2 \cdot (3^2)^2 \cdot 3^2 \cdot 3.$$

Now repeatedly compute the square, using the result from the previous squaring, e.g.

$$\begin{aligned} 3^2 &\equiv 2 \pmod 7, \\ (3^2)^2 &\equiv 2^2 \equiv 4 \pmod 7, \\ ((3^2)^2)^2 &\equiv 4^2 \equiv 2 \pmod 7, \\ (((3^2)^2)^2)^2 &\equiv 2^2 \equiv 4 \pmod 7. \end{aligned}$$

We finally obtain $3^{23} \equiv 4 \cdot 4 \cdot 2 \cdot 3 \equiv 5 \pmod 7$.

Compute $3^{189} \pmod{11}$ using the method of repeated squaring[1].

Problem 8 (sage)**.** Implement the following functions in sage:

1. Compute the inverse of a modulo m if $\gcd(a, m) = 1$.
2. Find all solutions for linear congruences $ax \equiv b \pmod m$.
3. Solve systems of linear congruences $x \equiv b_j \pmod{m_j}$ using the Chinese Remainder Theorem.
4. Compute $a^n \pmod m$, using repeated squaring.

[1] One can further optimize the computation, see `https://en.wikipedia.org/wiki/Exponentiation_by_squaring`