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.

Solution 1. If $ax \equiv b \pmod{m}$ has a solution $x \in \mathbb{Z}$, then there is some $k \in \mathbb{Z}$ with $ax + km = b$. Since $\gcd(a, m)$ divides the left-hand side, it must also divide b. In particular, if $\gcd(a, m) \nmid b$, then t he equation is not solvable.

We first show that for $\gcd(a, m) = 1$ the equation $ax \equiv b$ has a unique solution modulo m. By Bézout's Lemma, there exist $u, v \in \mathbb{Z}$ with $au + mv = 1$. Then $x = ub$ is a solution, since

$$ax \equiv a(ub) \equiv (au)b \equiv (1 - mv)b \equiv b \pmod{m}.$$

If there is a second solution x', then $ax \equiv b \pmod{m}$ and $ax' \equiv b \pmod{m}$ together imply $a(x - x') \equiv 0 \pmod{m}$, so there is some $k \in \mathbb{Z}$ such that $a(x - x') = mk$. Since $\gcd(a, m) = 1$, this implies $x \equiv x' \pmod{m}$, so x is unique modulo m.

Now if $d := \gcd(a, m)$ divides b, then we can divide both sides by d to obtain the equation

$$(a/d)x \equiv (b/d) \pmod{m/d}.$$

Since $\gcd(a/d, m/d) = 1$, this equation has a unique solution x_0 modulo m/d. Since x_0 is unique modulo m/d, each solution of $ax \equiv b \mod m$ must be of the form $x = x_0 + km/d$ for some $k \in \mathbb{N}$, and since $d \mid a$, these are indeed all solutions:

$$a(x_0 + km/d) = ax_0 + km(a/d) \equiv ax_0 \equiv b \pmod{m}.$$

It is now clear that the d incongruent solutions are given by $x_0 + km/d$ where $k \in \{0, \dots, d-1\}$.

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

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

Solution 2. Since $\gcd(5, 11) = 1$, the first equation has a unique solution modulo 11. By trying all values $x = 1, 2, 3, \dots, 11$, we find that $x = 4$ satisfies $5x = 20 \equiv 9 \pmod{11}$.

Since $\gcd(4, 12) = 4$ divides $b = 8$, the equation has 4 solutions modulo 12. Dividing by 4, we obtain the equation $x \equiv 2 \pmod{3}$, which has the solution $x_0 = 2$. All solutions are given by $x_0 + 3k, k = 0, 1, 2, 3$, that is $x \in \{2, 5, 8, 11\}$.

Since $\gcd(3, 6) = 3$ does not divide $b = 7$, the equation has no solutions.

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

Solution 3. Since $15 \equiv 1 \pmod 7$, we have $15^{10235} \equiv 1^{10235} \equiv 1 \pmod 7$.

Since $120 = 121 - 1 \equiv -1 \pmod{11}$, we have $120^{13} \equiv (-1)^{13} = -1 \equiv 10 \pmod{11}$.

One can compute $3^{2023} \pmod 7$ using that that $3^{\varphi(7)} = 3^6 \equiv 1 \pmod 7$, so

$$3^{2023} \equiv 3 \cdot 3^{2022} \equiv 3 \cdot (3^6)^{337} \equiv 3 \cdot 1^{337} \equiv 3 \pmod 7.$$

We have $\varphi(28) = 28(1 - \frac{1}{2})(1 - \frac{1}{7}) = 12$, so the inverse of 3 modulo 28 is given by $3^{11} \pmod{28}$. Since $3^3 = 27 \equiv -1 \pmod{28}$, we have

$$3^{-1} \equiv 3^{11} = (3^3)^3 \cdot 3^2 \equiv (-1)^3 \cdot 9 \equiv -9 \equiv 19 \pmod{28}.$$

Since $\varphi(11) = 10$, we have

$$5^{12345678} \equiv 5^{12345678 \,(\mathrm{mod}\, 10)} \equiv 5^8 \pmod{11}.$$

Now

$$5^8 \equiv 25^4 \equiv 3^4 \equiv 81 \equiv 4 \pmod{11}.$$

Problem 4. Solve the following system of linear congruences.

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

Solution 4. Let us write a_m^{-1} for the inverse of a modulo m. A solution is given by

$$x = 2 \cdot (5 \cdot 7) \cdot (5 \cdot 7)_3^{-1} + 4 \cdot (3 \cdot 7) \cdot (3 \cdot 7)_5^{-1} + 3 \cdot (3 \cdot 5) \cdot (3 \cdot 5)_7^{-1}.$$

We have

$$\begin{aligned} (5 \cdot 7)_3^{-1} &\equiv (2 \cdot 1)_3^{-1} \equiv 2_3^{-1} \equiv 2 \pmod 3, \\ (3 \cdot 7)_5^{-1} &\equiv (3 \cdot 2)_5^{-1} \equiv 1_5^{-1} \equiv 1 \pmod 5, \\ (3 \cdot 5)_7^{-1} &\equiv 15_7^{-1} \equiv 1 \pmod 7, \end{aligned}$$

so we find the solution modulo $3 \cdot 5 \cdot 7 = 105$,

$$x = 2 \cdot (5 \cdot 7) \cdot 2 + 4 \cdot (3 \cdot 7) + 3 \cdot (3 \cdot 5) = 140 + 84 + 45 = 296 \equiv 59 \pmod{105}.$$

Indeed, we have $59 \equiv 2 \pmod 3$, $59 \equiv 4 \pmod 5$, and $59 \equiv 3 \pmod 7$.

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.

Solution 5. By the Binomial Theorem, we have

$$(a+1)^p = \sum_{n=0}^{p} \binom{p}{n} a^n = 1 + \sum_{n=1}^{p-1} \binom{p}{n} a^n + a^p,$$

where we used that $\binom{p}{0} = \binom{p}{p} = 1$. Now p divides the binomial coefficient $\binom{p}{n}$ for $1 \le n \le p-1$ (since p divides the numerator $p!$, but not the denominator $n!(p-n)!$), so reducing modulo p we obtain

$$(a+1)^p \equiv a^p + 1.$$

It is easy to see that it suffices to prove Fermat's Little Theorem for $a \in \mathbb{N}$ (for $a = 0$ it is trivially true, and for $a < 0$ replace a with $-a$). Hence we can prove the theorem by induction on $a \in \mathbb{N}$. For $a = 1$ we have $1^p \equiv 1 \pmod{p}$, which is true. Now, if $a^p \equiv a \pmod{p}$ for some fixed a, then

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p},$$

which concludes the 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.

Solution 6.

1. Write $n = \sum_{j=0}^{k} a_j 10^j$ with digits $a_j \in \{0, \dots, 9\}$. The sum of digits is given by

$$n' = \sum_{j=0}^{k} a_j.$$

   We claim that $n \equiv n' \pmod{3}$. Indeed, since $10 \equiv 1 \pmod{3}$, we have $10^j \equiv 1^j \equiv 1 \pmod{3}$ for any j, hence

$$n - n' = \sum_{j=0}^{k} a_j(10^j - 1) \equiv \sum_{j=0}^{k} a_j(1-1) \equiv 0 \pmod{3}.$$

   This shows that n is divisible by 3 if and only if n' (the sum of the digits of n) is divisible by 3.

2. Write $n = 10a + b$ with $a \in \mathbb{N}_0$ and $b \in \{0, 1, \dots, 9\}$, i.e. b is the last digit of n, and a is the rest. We want to show that $10a + b$ is divisible by 7 if and only if $a - 2b$ is divisible by 7. Subtracting $21b$ from $n = 10a + b$ gives

$$n - 21b = 10a - 20b = 10(a - 2b).$$

   Since 10 is coprime to 7, and 21 is divisible by 7, we see that n is divisible by 7 if and only if $a - 2b$ is divisible by 7, which proves the claim.

3. Write $n = \sum_{j=0}^{k} a_j 10^j$ with digits $a_j \in \{0, \ldots, 9\}$. The alternating sum of digits is given by

$$n' = \sum_{j=0}^{k} (-1)^j a_j.$$

We claim that $n \equiv n' \pmod{11}$. Indeed, since $-1 \equiv 10 \pmod{11}$, we have $(-1)^j \equiv 10^j \pmod{11}$ for any j, hence

$$n - n' = \sum_{j=0}^{k} a_j(10^j - (-1)^j) \equiv \sum_{j=0}^{k} a_j(10^j - 10^j) \equiv 0 \pmod{11}.$$

Now we check whether 27797 is divisible by 3, 7, or 11. The sum of its digits is

$$2 + 7 + 7 + 9 + 7 = 32$$

which is not divisible by 3, so 27797 is not divisible by 3. Next, we repeatedy substract twice the last digit from the rest, and get

$$\begin{aligned} 2779 - 2 \cdot 7 &= 2765 \\ 276 - 2 \cdot 5 &= 266 \\ 26 - 2 \cdot 6 &= 14, \end{aligned}$$

and since 14 is divisible by 7, the original number 27797 is also divisible by 7. Finally, the alternating sum of the digits is

$$2 - 7 + 7 - 9 + 7 = 0,$$

which is divisible by 11, so 27797 is divisible by 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].

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

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.