Homework 6

Discrete Structures
Due Tuesday, February 16, 2021

Submit each question separately in .pdf format (except question 5)

---

1. Let $a, b \in \mathbf{Z}$ and $d \in \mathbf{N}$. Suppose that $d \mid a$ and $d \mid b$, and that there exist $x, y \in \mathbf{Z}$ with $ax + by = d$.

   (a) Use the definition of the gcd to prove that $\gcd(a, b) \mid d$.

   The definition of gcd says that $e = \gcd(a, b)$ if e is the largest integer such that $e \mid a$ and $e \mid b$. Since $e \mid a$, we also have $e \mid ax$, and similarly since $e \mid b$, we also have $e \mid by$. Hence $e \mid (ax + by)$, or $\gcd(a, b) \mid d$. □

   (b) Prove that $\gcd(a, b) = d$

   Since $\gcd(a, b) \mid d$, it follows that $\gcd(a, b) \leqslant d$. But since $d \mid a$ an $d \mid b$, and e is largest among such numbers, it must be that $d = e$. □

2. (a) Find the remainder when $7633^{705} + 2021^{75}$ is divided by 37.
   Hint: Use Fermat's little theorem.

   Note that $7633 \equiv 11 \pmod{37}$ and $2021 \equiv 23 \pmod{37}$. Since 37 is prime, Fermat's little theorem gives us that $11^{36} \equiv 1 \pmod{37}$ and $23^{36} \equiv 1 \pmod{37}$. Hence

   $$\begin{aligned} 7633^{705} + 2021^{75} &\equiv (11^{36})^{19} \cdot 11^{21} + (23^{36})^2 \cdot 23^3 \pmod{37} \\ &\equiv 11^{21} + 23^3 \pmod{37} \\ &\equiv 30 \pmod{37}. \end{aligned}$$

   This is quite an unpleasant number. The only practical solution is to use a calculator.

   However, if instead of 705 we had $685 = 36 \cdot 19 + 1$ and instead of 75 we had $73 = 36 \cdot 2 + 1$, then the answer would be $34 \pmod{37}$ without a calculator. □

   (b) Solve the linear congruence $77x \equiv 119 \pmod{840}$.

   We notice that $\gcd(77, 840) = 7$, and that $119/7 = 17$. Hence the congruence $77x \equiv 119 \pmod{840}$ is equivalent to the congruence $11x \equiv 17 \pmod{120}$. By trial and error, we find the answer to be 67. □

3. (a) Solve the system of linear congruences – find $(x, y) \in \{0, 1, \ldots, 10\} \times \{0, 1, \ldots, 10\}$ satisfying both conditions:

   $$\begin{cases} 5x + 4y \equiv 7 \pmod{11} \\ 7x + y \equiv 6 \pmod{11} \end{cases}$$

   Answer: $(x, y) = (6, 8)$.
   Multiply both sides of the latter congruence by 4 ($4 \cdot 7 = 28$ becomes 6; also $4 \cdot 6 = 24$ becomes 2 (replace large numbers by remainders $\pmod{11}$):

   $$\begin{cases} 5x + 4y \equiv 7 \pmod{11} \\ 6x + 4y \equiv 2 \pmod{11} \end{cases}$$

Subtract the first equation from the last:

$$x \equiv -5 \equiv 6 \pmod{11}.$$

Now plug this value into the congruence $7x + y \equiv 6 \pmod{11}$. We get

$$y \equiv 6 - 7x \equiv 6 - 7 \cdot 6 \equiv 6 - 42 \equiv 6 - 42 + 44 = 8 \pmod{11}.$$

So the solution is $x \equiv 6,\ y \equiv 8 \pmod{11}$. □

(b) Consider the following system of linear congruences:

$$\begin{cases} a_{11} \cdot x + a_{12} \cdot y \equiv b_1 \pmod{11}, \\ a_{21} \cdot x + a_{22} \cdot y \equiv b_2 \pmod{11}. \end{cases} \tag{1}$$

Prove or disprove the following statement: The system (1) has a unique solution (x, y) if and only if the expression $a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \not\equiv 0 \pmod{11}$.

The "if and only if" statement is correct; we prove it in both directions.

Part 1. Assume that

$$\Delta = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \not\equiv 0 \pmod{11}.$$

This expression Δ is called the *determinant* of the the 2×2 matrix. To show the solution of the system, multiply the first equation by a_{21}, the second equation by a_{11}:

$$\begin{cases} a_{21} \cdot a_{11} \cdot x + a_{21} \cdot a_{12} \cdot y \equiv a_{21} \cdot b_1 \pmod{11}, \\ a_{11} \cdot a_{21} \cdot x + a_{11} \cdot a_{22} \cdot y \equiv a_{11} \cdot b_2 \pmod{11}. \end{cases}$$

Subtract the first equation from the second one:

$$(a_{11} \cdot a_{21} - a_{21} \cdot a_{11}) \cdot x + (a_{11} \cdot a_{22} - a_{21} \cdot a_{12}) \cdot y \equiv a_{11} \cdot b_2 - a_{21} \cdot b_1 \pmod{11}.$$

Coefficients for variable x cancel out, and the y is actually multiplied by the determinant Δ. We get this:

$$\Delta \cdot y \equiv a_{11} \cdot b_2 - a_{21} \cdot b_1 \pmod{11}. \tag{2}$$

We assumed that Δ is not congruent to $0 \pmod{11}$; therefore there exists the inverse Δ^{-1}; a number with property that $\Delta^{-1} \cdot \Delta \equiv 1 \pmod{11}$. Multiply both sides of the latest equality by Δ^{-1} to get this:

$$\Delta^{-1} \cdot \Delta \cdot y \equiv \Delta^{-1} \cdot (a_{11} \cdot b_2 - a_{21} \cdot b_1) \pmod{11}.$$

$$y \equiv \Delta^{-1} \cdot (a_{11} \cdot b_2 - a_{21} \cdot b_1) \pmod{11}.$$

Now need to express variable x. We know that at least one of the two coefficients a_{11} or a_{21} is not 0 (otherwise the determinant Δ is 0). Assume that $a_{11} \not\equiv 0 \pmod{11}$ (the case with the 2nd equation is similar). Then we can also express x from the 1st equation (since y is already found).

$$x \equiv a_{11}^{-1} \cdot (b_1 - a_{12} \cdot y) \pmod{11}.$$

Part 1. Assume that

$$\Delta = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \equiv 0 \pmod{11}.$$

If the determinant Δ is congruent to 0, we can rewrite (2):

$$\Delta \cdot y \equiv a_{11} \cdot b_2 - a_{21} \cdot b_1 \pmod{11}.$$

For $\Delta \equiv 0$ it simplifies as this:

$$0 \equiv a_{11} \cdot b_2 - a_{21} \cdot b_1 \pmod{11}.$$

There are two cases:

- If $a_{11} \cdot b_2 - a_{21} \cdot b_1 \not\equiv 0$. In this case both equations contradict each other and the congruence system has no solutions at all.
- $a_{11} \cdot b_2 - a_{21} \cdot b_1 \equiv 0$. In this case we deal with just one congruence (and the system has a different solution x, no matter what value y is selected.

□

4. (a) Find the smallest positive integer k such that $16^k \equiv 1 \pmod{41}$.

Answer: $k = 5$.
We can raise to powers $\pmod{41}$:

$$\begin{cases} 16^1 \equiv 16 \pmod{41}, \\ 16^2 \equiv 10 \pmod{41}, \\ 16^3 \equiv 37 \pmod{41}, \\ 16^4 \equiv 18 \pmod{41}, \\ 16^5 \equiv 1 \pmod{41}. \end{cases}$$

□

(b) Write the first ten digits of a hexadecimal fraction $0.h_1h_2h_3\ldots$ that equals $1/41$; find the period of this fraction.

From the previous point we have $16^5 - 1 = 1048575$ divisible by 41; the result of division is 25575. Therefore we have

$$\frac{1}{41} = \frac{25575}{1048575} = 25575 \cdot \frac{1}{16^5 - 1} = 25575 \cdot \left(\frac{1}{16^5} + \frac{1}{16^{10}} + \frac{1}{16^{15}} + \frac{1}{16^{20}} + \ldots \right).$$

The last equality follows from the formula of infinite geometric series.
The hexadecimal representation of the fraction in the parentheses is

$$\frac{1}{1048575} = 0.000010000100001\ldots_{16}. \qquad (3)$$

Now convert the number 25575_{10} into hexadecimal notation by successively dividing by 16:

$$\begin{aligned} 25575 &= 1598 \cdot 16 + 7, \\ 1598 &= 99 \cdot 16 + 14, \\ 99 &= 6 \cdot 16 + 3, \\ 6 &= 0 \cdot 16 + 6. \end{aligned}$$

Therefore $25575_{10} = \texttt{063E7}_{16}$. We now multiply this by (3) (i.e. divide by 1048575 to get exactly the fraction $\frac{1}{41}$). We get that

$$\frac{25575}{1048575} = \frac{1}{41} = \texttt{0.063E7063E7063E7...}_{16} = \texttt{0.(063E7)}_{16}.$$

BTW, this is the way how the fraction $\frac{1}{41}$ is stored in a computer's RAM. The infinite hexadecimal/binary fraction is rounded to fit within a 4-byte or 8-byte register. □

(c) For what positive integers k does there exist some $a \in \{1, \ldots, 40\}$ such that all k numbers $a^1, \ldots, a^k$ give different remainders when divided by 41, and $a^k \equiv 1 \pmod{41}$.

Little Fermat theorem ensures that for any a not divisible by 41, we have $a^{40} \equiv 1 \pmod{41}$, but this theorem does not guarantee that the power $k = 40$ is the **first** one where $a^k \equiv 1 \pmod{41}$.

With a little trial and error we find that $b_1 = 6$ is a number for which all the 40 powers $b_1^1, \ldots, b_1^{40}$ are different and only $b_1^{40} \equiv 1 \pmod{41}$. Such numbers (that give all the possible congruence classes except 0) are called *primitive roots* modulo 41. (See `https://bit.ly/2OwgGSX`, where there is a table of primitive roots; including $p = 41$. For every prime number p there is at least one primitive root.)

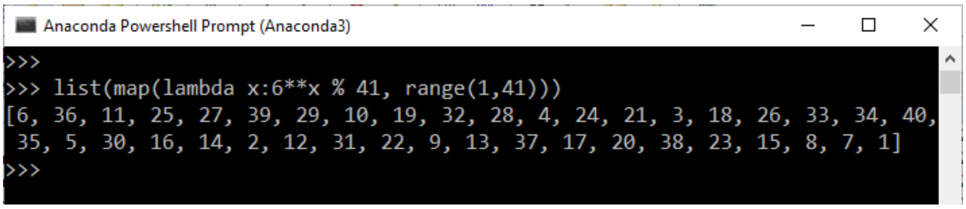

Figure 1: All 40 remainders 6^x are different, so 6 is a primitive root $\pmod{41}$

Let us pick the following powers of 6 (modulo 41): $b_2 = 6^2 \equiv 36$, $b_4 = 6^4 \equiv 25$, $b_5 = 6^5 \equiv 27$, $b_8 = 6^8 \equiv 10$, $b_{10} = 6^{10} \equiv 32$, $b_{20} = 6^{20} \equiv 40$, $b_{40} = 6^{40} \equiv 1$. We claim that they have all different periods (different values of k when $b_i^k \equiv 1$). Let us establish the periods:

$$\begin{cases} b_1^{40} & = 6^{40} & \equiv (6^1)^{40} & \equiv 6^{40} \equiv 1 & \pmod{41} \\ b_2^{20} & = 36^{20} & \equiv (6^2)^{20} & \equiv 6^{40} \equiv 1 & \pmod{41} \\ b_4^{10} & = 25^{10} & \equiv (6^4)^{10} & \equiv 6^{40} \equiv 1 & \pmod{41} \\ b_5^{8} & = 27^{8} & \equiv (6^5)^{8} & \equiv 6^{40} \equiv 1 & \pmod{41} \\ b_8^{5} & = 10^{5} & \equiv (6^8)^{5} & \equiv 6^{40} \equiv 1 & \pmod{41} \\ b_{10}^{4} & = 32^{4} & \equiv (6^{10})^{4} & \equiv 6^{40} \equiv 1 & \pmod{41} \\ b_{20}^{2} & = 40^{2} & \equiv (6^{20})^{2} & \equiv 6^{40} \equiv 1 & \pmod{41} \\ b_{40}^{1} & = 1^{4} & \equiv (6^{40})^{1} & \equiv 6^{40} \equiv 1 & \pmod{41} \end{cases}$$

These numbers $b_1, b_2, b_4, b_5, b_8, b_{10}, b_{20}, b_{40}$ have these periods (of lengths $40, 20, 10, 8, 5, 4, 2, 1$ respectively). They cannot have shorter periods. If we assume that, say

$$b_2^k = 36^k \equiv 1, \quad \text{for some } k < 20,$$

then we would get also $6^{2k} \equiv 1 \pmod{41}$ for some power $2k < 40$, but as we saw in Figure 1, number 6 is the primitive root (its period is exactly 40).

Moreover, no number a can have a period that is not a divisor of 40, because otherwise it would violate the Little Fermat theorem (we would have $a^{40} \not\equiv 1 \pmod{41}$). □

5. Complete the proofs in Coq. You may use the non-constructive `classic` and `NNPP` axioms if needed (and also various results from the library `ZArith`). Submit your file as plain-text `hw6_question5.v`.

Full answer is available in the course Webpage under *Discrete 2021: Assignments*. See `https://bit.ly/3rq8K3V`.

□

```
Require Import ZArith.
Require Import Znumtheory.

Section Homework6_Problems.

Open Scope Z_scope.

(* See Theorem1 (i), p.252 in the textbook *)
Lemma sample6_1: forall a b c:Z, (a | b) -> (a | c) -> (a | b+c).
Proof.
  Admitted.


(* See Theorem1 (ii), p.252 in the textbook *)
Lemma sample6_2: forall a b c:Z, (a | b) -> (a | b*c).
Proof.
  Admitted.


(* See Theorem1 (iii), p.252 in the textbook *)
Lemma sample6_3: forall a b c: Z, (a | b) -> (b | c) -> (a | c).
Proof.
  Admitted.


(* See Theorem4, p.255 in the textbook *)
Lemma sample6_4: forall a b m: Z, (m <> 0) ->
    ((a mod m) = (b mod m) <-> (exists k:Z, a = b+k*m)).
Proof.
  Admitted.


Lemma sample6_5 : forall a b c : Z, (a|b) \/ (a|c) -> (a| b*c).
Proof.
  Admitted.

Close Scope Z_scope.

End Homework6_Problems.
```