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 $\gcd(a, b) \mid d$.

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

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

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

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

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

   (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 $a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \not\equiv 0 \pmod{11}$.

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

   (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.

   (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 $a^k \equiv 1 \pmod{41}$.

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`.

```
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.
```