Discrete Mathematics **DSBA**

Seminar 12. Numbers II. The Euclidean Algorithm

Preambula. If you are asked to find the number of solutions of an equation modulo N then you shall find the number of reminders (or congruence classes modulo N) satisfying the equation.

1. Find all integers x and y for which $45x - 37y = 25$.

2. Find the number of solutions of the equation $39x \equiv 104 \pmod{221}$.

3. Let $\gcd(a, b) = 1$. Find all possible values of $\gcd(a + b, a^2 + b^2)$.

4. Solve the system of modulo congruence equations

$$\begin{aligned} x &\equiv 3 \pmod{13}, \\ x &\equiv 4 \pmod{14}, \\ x &\equiv 5 \pmod{15}. \end{aligned}$$

5. Solve the system of modulo congruence equations

$$\begin{aligned} x &\equiv 3 \pmod{15}, \\ x &\equiv 4 \pmod{21}, \\ x &\equiv 5 \pmod{35}. \end{aligned}$$

6. Find the reminder after devision of **a)** 19^{10} by 66; **b)** 19^{14} by 70; **c)** 17^9 by 48; **d)** $14^{14^{14}}$ by 100.

7. Find the remainder of $\underbrace{111\ldots111}_{105 \text{ digits}}$ after devision by 107.

8. Prove inclusion-exclusion formulas for gcd and lcm (least common multiple).

a) $\operatorname{lcm}(x, y) = \dfrac{xy}{\gcd(x, y)}$;

b) $\operatorname{lcm}(x, y, z) = \dfrac{xyz \cdot \gcd(x, y, z)}{\gcd(x, y) \cdot \gcd(x, z) \cdot \gcd(y, z)}$;

9. Prove that $(p - 1)! \equiv -1 \pmod{p}$ for any prime number p.

Discrete Mathematics **DSBA**

Home Assignment 12

1. Find all integers x and y for which $102x + 39y = 27$.

2. Find the number of of positive integers x that are smaller or equal than 10800 and relatively prime with 10800 (i.e. $\gcd(x, 10800) = 1$).

3. Compute $9^{10^{3979}} \mod 19$.

4. Prove that if $\gcd(a, b) = \gcd(a, c) = 1$ then $\gcd(a, bc) = 1$.

5. Find the multiplicative inverse of 74 modulo 47.

6. Do there exist nonnegative integers x and y that are the solution of the equation $31x + 75y = 2345$?

7. Compute $\gcd(3^{168} - 1, 3^{140} - 1)$.

8. Solve the congruence equation $x^3 \equiv x \pmod{125}$. (You shall find all the remainders modulo 125 satisfying the equation.)