Mathematical Institute University of Szczecin Prof. Dr. Habil. Oleg Bogopolski

Your should bring your solutions to the lecture on 10.03.

Cryptography

Series 1

Problem 1.

- (a) Find the greatest common divisor gcd(78, 34).
- (b) Find some integer numbers u, v such that $78u + 34v = \gcd(78, 34)$.

Problem 2.

(a) Let a and n be two coprime natural numbers. Prove that there exists a natural number u such that

$$au \equiv 1 \pmod{n}$$
.

(Hint: Use Theorem 1.1 about Euclidean algorithm.)

(b) Find all integer numbers x such that

$$\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 2 \pmod{5}, \\ x \equiv 3 \pmod{8}. \end{cases}$$

(Hint: Use Chinese remainder theorem.)

Problem 3. Let F_n be the *n*-th Fibonacci number.

[4+6 points]

- (a) Find the minimal prime number n > 2 such that F_n is not a prime number.
- (b) Prove Cassini's identity $F_{n-1}F_{n+1} F_n^2 = (-1)^n$.

[4+6 points]

[4+6 points]