Fachbereich Mathematik — WS 2017/18
Elena Klimenko — Homework 6

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, December 1st, at 12:05 pm.

We start with a definition.

Definition. Let n be an odd positive integer and $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ its prime factorization. Then for $a \in \mathbb{Z}$ the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined as follows:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{k_1} \cdot \left(\frac{a}{p_2}\right)^{k_2} \cdots \left(\frac{a}{p_r}\right)^{k_r},$$

where all $\left(\frac{a}{p_i}\right)$ are the Legendre symbols.

The Jacobi symbol is a generalization of the Legendre symbol and has the following **properties** (here all a, b, n, $m \in \mathbb{Z}$ and, moreover, n and m are odd and positive).

J1. If $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

J2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$

J3. $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{a}{m}\right)$

J4. If $\gcd(b, n) = 1$, then $\left(\frac{ab^2}{n}\right) = \left(\frac{a}{n}\right)$.

J5. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4} \\ -1 & \text{if } n \equiv 3 \pmod{4} \end{cases}$

J6. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8} \\ -1 & \text{if } n \equiv \pm 3 \pmod{8} \end{cases}$

J7. $\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}} \left(\frac{m}{n}\right) = \begin{cases} \left(\frac{m}{n}\right) & \text{if } n \equiv 1 \pmod{4} \text{ or } m \equiv 1 \pmod{4} \\ -\left(\frac{m}{n}\right) & \text{if } n \equiv m \equiv 3 \pmod{4} \end{cases}$

Here (and on the back) are the problems for homework.

1. Prove properties J4–J7 from the list above.

2. (a) Assume $\left(\frac{a}{n}\right) = 1$, where n is an odd positive integer and $a \in \mathbb{Z}$. Does it mean that $x^2 \equiv a \pmod{n}$ has a solution? If yes, then prove this. If no, then give a counterexample with a full explanation.

(b) Does the congruence

$$x^2 \equiv 888 \pmod{1999}$$

have a solution?

Hint. Try to find the shortest way to answer this question. The Jacobi symbol helps!

(c) Determine all odd primes p for which the equation

$$x^2 \equiv 3 \pmod{p}$$

has a solution.

3. Prove that for every positive integer n there is a prime number p so that all numbers $1, 2, \ldots, n$ are quadratic residues modulo p.

Hint. Use properties of the Legendre symbol and the following

Theorem (Dirichlet). For each $a \in \mathbb{N}$ there are infinitely many primes of the form $1 + ak$ with $k \in \mathbb{N}$.

4. (a) Prove that if $M_n = 2^n - 1$ is prime, then n is also prime.

(b) Let $u = 2+\sqrt{3}$, $v = 2-\sqrt{3}$, and let the siquence $(L_n)_{n\in\mathbb{N}}$ be defined as follows:

$$L_1 = 4, \quad L_n = L_{n-1}^2 - 2 \quad \text{for all} \quad n \geq 2.$$

Prove that $L_n = u^{2^{n-1}} + v^{2^{n-1}}$.