

Prof. Valentin Blomer

University of Toronto Mississauga
Department of Mathematical and Computational Sciences

Introduction to Number Theory

Problem Set 9 (due Mar 25, 2008)

9.1. a) Compute $\left(\frac{85}{101}\right)$, $\left(\frac{29}{541}\right)$, $\left(\frac{101}{1987}\right)$. *Hint:* 101, 541, 1987 are prime.

b) One can show that $p := 2^{127} - 1$ is prime. Show that $\left(\frac{2310}{p}\right) = -1$. *Hint:* factor 2310, use quadratic reciprocity, and Little Fermat.

9.2. The Legendre-symbol $\left(\frac{a}{p}\right)$ is only defined for p a prime. Here we define the following generalization (which is then called “Jacobi-symbol”): if $m = \prod_j p_j^{e_j}$ is odd and $\gcd(a, m) = 1$, we define

$$\left(\frac{a}{m}\right) := \prod_j \left(\frac{a}{p_j}\right)^{e_j}$$

where on the right hand side we have the usual Legendre symbols. Show

$$\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right) \quad \text{if } n \equiv n' \pmod{m}, \gcd(n, m) = 1,$$

and show that

$$\left(\frac{n}{m}\right) \left(\frac{n}{m'}\right) = \left(\frac{n}{mm'}\right), \quad \left(\frac{n}{m}\right) \left(\frac{n'}{m}\right) = \left(\frac{nn'}{m}\right)$$

for any odd m, m' and any n, n' with $\gcd(nn', mm') = 1$. If $\left(\frac{n}{m}\right) = 1$, can we conclude that n is a quadratic residue modulo m ? Justify your answer.

9.3. Let p be an odd prime, and assume q is the smallest positive integer with $\left(\frac{q}{p}\right) = -1$, that is, the smallest quadratic nonresidue modulo p .

a) Show that q is prime.

b) Show that $q < \sqrt{p} + 1$ as follows: Using the multiplicative properties of the Legendre symbol, show first that $\left(\frac{kq}{p}\right) = -1$ for $1 \leq k \leq q - 1$. Now assume that there is a $k \in [1, q - 1]$ such that $kq > p$. Let k_0 be the smallest such k . Show that $p < k_0q < p + q$, and conclude that kq is a quadratic residue modulo p . From this contradiction derive $(q - 1)q < p$, and thus the claim.