

Prof. Valentin Blomer

University of Toronto Mississauga  
Department of Mathematical and Computational Sciences

## Introduction to Number Theory

### Problem Set 8 (due Mar 18, 2008)

**8.1.** Let  $n, m > 1$  be integers, and assume  $\gcd(a, n) = 1$ . Let  $k$  be the order of  $a$  modulo  $n$ . Show that the order of  $a^m$  is  $k/\gcd(m, k)$ . Conclude that if  $(\mathbb{Z}/n\mathbb{Z})^*$  has primitive roots at all, then there are exactly  $\phi(\phi(n))$  primitive roots.

**8.2.** Find a primitive root modulo 13, and express all  $[a] \in (\mathbb{Z}/13\mathbb{Z})^*$  as a power of this primitive root. What are the quadratic residues modulo 13? Express them as powers of the primitive root.

b) Let  $n > 2$  be any integer such that  $(\mathbb{Z}/n\mathbb{Z})^*$  is cyclic and let  $g$  be a primitive root. Then every  $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$  can be written as  $[a] = [g]^j$  for some  $j$  that is determined modulo  $\phi(n)$ . With this notation let us define

$$\text{ind}_g(a) = j \quad (\in \mathbb{Z}/\phi(n)\mathbb{Z})$$

the index of  $a$  with respect to the primitive root  $g$ . Show

$$\begin{aligned}\text{ind}_g(ab) &= \text{ind}_g(a) + \text{ind}_g(b), & \text{ind}_g(a^m) &= m \cdot \text{ind}_g(a), \\ \text{ind}_g(1) &= 0, & \text{ind}_g(g) &= 1, \\ \text{ind}_g(-1) &= \frac{1}{2}\phi(n), & \text{ind}_g(n-a) &= \text{ind}_g(-a) = \frac{1}{2}\phi(n) + \text{ind}_g(a).\end{aligned}$$

**8.3.** a) Show that the only quadratic residue modulo 2 is 1 and the only quadratic residue modulo 4 is 1.

b) Let  $e \geq 3$ , and let  $a$  be a quadratic residue modulo  $2^e$ . Show that  $a \equiv 1 \pmod{8}$ .

c) Let  $e \geq 3$ . How many quadratic residues modulo  $2^e$  are there? (*Hint:* we did this in class.) Use part b) to show that the quadratic residues modulo  $2^e$  are exactly all  $a \equiv 1 \pmod{8}$ .

**8.4.** On page 130 in the book you find the following table that calculates the values  $\left(\frac{q}{p}\right)$ :

	q=3	5	7	11	13	17	19
p=3	0	-1	1	-1	1	-1	1
5	-1	0	-1	1	-1	-1	1
7	-1	-1	0	1	-1	-1	-1
11	1	1	-1	0	-1	-1	-1
13	1	-1	-1	-1	0	1	-1
17	-1	-1	-1	-1	1	0	1
19	-1	1	1	1	-1	1	0

Add the the next two lines and columns.