

Prof. Valentin Blomer

University of Toronto Mississauga  
Department of Mathematical and Computational Sciences

## Introduction to Number Theory

### Problem Set 4 (due Feb 5, 2008)

**4.1.** a) Show that the congruence  $x^2 \equiv a \pmod{8}$  has solutions only if  $a \in \{0, 1, 4\}$ . Conclude that an odd square is congruent to 1 (mod 8).

b) Show that the congruence  $x^2 + y^2 + z^2 \equiv 7 \pmod{8}$  has no solutions  $x, y, z \in \mathbb{Z}$ . Conclude that the equation  $x^2 + y^2 + z^2 = n$  has no integer solutions if  $n \equiv 7 \pmod{8}$ .

c) Let  $n \in \mathbb{N}$  and assume that  $x, y, z$  are a solution to  $x^2 + y^2 + z^2 = 4n$ . Show that  $x, y, z$  are even, and conclude that the equation  $x^2 + y^2 + z^2 = n$  has a solution.

d) Show that the equation  $x^2 + y^2 + z^2 = n$  has no solution if  $n = 4^k(8m + 7)$  for any  $k, m \in \mathbb{N}_0$ .

**4.2.** Find all solutions of the congruence  $513x \equiv 24 \pmod{1194}$ .

**4.3.** Find all solutions of the following system of congruences:

$$x^3 \equiv 6 \pmod{7}, \quad 13x \equiv 2 \pmod{17}, \quad 6x \equiv 15 \pmod{27}.$$

**4.4.** We want to find all solutions of the equation  $x^2 + y^2 = z^2$  with  $\gcd(x, y, z) = 1$ . Proceed as follows:

a) Show that under the assumption  $\gcd(x, y, z) = 1$ ,  $z$  must be odd and exactly one of the numbers  $x, y$  must be even. Without loss of generality assume that  $y$  is even.

*Hint:* Proceed as in problem 4.1a

b) Show that  $x \pm z$  is even, and  $\gcd\left(\frac{x+z}{2}, \frac{x-z}{2}\right) = 1$ .

c) Use part b) to show that  $x = u^2 - v^2$ ,  $y = 2uv$ ,  $z = u^2 + v^2$  for two coprime integers  $u, v \in \mathbb{Z}$  one of which is even and the other is odd.

d) Check by substituting that the expressions for  $x, y, z$  are indeed solutions to  $x^2 + y^2 = z^2$ , and that  $\gcd(x, y, z) = 1$ .