

Algebra I: Homework assignment 1
Due date: September 8

1. Find all integer solutions of a Diophantine equation

$$27x + 16y = 1.$$

Definition: A residue a modulo n is called *quadratic residue*, if the equation $x^2 = a \pmod n$ has an integer solution. Otherwise, a is called *quadratic non-residue*.

2. Let p be a prime number.

(a) Show that the number of nonzero quadratic residues modulo p coincides with the number of quadratic non-residues. Give a counterexample to this statement, when p is not prime.

(b) Show that the equation $x^2 + y^2 = a \pmod p$ has an integer solution for any integer a . Give a counterexample to this statement, when p is not prime.

- (c) Show that -1 modulo p is a quadratic residue iff $p = 2$ or $p = 1 \pmod 4$.

3. Using that

$$718865222040754575648532881408$$

is equal to x^{13} for some integer x , find x without calculator.

Hint: use criteria for divisibility by 2, 9 and 11.

4. (a) Let m and n be relatively prime integers. Prove that

$$(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/mn\mathbb{Z})^*.$$

(b) Let $n = p_1^{m_1} \dots p_k^{m_k}$ be the decomposition of n into prime factors. Find the order of the group $(\mathbb{Z}/n\mathbb{Z})^*$.

5. For each pair of the groups below, find out if they are isomorphic. Justify your answer.

(a) $(\mathbb{Z}/5\mathbb{Z})^*$ and $(\mathbb{Z}/8\mathbb{Z})^*$;

(b) (\mathbb{Q}^*, \times) and $(\mathbb{Q}, +)$;

(c) (\mathbb{R}^*, \times) and $(\mathbb{R}, +)$.

6. Let G be a group. Prove that if $x^2 = 1$ for every $x \in G$, then G is abelian.