Assignment 0x03

Frank Kaiser – 1742945, Jan Martin – 1796943

December 17, 2017

Contents

1 Task 1: Number Theory and Algebra

1.1 Explain why the integers Z form a ring, and the rationals Q form a field.

A ring is a set R with two operations "+" and "*". (R,+) is an abelian group, that means it is associative, commutative and has a neutral and inverse element. (R,*) is a monoid, that means it is associative and has a neutral element. Lastly multiplication is distributive with respect to addition. If all axioms hold, a set is a ring. And they hold for Z.

A field is a ring but with the special case that (R
$\{0\}$, *) is an abelian group. Meaning that associativity and commutativity hold for all elements except 0 and that there also exists a neutral and inverse element for every element of the field.

1.2 Find the inverses of all elements in Z_7^*. Why do all numbers between 1 and 6 have an inverse?

$Z_7^* = 1, 2, 3, 4, 5, 6$

2 Task 2: The RSA cryptosystem