Algebra 1

(Prof. F. Brenti)

Test di Autovalutazione

(9 Dicembre, 2015)

1. State comunicando con il codice RSA. Avete due interlocutori A e B le cui chiavi pubbliche sono $n = 2419$ ed $e = 7$ (A) e $n = 1403$ ed $e = 4$ (B). Le vostre chiavi sono $n = 1157$ ed $e = 497$ (pubbliche) e $d = 17$ (privata). Ricevete da A il messaggio 11. Decodificatelo.

2. Trovare un numero complesso $z \in \mathbf{C}$ tale che $z^3 + 1 - i = 0$.

3. Scrivere il numero 56739 in base 3.

4. Siano G e G' gruppi, $f : G \mapsto G'$ un omomorfismo suriettivo, e $a \in G$. Dimostrare che, allora, $Na = \{x \in G : f(x) = f(a)\}$ dove $N = Ker(f)$ è il nucleo di f. È vero questo risultato se f non è suriettivo?

5. Sia $S = \{12345, 23451, 34512, 45123, 51234, 54321\}$. Decidere se S è un sottogruppo di S_5.

6. Due elementi x, y di un gruppo G si dicono *coniugati* se esiste un elemento $g \in G$ tale che $gxg^{-1} = y$. Dimostrare che x e y sono coniugati se e solo se esistono $a, b \in G$ tali che $x = ab$ e $y = ba$.