Algebra A: Prova 2

UNOFFICIAL

1. Sia R un anello commutativo con unità 1 e sia $I \subset R$ un ideale. Dimostrare che I è massimale se e solo se R/I è un campo.

2. Consideriamo un sistema RSA con chiave pubblica $(13, 209)$.

   (a) Calcolare la chiave privata.

   (b) Calcolare l'unico intero a tale che $0 \leq a < 209$ e $a \equiv 18^{13} \mod 209$, usando l'esponenziazione veloce (metodo dei quadrati ripetuti) e calcoli mod 11, mod 19 e il teorema cinese dei resti.

   (c) Enumeriamo le lettere A-Z da 0 a 25. Si scrive ogni intero tra 0 e 91 come $a_0 + 26a_1$ con $0 \leq a_i \leq 25$. Così ogni lettera viene criptata con due lettere. Criptare la lettera S.

3. Sia $f : \mathbb{Z}[i] \to \mathbb{Z}/29\mathbb{Z}$ definita da $f(a + bi) = [a - 12b]_{29}$. Sia $I = \langle 5 - 2i \rangle$ l'ideale di $\mathbb{Z}[i]$ generato da $5 - 2i$.

   (a) Dimostrare che f è un omomorfismo suriettivo di anelli.

   (b) Dimostrare che 29, $12 + i$ stanno in I.

   (c) Dimostrare che il nucleo di f è I. (Suggerimento: per una direzione osservare che $a + bi = a - 12b + (12 + i)b$.)

   (d) Dimostrare che $\mathbb{Z}[i]/I$ è isomorfo a $\mathbb{Z}/29\mathbb{Z}$.

   (e) Dimostrare che I è massimale.