ALGEBRA 1

a.a. 2017/18

Valentina Barucci e Domenico Fiorenza

Foglio di Esercizi n.3

1. Calcolare le ultime tre cifre decimali di 111^{111} scrivendo $111 = 11 \cdot 10 + 1$ ed utilizzando la formula del binomio di Newton modulo 1000.

2. Calcolare il resto della divisione di 4^{2013} per 15 e per 51.

3. Calcolare le ultime due cifre decimali di 12345^{9876}.

4. Sia
$$f : \mathbb{Z}/(11) \to \mathbb{Z}/(11)$$
l'applicazione definita ponendo $f([a]_{11}) = ([a]_{11})^3$.

   a) f è biiettiva?

   b) Nel caso in cui f sia biiettiva, trovare l'applicazione inversa.

   c) Calcolare $f^{-1}([9]_{11})$

5. Si consideri una criptazione RSA con chiave pubblica $(n, e) = (323, 5)$. Scoprire la chiave privata e decifrare il messaggio $y \equiv 100 \pmod{323}$.

6. Dimostrare che un anello commutativo (con unità) finito è un dominio d'integrità se e soltanto se è un campo (ovvero se e solo se ogni elemento diverso da zero è invertibile). Mostrare con un controesempio che questo non è necessariamente vero se l'anello non è finito.

7. Quali sono i numeri che in base 2 si scrivono come una successione di 1? (ad esempio $7 = 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$ si scrive in base 2 come 111). Mostrare che se un numero di questo tipo è primo allora il numero di volte che compare 1 nella sua scrittura in base 2 è anch'esso un numero primo. È vero il viceversa?

8. Siano p e q due primi distinti maggiori di 2. Dimostrare che l'equazione $x^2 - 1 = 0$ ha esattamente quattro radici distinte in $\mathbb{Z}/(pq)$.

9. Calcolare il MCD della seguente coppia di polinomi
$$(x^4 - 2x^2 - x - 3, x^3 - 3x^2 + x + 1),$$
considerando tali polinomi prima come elementi di $\mathbb{Q}[x]$ e poi come elementi di $\mathbb{F}_7[x]$.