

Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2008/2009
TN1 - Introduzione alla teoria dei numeri
Appello B
2 luglio 2009

Cognome_____ Nome_____

Numero di matricola_____

Avvertenza: Svolgere ogni esercizio nello spazio assegnato, senza consegnare altri fogli e **giustificando tutte le affermazioni fatte**. E' consentito l'uso di libri, appunti e calcolatrici.

1. Dire se le seguenti equazioni diofantee in tre indeterminate ammettono soluzioni e, in caso affermativo, determinarle:
 - (a) $2X + Y - 3Z = 7$
 - (b) $3X + 21Y + 6Z = 15$
 - (c) $6X + 54Y + 201Z = 19$

2. Sia p un numero primo. Dimostrare che se a e b sono interi tali che $a^p \equiv b^p \pmod{p}$, allora $a^p \equiv b^p \pmod{p^2}$.

3. Determinare tutte le (eventuali) soluzioni della seguente congruenza polinomiale:

$$f(X) = X^6 - 5X^5 + 4X^3 - X + 22 \equiv 0 \pmod{441}$$

4. Sia p un numero primo dispari tale che $q := 2p + 1$ è un numero primo. Sia r una radice primitiva (modulo q).
- (a) Determinare il numero delle radici primitive (modulo q).
 - (b) Descrivere l'insieme di tutte le radici primitive (modulo q) mediante r .
 - (c) Descrivere il gruppo dei residui quadratici di q mediante r .
 - (d) Utilizzando i due punti precedenti, determinare una partizione di U_q .
 - (e) Verificare che -4 è un non residuo quadratico di q .
 - (f) Provare che -4 è una radice primitiva (modulo q).

5. (a) Sapendo che 2 è una radice primitiva (modulo 11), trovare tutte le radici primitive (modulo 22).
- (b) Risolvere le seguenti congruenze:
- i. $X^7 \equiv 17 \pmod{22}$;
 - ii. $9^X \equiv 3 \pmod{22}$;
 - iii. (**FAC.**) $5^X \equiv 15X \pmod{22}$.

6. Provare che un numero intero $n > 1$ è composto se e solo se $\sigma(n) > n + \sqrt{n}$.