Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2008/2009
TN1 - Introduzione alla teoria dei numeri
Appello A
8 giugno 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. Sia p un numero primo dispari. Provare che per ogni $n \geqslant 1$ si ha:

$$[(p-1)!]^{p^{n-1}} \equiv -1 \pmod{p^n}.$$

2. Risolvere, se possibile, il seguente sistema lineare in tre indeterminate:

$$\begin{cases} \begin{array}{rcrcrcll} X & + & 2Y & + & 3Z & \equiv & 1 & \pmod 7 \\ & & Y & + & 2Z & \equiv & 3 & \pmod 7 \\ 2X & + & & + & 5Z & \equiv & 4 & \pmod 7 \end{array} \end{cases}$$

3. (a) Sapendo che 3 è una radice primitiva modulo 17, verificare che 3 è anche una radice primitiva modulo 34.
   (b) Trovare tutte le radici primitive modulo 34.
   (c) Risolvere le seguenti congruenze:
      i. $X^{14} \equiv 15 \pmod{34}$;
      ii. $5^X \equiv 29 \pmod{34}$.

4. Si consideri la congruenza quadratica

$$X^2 + 4X + 2 \equiv 0 \pmod{p} \qquad (*)$$

(a) Determinare i numeri primi p per i quali la congruenza $(*)$ è risolubile.

(b) Trovare le soluzioni della conguenza

$$X^2 + 4X + 2 \equiv 0 \pmod{31 \cdot 17^2}$$

5. (a) Sia p un primo dispari. Provare che se p divide $a^2 + b^2$ con a e b numeri interi primi tra loro, allora $p \equiv 1 \pmod 4$.

   (b) Utilizzando il punto (a), provare che ogni divisore positivo di una somma di due quadrati di interi primi tra loro è esso stesso una somma di due quadrati.

6. Si consideri la funzione moltiplicativa $F = \tau * \varphi$.

(a) Calcolare $F(33)$ e $F^{-1}(33)$.

(b) Sia f la funzione aritmetica determinata dalla formula di inversione di Möbius. Calcolare $f(33)$.