Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2011/2012
TN410 - Introduzione alla teoria dei numeri
Appello A - Prima parte
15 giugno 2012

*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. Determinare tutte le eventuali soluzioni del seguente sistema di congruenze lineari:

$$\begin{cases} 6X \equiv 9 \pmod{15} \\ 10X \equiv 4 \pmod{32} \\ 17X \equiv 4 \pmod{19} \\ 9X \equiv 5 \pmod{11} \end{cases}$$

2. Siano p un numero primo e k un numero naturale tale che $0 \leqslant k \leqslant p-1$; provare che:

$$k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}$$

3. (a) Determinare tutte le radici primitive modulo 54.
   (b) Scrivere la tabella degli indici rispetto alla più piccola radice primitiva positiva modulo 54.
   (c) Risolvere le seguenti congruenze:
      i. $X^6 \equiv 37 \pmod{54}$;
      ii. $43^X \equiv 19 \pmod{54}$.

Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2011/2012
TN410 - Introduzione alla teoria dei numeri
Appello A - seconda parte
15 giugno 2012

*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. Si consideri la congruenza quadratica:

$$X^2 \equiv 169 \pmod{2^4 \cdot 5^3 \cdot 7^2} \qquad (*)$$

   (a) Verificare che la congruenza $(*)$ è risolubile e deterrminare il numero delle sue soluzioni.

   (b) Trovare le soluzioni delle seguenti congruenze:

      i. $X^2 \equiv 169 \pmod{2^4}$;
      ii. $X^2 \equiv 169 \pmod{5^3}$;
      iii. $X^2 \equiv 169 \pmod{7^2}$.

2. Sia p un numero primo dispari tale che $p \equiv 1 \pmod 4$.

   (a) Motivare il fatto che esiste una radice primitiva dispari r di p. Verificare che esiste un numero naturale k, $1 \leqslant k \leqslant p-1$ tale che $r^k \equiv 2 \pmod p$.

   (b) Provare che $r^{2\left(k+\frac{p-1}{4}\right)} \equiv -4 \pmod p$.

   (c) Dedurre dai punti precedenti che p divide la somma di due quadrati tra loro coprimi e ciascuno dei quali maggiore di 3.

3. Provare che per ogni intero positivo n si ha:

$$\left(\sum_{d|n} \tau(d)\right)^2 = \sum_{d|n} \tau(d)^3$$