Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2010/2011
TN410 - Introduzione alla teoria dei numeri
Appello A - Prima parte
17 giugno 2011

*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. Trovare, al variare del parametro λ ($0 \leq \lambda \leq 4$), le soluzioni del seguente sistema lineare in tre indeterminate:

$$\begin{cases} X + Y + \lambda Z \equiv 1 \pmod 5 \\ X + \lambda Y + Z \equiv 1 \pmod 5 \\ \lambda X + Y + Z \equiv \lambda \pmod 5 \end{cases}$$

2. Determinare tutte le (eventuali) soluzioni della seguente congruenza polinomiale:
$$f(X) = X^6 - 2X^5 - 35 \equiv 0 \pmod{6125}$$

3. Siano p e q numeri primi dispari tali che

$$p = 2q + 1$$

Provare che se a è un numero intero tale che $1 < a < p - 1$, allora $p - a^2$ è una radice primitiva dell'unità modulo p.

Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2010/2011
TN410 - Introduzione alla teoria dei numeri
Appello A - seconda parte
17 giugno 2011

*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.

   Sia a un numero intero tale che $\mathrm{MCD}(a, p) = 1$; a si dice un *residuo biquadratico* di p se esiste un numero intero x tale che $x^4 \equiv a \pmod p$.

   (a) Provare che -1 è un residuo biquadratico di p se e solo se $p \equiv 1 \pmod 8$.

   (b) Sia $p \equiv 3 \pmod 4$ e sia a un intero tale che $\mathrm{MCD}(a, p) = 1$.

      i. Provare che uno soltanto tra a e $-a$ è un residuo quadratico di p.

      ii. Provare che a è un residuo biquadratico di p se e solo se a è un residuo quadratico di p.

2. (a) Verificare che:

   (1) $\frac{382}{73} = [5; 4, 3, 2, 2]$;
   (2) $\frac{2365}{382} = [6; 5, 4, 3, 2, 2]$;

   (b) Sia $(a_n)_{n \geqslant 0}$ la successione di numeri naturali definita da:
   $a_0 := 1$, $a_1 := 2$ e $a_n := na_{n-1} + a_{n-2}$ per $n \geqslant 2$.
   Provare che per ogni $n \geqslant 2$ si ha:

$$\frac{a_n}{a_{n-1}} = [\underbrace{n; n-1, n-2, \cdots, 4, 3, 2, 2}_{n}]$$

3. Sia $n = p_1^{e_1} \cdot ... \cdot p_r^{e_r}$ la fattorizzazione in primi distinti di un numero naturale $n \geqslant 2$ con $e_i \geqslant 1$ per $1 \leqslant i \leqslant r$.

   Si consideri la seguente funzione aritmetica:

$$\omega(n) := \begin{cases} 0 & \text{se } \; n = 1 \\ \\ r & \text{se } n \geqslant 2 \end{cases} .$$

   Si dia per noto che la funzione aritmetica $n \longmapsto 2^{\omega(n)}$ è moltiplicativa. (vedere il 2 esonero).

   Si consideri la funzione aritmetica ψ definita da $\psi(n) = \tau(n^2)$ per ogni $n \in \mathbb{N}^+$.

   Provare che per ogni $n \in \mathbb{N}^+$ si ha che

$$\psi(n) = \sum_{d|n} 2^{\omega(d)}$$