Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2007/2008
TN1 - Introduzione alla teoria dei numeri
Prova di esame - Appello A
12 giugno 2008

*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 della congruenza polinomiale:

$$X^4 + 51X^3 + 35X^2 + 21X + 36 \equiv 0 \pmod{189}.$$

2. Sapendo che 2 è una radice primitiva $\pmod{29}$, risolvere le seguenti congruenze:

   (a) $X^7 \equiv 1 \pmod{29}$;

   (b) $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \equiv 0 \pmod{29}$.

3. Sia p un numero primo $\equiv 3 \pmod{4}$.

   (a) Provare che se a è un residuo quadratico modulo p, allora $a^{\frac{p+1}{4}}$ è una soluzione della congruenza

   $$X^2 \equiv a \pmod{p}.$$

   (b) Trovare una soluzione della congruenza $X^2 \equiv 7 \pmod{787}$.

   (c) Trovare le due soluzioni della congruenza $X^2 \equiv 7 \pmod{787}$ comprese tra 1 e 786.

4. Sia p un numero primo $\equiv 1$ o $3 \pmod 8$.

   (a) Calcolare $\left(\frac{-2}{p}\right)$.

   (b) Provare che l'equazione $X^2 + 2Y^2 = p$ ha soluzioni in $\mathbb{Z}$.

5. Si dimostri che l'equazione diofantea $Y^2 = X^3 + 7$ non ha soluzioni intere nel modo seguente:

   si supponga che $x_0, y_0 \in \mathbb{Z}$ siano tali che $y_0^2 = x_0^3 + 7$;

   - provare che x_0 è dispari;
   - aggiungendo 1 ad entrambi i membri di $y_0^2 = x_0^3 + 7$ si ottiene $y_0^2 + 1 = x_0^3 + 8$; dimostrare che non tutti i fattori primi di $x_0^3 + 8$ sono congrui a 1 (mod 4);
   - dedurre dal punto precedente una contraddizione.

6. Sia $n > 1$ un numero intero. Provare che:

   (a) se n è un numero primo, allora $\frac{\varphi(n)\sigma(n)+1}{n}$ è un numero intero;

   (b) se n è divisibile per il quadrato di un numero primo, allora $\frac{\varphi(n)\sigma(n)+1}{n}$ non è un numero intero.