Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2011/2012
TN410 - Introduzione alla teoria dei numeri
Appello B
3 luglio 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 il seguente sistema lineare in due variabili:

$$\begin{cases} \lambda X - 2Y \equiv \mu \pmod{11} \\ 3X + \lambda Y \equiv 5\mu + 2 \pmod{11} \end{cases}$$

   (a) Stabilire quando, al variare di λ e μ con $0 \leq \lambda,\ \mu \leq 10$, il sistema è risolubile e nei casi in cui è risolubile quante soluzioni ammette.

   (b) Trovare, se esistono, le soluzioni del sistema dato per $4 \leqslant \lambda \leqslant 5$ e $5 \leqslant \mu \leqslant 6$.

2. Siano p e q numeri primi.

   Si consideri il polinomio ciclotomico

$$\Phi_q(X) = X^{q-1} + X^{q-2} + \cdots + X + 1 \in \mathbb{Z}_p[X]$$

   Provare che

   (a) se $p = q$, allora $\Phi_q(X)$ ha una sola radice in $\mathbb{Z}_p$;
   (b) se $p \equiv 1 \pmod{q}$, allora $\Phi_q(X)$ ha $q - 1$ radici in $\mathbb{Z}_p$;
   (c) negli altri casi $\Phi_q(X)$ non ha radici in $\mathbb{Z}_p$.

   (SUGG: Si ricordi il Piccolo Teorema di Fermat ed il Teorema di Lagrange)

3. Determinare tutte le (eventuali) soluzioni della seguente congruenza polinomiale:
$$f(X) = X^3 + 3X^2 + 2X + 1 \equiv 0 \pmod{343}$$

4. Sapendo che 2 è una radice primitiva (mod 19)

   (a) trovare tutte le radici primitive (mod 19);

   (b) trovare le (eventuali) soluzioni della congruenza

   $$7X^{13} \equiv 11 \pmod{19};$$

   (c) trovare le (eventuali) soluzioni della congruenza

   $$7^X \equiv 15 \pmod{19}.$$

5. Utilizzando la LRQ, trovare il valore dei seguenti simboli di Legendre:

$$\left(\frac{63}{79}\right), \quad \left(\frac{-228}{409}\right), \quad \left(\frac{464}{829}\right), \quad \left(\frac{-264}{977}\right).$$

6. Siano n ed m numeri naturali maggiori di 1 tali che ogni numero primo che divide n divide anche m. Provare che

$$\varphi(nm) = n\varphi(m)$$

In particolare, per ogni numero naturale positivo n, si ha che

$$\varphi(n^2) = n\varphi(n)$$