Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2005/2006
TN 1
Prima prova di valutazione intermedia - 7 aprile 2006

NOTA: Svolgere gli esercizi nello spazio assegnato, senza consegnare altri fogli e giustificando tutte le affermazioni. **E' consentito l'uso della calcolatrice.** Non è consentito l'uso di libri e appunti.

Esercizio 1. Sia $n \in \mathbb{N}$, $n \geq 2$. Si consideri il seguente sistema di congruenze:

$$\begin{cases} 5X \equiv 4 \, (\text{mod } 12) \\ 5X \equiv 1 \, (\text{mod } 7) \\ 5X \equiv 5 \, (\text{mod } n) \end{cases}$$

(a) Determinare se il sistema ha soluzione per $n = 8$.

(b) Determinare il più piccolo intero $n_0 \geq 2$ per il quale il teorema cinese dei resti ci assicura che il sistema, per $n = n_0$, ha <u>un'unica soluzione</u> $(\text{mod } 12 \cdot 7 \cdot n_0)$.

(c) Determinare la soluzione del sistema per $n = n_0$.

Esercizio 2. Si consideri l'equazione diofantea in due indeterminate:

$$(3\lambda + 1)X + 6Y = 15.$$

(a) Determinare per quali $\lambda \in \mathbb{Z}$ l'equazione diofantea ha soluzione.

(b) Determinare tutte le soluzioni dell'equazione diofantea per il più piccolo $\lambda \geq 1$ per cui l'equazione ha soluzione.

Esercizio 3. Si consideri il polinomio $f(X) := 6X^7 + 7X^4 - 16X + 3 \in \mathbb{Z}[X]$.

(a) Dare una stima (giustificandola) del numero massimo di soluzioni che può avere la congruenza $f(X) \equiv 0(\text{mod } 6)$ (senza risolverla!).

(b) Determinare tutte le soluzioni della congruenza $f(X) \equiv 0(\text{mod } 54)$.

Esercizio 4.

(a) Dare la definizione di radice primitiva dell'unità modulo un intero n e di indice di un intero a rispetto a una radice primitiva.

(b) Determinare tutte le radici primitive (mod 23).

(c) Determinare per quali valori di $a \in \mathbb{N}$ la congruenza $X^8 \equiv a(\text{mod } 23)$ ha soluzione.

(d) Determinare tutte le soluzioni della congruenza per il più piccolo $a > 0$ per il quale ha soluzione.

Esercizio 5. Vogliamo dimostrare che esistono infiniti primi congrui a 2 (mod 3). Ragioniamo per assurdo: si supponga che $\{p_1, p_2, \ldots, p_n\}$, $n \in \mathbb{N}$, sia l'insieme di tutti e soli i numeri primi congrui a $2 \pmod 3$. Sia $a := p_1 p_2 \ldots p_n + 1$ e $b := p_1 p_2 \ldots p_n + 3$.

(a) Mostrare che a e b non sono divisibili per nessun primo congruo a $2 \pmod 3$.

(b) Dimostrare che $2^n \equiv 1 \pmod 3$ se n è pari e $2^n \equiv 2 \pmod 3$ se n è dispari.

(c) Se n è pari, dimostrare che a deve essere divisibile per un primo congruo a 2 (mod 3).

(d) Se n è dispari, dimostrare che b deve essere divisibile per un primo congruo a 2 (mod 3).

(e) Dedurne che esistono infiniti primi congrui a 2 (mod 3).