**TN01 - Introduzione alla teoria dei numeri - A.A. 2002/2003**

**Appello X**

**MATRICOLA:** ...............

**COGNOME:** ........................... **NOME:** .....................

**ESERCIZIO 1.** (**7pt**)

$$\begin{cases} 3X + 11\lambda Y \equiv 13\lambda \pmod{17} \\ 11X + 7Y \equiv 1 + 9\mu \pmod{17}\,. \end{cases}$$

(1) Studiare la risolubilità del sistema assegnato al variare di $\lambda$ e $\mu$, con $0 \leq \lambda, \mu \leq 16$ (cioè dire quando è risolubile e, nei casi in cui è risolubile, dire quante soluzioni ammette).
(2) Al variare di $1 \leq \lambda \leq 2$ e $15 \leq \mu \leq 16$, trovare tutte le (eventuali) soluzioni del sistema.

**ESERCIZIO 2.** (**7pt**) Determinare tutte le (eventuali) soluzioni della congruenza polinomiale:

$$X^4 + 55X^3 + 93X^2 + 91X \equiv 0 \pmod{135}.$$

**ESERCIZIO 3.** (**5pt**) Avendo a disposizione 50 asticelle da 34 cm e 70 asticelle da 26 cm, descrivere tutte le possibili combinazioni di asticelle in modo da ottenere una lunghezza pari a $2,40$ m.

**ESERCIZIO 4.** (**4pt**) Determinare in funzione di $\lambda$, con $0 \leq \lambda \leq 10$, quando la congruenza quadratica

$$X^2 + 6X + 5 + 7\lambda \equiv 0 \pmod{11}$$

è risolubile.

(**2pt**) Per ciascun valore di $\lambda$, con $0 \leq \lambda \leq 10$, per il quale la congruenza è risolubile determinare tutte le sue soluzioni.

**ESERCIZIO 5.**

(**5pt**) Mostrare che se $r$ è una radice primitiva di un primo $p$ allora esiste un intero $k$ tale che:

$$r^{k+1} \equiv r^k + 1 \pmod{p}.$$

## SOLUZIONI

**Soluzione Esercizio 1.**

(1) Abbiamo che $\Delta \equiv 4 - 2\lambda \pmod{17}$. Il sistema ammette un'unica soluzione se e soltanto se $\Delta \not\equiv 0 \pmod{17}$, ovvero per $\lambda \not\equiv 2 \pmod{17}$, qualunque sia il valore assunto da $\mu \in \mathbb{Z}$.
Se $\lambda \equiv 2 \pmod{17}$ allora $\Delta \equiv 0 \pmod{17}$, quindi il sistema è risolubile se e soltanto se $\alpha \equiv 0 \pmod{17}$ e $\beta \equiv 0 \pmod{17}$ e tale condizione si verifica se e soltanto se $\mu \equiv 13 \pmod{17}$.

(2) Se $\lambda \equiv 1 \pmod{17}$ e $\mu \equiv 15 \pmod{17}$ oppure $\mu \equiv 16 \pmod{17}$ il sistema ammette un'unica soluzione data, rispettivamente, da $(3, 5)$ e $(13, 10)$.
Se $\lambda \equiv 2 \pmod{17}$ e $\mu \equiv 15, 16 \pmod{17}$, il sistema non è risolubile.

**Soluzione Esercizio 2.** Sia $X^4 + 55X^3 + 93X^2 + 91X \equiv 0 \pmod{135}$. Allora:
$f(X) \equiv 0 \pmod 5$ ha soluzione: $0, 1, 2$;
$f(X) \equiv 0 \pmod 3$ ha soluzioni: $0, 1$;
$f(X) \equiv 0 \pmod 9$ ha soluzioni: $0,\ 7$;
$f(X) \equiv 0 \pmod{27}$ ha soluzioni: $2,\ 7$;
$f(X) \equiv 0 \pmod{54}$ ha soluzioni: $0, 7, 27, 61, 81, 115$.

**Soluzione Esercizio 3.**

Basta risolvere l'equazione diofantea $34X + 26Y = 240$ (dove $X$ rappresenta il numero di asticelle da 34 cm ed $Y$ quelle da 26 cm). Dividendo tutto per 2 l'equazione diventa $17X + 13Y = 120$. Una soluzione particolare dell'equazione è $(4, 4)$, da cui si ricavano le soluzioni generali:

$$\begin{cases} x_t \equiv 4 - 13t \\ y_t \equiv 4 + 17t \end{cases}$$

al variare di $t \in \mathbb{Z}$.

Le soluzioni cercate devono sottostare alle limitazioni:

$$0 \le x_t \le 50, \qquad 0 \le y_t \le 70.$$

Si ricava che $t = 0$, quindi l'unica possibile soluzione è $(4, 4)$.

**Soluzione Esercizio 4.**

(1) La congruenza data è equivalente alla congruenza

$$(X + 3)^2 \equiv 4 + 4\lambda \pmod{11},$$

Quindi, ponendo $Y := X + 3$, ci si riduce a studiare la congruenza $Y^2 \equiv 4+4\lambda \pmod{11}$. Per la risolubilità si studia il simbolo di Legendre $(\frac{4+4\lambda}{11}) = (\frac{1+\lambda}{11})$, con $0 \le \lambda \le 10$. La congruenza è risolubile per $\lambda \equiv 0, 2, 3, 4, 8, 10$.

(2) Le soluzioni sono le seguenti:
$\lambda = 0 \longrightarrow x \equiv 6, 10 \pmod{11}$;
$\lambda = 2 \longrightarrow x \equiv 9, 7 \pmod{11}$;
$\lambda = 3 \longrightarrow x \equiv 1, 4 \pmod{11}$;
$\lambda = 4 \longrightarrow x \equiv 0, 5 \pmod{11}$;
$\lambda = 8 \longrightarrow x \equiv 2, 3 \pmod{11}$;
$\lambda = 10 \longrightarrow x \equiv 8 \pmod{11}$.

**Soluzione Esercizio 5.** Poniamo $x := r^k$. La congruenza diventa quindi $rx \equiv x + 1 \pmod{p}$. da questa si ricava $x(r-1) \equiv 1 \pmod{p}$ e $x \equiv (r-1)^* \pmod{p}$. Dunque, $k = \mathrm{ind}_r(x) = \mathrm{ind}_r((r-1)^*)$.