TN1 - Introduzione alla teoria dei numeri - A.A. 2009/2010
Valutazione "in itinere" - I Prova

MATRICOLA (o, altro identificativo): .....
COGNOME: ..... **NOME:** .....

esercizio	1	(2.1)	(2.2)	3	(4.1)	(4.2)	(4.3)	(5.1)	(5.2)
punteggio max	6	5	5	8	4	4	3	5	3
punteggio assegnato									
totale									

ESERCIZIO 1. Determinare, al variare di λ, con $4 \leq \lambda \leq 6$, e di μ, con $10 \leq \mu \leq 11$, tutte le (eventuali) soluzioni del seguente sistema di congruenze lineari in due indeterminate:

$$\begin{cases} 12X + 7\lambda Y \equiv \mu + 3 \pmod{17} \\ 15X + 14Y \equiv 9 \pmod{17}\,. \end{cases}$$

ESERCIZIO 2. **(1)** Determinare tutte le eventuali soluzioni del seguente sistema di congruenze, descrivendo brevemente il metodo utilizzato.

$$\begin{cases} 3X \equiv -2 \pmod 5 \\ 2X \equiv 1 \pmod 3 \\ 4X \equiv 5 \pmod 7 \\ 6X \equiv 7 \pmod{11}\,. \end{cases}$$

(2) Stabilire per quali valori del parametro t, limitatamente ai casi $0 \leq t \leq 4$, il seguente sistema di congruenze è risolubile. Per quei valori di t per il quale il sistema è risolubile, determinare tutte le soluzioni in $\mathbb{Z}$, descrivendo brevemente il metodo usato.

$$\begin{cases} 3X \equiv t \pmod 4 \\ X \equiv 5 \pmod 6 \\ 3X \equiv 1 \pmod{10}\,. \end{cases}$$

ESERCIZIO 3. Determinare tutte le (eventuali) soluzioni della congruenza polinomiale, descrivendo brevemente il metodo seguito:

$$4X^3 + 25X^2 + 24X + 36 \equiv 0 \pmod{54}\,.$$

ESERCIZIO 4. Sia p un primo dispari.

(1) Per ogni intero h, con $1 < h < p-1$, mostare che esiste un unico intero $k_h \neq h$, con $1 < k_h < p-1$, tale che $hk_h \equiv 1 \pmod{p}$.

(2) Dimostrare esplicitamente che,

- **(a)** per ogni primo p, sussiste la seguente congruenza $(p-1)! \equiv -1 \pmod{p}$ [Teorema di Wilson];
- **(b)** per ogni primo p dispari, sussiste la seguente congruenza $(p-2)! \equiv 1 \pmod{p}$.

(3) Determinare k, con $0 \leq k \leq 246$, in modo tale che $12! \cdot 18! + 12! + 18! \equiv k \pmod{247}$.

ESERCIZIO 5. (1) Sia a un intero, con $0 \leq a \leq 528$ (dove $529 = 23^2$). Se $23 \nmid a$, determinare h_a, con $0 \leq h_a \leq 528$, in modo tale che

$$a^{507} \equiv h_a \pmod{529}.$$

Se $23 \mid a$, determinare k, con $0 \leq k \leq 528$, in modo tale che

$$23^{507} \equiv k \pmod{529}.$$

(2) Calcolare $5^{1520} \pmod{529}$, descrivendo il metodo seguito.

SOLUZIONI

Soluzione Esercizio 1. Abbiamo che $\Delta \equiv 14\lambda + 15 \pmod{17}$. Il sistema ammette un'unica soluzione per $\Delta \not\equiv 0 \pmod{17}$ ovvero per $\lambda \not\equiv 5 \pmod{17}$, qualunque sia il valore assunto da $\mu \in \mathbb{Z}$.

Se $\lambda = 4$ e $\mu = 10$, allora l'unica soluzione del sistema è data da (5, 5).

Se $\lambda = 4$ e $\mu = 11$, allora l'unica soluzione del sistema è data da (4, 0).

Se $\lambda = 6$ e $\mu = 10$, allora l'unica soluzione del sistema è data da (3, 12).

Se $\lambda = 6$ e $\mu = 11$, allora l'unica soluzione del sistema è data da (4, 0).

Per $\lambda \equiv 5 \pmod{17}$ abbiamo che $\Delta \equiv 0 \pmod{17}$ ed il sistema è risolubile se e soltanto se $14(\mu + 3) - 7 \cdot 5 \cdot 9 \equiv 0 \pmod{17}$ e $12 \cdot 9 - 15(\mu + 3) \equiv 0 \pmod{17}$, cioè se e soltanto se

$\mu \equiv 11 \equiv -6 \pmod{17}$. In tal caso le due congruenze del sistema sono una multipla dell'altra, pertanto le soluzioni del sistema sono le soluzioni di una delle due congruenze del sistema. Le 17 soluzioni distinte (modulo 17) sono le seguenti: $(4,0), (11,1), (1,2), (8,3), (15,4), (5,5), (12,6), (2,7), (9,8), (16,9), (6,10), (13,11), (3,12), (10,13), (0,14), (7,15), (14,16)$.

Infine, se $\lambda = 5$ e $\mu = 10$ il sistema non è risolubile.

Soluzione Esercizio 2. **(1)** L'unica soluzione (mod 1155) è data da

$$1 * 231 + 2 * 385 + 3 * 330 + 3 * 210 \equiv 311 \pmod{1155}.$$

(2) Il sistema dato è equivalente al seguente:

$$\begin{cases} X \equiv 3t \pmod{4} \\ X \equiv 5 \pmod{6} \\ X \equiv 7 \pmod{10}\,. \end{cases}$$

Tale sistema è risolubile se (e soltanto se) $\mathrm{MCD}(n_i, n_j) \mid a_i - a_j$, presi comunque $1 \leq i \lneq j \leq 3$. Pertanto, deve essere $2 \mid 3t - 5$ e $2 \mid 3t - 7$, cioè $2 \mid t - 1$, ovvero $t = 1, 3$ Con il metodo di sostituzione, si vede facilmente che

• per $t = 1$, tutte le soluzioni sono date da $x_h := 47 + h \cdot 60$, $h \in \mathbb{Z}$, dove $60 = \mathrm{mcm}(4, 6, 10)$.

• per $t = 3$, tutte le soluzioni sono date da $x_k := 17 + k \cdot 60$, $k \in \mathbb{Z}$, dove $60 = \mathrm{mcm}(4, 6, 10)$;

Soluzione Esercizio 3. Sia $f(X) := 4X^3 + 25X^2 + 24X + 36$. Allora:

$f(X) \equiv 0 \pmod{2}$ ha soluzione: 0;

$f(X) \equiv 0 \pmod{3}$ ha soluzioni: 0, 2;

$f(X) \equiv 0 \pmod{9}$ ha soluzioni: 0, 2, 3, 6;

$f(X) \equiv 0 \pmod{27}$ ha soluzioni: 2, 6, 15, 24;

$f(X) \equiv 0 \pmod{54}$ ha soluzioni: 2, 6, 24, 42.

Soluzione Esercizio 4. **(1)** Basta osservare che se $1 < h < p - 1$ allora $\mathrm{MCD}(h, p) = 1$ ed inoltre $h^2 \not\equiv 1 \pmod{p}$. Infatti se $h^2 \equiv 1 \pmod{p}$, allora $p \mid (h^2 - 1)$, cioè $p \mid (h + 1)(h - 1)$. Dunque $p \mid (h + 1)$ oppure $p \mid (h - 1)$ ed allora $h \equiv -1 \equiv p - 1 \pmod{p}$ oppure $h \equiv 1 \pmod{p}$, contro le ipotesi.

(2) $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = 1 \cdot \left(\prod_{1 \lneq h \lneq (p-1)} (h \cdot k_h)\right) (p-1) \equiv p - 1 \equiv -1 \pmod{p}$. Essendo $\mathrm{MCD}(p - 1, p) = 1$, moltiplicando ambo i membri per l'inverso aritmetico di $p - 1 \pmod{p}$, si ottiene $(p - 2)! \equiv 1 \pmod{p}$.

(3) $19 \mid (18!+1)$ e $13 \mid (12!+1)$, quindi $247 = 19 \cdot 13 \mid (18!+1)(12!+1) = 18!12! + 18! + 12! + 1$. Pertanto, $k = 246 \equiv -1 \pmod{247}$.

Soluzione Esercizio 5.
Si ricordi che $\varphi(p^2) = p(p-1)$ e che, se $p \nmid a$, $a^{\varphi(p^2)} \equiv 1 \pmod{p^2}$.
(1) $\varphi(529) = 23 * 22 = 506$, quindi
– se $23 \nmid a$, allora $a^{506} \equiv 1 \pmod{529}$, quindi $a^{507} \equiv a \pmod{529}$, e
– se $23 \mid a$, allora $a^{507} \equiv 0 \pmod{529}$.
(2) $1520 = 3 * 506 + 2$, quindi $5^{1520} \equiv 5^2 = 25 \pmod{529}$.