TN1 - Introduzione alla teoria dei numeri - A.A. 2001/2002

Valutazione "in itinere" - I Prova

MATRICOLA: ....

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

esercizio	1	2	3	4	5.1	5.2	5.3	5.4
punteggio max	10	10	15	10	5	2	3	5
punteggio assegnato								
totale								

ESERCIZIO 1. Dimostrare esplicitamente che, per ogni primo p, sussiste la seguente congruenza $(p-1)! \equiv -1 \pmod p$ [Teorema di Wilson].

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

$$4X^3 + 7X^2 + 12X + 9 \equiv 0 \pmod{54}.$$

ESERCIZIO 3. Si supponga di possedere:

- **50** pesi di piombo da **1,3 hg** (ettogrammi) ciascuno,
- **120** pesi di piombo da **7 g** (grammi) ciascuno,
- **80** pesi di piombo da **1,25 hg** (ettogrammi) ciascuno.

Determinare tutte le (eventuali) possibilità di combinare i pesi disponibili in modo da ottenere un peso complessivo di **2,5 kg** (chilogrammi), utilizzando *almeno* **12** pesi da **1,3 hg**.

ESERCIZIO 4. Determinare, al variare di λ, con $4 \leq \lambda \leq 6$ e $15 \leq \mu \leq 16$, tutte le (eventuali) soluzioni del seguente sistema di congruenze lineari in due indeterminate:

$$\begin{cases} 7\lambda X + 12Y \equiv 3\mu \pmod{17} \\ 14X - 2Y \equiv 9 \pmod{17}. \end{cases}$$

ESERCIZIO 5. 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. Per ogni intero h, con $1 < h < p-1$, mostrare che l'unico intero k_h del punto precedente [cioè, $1 < k_h < p-1$, con $hk_h \equiv 1 \pmod p$] è tale che:
$$k_h \equiv \frac{-(p-1)!}{h} \pmod p \ \left(\text{ovvero, } \ p - k_h \equiv \frac{(p-1)!}{h} \pmod p\right).$$
3. Mostrare che
$$\sum_{h=1}^{p-1} h = 1 + \sum_{h=2}^{p-2} k_h + (p-1) \equiv 0 \pmod p.$$
4. Si ponga
$$\frac{u_p}{(p-1)!} := \sum_{h=1}^{p-1} \frac{1}{h}.$$
Mostrare che u_p è divisibile per p.

SOLUZIONI

Soluzione Esercizio 2. Sia $f(X) := 4X^3 + 7X^2 + 12X + 9$. Allora:
$f(X) \equiv 0 \pmod 2$ ha soluzione: 1;
$f(X) \equiv 0 \pmod 3$ ha soluzioni: 0, 2;
$f(X) \equiv 0 \pmod 9$ ha soluzioni: 0, 3, 6, 8;
$f(X) \equiv 0 \pmod{27}$ ha soluzioni: 3, 12, 21, 26;
$f(X) \equiv 0 \pmod{54}$ ha soluzioni: 3, 21, 39, 53.

Soluzione Esercizio 3.
Il problema si riduce alla soluzione di un'equazione diofantea in 3 indeterminate del tipo:

$$130X + 7Y + 125Z = 2500\,,$$

della quale si ricercano soluzioni intere non negative.
Una soluzione dell'equazione diofantea precedente è data da

$$(x_0, y_0, z_0) = (19, 540, -30)$$

(che si calcola "in modo standard" spezzando l'equazione diofantea data in due equazioni diofantee lineari in 2 indeterminate). Quindi, come noto, tutte le soluzioni della congruenza sono date da $(x, y, z) = (x_0+t, y_0-18\cdot 130t+125s, z_0+(-1)(-130)t-7s) = (19 + t, 540 - 2340t + 125s, -30 + 130t - 7s)$, al variare di s e t in $\mathbb{Z}$.
Inoltre, bisogna avere $x \geq 0$, $y \geq 0$ e $z \geq 0$, vale a dire $t \geq -19$ ed anche:

$$(*) \qquad \lceil \frac{468t - 108}{25} \rceil \leq s \leq \lfloor \frac{130t - 30}{7} \rfloor .$$

Condizione necessaria affinché siano verificate entrambe le disuguaglianze di (*) è che $(-19 \leq)\, t \leq 0$. Inoltre, dovendo prendere almeno 12 pesi da **1,3** hg, deve anche essere $-7 \leq t$.

- Per $t = 0, -2, -5$ si ha che

$$\lceil \frac{468t - 108}{25} \rceil \geq \lfloor \frac{130t - 30}{7} \rfloor\,,$$

quindi questi valori di t non sono accettabili.

- Per $t = -1$, l'unica scelta possibile per s è: $s = -23$; in tal caso la soluzione è $(18, 5, 1)$.
- Per $t = -3$, l'unica scelta possibile per s è: $s = -60$; in tal caso la soluzione è $(16, 60, 0)$.
- Per $t = -4$, l'unica scelta possibile per s è: $s = -79$; in tal caso la soluzione è $(15, 25, 3)$.
- Per $t = -6$, l'unica scelta possibile per s è: $s = -116$; in tal caso la soluzione è $(13, 80, 2)$.
- Per $t = -7$, l'unica scelta possibile per s è: $s = -135$; in tal caso la soluzione è $(12, 45, 5)$.

Soluzione Esercizio 4. Abbiamo che $\Delta \equiv 3\lambda+2 \pmod{17}$. 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 $\mu = 15$, allora l'unica soluzione del sistema è data da (15, 7).
Se $\lambda = 4$ e $\mu = 16$, allora l'unica soluzione del sistema è data da (0, 4).
Se $\lambda = 6$ e $\mu = 15$, allora l'unica soluzione del sistema è data da (2, 1).
Se $\lambda = 6$ e $\mu = 16$, allora l'unica soluzione del sistema è data da (0, 4).

Per $\lambda \equiv 5 \pmod{17}$ abbiamo che $\Delta \equiv 0 \pmod{17}$ ed il sistema è risolubile se e soltanto se $\mu \equiv 16 \equiv -1 \pmod{17}$. 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: $(0,4), (1,11), (2,1), (3,8), (4,15), (5,5), (6,12), (7,2), (8,9), (9,16), (10,6), (11,13), (12,3), (13,10), (14,0), (15,7), (16,14)$.

Soluzione Esercizio 5.

1. Basta osservare che se $1 < h < p-1$ allora $h^2 \not\equiv 1 \pmod{p}$. 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. Basta osservare che dal Teorema di Wilson discende che:
$$\frac{(p-1)!}{h} h = (p-1)! \equiv -1 \pmod{p}.$$
3. Basta osservare che se p è (un primo) dispari, allora $p-1$ è pari e, quindi, per quanto riguarda la somma degli interi del sistema ridotto di residui minimo positivo $\pmod{p}$ si ha:
$$\sum_{h=1}^{p-1} h = \sum_{i=1}^{(p-1)/2} i + (p-i) = \frac{(p-1)}{2} p \equiv 0 \pmod{p}.$$
4. Si noti che:
$$\sum_{h=1}^{p-1} \frac{1}{h} = \frac{(p-1)! + \frac{(p-1)!}{2} + \frac{(p-1)!}{3} + \cdots + \frac{(p-1)!}{p-2} + \frac{(p-1)!}{p-1}}{(p-1)!}.$$
Osserviamo che, per il punto precedente,
$$-k_h \equiv \frac{(p-1)!}{h} \pmod{p},$$
quando $1 < h < p-1$. Inoltre:
$$\sum_{h=2}^{p-2} k_h = \sum_{h=2}^{p-2} h.$$
Quindi:
$$\begin{aligned} u_p &= (p-1)! + \tfrac{(p-1)!}{2} + \tfrac{(p-1)!}{3} + \cdots + \tfrac{(p-1)!}{p-2} + \tfrac{(p-1)!}{p-1} \equiv \\ &\equiv -1 + \tfrac{(p-1)!}{2} + \tfrac{(p-1)!}{3} + \cdots + \tfrac{(p-1)!}{p-2} + (p-2)! \equiv \\ &\equiv -1 - k_2 - k_3 + \cdots - k_{p-2} + 1 \equiv \\ &\equiv -1 - (\textstyle\sum_{h=2}^{p-2} k_h) - (p-1) \equiv \\ &\equiv -(1 + (\textstyle\sum_{h=2}^{p-2} h) + (p-1)) \equiv \\ &\equiv -(\textstyle\sum_{h=1}^{p-1} h) \equiv 0 \pmod{p}. \end{aligned}$$