UNIVERSITÀ DEGLI STUDI ROMA TRE
Corso di Laurea in Matematica
TN01 - Introduzione alla teoria dei numeri - A.A. 2002/2003

Valutazione "in itinere" - I Prova

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

Avvertenza: Svolgere ogni esercizio nello spazio assegnato, senza consegnare altri fogli e giustificando tutte le affermazioni fatte. Non è consentito l'uso di libri e appunti.

ESERCIZIO 1. Dato il sistema:

$$\begin{cases} 8X + 13\lambda Y \equiv 15 \pmod{29} \\ 22X + 14Y \equiv 3\mu \pmod{29}\,. \end{cases}$$

(1) (**3pt**) Studiare la risolubilità del sistema assegnato al variare di λ e μ, con $0 \leq \lambda, \mu \leq 28$ (cioè dire quando è risolubile e, nei casi in cui è risolubile, dire quante soluzioni ammette).
(2) (**4pt**) Al variare di λ e μ, con $1 \leq \lambda \leq 2$ e $20 \leq \mu \leq 21$, trovare tutte le (eventuali) soluzioni del sistema. Nel caso in cui vi siano più di una soluzione, è possibile descrivere tutte le soluzioni anche attraverso una forma parametrica.

ESERCIZIO 2. (**9pt**) Determinare tutte le (eventuali) soluzioni della congruenza polinomiale:

$$X^4 + 78X^3 + 181X^2 + 93X + 25 \equiv 0 \pmod{54}\,.$$

ESERCIZIO 3. Sia p un primo dispari.

(1) (**2pt**) Se a è un intero tale che $a \not\equiv 1, 0 \,(\mathrm{mod}\, p)$ e $t := \mathrm{ord}_p(a)$, mostrare che:

$$a^{t-1} + a^{t-2} + \cdots + a + 1 \equiv 0 \,(\mathrm{mod}\, p).$$

(2) (**4pt**) Se, inoltre, $p \neq 5$, dimostrare che p divide qualche numero della forma 1111...11 (k cifre, con k da determinare).

ESERCIZIO 4. Data l'equazione diofantea:

$$4(\lambda - 3)X + 27Y = 120,$$

(1) (**3pt**) determinare per quali valori di $\lambda \in \mathbb{Z}$ l'equazione è risolubile;
(2) (**2pt**) scrivere esplicitamente le soluzioni dell'equazione assegnata per $\lambda = 4$;
(3) (**3pt**) avendo a disposizione 50 asticelle da 4 cm e 10 asticelle da 27 cm, descrivere tutte le possibili combinazioni di asticelle in modo da ottenere una lunghezza pari a 1,20 m.

SOLUZIONI

Soluzione Esercizio 1.

(1) Abbiamo che $\Delta \equiv 4\lambda - 4 \pmod{29}$. Il sistema ammette un'unica soluzione se e soltanto se $\Delta \not\equiv 0 \pmod{29}$, ovvero per $\lambda \not\equiv 1 \pmod{29}$, qualunque sia il valore assunto da $\mu \in \mathbb{Z}$.
Se $\lambda \equiv 1 \pmod{29}$ allora $\Delta \equiv 0 \pmod{29}$, quindi il sistema è risolubile se e soltanto se $\alpha \equiv \beta \equiv 0 \pmod{29}$. Adesso, $\alpha \equiv 7 - 10\lambda\mu \pmod{29}$ e $\beta \equiv 24\mu - 11 \pmod{29}$. Se $\lambda \equiv 1 \pmod{29}$, allora $\alpha \equiv \beta \equiv 0 \pmod{29}$ se e soltanto se $\mu \equiv 21 \pmod{29}$.
Dunque se $\lambda \equiv 1 \pmod{29}$ e $\mu \equiv 21 \pmod{29}$ il sistema ammette 29 soluzioni distinte. Se $\lambda \equiv 1 \pmod{29}$ e $\mu \not\equiv 21 \pmod{29}$ il sistema non è risolubile.

(2) Se $\lambda = 2$ e $\mu = 20$, l'unica soluzione del sistema è $(25, 23)$.
Se $\lambda = 2$ e $\mu = 21$, l'unica soluzione del sistema è $(20, 0)$.
Se $\lambda = 1$ e $\mu = 20$ il sistema non è risolubile.
Se $\lambda = 1$ e $\mu = 21$ 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. Il sistema ammette 29 soluzioni distinte che si possono esprimere brevemente attraverso la seguente forma parametrica:

$$(x_t \equiv (15 - 13t)11 \pmod{29},\, y_t \equiv t \pmod{29}), \quad 0 \le t \le 28.$$

Soluzione Esercizio 2.

Sia $f(X) := X^4 + 78X^3 + 181X^2 + 93X + 25$. Allora:
$f(X) \equiv 0 \pmod 2$ ha soluzione: 1;
$f(X) \equiv 0 \pmod 3$ ha soluzioni: 1, 2;
$f(X) \equiv 0 \pmod 9$ ha soluzioni: 1, 2, 4, 5, 7, 8;
$f(X) \equiv 0 \pmod{27}$ ha soluzioni: 1, 5, 10, 14, 19, 23;
$f(X) \equiv 0 \pmod{54}$ ha soluzioni: $1, 5, 19, 23, 37, 41$.

Soluzione Esercizio 3.

(1) Se $t := \mathrm{ord}_p(a)$, allora $a^t - 1 \equiv 0 \pmod p$. Quindi

$$(a-1)(a^{t-1} + a^{t-2} + \cdots + a + 1 \equiv 0 \pmod p).$$

Poiché $\mathbb{Z}_p$ è un campo, uno dei due termini deve essere congruo a 0. Ma, per ipotesi, $a \not\equiv 0 \pmod p$, quindi deve essere $(a^{t-1} + a^{t-2} + \cdots + a + 1 \equiv 0 \pmod p)$.

(2) Osserviamo che se p è dispari e $p \neq 5$, allora $\mathrm{MCD}(10, p) = 1$. Se $p = 3$, allora $3 \mid 111$. Se $p \neq 3$, allora $10 \not\equiv 1 \pmod p$, quindi si può definire l'ordine di 10 modulo p. Sia $k := \mathrm{ord}_p(10)$. Per il punto (1),

$$10^{k-1} + 10^{k-2} + \cdots + 10 + 1 \equiv 0 \pmod p.$$

Ma $10^{k-1} + 10^{k-2} + \cdots + 10 + 1 = 111 \cdots 11$ (k cifre). Quindi abbiamo trovato un numero del tipo $111 \cdots 11$ (k cifre) divisibile per p.

Soluzione Esercizio 4.

(1) L'equazione diofantea è risolubile se e soltanto se $d = \mathrm{MCD}(4(\lambda - 3), 27) \mid 120$. Ma d può essere uguale a $1, 3, 9, 27$, quindi per avere che $d \mid 120$ deve essere $d = 1, 3$. Per escludere le altre due possibilità (cioè che $d = 9, 27$) è sufficiente che $d \not\equiv 0 \pmod 9$. Questo accade se e soltanto se $\lambda \not\equiv 3 \pmod 9$.

(2) Per $\lambda = 4$ otteniamo l'equazione diofantea $4X + 27Y = 120$. Una soluzione particolare di questa equazione è $(30, 0)$. Tutte le altre soluzioni sono del tipo:

$$x_t = 30 + 27t, \qquad y_t = -4t,$$

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

(3) Basta risolvere l'equazione diofantea $4X + 27Y = 120$ (dove X rappresenta le asticelle da 4 cm ed Y quelle da 27 cm) prendendo le soluzioni (x_t, y_t) con le seguenti limitazioni:

$$0 \leq x_t \leq 50, \qquad 0 \leq y_t \leq 10.$$

Si ricava che $0 \leq t \leq 1$, quindi le possibili soluzioni sono $(30, 0)$ e $(3, 4)$.