TN1 - Introduzione alla teoria dei numeri - A.A. 2009/2010
Appello B - Luglio 2010

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

ESERCIZIO 1. Studiare la risolubilità della congruenza:

$$7^X - 5X^3 \equiv 0 \pmod{33},$$

e determinarne le eventuali soluzioni intere x, con $0 \leq x \leq 110$.

ESERCIZIO 2. **(a)** Enunciare il teorema fondamentale sulle terne pitagoriche primitive positive (cioè, descrivere tutte le terne pitagoriche primitive positive (x, y, z) in funzione di due parametri interi positivi (s, t)).

(b) Dimostrare che se (x, y, z) è una terna pitagorica primitiva, allora $3 \mid x$ oppure $3 \mid y$.

(c) Dimostrare che se (x, y, z) è una terna pitagorica, allora almeno uno tra gli interi x, y, z è divisibile per 5.

ESERCIZIO 3. **(a)** Trovare la radice primitiva minima positiva di 31.

(b) Descrivere la tabella degli indici rispetto alla radice primitiva minima positiva di 31.

(c) Ricordando che $X^{10} - 1 = (X - 1)(1 + X + X^2 + \cdots + X^9)$, trovare, se esistono, tutte le soluzioni della congruenza:

$$1 + X + X^2 + X^3 + X^4 + X^5 + X^6 + X^7 + X^8 + X^9 \equiv 0 \pmod{31}.$$

ESERCIZIO 4. **(a)** Si diano esplicitamente le definizioni di *funzione aritmetica moltiplicativa* e di *funzione aritmetica totalmente moltiplicativa.*

(b) Sia f una funzione aritmetica. Mostrare che
f è invertibile rispetto al prodotto di Dirichlet se e soltanto se $f(1) \neq 0$.

(c) Sia f una funzione aritmetica moltiplicativa. Dimostrare che

$$f \text{ è totalmente moltiplicativa se e soltanto se } f^{-1} = \mu f$$

(cioè, $f^{-1}(n) = \mu(n) \cdot f(n)$, per ogni $n \geq 0$, dove μ è la funzione di Möbius ed f^{-1} è la funzione inversa di f, rispetto al prodotto di convoluzione di Dirichlet).

(d) Calcolare $(\sigma * \tau)^{-1}(10)$.

ESERCIZIO 5. Trovare tutte le eventuali soluzioni della congruenza

$$X^3 + X^2 + X - 3 \equiv 0 \pmod{27}.$$

ESERCIZIO 6. Determinare tutte le eventuali soluzioni del seguente sistema di congruenze, descrivendo brevemente il metodo utilizzato.

$$\begin{cases} 3X \equiv 2 \pmod{14} \\ 5X \equiv 6 \pmod{18} \\ 4X \equiv 6 \pmod{11}. \end{cases}$$

ESERCIZIO 1: Soluzione.

La risolubilità della congruenza data equivale alla risolubilità del sistema:

$$(\star) \qquad \begin{cases} 7^X - 5X^3 \equiv 0 \pmod 3 \\ 7^X - 5X^3 \equiv 0 \pmod{11}. \end{cases}$$

La congruenza $(\star')$ $\quad 7^X - 5X^3 \equiv 0 \pmod 3$ è equivalente alla congruenza $1^X - 2X^3 \equiv 1 - 2X \equiv 0 \pmod 3$, la quale ha un'unica soluzione $x \equiv 2 \pmod 3$.

La congruenza $(\star'')$ $\quad 7^X - 5X^3 \equiv 0 \pmod{11}$ si può risolvere utilizzando la teoria degli indici. Una radice primitiva di 11 è $r = 2$.
Per $a = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ si ha, rispettivamente, che
$\mathrm{ind}_2(a) = 10, 1, 8, 2, 4, 9, 7, 3, 6, 5$.
Dal momento che $\mathrm{ind}_2(7) = 7$, $\mathrm{ind}_2(5) = 4$, allora le soluzioni di $(\star'')$ sono tutte e sole le soluzioni del sistema:

$$\begin{cases} X \equiv a \pmod{11} \\ 7X \equiv 4 + 3\,\mathrm{ind}_2(a) \pmod{10} \end{cases}$$

ovvero del sistema

$$\begin{cases} X \equiv a \pmod{11} \\ X \equiv 3(4 + 3\,\mathrm{ind}_2(a)) \equiv 2 + 9\,\mathrm{ind}_2(a) \pmod{10} \end{cases}$$

Tale sistema ha le seguenti dieci soluzioni

$$x \equiv 12, 14, 19, 38, 70, 83, 86, 87, 95, 101 \pmod{110}.$$

Tra queste, le soluzioni congruenti a $2 \pmod 3$ (cioè le soluzioni di $(\star'')$ che sono anche soluzioni di $(\star')$) sono $14, 38, 83, 86, 95, 101 \pmod{110}$ e quindi queste sono le soluzioni intere non negative della congruenza data inferiori a 110.

ESERCIZIO 2: Soluzione. La dimostrazione di tutti i punti è sviluppato esplicitamente negli appunti del corso.

ESERCIZIO 3: Soluzione. (a) $r = 3$.

(b) $\mathrm{ind}_3(1) \rightsquigarrow 30$;
$\mathrm{ind}_3(2) \rightsquigarrow 24$;
$\mathrm{ind}_3(3) \rightsquigarrow 1$;
$\mathrm{ind}_3(4) \rightsquigarrow 18$;
$\mathrm{ind}_3(5) \rightsquigarrow 20$;
$\mathrm{ind}_3(6) \rightsquigarrow 25$;
$\mathrm{ind}_3(7) \rightsquigarrow 28$;
$\mathrm{ind}_3(8) \rightsquigarrow 12$;
$\mathrm{ind}_3(9) \rightsquigarrow 2$;
$\mathrm{ind}_3(10) \rightsquigarrow 14$;
$\mathrm{ind}_3(11) \rightsquigarrow 23$;
$\mathrm{ind}_3(12) \rightsquigarrow 19$;
$\mathrm{ind}_3(13) \rightsquigarrow 11$;
$\mathrm{ind}_3(14) \rightsquigarrow 22$;
$\mathrm{ind}_3(15) \rightsquigarrow 21$;
$\mathrm{ind}_3(16) \rightsquigarrow 6$;
$\mathrm{ind}_3(17) \rightsquigarrow 7$;
$\mathrm{ind}_3(18) \rightsquigarrow 26$;

$\text{ind}_3(19) \rightsquigarrow 4$;
$\text{ind}_3(20) \rightsquigarrow 8$;
$\text{ind}_3(21) \rightsquigarrow 29$;
$\text{ind}_3(22) \rightsquigarrow 17$;
$\text{ind}_3(23) \rightsquigarrow 27$;
$\text{ind}_3(24) \rightsquigarrow 13$;
$\text{ind}_3(25) \rightsquigarrow 10$;
$\text{ind}_3(26) \rightsquigarrow 5$;
$\text{ind}_3(27) \rightsquigarrow 3$;
$\text{ind}_3(28) \rightsquigarrow 16$;
$\text{ind}_3(29) \rightsquigarrow 9$;
$\text{ind}_3(30) \rightsquigarrow 15$.
(c) Le soluzioni sono $x = 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$.

ESERCIZIO 4: Soluzione.
(a), (b) sono enunciati/dimostrati sugli appunti, così come la necessità di **(c)**(cioè il fatto che se f è totalmente moltiplicativa allora $f^{-1} = \mu f$). Per l'implicazione inversa basta osservare che $u = (\mu f) * f$ (dove u è la funzione unità rispetto al prodotto $*$) e che u è totalmente moltiplicativa. Da questo discende per induzione che $f(p^e) = (f(p))^e$, per ogni $e \geq 1$. Essendo f moltiplicativa per ipotesi, allora è anche totalmente moltiplicativa.
(d) Infine, $(\sigma * \tau)^{-1}(10) = (\tau^{-1} * \sigma^{-1})(10) = \tau^{-1}(1)\sigma^{-1}(10) + \tau^{-1}(2)\sigma^{-1}(5) + \tau^{-1}(5)\sigma^{-1}(2) + \tau^{-1}(10)\sigma^{-1}(1)$.
Si noti che $\sigma^{-1} = \mu e * \mu$ e $\tau^{-1} = \mu * \mu$. Quindi,

$$\tau^{-1}(1) = 1,\ \tau^{-1}(2) = -2\ ,\ \tau^{-1}(5) = -2,\ \tau^{-1}(10) = 4;$$
$$\sigma^{-1}(1) = 1,\ \sigma^{-1}(2) = -3\ ,\ \sigma^{-1}(5) = -6,\ \sigma^{-1}(10) = 18.$$

Pertanto,

$$(\sigma * \tau)^{-1}(10) = 1 \cdot 18 + (-2) \cdot (-6) + (-2) \cdot (-3) + 4 \cdot 1 = 40\,.$$

ESERCIZIO 5: Soluzione.
$X^3 + X^2 + X - 3 \equiv 0 \pmod{3} \rightsquigarrow x = 0, 1 \pmod{3}$;
$X^3 + X^2 + X - 3 \equiv 0 \pmod{9} \rightsquigarrow x = 1, 3, 4, 7 \pmod{9}$;
$X^3 + X^2 + X - 3 \equiv 0 \pmod{27} \rightsquigarrow x = 1, 4, 10, 13, 19, 21, 22 \pmod{27}$;

ESERCIZIO 6: Soluzione. $x \equiv 1074 \pmod{1386}$.