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

Valutazione "in itinere" - II Prova

MATRICOLA (O ALTRO IDENTIFICATIVO): ....
COGNOME: .... **NOME:** ....

esercizio	1	2a	2b	3	4a	4b	4c
punteggio max	10 (+ 8)	5	8	16	6	6	12
punteggio assegnato							
totale							

ESERCIZIO 1. Dimostrare almeno uno dei seguenti enunciati:

(a) Vale la seguente formula:

$$n = \sum_{d|n} \varphi(d)\,.$$

(b) Sia f una funzione aritmetica moltiplicativa. Dimostrare che f è totalmente moltiplicativa se e soltanto se $f^{-1} = \mu f$ (dove μ è la funzione di Möbius ed f^{-1} è la funzione inversa di f, rispetto al prodotto di convoluzione di Dirichlet).

(c) Sia f una funzione aritmetica. Mostrare che f è invertibile rispetto al prodotto di Dirichlet se e soltanto se $f(1) \neq 0$. Calcolare $(\sigma * \tau)^{-1}(6)$.

ESERCIZIO 2. **(a)** Trovare la radice primitiva minima positiva di 29.

(b) Ricordando che $X^7 - 1 = (X-1)(1+X+X^2+\cdots+X^6)$, trovare, se esistono, le soluzioni della congruenza:

$$1 + X + X^2 + X^3 + X^4 + X^5 + X^6 \equiv 0 \pmod{29}.$$

ESERCIZIO 3. Studiare la risolubilità della congruenza:

$$7^X - 5X^3 \equiv 0 \pmod{22}\,,$$

e determinarne le eventuali soluzioni (mod 110).

ESERCIZIO 4. Sia $n = 18$.

(a) Determinare se n possiede una radice primitiva dell'unità. In caso affermativo determinare la più piccola radice primitiva r (mod 18) e descrivere la tabella degli indici rispetto ad r, al variare di a nel sistema ridotto minimo positivo (mod 18).

(b) Calcolare il simbolo di Jacobi:

$$\left(\frac{83+\lambda}{18}\right)$$

al variare di λ, $0 \leq \lambda \leq 2$.

(c) Determinare per quali valori di λ, $0 \leq \lambda \leq 2$, l'equazione diofantea in due indeterminate:

$$X^2 - 18Y - 83 - \lambda = 0$$

è risolubile e, per ciascuno dei valori di λ per i quali è risolubile, determinare esplicitamente le sue soluzioni.

ESERCIZIO 0. Sia $f(X) := X^5 - 2X^3 + 11X^2 - 12 = 0$.
Determinare tutte le eventuali soluzioni di

$$f(X) \equiv 0 \pmod{8 * 9}.$$

ESERCIZIO 1. Soluzione. (a), (c) sono dimostrati sugli appunti, così come la necessità di **(b)**(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 necessariamente che $f(p^e) = f(p)(f(p))^{-1}$ e, quindi, per induzione che $f(p^e) = (f(p))^e$, per ogni $e \geq 1$.

Infine, $(\sigma * \tau)^{-1}(6) = (\tau^{-1} * \sigma^{-1})(6) = \tau^{-1}(1)\sigma^{-1}(6) + \tau^{-1}(2)\sigma^{-1}(3) + \tau^{-1}(3)\sigma^{-1}(2) + \tau^{-1}(6)\sigma^{-1}(1) = 1 \cdot 12 + (-2) \cdot (-4) + (-2) \cdot (-3) + 4 \cdot 1 = 30$.

ESERCIZIO 2. Soluzione.

(a) 2 è una radice primitiva di 29. Precisamente,
Per $a = 1, 2, 3, \ldots, 28$ si ha, rispettivamente, che
$\operatorname{ind}_2(a) = 28, 1, 5, 2, 22, 6, 12, 3, 10, 23, 25, 7, 18, 13, 27, 4, 21, 11, 9, 24, 17, 26, 20, 8, 16, 19, 15, 14$.

(b) Osserviamo che $X^7 - 1 = (X-1)(1 + X + X^2 + \cdots + X^6)$. Dunque le soluzioni della congruenza data sono tutte le soluzioni, diverse da 1, della congruenza $X^7 - 1 \equiv 0 \pmod{29}$, le quali si ottengono risolvendo la congruenza (nell'incognita $\operatorname{ind}_2(X)$):

$$7 \operatorname{ind}_2(X) \equiv 0 \pmod{28} \;\; \text{ovvero} \;\; \operatorname{ind}_2(X) \equiv 0 \pmod{4}.$$

Le soluzioni sono $\operatorname{ind}_2(x) \equiv 4, 8, 12, 16, 20, 24 \pmod{28}$ e, quindi, $x \equiv 7, 16, 20, 23, 24, 25 \pmod{29}$.

ESERCIZIO 3: Soluzione.

La risolubilità della congruenza data equivale alla risolubilità del sistema:

$$(\star) \quad \begin{cases} 7^X - 5X^3 \equiv 0 \pmod{2} \\ 7^X - 5X^3 \equiv 0 \pmod{11}. \end{cases}$$

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

La congruenza $(\star'')$ $\;7^X - 5X^3 \equiv 0 \pmod{11}$ 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
$\operatorname{ind}_2(a) = 10, 1, 8, 2, 4, 9, 7, 3, 6, 5$.
Dal momento che $\operatorname{ind}_2(7) = 7$, $\operatorname{ind}_2(5) = 4$, allora le soluzioni di $(\star'')$ sono tutte e sole le soluzioni del sistema:

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

ovvero del sistema

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

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 $1 \pmod{2}$ (cioè le soluzioni di $(\star'')$ che sono anche soluzioni di $(\star')$) sono le soluzioni dispari e cioè $19, 83, 87, 95, 101 \pmod{110}$ e quindi queste sono le soluzioni della congruenza data.

ESERCIZIO 4: Soluzione.

(a) Si noti anzitutto che $\varphi(18) = \varphi(9) = 6$. Non è difficile verificare che $r = 5$ ha ordine 6 (mod 18), dove $\{1, 5, 7, 11, 13, 17\}$ sono gli elementi del sistema ridotto di residui (minimo positivo) che sono relativamente primi con $n = 18$ ed inoltre:

$r^1 \equiv 5 \pmod{18} \quad \Rightarrow \quad \text{ind}_5(5) = 1\,;$
$r^2 \equiv 7 \pmod{18} \quad \Rightarrow \quad \text{ind}_5(7) = 2\,;$
$r^3 \equiv 17 \pmod{18} \quad \Rightarrow \quad \text{ind}_5(17) = 3\,;$
$r^4 \equiv 13 \pmod{18} \quad \Rightarrow \quad \text{ind}_5(13) = 4\,;$
$r^5 \equiv 11 \pmod{18} \quad \Rightarrow \quad \text{ind}_5(11) = 5\,;$
$r^6 \equiv 1 \pmod{18} \quad \Rightarrow \quad \text{ind}_5(1) = 6\,.$

(b)

$$\left(\frac{83}{18}\right) = \left(\frac{11}{18}\right) = \left(\frac{11}{2}\right)\left(\frac{11}{9}\right) = 1\,,$$
$$\left(\frac{84}{18}\right) = \left(\frac{12}{18}\right) = \left(\frac{12}{2}\right)\left(\frac{12}{9}\right) = 0\,,$$
$$\left(\frac{85}{18}\right) = \left(\frac{13}{18}\right) = \left(\frac{13}{2}\right)\left(\frac{13}{9}\right) = 1\,.$$

(c) Al variare di λ $(0 \leq \lambda \leq 2)$, si consideri la congruenza

$$f_\lambda(X) := X^2 - (83 + \lambda) \equiv 0 \pmod{18}\,.$$

Allora,

$f_0(X) \equiv 0 \pmod{2} \rightarrow x = 1\,;$
$f_0(X) \equiv 0 \pmod{3} \rightarrow \emptyset\,;$
$f_0(X) \equiv 0 \pmod{9} \rightarrow \emptyset\,;$
$f_0(X) \equiv 0 \pmod{18} \rightarrow \emptyset\,.$

$f_1(X) \equiv 0 \pmod{2} \rightarrow x = 0\,;$
$f_1(X) \equiv 0 \pmod{3} \rightarrow x = 0\,;$
$f_1(X) \equiv 0 \pmod{9} \rightarrow \emptyset\,;$
$f_1(X) \equiv 0 \pmod{18} \rightarrow \emptyset\,.$

$f_2(X) \equiv 0 \pmod{2} \rightarrow x = 1\,;$
$f_2(X) \equiv 0 \pmod{3} \rightarrow x = 1, 2\,;$
$f_2(X) \equiv 0 \pmod{9} \rightarrow x = 2, 7\,;$
$f_2(X) \equiv 0 \pmod{18} \rightarrow x = 7, 11\,.$

Pertanto, le soluzioni dell'equazione diofantea

$$X^2 - 18Y - 85 = 0$$

sono $(7+18k, -2+18k^2+2\cdot 7k)$ e $(11+18k, 2+18k^2+2\cdot 11k)$, al variare comunque di k negli interi relativi, in quanto:

$$(7 + 18k)^2 - 85 = 7^2 + 18(18k^2 + 2\cdot 7k) - 85 = -36 + 18(18k^2 + 2\cdot 7k)\,,$$

quindi:

$$(7 + 18k)^2 - 85 - 18(-2 + 18k^2 + 2\cdot 7k) = 0\,;$$

$$(11 + 18k)^2 - 85 = 11^2 + 18(18k^2 + 2\cdot 11k) - 85 = 36 + 18(18k^2 + 2\cdot 11k)\,,$$

quindi:

$$(7 + 18k)^2 - 85 - 18(2 + 18k^2 + 2\cdot 11k) = 0\,.$$

ESERCIZIO 0: Soluzione. Le soluzioni sono le seguenti:

$f(X) \equiv 0 \pmod{2} \ \rightarrow \ 0,\ 1$
$f(X) \equiv 0 \pmod{4} \ \rightarrow \ 0,\ 1,\ 2$
$f(X) \equiv 0 \pmod{8} \ \rightarrow \ 1,\ 2,\ 6$

$f(X) \equiv 0 \pmod{3} \ \rightarrow \ 0,\ 1$
$f(X) \equiv 0 \pmod{9} \ \rightarrow \ 1$

$f(X) \equiv 0 \pmod{8 \cdot 9} \ \rightarrow \ 1,\ 10,\ 46$