

ESERCIZI SU DIVISIBILITA' NEI NATURALI E NEGLI INTERI. PRIMI ESERCIZI SULLE CONGRUENZE

1. DIVISIBILITÀ

Nei seguenti esercizi, se a, b sono interi non entrambi nulli, (a, b) debote il massimo comun divisore di a, b .

- (1) Determinare quoziente e resto della divisione di a per b , dove
 - (a) $a = 26, b = 3$;
 - (b) $a = 26, b = -3$;
 - (c) $a = -26, b = 3$;
 - (d) $a = -26, b = -3$;

- (2) Sia R la relazione binaria su $\mathbb{N}$ definita da:

$$a R b \quad \Leftrightarrow \quad (a, b) = 1$$

Si ha:

V	F	R è riflessiva;
V	F	R è simmetrica;
V	F	R è transitiva.

- (3) Trovare il massimo comun divisore di 36 e 56 utilizzando la fattorizzazione unica in primi e l'algoritmo di Euclide. Esprimere tale massimo comun divisore come combinazione lineare di 36 e 56.
- (4) Dimostrare che 43 e 16 sono relativamente primi utilizzando l'algoritmo di Euclide. Esprimere il numero 1 come combinazione lineare di 43 e 16.
- (5) Dati a, b interi, supponiamo che 1 sia combinazione lineare di a e b . Dimostrare che $(a, b) = 1$
(suggerimento se d è un divisore comune di a, b allora d divide ogni combinazione lineare di a e b , quindi d divide $\dots$).
- (6) Utilizzare l'esercizio precedente per dimostrare che due numeri successivi $a, b = a + 1$ sono sempre relativamente primi,
- (7) Dati a, b interi non entrambi nulli, dimostrare che $(a, b) = 1$ se e solo se ogni numero intero si può scrivere come combinazione lineare di a e b .

Dati a, b interi non entrambi nulli, dimostrare che $(a, b) \neq 1$ se e solo se esiste un numero primo p che divide sia a che b .

- (8) Siano a, b numeri naturali e $n \geq 1$. Dimostrare che, se $(a, n) = 1$ e $(b, n) = 1$ allora $(ab, n) = 1$. (suggerimento: fare una dimostrazione per assurdo, e usare l'esercizio precedente e le proprietà dei primi).
- (9) Sia $n > 1$ un numero naturale che soddisfa la seguente proprietà:
per ogni coppia di numeri naturali a, b , se $n|ab$ allora $n|a$ oppure $n|b$. Dimostrare che n è un numero primo.
- (10) Dimostrare per induzione che per ogni $n \geq 1$ il numero $5^n - 1$ è divisibile per 4.
- (11) Sia p un numero primo, a, b due numeri interi tali che $p^2|ab$. Si ha:

V	F	$p^2 a^2$ oppure $p^2 b^2$;
V	F	$p a$ oppure $p b$;
V	F	$p^2 a$ oppure $p^2 b$;

- (12) Siano $a > 0, b > 0$ e $c > 0$; dimostrare che, se $a|c, b|c$ e $(a, b) = 1$, allora $ab|c$
(dare due dimostrazioni: una utilizzando l'identità di Bezout, l'altra utilizzando il Teorema della fattorizzazione unica in prodotto di primi,)
- (13) Se q è un numero razionale tale che sia $18q$ che $25q$ sono interi, allora q è un intero. (Suggerimento: scrivere $q = \frac{m}{n}$ con m, n interi relativamente primi (cioè: $(m, n) = 1$); dalle ipotesi segue che $n|18m$ e $n|25m$, quindi...).
- (14) Determinare i numeri naturali n per cui $n^2 - 1$ è primo.
- (15) Siano $a, b > 0$ e siano q, r con $q > 0$ e $0 \leq r < b$ il quoziente ed il resto della divisione di a per b (quindi vale $a = qb + r$, con $0 \leq r < |b|$). Qual è il quoziente e qual è il resto della divisione dell'intero $-a$ per b ? E di a per $-b$? E di $-a$ per $-b$?
- (16) Dimostrare che se n non è divisibile per 3, allora $n^4 + n^2 + 1$ è divisibile per 3. (Suggerimento: se n non è divisibile per 3 allora è necessariamente congruo a ... oppure a ... modulo 3. In entrambi i casi, $n^4 + n^2 + 1$ è congruo a ... modulo 3.)
- (17) Se p è un numero primo e k un numero naturale, dimostrare che vale, per ogni a con $1 \leq a \leq p^k$:

$$(a, p^k) \neq 1 \Leftrightarrow a \text{ è un multiplo di } p.$$

Dedurre quindi che i numeri a con $1 \leq a \leq p^k$ e $(a, p^k) \neq 1$ sono p^{k-1} .

Dedurre infine che il numero dei numeri più piccoli di p^k e relativamente primi con p^k è $p^k - p^{k-1}$.

- (18) Sia
- n
- un numero intero positivo e

$$n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

la sua decomposizione in prodotto di numeri primi positivi distinti.
Dimostrare che il numero dei divisori positivi di n è

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1).$$

- (19) Dimostrare che, se
- b, c
- sono numeri interi relativamente primi e
- $d = (b - c, b + c)$
- , allora
- $d = 1$
- oppure
- $d = 2$
- .

2. CONGRUENZE

- (20) Si ha:

V	F	$15 + 27 \equiv 0$ modulo 14;
V	F	$15 - 27 \equiv 0$ modulo 14;
V	F	-5 è congruo a 7 modulo 12;

- (21) Si ha:

V	F	se $a \equiv_n b$ allora per ogni $k \in \mathbb{Z}$ si ha $a^k \equiv_n b^k$;
V	F	se $a \equiv_n b$ allora per ogni $k \in \mathbb{Z}$ si ha $ka \equiv_n kb$;
V	F	se $a \equiv_n b$ allora per ogni $k \in \mathbb{Z}$ si ha $k^a \equiv_n k^b$.

- (22) Per ogni numero
- $a \in \{0, 1, 2, \dots, 9\}$
- trovare un numero
- $b \in \{0, 1, 2, \dots, 9\}$
- tale che
- $a + b \equiv 0$
- modulo 9.

Per quali numeri $a \in \{0, 1, 2, \dots, 9\}$ esiste un $b \in \{0, 1, 2, \dots, 9\}$ tale che $ab \equiv 1$ modulo 9?

- (23) Sia
- $\equiv_{12}$
- la congruenza modulo 12 sugli interi. Il seguente insieme
- A
- è un insieme di rappresentanti per le classi d'equivalenza di
- $\equiv_{12}$
- su
- $\mathbb{Z}$
- :

V	F	$A = \{0, 1, \dots, 12\}$;
V	F	$A = \{12, 13, \dots, 23\}$;
V	F	$A = \{-12, -11, \dots, -1\}$.

- (24) Sia
- $\equiv_{10}$
- la congruenza modulo 10 sugli interi e
- $X = \{0, \dots, 9\}$
- l'insieme dei resti modulo 10. Per ognuno dei numeri interi seguenti
- a
- , trovare un elemento
- $x \in X$
- tale che
- $a \equiv_{10} x$
- (cercando di fare il minor numero possibile di calcoli...).

$$a = -1, \quad a = 13, \quad a = 10^2, \quad a = 10^3 + 13 \quad a = 10^4 \cdot 13.$$