# Allenamenti EGMO 2018 – Teoria dei numeri

## 1.1 Divisibilità

Ricordiamo che, dati due numeri interi $a$, $m$, esistono unici $q$ ed $r$ interi con $0 \leq r < m$, tali che

$$a = mq + r\,.$$

Chiamiamo $r$ il *resto* della divisione di $a$ per $m$.

Dati $a, m$ interi, diciamo che $a$ è divisibile per $m$ (o $m$ divide $a$, o $m$ è un *divisore* di $a$) se il resto della divisione di $a$ per $m$ è 0, cioè se esiste un intero $q$ tale che $a = mq$. In questo caso denotiamo $m \mid a$, che si legge "$m$ divide $a$".

Un numero intero si dice *primo* se gli unici suoi divisori sono 1 e se stesso. Spesso indicheremo i numeri primi con le lettere $p, q$.

Infine ricordiamo che ogni $n \in \mathbb{N}$ ammette un'unica *fattorizzazione* in primi, cioè esiste un unico modo (a meno dell'ordine dei fattori) di scrivere $n$ come

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$$

dove $p_1, \ldots, p_s$ sono primi distinti e $\alpha_1, \ldots, \alpha_s$ sono interi strettamente positivi.

**Esercizio 1.1.** Dati $a, b, c$ interi, dimostrare le seguenti proprietà della divisibilità:

1. Se $a \mid b$ e $a \mid c$, allora $a \mid xb + yc$ per ogni $x, y$ interi.
2. Si ha che $a \mid b$ se e solo se $a \mid b + ka$ per un qualche $k$ intero se e solo se $a \mid b + ka$ per ogni $k$ intero.
3. Se $a \mid bc$ e $(a, c) = 1$ (ovvero $a$ e $c$ non hanno fattori in comune), allora $a \mid b$.
4. Dato un primo $p$, allora $p \mid ab$ se e solo se $p \mid a$ oppure $p \mid b$.

[Hint]

**Esercizio 1.2.** Trovare il più grande valore possibile di $a$ tale che esistono $p$ e $q$ numeri primi per cui $a = p + q$ e $a = \frac{pq-1}{2}$. [Hint]

## 1.2 Algoritmo di Euclide

**Definizione 1.1.** Dati due numeri naturali $a$ e $b$, si definisce *massimo comun divisore* fra $a$ e $b$, che denoteremo $MCD(a, b)$ o $(a, b)$, il più grande dei divisori comuni di $a$ e $b$.

Il primo modo che viene in mente per calcolare l'MCD fra due numeri $a, b$ è fattorizzare i due numeri come

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}\,, \quad b = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}\,,$$

dove eventualmente $\alpha_i$ o $\beta_i$ sono 0 per qualche $i$, in modo che nella fattorizzazione compaiano gli stessi primi. Allora l'MCD fra $a$ e $b$ sarà

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s, \beta_s\}}\,.$$

Esiste però un modo più rapido della fattorizzazione e che richiede solo operazioni elementari per calcolare l'MCD: l'*algoritmo di Euclide*, che descriviamo di seguito. L'idea è procedere tramite delle divisioni successive, basandosi sul seguente lemma.

**Lemma.** *Dati due interi $a$ e $b$ si ha che $(a, b) = (r, b)$, dove $r$ è il resto della divisione di $a$ per $b$.*

**Esercizio 1.3.** Dimostrare il lemma per esercizio. [Hint]

Dunque consideriamo due interi $a_0 \geq a_1 > 0$, di cui vogliamo calcolare l'MCD $(a_0, a_1)$. Grazie al lemma precedente $(a_0, a_1) = (a_1, a_2)$, dove $a_2$ è il resto della divisione di $a_0$ per $a_1$ e dunque in particolare $0 \leq a_2 < a_1$.

Se $a_2 = 0$, abbiamo trovato che $(a_0, a_1) = (a_1, 0) = a_1$ e abbiamo quindi concluso il calcolo dell'MCD. Altrimenti possiamo ripetere il procedimento e ottenere che $(a_1, a_2) = (a_2, a_3)$, dove $a_3$ è il resto della divisione di $a_1$ per $a_2$.

Procediamo dunque analogamente trovando una successione di interi $a_2, a_3, \ldots, a_n$, di cui $a_{i+2}$ è il resto della divisione di $a_i$ per $a_{i+1}$ per ogni $i \geq 0$.

Notiamo che $a_1 > a_2 > \ldots > a_n$ è una successione *strettamente* decrescente di numeri interi positivi; dunque, continuando l'algoritmo, finiremo a 0 dopo un numero *finito* di passaggi. Questo vuol dire che esisterà $n \geq 1$ tale che $a_{n+1} = 0$ e quindi

$$(a_0, a_1) = (a_1, a_2) = \ldots = (a_n, 0) = a_n \,.$$

**Esercizio 1.4.** Trovare il massimo valore possibile di $(100+n^2, 100+(n+1)^2)$ al variare di $n \in \mathbb{N}$.

## 1.3 Identità di Bezout

**Teorema 1.2** (Bezout)**.** *Dati due numeri interi $a_0$ e $a_1$ con massimo comun divisore $d = (a_0, a_1)$ esistono due interi $x$ e $y$ tali che:*

$$a_0 x + a_1 y = d \,.$$

Per trovare i coefficienti $x$ e $y$ basta infatti percorrere al contrario le divisioni fatte nell'algoritmo di Euclide.

Supponiamo infatti che la successione di interi costruita tramite l'algoritmo di Euclide sia $a_0 \geq a_1 > a_2 > \ldots > a_n = d$. Allora esistono $q_1, \ldots, q_{n-1}$ tali che $a_k = q_{k+1}a_{k+1} + a_{k+2}$ per ogni $k = 0, \ldots, n-2$ e di conseguenza abbiamo che

$$d = a_n = a_{n-2} - q_{n-1}a_{n-1} = a_{n-2} - q_{n-1}(a_{n-3} - q_{n-2}a_{n-2}) = -q_{n-1}a_{n-3} + (1 + q_{n-1}q_{n-2})a_{n-2}$$

Continuando in questo modo, sostituendo sempre l'$a_i$ con indice maggiore con i due precedenti, arriviamo a scrivere $d$ in funzione di $a_0$ e $a_1$, trovando quindi i coefficienti $x$ e $y$ tali che $a_0 x + a_1 y = d$.

**Esercizio 1.5.** Trovare $d = (66, 51)$ ed i coefficienti $x$ e $y$ tali che $66x + 51y = d$.

### Equazioni diofantee lineari

Abbiamo ora gli strumenti per affrontare il seguente problema: dati $a, b, c$ interi, studiare l'equazione

$$ax + by = c \tag{1.1}$$

per $x$, $y$ interi.

**Esercizio 1.6.** L'Equazione (1.1) ha soluzione se e solo se $(a, b) \mid c$ e in tal caso ammette *infinite* coppie $(x, y)$ che rispettano l'equazione.

Risolvere l'esercizio seguendo la linea risolutiva:

1. Dimostrare che se esistono $x, y$ interi tali che $ax + by = c$, allora $(a, b) \mid c$.
2. Dimostrare che se $(a, b) \mid c$, allora esistono $x, y$ interi tali che $ax+by = c$, utilizzando il Teorema 1.2 (Bezout).
3. Dimostrare che se $(x_0, y_0)$ risolve l'equazione, allora anche

$$\left(x_0 - \frac{b}{(a, b)}k, y_0 + \frac{a}{(a, b)}k\right)$$

per ogni $k$ intero risolve l'equazione. Inoltre le soluzioni sono tutte di questa forma.

## 1.4 Congruenze

**Definizione 1.3.** Si dice che $a$ è *congruo* a $b$ modulo $m$ e si indica $a \equiv b \pmod{m}$, se $a$ e $b$ hanno lo stesso resto nella divisione per $m$.

**Esercizio 1.7.** La congruenza è una *relazione di equivalenza*, cioè se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, allora $a \equiv c \pmod{m}$. Dunque, fissato il modulo $m$, chiamiamo *classe di congruenza* tutti i numeri con lo stesso resto nella divisione per $m$.

**Esercizio 1.8.** Dimostrare che le seguenti affermazioni sono equivalenti:

1. $a$ è congruo a $b$ modulo $m$;
2. $m \mid a - b$;
3. esiste $k$ tale che $a = km + b$ (*attenzione*: in questo caso $k$ e $b$ non sono necessariamente $q$ e $r$ della divisione euclidea).

Dalla definizione è ovvio che, dati due interi $a$ ed $m$, allora $a \equiv r \pmod{m}$, dove $0 \leq r < m$ è il resto della divisione di $a$ per $m$.

Fissato il modulo $m$, possiamo dunque associare ad ogni intero $a$ il suo resto nella divisione euclidea per $m$. Tale elemento, compreso fra 0 e $m - 1$, sarà il "rappresentante privilegiato" della classe di congruenza di $a$. Spesso con "$a$ modulo $m$" o "$a$ mod $m$" intendiamo direttamente tale elemento privilegiato della classe di congruenza di $a$.

*Nota.* Notare che dati $0 \leq a, b < m$ con $a \neq b$, non può valere $a \equiv b \pmod{m}$.

Le congruenze soddisfano diverse proprietà (che si possono ricavare dalle proprietà della divisione) che elenchiamo di seguito:

1. Se $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$, allora $a + b \equiv a' + b' \pmod{m}$

   *Dimostrazione.* Per definizione, se $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$, allora $m \mid a - a'$ e $m \mid b - b'$ e per le proprietà della divisione ricavo che $m \mid a - a' + b - b' = (a + b) - (a' + b')$, cioè dunque $a + b \equiv a' + b' \pmod{m}$. □

2. Se $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$, allora $a \cdot b \equiv a' \cdot b' \pmod{m}$

   *Dimostrazione.* Se $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$, allora esistono $k, h$ tali che $a = km + a'$ e $b = hm + b'$. Moltiplicando, ricavo dunque $ab = (km + a')(hm + b') = khm^2 + kb'm + ha'm + a'b' \equiv a'b' \pmod{m}$. □

**Esercizio 1.9.** Per quali numeri $n$ si ha che 3 divide $1 + 2 + 3 + \cdots + (n - 1) + n$? [Hint]

**Esercizio 1.10.** Dati $a, b, m$ interi positivi tali che $a \equiv b \pmod{m}$, dimostrare che $(a, m) = (b, m)$.

### Equazioni diofantee lineari in modulo

Vogliamo ora studiare quando l'equazione

$$ax \equiv b \pmod{m} \tag{1.2}$$

ha soluzione per $a, b, m$ interi positivi.

**Esercizio 1.11.** Dimostrare che, se $(a, m) = 1$, allora l'Equazione (1.2) ammette soluzione, sfruttando l'Esercizio 1.6. [Hint]

**Esercizio 1.12.** Trovare un esempio in cui $(a, m) \neq 1$ e

1. l'Equazione (1.2) non ammette soluzione;
2. l'Equazione (1.2) ammette soluzione.

Notare in particolare che se $a, m$ sono due interi positivi coprimi, allora esiste sempre l'inverso di $a$ modulo $m$, cioè un intero $x$ tale che $ax \equiv 1 \pmod{m}$.

### Criteri di congruenza

**Esercizio 1.13.** Dimostrare i seguenti criteri di congruenza:

- Un numero è congruo modulo 2 alla sua cifra delle unità.
- Un numero è congruo modulo 3 alla somma delle sue cifre.
- Un numero è congruo modulo 4 al numero costituito dalle ultime sue due cifre.
- Un numero è congruo modulo 9 alla somma delle sue cifre.
- Un numero è congruo modulo 11 alla somma delle sue cifre a segno alterno, in modo che la cifra delle unità abbia segno positivo.

[Hint]

## 1.5 Esercizi base

In questa sezione presentiamo una serie di esercizi che vi guideranno nel prendere maneggevolezza con le nozioni di base di teoria dei numeri.

**Esercizio 1.14.** Per quali valori di $n \in \mathbb{N}$ il numero $\frac{n^2+3n-5}{n-2}$ è intero? [Hint]

**Esercizio 1.15.** Per quali valori di $n \in \mathbb{N}$ il numero $\frac{n^3+5}{n^2-1}$ è intero? Seguire questa linea dimostrativa:

1. Scrivere $\frac{n^3+5}{n^2-1}$ nella forma $p(n) + \frac{q(n)}{n^2-1}$ con $p$ e $q$ polinomi a coefficienti interi, e $q$ di grado minore o uguale a 1.
2. Vedere per quali $n$ si ha $|q(n)| < |n^2 - 1|$ e convincersi che per questi $n$ il numero iniziale non è intero, tranne se $q(n) = 0$.
3. Fare *a mano* i (pochi!) casi rimasti.

**Esercizio 1.16.** Per quali valori interi di $a$ il numero $a^2 + 27a + 91$ è un quadrato perfetto? [Hint]

**Esercizio 1.17.** Trovare tutte le terne di interi $(a, b, c)$ tali che $a^n + b^n + c^n = 0$ per infiniti valori di $n \in \mathbb{N}$. [Hint]

**Esercizio 1.18.** Per quali interi $n$ si ha $(2n + 3, n + 7) = 1$? Per quali interi $n$ si ha invece che $(4n^2 - 2, 2n + 5) = 1$? [Hint]

**Esercizio 1.19.** Sia $k$ un numero intero, siano $A = 2^k - 2$ e $B = 2^k \cdot A$. Dimostrare che $A + 1$ e $B + 1$ hanno lo stesso insieme di divisori primi. [Hint]

**Esercizio 1.20.** Dimostrare che non esiste un polinomio a coefficienti interi $f(x)$ tale che $f(7) = 11$ e $f(11) = 13$. [Hint]

**Esercizio 1.21.** Dimostrare che non esiste un intero $n$ tale che la somma delle cifre di $n^2$ sia uguale a 15. [Hint]

**Esercizio 1.22.** Dimostrare che le seguenti equazioni non hanno soluzioni per $n, m$ e $a$ interi:

1. $3n - 1 = a^2$;
2. $5n - 2 = a^2$;
3. $7n + 5 = a^2$;
4. $4n + 2 = a^2$;
5. $15n^2 - 7m^2 = 9$.

[Hint]

**Esercizio 1.23.** Dimostrare che non esiste un triangolo rettangolo con i lati di lunghezza intera ed entrambi i cateti di lunghezza dispari. [Hint]

**Esercizio 1.24.** Considerare la sequenza dei numeri di Fibonacci, che ricordiamo essere definita come $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$ per $n \geq 1$. Dimostrare che esiste $n > 0$ tale che $F_n$ è divisibile per 2017. [Hint]

**Esercizio 1.25.** Dimostrare che scegliendo $n + 1$ numeri tra $\{1, 2, \ldots, 2n\}$:

1. ce ne sono due coprimi;
2. ci sono $a, b$ distinti tali che $a$ è multiplo di $b$.

[Hint]

**Esercizio 1.26.** Dimostrare che dati 5 interi ne esistono 3 con somma multipla di 3. [Hint]

**Esercizio 1.27.** Dimostrare che se $p$ è un numero primo e $a \in \mathbb{N}$ allora $a^2 - p$ non è divisibile per $p^2$. [Hint]

**Esercizio 1.28.** Trovare tutte le soluzioni intere positive di $3^y - x^2 = 17$. Seguire questa via:

1. Dimostrare che $x$ deve essere pari, quindi scriverlo nella forma $x = 2a$ e sostituirlo nell'equazione iniziale.
2. Guardare la nuova equazione modulo 4 e dedurne che $y$ è pari, dunque porre $y = 2b$ e riscrivere l'equazione.
3. Accorgersi che il membro sinistro è una differenza di quadrati: fattorizzare, ricordarsi che 17 è un numero primo quindi i due fattori devono essere 1 e 17, quindi risolvere il sistema che ne deriva.

**Esercizio 1.29.** Dato un intero positivo $n$ indichiamo con $d(n)$ il numero dei suoi divisori. Per quali $n$ interi positivi $d(n)^2 = n$? Seguire la linea dimostrativa:

1. Scrivere la fattorizzazione di $n$ come $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ e dimostrare che
$$d(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1)\,.$$
2. Dal fatto che $n$ è un quadrato, dedurre la parità degli $\alpha_i$ e di conseguenza di $d(n)$.
3. Considerare il caso in cui $n$ sia una potenza di un primo $p$: dimostrare per induzione che $p^b > (b+1)^2$ per $b$ "grande" e quindi in tal caso non ci possono essere soluzioni. Fare a mano i casi con $b$ "piccolo".
4. Estendere al caso con più di un fattore primo, moltiplicando tra loro le disuguaglianze del punto precedente. Concludere che esiste un unico $n$ che va bene.

[Hint]

## 1.6 Teorema cinese del resto

Cerchiamo ora di capire quando un sistema di congruenze ha soluzione.

Chiaramente sistemi come
$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 4 \end{cases}$$
non hanno soluzione (non ci sono numeri dispari congrui a 2 modulo 4). Questo succede perché i moduli che abbiamo considerato (2 e 4) non sono coprimi. Sorge allora spontanea la domanda: e se i moduli sono coprimi cosa succede? Il teorema cinese del resto risponde a questo problema.

**Teorema 1.4** (Teorema cinese del resto)**.** *Siano $n_1$ , $n_2$ due interi tali che $(n_1, n_2) = 1$ e $a_1$ , $a_2$ due interi qualsiasi. Allora il sistema*
$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases} \tag{1.3}$$
*ha un'unica soluzione modulo $n_1 \cdot n_2$.*

Il teorema ci dice quindi che il sistema 1.3 ha sempre soluzione purché i moduli considerati siano coprimi. In particolare il sistema ha infinite soluzioni in $\mathbb{N}$ ma soltanto una negli interi modulo $n_1 \cdot n_2$ (cioè compresi fra 0 e $n_1 \cdot n_2 - 1$).

Il teorema si può generalizzare a sistemi di tre o più congruenze, vediamo come. Siano $k \in \mathbb{N}$ e $n_1\,, n_2\,, \ldots\,, n_k$ degli interi positivi a due a due coprimi. Consideriamo poi $a_1\,, a_2\,, \ldots\,, a_k$ degli interi qualsiasi, allora il sistema

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

ha un'unica soluzione modulo $n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

Da un punto di vista pratico, trovare la soluzione del sistema non è difficile. Vediamolo in questo esempio.

**Esempio.** Vogliamo risolvere il sistema

$$\begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 4 \pmod{7} \end{cases}$$

La prima equazione ci dice che $12 \mid x - 5$, cioè esiste $k \in \mathbb{Z}$ tale che $x = 12k + 5$. Sostituendo ciò nella seconda condizione del sistema abbiamo che

$$5 + 12k \equiv 4 \pmod{7}\,,$$

cioè $12k \equiv -1 \pmod{7}$. L'inverso moltiplicativo di $12 \equiv 5 \pmod{7}$ è 3 e quindi se moltiplichiamo per 3 otteniamo:

$$k \equiv -3 \equiv 4 \pmod{7}$$

cioè esiste $j \in \mathbb{Z}$ tale che $k = 7j + 4$. Quindi in particolare

$$x = 5 + 12k = 5 + 12(7j + 4) = 5 + 84j + 48 = 53 + 84j\,.$$

Abbiamo così trovato la soluzione del sistema, cioè $x \equiv 53 \pmod{84}$.

Da un punto di vista più teorico, il Teorema 1.4 (Teorema cinese del resto) è essenziale in problemi come i seguenti.

**Esercizio 1.30.** Dimostrare che esistono 2017 interi consecutivi, ciascuno multiplo di un quadrato maggiore di 1. [Hint]

**Esercizio 1.31.** Dimostrare che, per ogni intero positivo $n$, esistono $n$ interi consecutivi che non sono potenze perfette. Diciamo che un intero positivo è una potenza perfetta se si può scrivere nella forma $m^k$, con $m, k$ interi positivi maggiori di 1. [Hint]

## 1.7 Struttura moltiplicativa

L'obiettivo di questa sezione è studiare come si comportano le potenze di un intero $a$ modulo un altro intero $m$, cioè $a^0, a^1, a^2, \dots$ modulo $m$. Di particolare interesse sarà il caso in cui $(a, m) = 1$, cioè quando $a$ ed $m$ sono coprimi.

**Esercizio 1.32.** Dimostrare che la successione $\{a^n \bmod m\}_{n\in\mathbb{N}}$, costituita dalle classi di congruenza di $a^n$ modulo $m$, è definitivamente periodica, cioè esistono $k, N \in \mathbb{N}$ tali che

$$a^{k+n} \equiv a^n \pmod{m} \qquad \text{per ogni } n \geq N\,.$$

Inoltre mostrare che se $(a, m) = 1$, allora tale successione è periodica (cioè la proprietà vale con $N = 0$). [Hint]

**Definizione 1.5.** Dati $a, m \in \mathbb{N}$ tali che $(a, m) = 1$, il periodo delle potenze di $a$ modulo $m$ (che esiste per l'esercizio precedente) è detto *ordine* di $a$ modulo $m$ e si denota $\mathrm{ord}_m(a)$.

Ricordiamo che il *periodo* di una successione periodica $\{a_n\}_{n\in\mathbb{N}}$ è il più piccolo $k \in \mathbb{N}$ tale che $a_{n+k} = a_n$ per ogni $n \in \mathbb{N}$.

**Esercizio 1.33.** Dati $a, m \in \mathbb{N}$ coprimi, supponiamo che $a^n \equiv 1 \pmod{m}$ per un certo $n \in \mathbb{N}$. Allora $\mathrm{ord}_p(a)$ divide $n$.

### Piccolo teorema di Fermat

Concentriamoci innanzitutto sul caso in cui $m$ sia uguale ad un numero primo $p$. Notiamo innanzitutto che se $(a, p) \neq 1$, allora necessariamente $p$ divide $a$, ma in questo caso osserviamo che banalmente $a^k \equiv 0 \pmod{p}$ per ogni $k \in \mathbb{N}$. Dunque il caso interessante su cui ci concentreremo sarà quello in cui $a$ è coprimo con $p$.

**Teorema 1.6** (Piccolo teorema di Fermat)**.** *Dato un primo $p \in \mathbb{N}$, vale che*

$$a^p \equiv a \pmod{p}$$

*per ogni $a \in \mathbb{N}$.*

Osserviamo che se $a \equiv 0 \pmod{p}$ la tesi del teorema è ovvia. Altrimenti, se $(a, p) = 1$, il Teorema 1.6 (Piccolo teorema di Fermat) mostra che

$$a^{p-1} \equiv 1 \pmod{p}\,.$$

Vediamo ora due differenti dimostrazioni del Teorema 1.6 (Piccolo teorema di Fermat), presentate attraverso i seguenti due esercizi.

**Esercizio 1.34.** Dimostrare il Teorema 1.6 (Piccolo teorema di Fermat) per induzione su $a$.

**Esercizio 1.35.** Dimostrare il Teorema 1.6 (Piccolo teorema di Fermat) attraverso le seguenti osservazioni:

1. Gli elementi $a, 2a, \ldots, (p-1)a \pmod p$ rappresentano tutte le classi di congruenza modulo $p$.
2. Grazie al punto precedente abbiamo che $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a \cdot 2a \cdot \ldots \cdot (p-1)a \pmod p$.

**Esercizio 1.36.** Calcolare la classe di congruenza di $4^{2017}$ modulo 11.

**Esercizio 1.37.** Trovare tutte le coppie di primi $(p, q)$ tali che $pq \mid 2^{pq} + 1$. [Hint]

### Funzione $\phi$ di Eulero

**Definizione 1.7.** Dato un intero $n \in \mathbb{N}$ definiamo $\phi(n)$ (detta *funzione $\phi$ di Eulero*) come il numero degli interi fra 1 ed $n$ che sono relativamente primi con $n$.

**Esercizio 1.38.** Dato un numero primo $p$ vale che $\phi(p) = p - 1$ e più in generale che $\phi(p^k) = p^{k+1}(p-1)$ per ogni $k \in \mathbb{N}$. [Hint]

**Esercizio 1.39.** Dati $a, b \in \mathbb{N}$ interi coprimi, vale che $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. In altre parole la funzione $\phi$ di Eulero è moltiplicativa sugli interi coprimi.

Mostrare il risultato appena enunciato seguendo la seguente traccia dimostrativa.

Dato $m \in \mathbb{N}$ definiamo $A_m = \{x \ : \ 0 \leq x < m\,,\, (m, x) = 1\}$. Osservare che la cardinalità di $A_m$ è esattamente $\phi(m)$.

Consideriamo quindi la funzione $\Theta : A_{a \cdot b} \to A_a \times A_b$ definita da

$$\Theta(x) = (x \bmod a, x \bmod b)\,,$$

cioè la funzione che prende un intero $0 \leq x < m$ coprimo con $m$ e lo riduce rispettivamente modulo $a$ e modulo $b$.

1. Dimostare che un intero $x \in \mathbb{N}$ è coprimo con $a \cdot b$ se e solo se è coprimo sia con $a$ che con $b$. Dunque la funzione $\Theta$ è ben definita.
2. Dimostrare che la funzione $\Theta$ è iniettiva e surgettiva grazie al Teorema 1.4 (Teorema cinese del resto).
3. Concludere che gli insiemi $A_{a \cdot b}$ e $A_a \times A_b$ hanno la stessa cardinalità e dunque $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

**Esercizio 1.40.** Sia $n$ un intero positivo con fattorizzazione $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$. Allora vale che

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_s - 1) = n \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right)\,.$$

[Hint]

**Esercizio 1.41.** Dato un intero positivo $n$ dimostrare che

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

cioè che la somma di $\phi(d)$ sui divisori $d$ di $n$ è uguale $n$. [Hint]

### Teorema di Eulero - Fermat

Vediamo ora un'estensione del Teorema 1.6 (Piccolo teorema di Fermat) al caso non necessariamente primo, cioè studiamo in generale le classi di congruenza di $a^0, a^1, a^2, \ldots$ modulo $m$ per due interi $a, m$ coprimi generici.

**Teorema 1.8** (Eulero-Fermat)**.** *Dato un intero $m \in \mathbb{N}$, vale che*

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

*per ogni $a \in \mathbb{N}$ coprimo con $m$.*

Notare che questo risultato è esattamente il Teorema 1.6 (Piccolo teorema di Fermat) nel caso in cui $m$ sia uguale ad un primo $p$.

**Esercizio 1.42.** Provare a riadattare la dimostrazione del Teorema 1.6 (Piccolo teorema di Fermat) vista nell'Esercizio 1.35 per dimostrare anche questo caso più generale. [Hint]

## 1.8 Hints

**Esercizio 1.1:** Utilizzare la definizione di divisibilità. (Testo)

**Esercizio 1.2:** Unendo le due equazioni ricavo $p+q = \frac{pq-1}{2}$, da cui $q = \frac{2p+1}{p-2}$, ma quando è che $p-2 \mid 2p+1$? (Testo)

**Esercizio 1.3:** Mostrare che un intero $d$ divide sia $a$ che $b$ se e solo se divide sia $r$ che $b$. Notare poi che questo è sufficiente a concludere. (Testo)

**Esercizio 1.9:** Quali sono le classi di congruenza di $k$, $k+1$, $k+2$? (Testo)

**Esercizio 1.11:** L'Equazione (1.2) ammette soluzione se e solo se esiste un intero $y$ tale che $ax - my = b$. (Testo)

**Esercizio 1.13:** Scrivere il numero $n$ considerato in base 10, cioè $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots a_1 \cdot 10 + a_0$, con $0 \leq a_i < 10$ per ogni $i = 0, \ldots, k$, e applicare le proprietà delle congruenze per studiare $n$ modulo i vari numeri considerati. (Testo)

**Esercizio 1.14:** Fare la divisione di polinomi e scrivere il numero nella forma $p(n) + \frac{b}{n-2}$ per un opportuno polinomio $p$ a coefficienti interi e un opportuno numero intero $b$. Considerare poi i divisori di $b$ (anche quelli negativi...). (Testo)

**Esercizio 1.16:** Stringere la quantità $a^2 + 27a + 91$ tra due quadrati, in particolare trovare due interi $b$ e $c$ tali che $(a+b)^2 < a^2 + 27a + 91 < (a+c)^2$. A questo punto, detto $n^2$ il quadrato perfetto uguale ad $a^2 + 27a + 91$, $n$ deve necessariamente essere uguale a uno tra $a+b+1, a+b+2, \ldots, a+c-1$. (Testo)

**Esercizio 1.17:** Risolvere dapprima il caso in cui (almeno) uno tra $a, b$ e $c$ è uguale a 0. Poi, senza perdita di generalità, si può assumere che l'intero massimo, in valore assoluto, sia $a$. Allora scrivere $a^n = -b^n - c^n$ e dividere entrambi i membri per $a^n$. Cosa succede per $n$ *grande* alle potenze $n$-esime di un numero minore di 1? (Testo)

**Esercizio 1.18:** Ricordarsi che $(a, b) = (a - bc, b)$ per ogni $c$ intero e usarlo per ricondursi all'MCD fra un numero intero e una quantità che dipende da $n$ ($(2n+3, n+7) = ((2n+3) - 2 \cdot (n+7), n+7) = (11, n+7)$). (Testo)

**Esercizio 1.19:** Dimostrare che se $p$ è un numero primo tale che $p \mid A+1$ allora $p \mid B+1$ e viceversa. (Testo)

**Esercizio 1.20:** Usare l'esercizio visto ad algebra, che dice che per ogni $h$, k interi vale che $h - k \mid f(h) - f(k)$. (Testo)

**Esercizio 1.21:** Ricordarsi i criteri di divisibilità per 3 e per 9. (Testo)

**Esercizio 1.22:** Considerare la prima equazione modulo 3, sfruttando che $a^2$ può assumere solo i valori $0, 1$ modulo 3. Guardare anche le altre equazioni modulo un numero opportuno. (Testo)

**Esercizio 1.23:** Chiamare $a$ e $b$ i cateti e $c$ l'ipotenusa. Che equazione soddisfano? Guardarla modulo 4. (Testo)

**Esercizio 1.24:** La sequenza modulo 2017 è periodica (senza antiperiodo!) (Testo)

**Esercizio 1.25:** Per la prima parte, dimostrare che esiste $a$ tale che sia $a$ sia $a+1$ stanno nell'insieme dei numeri scelti; per la seconda parte, scrivere ogni numero nella forma $2^k \cdot d$ con $d$ dispari. (Testo)

**Esercizio 1.26:** I numeri possono essere congrui a 0, 1 o 2 modulo 3. Se ce ne sono tre dello stesso tipo, la tesi è vera (perché?); altrimenti ce ne è almeno uno per tipo, e anche in questo caso la tesi è vera (perché?). (Testo)

**Esercizio 1.27:** Ragionare per assurdo: se la tesi fosse falsa avrei $a^2 \equiv p \pmod{p^2}$ e quindi esisterebbe un intero $b$ tale che $a^2 = bp^2 + p = p(1+bp)$. Ora guardare la parità dei fattori $p$ in $a^2$ e $p(1+bp)$ e trovare un assurdo. (Testo)

**Esercizio 1.29:** Nel punto 3, più precisamente, dimostrare per induzione su $b$ che la disuguaglianza vale per $p > 3$ e $b \geq 2$, e vale per $p = 3$ e $b \geq 3$. Il caso $p = 3$, $b = 2$ fornisce in effetti l'unico $n$ che va bene! (Testo)

**Esercizio 1.30:** Se $p$ è un primo, allora un numero $x$ multiplo di $p^2$ soddisfa $x \equiv 0 \pmod{p^2}$. Dunque scegliamo 2017 numeri primi distinti $p_0, \dots, p_{2016}$ e cerchiamo un intero $n$ tale che $n+k$ sia multiplo di $p_k^2$ per ogni $k = 0, \dots, 2016$. Questo si riduce ad un sistema di congruenze che possiamo risolvere con il Teorema 1.4 (Teorema cinese del resto). (Testo)

**Esercizio 1.31:** Notare che se un intero $x$ rispetta $x \equiv p \pmod{p^2}$ per qualche primo $p$, allora non può essere una potenza perfetta. (Testo)

**Esercizio 1.32:** Considerare i valori di $a^0, a^1, \dots, a^m$ modulo $m$ e osservare che per il principio dei cassetti almeno due di questi valori devono coincidere. Nel caso in cui $(a, m) = 1$, osservare che se $a^{n+k} \equiv a^n \pmod{m}$ è possibile semplificare $a^n$ ed ottenere $a^k \equiv 1 \pmod{m}$. (Testo)

**Esercizio 1.37:** Deve valere che $2^{pq} \equiv -1 \pmod{p}$, ma questo implica che $2^{2q} \equiv 1 \pmod{p}$ (perché?) e quindi $\mathrm{ord}_p(2) \mid 2q$. Notare che questo mi dice che $\mathrm{ord}_p(2)$ è uno fra $1, 2, q, 2q$. Fare ora lo stesso ragionamento scambiando $p$ e $q$. (Testo)

**Esercizio 1.38:** Quanti sono i multipli di $p$ fra 1 e $p-1$? E fra 1 e $p^k - 1$? (Testo)

**Esercizio 1.40:** Utilizzare gli esercizi precedenti. (Testo)

**Esercizio 1.41:** Considerare le frazioni $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$ e ridurle ai minimi termini (cioè semplificare i fattori comuni a numeratore e denominatore in ogni frazione). Allora il numero di frazioni che dopo la semplificazione avrà denominatore uguale a $d$, con $d \mid n$, è esattamente $\phi(d)$. (Testo)

**Esercizio 1.42:** Questa volta considerare le classi $\{x_1, \ldots, x_{\phi(m)}\}$ coprime con $m$ e notare che $\{ax_1, \ldots, ax_{\phi(m)}\}$ rappresentano le stesse classi (eventualmente permutate). (Testo)

## 1.9 Problemi

**N1.** Trovare tutte le quadruple $(p, q, r, n)$ di interi positivi tali che $p$ e $q$ sono primi, $p + q$ non è divisibile per 3 e inoltre

$$p + q = r(p - q)^n .$$

**N2.** Dato un primo $p$ congruo a 2 modulo 3, dimostrare che esistono al massimo $p - 1$ coppie di interi $(m, n)$ con $0 < m, n < p$ tali che $p$ divida $n^3 - m^2 + 1$.

**N3.** Dato un intero positivo $n$, dimostrare che ogni naturale $m \leq n!$ può essere scritto come somma di al più $n$ divisori distinti di $n!$.

**N4.** Siano $a, b$ interi positivi strettamente maggiori di 1 e sia inoltre $f(n)$ un polinomio a coefficienti interi. Si sa che esiste $N > 0$ naturale tale che

$$b^n \mid a^n + f(n)$$

per ogni $n > N$. Dimostrare che $b \mid a$ e $f(n)$ è il polinomio nullo.