G. Pareschi

COMPLEMENTI ED ESEMPI SUI NUMERI INTERI.

1. Divisione con resto di numeri interi

1.1. **Divisione con resto.** Per evitare fraintendimenti nel caso in cui il numero a del Teorema 0.4 sia negativo, facciamo un esempio.

Esempio 1.1. (a) 15 diviso 7: $15 = 2 \cdot 7 + 1$. -15 diviso 7: $-15 = -3 \cdot 7 + 6$.
Quindi il resto della divisione di 15 per 7 è 1, mentre il resto della divisione di -15 per 7 è 6.

1.2. **Rappresentazione in base n.** Un'applicazione della divisione con resto di numeri interi è la *rappresentazione in base n*, dove n è un qualsiasi numero naturale. Essa si riassume nel seguente

Teorema/Definizione/Notazione 1.2. Sia $n \in \mathbb{N}$ un numero naturale fissato. Sia $m \in \mathbb{N}$ un altro numero naturale. Allora esistono e sono unici $k \in \mathbb{N}$ e numeri interi non negativi $a_0, a_1, \ldots, a_k$ tali che $a_0, a_1, \ldots, a_k < n$, $a_k \neq 0$ e

$$m = a_k n^k + \cdots + a_1 n + a_0$$

Tale scrittura si chiama *rappresentazione del numero m in base n* e si indica

$$m = (a_k \ldots a_1 a_0)_n.$$

Proof. Esistenza della rappresentazione. Dividiamo m per n. Risulta che $m = q_0 n + a_0$ con $0 \leq a_0 < n$. Se $q_0 = 0$ (ossia $m < n$) ci fermiamo. Altrimenti, dividiamo q_0 per n. Si ha $q_0 = q_1 n + a_1$, con $0 \leq a_1 < n$. Se $q_1 = 0$, ossia $q_0 < n$, ci fermiamo e

$$m = a_1 n + a_0$$

Altrimenti

$$m = (q_1 n + a_1)n + a_0 = q_1 n^2 + a_1 n + a_0$$

e continuiamo dividendo q_1 per n: $q_1 = q_2 n + a_2$ e così via. È chiaro che questo processo deve terminare ad un certo punto (in altre parole, esisterà un $k \in \mathbb{N}$ tale che $0 \neq q_k < n$, cioè $q_k = a_k \neq 0$). Otteniamo dunque la rappresentazione cercata

$$m = a_k n^k + \cdots + a_1 n + a_0$$

Unicità della rappresentazione. Supponiamo che esistano altri numeri $h \in \mathbb{N}$ e $b_h, \ldots, b_1, b_0$ tali che $b_h, \ldots, b_0 < n$, $b_h \neq 0$ e

$$m = b_h n^h + \cdots + b_1 n + b_0.$$

Dimostriamo per induzione che $h = k$ e che $a_i = b_i$ per $i = 0, \ldots k$. Poichè

$$m = (a_k n^{k-1} + \ldots a_1)n + a_0 = (b_{h-1} n^{h-1} + \ldots b_1)n + b_0$$

si ha, per il Teorema 0.4 della dispensa EALInteri, che

$$a_0 = b_0$$

e che

$$a_k n^{k-1} + \ldots a_1 = b_{h-1} n^{h-1} + \ldots b_1.$$

Chiamiamo p questo ultimo numero. Abbiamo quindi dimostrato il passo base ($a_0 = b_0$). Inoltre, supponiamo vero l'enunciato per ogni numero strettamente minore di m, (quindi applichiamo il principio di induzione nella Variante 1.5 (Dispensa INDUZIONE). Poichè $p < m$, applicando l'ipotesi induttiva al numero p si ha che

$$k-1 = h-1 \qquad e \qquad a_i = b_i, \quad i = 1, \dots, k$$

Dunque anche l'unicità è dimostrata. □

Esempio 1.3. (a) Scriviamo il numero 49 in base 2: $49 = 24 \cdot 2 + 1$. $24 = 12 \cdot 2 + 0$. $12 = 6 \cdot 2 + 0$. $6 = 3 \cdot 2 + 0$. $3 = 1 \cdot 2 + 1$. Dunque

$$49 = 24 \cdot 2 + 1 = 12 \cdot 2^2 + 0 \cdot 2 + 1 = 6 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1 = 3 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1 =$$
$$= 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1$$

Quindi

$$49 = (110001)_2$$

(b) Scriviamo il numero 49 in base 3: $49 = 16 \cdot 3 + 1$. $16 = 5 \cdot 3 + 1$. $5 = 1 \cdot 3 + 2$. Dunque

$$49 = 16 \cdot 3 + 1 = 5 \cdot 3^2 + 1 \cdot 3 + 1 = 1 \cdot 3^3 + 2 \cdot 3^2 + 1 \cdot 3 + 1$$

Dunque

$$49 = (1211)_3$$

(c) Scriviamo il numero 49 in base 8: $49 = 6 \cdot 8 + 1$. Dunque

$$49 = (61)_8$$

Osservazione 1.4. Esattamente come nel caso a noi più familiare della base 10, si possono descrivere facilmente gli algoritmi per la somma (con "riporto"), la sottrazione, la moltiplicazione e la divisione con resto in base n.

2. Facili applicazioni delle proprietà delle congruenze

La proposizione 0.15, punti (a) e (b), significa che la relazione di equivalenza di congruenza modulo n è *compatibile* con le operazioni di somma e moltiplicazione. Vediamo alcune applicazioni di questo punto. Come nella dispensa EALgruppi, fissato $n \in \mathbb{N}$, dato $a \in \mathbb{Z}$ denotiamo con $\bar{a}$ la classe di equivalenza di a rispetto alla congruenza modulo n. Dunque, la suddetta proposizione dice che

$$\overline{a+b} = \overline{a} + \overline{b}$$
$$\overline{a\,b} = \overline{a}\,\overline{b}$$

Esempio 2.1. *Il resto della divisione per* 3 *(o per* 9*) di un dato numero naturale è uguale al resto della divisione per* 3 *(o per* 9*) della somma delle sue cifre decimali.* In simboli: dato il numero k la cui rappresentazione decimale è $a_s\, a_{s-1} \dots .\, a_1\, a_0$, si ha che

$$k \equiv a_s + a_{s-1} + \cdots + a_1 + a_0 \pmod 3$$

(la stessa cosa mod 9).
Infatti $z = a_s 10^s + a_{s-1} 10^{s-1} + \cdots + a_1 10 + a_0$. Dunque

$$\overline{z} = \overline{a_s 10^s + a_{s-1} 10^{s-1} + \cdots + a_1 10 + a_0} = \overline{a_s}\,\overline{10}^s + \cdots + \overline{a_1}\,\overline{10} + \overline{a_0}$$

Ma, modulo 3 o 9, $\overline{10} = \overline{1}$. Quindi $\overline{10}^s = \overline{1}^s = \overline{1^s} = \overline{1}$. Dunque

$$\overline{z} = \overline{a_s}\,\overline{10}^s + \cdots + \overline{a_1}\,\overline{10} + \overline{a_0} = \overline{a_s} + \cdots \overline{a_0} = \overline{a_s + \cdots + a_0}$$

Ad esempio, per calcolare il resto della divisione per 9 del numero 579146897632 si osserva che, modulo 9,

$$\overline{579146897632} = \overline{5+7+9+1+4+6+8+9+7+6+3+2} = \overline{4}.$$

Dunque il resto cercato è 4.

Esempio 2.2. *Il resto della divisione per* 11 *di un dato numero naturale è uguale al resto della divisione per* 11 *della somma* alternata *delle sue cifre decimali.* In simboli: dato il numero k la cui rappresentazione decimale è $a_s\, a_{s-1} \,....\, a_1\, a_0$, si ha che

$$k \equiv a_0 - a_1 + a_2 + \cdots + (-1)^s a_s \pmod{11}$$

La dimostrazione è uguale alla precedente, e usa il fatto che, $10 \equiv -1 \pmod{11}$. Dunque, modulo 11,

$$\overline{10^i} = \overline{10}^i = \overline{-1}^i = \overline{-1^i}.$$

Ad esempio per calcolare il resto della divisione per 11 del numero 579146897632 si osserva che, modulo 11,

$$\overline{579146897632} = \overline{-5+7-9+1-4+6-8+9-7+6-3+2} = \overline{6}.$$

Dunque il resto cercato è 6.

Esempio 2.3. *Il resto della divisione per* 4 *di un dato numero naturale è uguale al resto della divisione per* 4 *del numero rappresentato dalla sue ultime due cifre decimali.* In simboli: dato il numero k la cui rappresentazione decimale è $a_s\, a_{s-1} \,....\, a_1\, a_0$, si ha che

$$k \equiv a_1 10 + a_0 \pmod{4}$$

Questo perchè $10^i \equiv 0 \pmod{4}$ se $i \geq 2$. Ad esempio, per calcolare il resto della divisione per 4 del numero 579146897632 si osserva che, modulo 4,

$$\overline{579146897632} = \overline{32} = \overline{0}.$$

Dunque 579146897632 è un multiplo di 4.

Esempio 2.4. *Il resto della divisione per* 5 *di un dato numero naturale è uguale al resto della divisione per* 5 *della sua ultima cifra decimale.* Questo perchè $10^i \equiv 0 \pmod{5}$ se $i \geq 1$. Ad esempio, per calcolare il resto della divisione per 5 del numero 579146897638 si osserva che, modulo 5,

$$\overline{579146897638} = \overline{8} = \overline{3}.$$

Dunque il resto cercato è 3.

Esempio 2.5. *Il resto della divisione per* 8 *di un dato numero naturale è uguale al resto della divisone per* 8 *della somma delle cifre della sua rappresentazione in base* 7. In simboli: se $k = (a_s\, a_{s-1} \,....\, a_1\, a_0)_7$ allora

$$k \equiv a_s + a_{s-1} + ... + a_1 + a_0 \pmod{8}$$

Qua il punto è che $8 \equiv 1 \pmod{7}$. Ed esempio, per calcolare il resto della divisione per 8 del numero $(579146897632)_7$, si osserva che, modulo 8,

$$(579146897632)_7 \equiv \overline{5+7+9+1+4+6+8+9+7+6+3+2} = \overline{3}$$

3. Alcune osservazioni sulle potenze di numeri interi

Osservazione 3.1. *(Potenze negative)*
(a) *(Inverso moltiplicativo)* Sia $a \in \mathbb{Z}$ tale che $\bar{a} \in \mathbb{Z}_n^*$, cioè $mcd(a, n) = 1$. Ricordiamo che $\bar{a}^{-1} \in \mathbb{Z}_p$ è la classe $\pmod p$ della soluzione della congruenza

$$ax \equiv 1 \pmod n$$

(b) Dato $\bar{a} \in \mathbb{Z}_n^*$ e dato $n \in \mathbb{N}$, per $\bar{a}^{-n}$ si intende l'inverso moltiplicativo di $\bar{a}^n$. Risulta subito che,

$$\bar{a}^{-n} = \bar{a}^{-1} \cdots \bar{a}^{-1} \qquad \text{(n volte)}$$

Dal (piccolo) Teorema di Fermat (Teorema 1.12 Dispensa EALgruppi) segue la seguente proposizione.

Proposizione 3.2. Sia p un numero primo e $a \in Z$ tale che $mcd(a, p) = 1$ (in altre parole x non è multiplo di p). Siano inoltre $k, h \in \mathbb{Z}$. Se

$$k \equiv h \pmod{p-1}$$

allora

$$a^k \equiv a^h \pmod p$$

Proof. Il fatto che $h \equiv k \pmod{p-1}$ significa che esiste $t \in \mathbb{Z}$ tale che $h - k = t\,(p-1)$ cioè $h = t\,(p-1) + k$. Quindi

$$a^h = a^{t(p-1)+k} = a^{t(p-1)}\, a^k = (a^{p-1})^t\, a^k.$$

Poichè, per il Piccolo Teorema di Fermat $a^{p-1} \equiv 1 \pmod p$, si ha che $(a^{p-1})^t \equiv 1^t = 1 \pmod p$ e quindi

$$a^h = (a^{p-1})^t\, a^k \equiv a^k \pmod p.$$

□

Corollario 3.3. Sia p un numero primo e $a \in \mathbb{Z}$ tale che $mcd(a, p) = 1$ (in altre parole a non è multiplo di p). Sia inoltre $k \in \mathbb{Z}$. Se il resto della divisione di k per $p-1$ è r allora

$$a^k \equiv a^r \pmod p.$$

Osservazione 3.4 (importante)**.** Si noti che la Proposizione 3.2 vale anche per potenze negative, cioè se k o h sono negativi.

Esempio 3.5. Calcolare il resto della divisione per 11 del numero $37954219871541^{154578998}$.
Per semplificarci la vita, cominciamo a ridurre la base modulo 11. Per uno degli esempi della sezione precedente

$$37954219871541 \equiv -3 + 7 - 9 + 5 - 4 + 2 - 1 + 9 - 8 + 7 - 1 + 5 - 4 + 1 \equiv -2 \equiv 9 \pmod{11}$$

Quindi

$$37954219871541^{154578998} \equiv (-2)^{154578998} \equiv 9^{154578998}$$

Adesso riduciamo l'esponente modulo $10 (= 11 - 1)$. Si ha, evidentemente, che

$$154578998 \equiv 8 \equiv -2 \pmod{10}.$$

Dunque

$$37954219871541^{154578998} \equiv (-2)^{-2} = \big((-2)^2\big)^{-1} = 4^{-1} \pmod{11}.$$

Risolvendo la congruenza

$$4x \equiv 1 \pmod{11}$$

si vede facilmente che $x \equiv 3 \pmod{11}$ ($4 \cdot 3 = 12 \equiv 1 \pmod{11}$). Dunque

$$37954219871541^{154578998} \equiv 4^{-1} \equiv 3 \pmod{11}$$

e il resto cercato è 3.

Esempio 3.6. Calcolare il resto della divisione per 55 del numero precedente, cioè $37954219871541^{154578998}$. Sia r tale resto. Per il Teorema cinese del resto, r è soluzione del sistema di congruenze

$$\begin{cases} x \equiv 37954219871541^{154578998} \pmod{11} \\ x \equiv 37954219871541^{154578998} \pmod{5} \end{cases}$$

Abbiamo già visto che la prima congruenza è equivalente a $x \equiv 3 \pmod{11}$. Per quanto riguarda la seconda congruenza, riducendo la base $\pmod 5$ si ottiene

$$37954219871541 \equiv 1 \pmod{5}.$$

Dunque

$$37954219871541^{154578998} \equiv 1^{154578998} = 1 \pmod{5}$$

Quindi il sistema è equivalente a

$$\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 1 \pmod{5} \end{cases}$$

Quindi $x = 1 + 5k$ e $1 + 5k \equiv 3 \pmod{11}$. Dunque

$$5k \equiv 2 \pmod{11}.$$

Questa congruenza si può risolvere in tanti modi. In questo caso, i numeri sono talmente piccoli che si possono provare i vari numeri $2, 3$ eccetera fino a trovare che la soluzione è 7. Ecco un altro modo: $5 \cdot 2 = -1$. Quindi $5 \cdot (-2) = 1$ (in altre parole, la classe di -2 è l'inverso moltiplicativo di 5 modulo 11). Dunque $5 \cdot 5 \cdot (2 \cdot (-2)) = 2$. Quindi la classe di $2 \cdot (-2) = -4$ è la soluzione della congruenza precedente. Dunque $k = -4 + 11h$. Quindi

$$x = 1 + 5(-4 + 11h) = -19 + 55h$$

ed il resto cercato r è il più piccolo numero positivo congruente a $-19 \pmod{55}$, cioè $-19+55 = 36$.

Esempio 3.7. Calcolare il resto della divisione per $91 (= 7 \cdot 13)$ del numero $3534534^{45673565}$. Sia r tale resto. Per il Teorema cinese del resto, r è soluzione del sistema di congruenze

$$\begin{cases} x \equiv 3534534^{45673565} \pmod{7} \\ x \equiv 3534534^{45673565} \pmod{11} \end{cases}$$

Cerchiamo di semplificare le due congruenze che compongono il sistema. Facendo la divisione con resto, risulta che $3534534 = 504933 \cdot 7 + 3$. Dunque $3534534 \equiv 3 \pmod{7}$. Quindi $3534534^{45673565} \equiv 3^{45673565} \pmod{7}$. Riduciamo ora l'esponente 45673565 modulo $6 (= 7 - 1)$. Facendo la divisione con resto, risulta che $45673565 \equiv 5 \equiv -1 \pmod{6}$.[1] Dunque $3534534^{45673565} \equiv 3^{-1} \pmod{7}$. Poichè la soluzione della congruenza $3x \equiv 1 \pmod{7}$ è 5, $(3 \cdot 5 = 15 = 2 \cdot 7 + 1)$, si ha che che la prima congruenza del sistema è equivalente a $x \equiv 5 \pmod{7}$.
Per quanto riguarda la seconda congruenza, riduciamo prima la base modulo 13. Si potrebbe fare la divisione con resto. Altrimenti usiamo che $10 \equiv -3 \pmod{13}$. Quindi $10^2 \equiv (-3)^2 = 9 \equiv$

[1] Alternativamente, si può notare che il resto della divisione di 45673565 per 6 è soluzione della congruenza $\begin{cases} x \equiv 45673565 \pmod{2} \\ x \equiv 45673565 \pmod{3} \end{cases}$ che è equivalente a $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv -1 \pmod{3} \end{cases}$ che ha come soluzione -1.

$-4 \pmod{13}$. Quindi $10^3 \equiv (-3)(-4) = 12 \equiv -1 \pmod{13}$. Proseguendo $10^4 \equiv (-3)(-1) = 3 \pmod{13}$, $10^5 = (-3)3 = -9 \equiv 4 \pmod{13}$, $10^6 = (-1)(-1) = 1 \pmod{13}$. Dunque

$$3534534 \equiv 1 \cdot 3 + 4 \cdot 5 + 3 \cdot 3 + (-1)4 + (-4)5 + (-3)3 + 4 \equiv 1 \pmod{13}.$$

Quindi $3534534^{45673565} \equiv 1^{45673565} = 1 \pmod{13}$ ed il sistema è equivalente a

$$\begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{13}. \end{cases}$$

Ne segue che $x = 13\,k + 1 \equiv 5 \pmod{7}$ e che $13k \equiv 4 \pmod{7}$. Poichè $13 \equiv -1 \pmod{7}$, si ha che $-k \equiv 4 \pmod{7}$, cioè $x \equiv -4 \equiv 3 \pmod{7}$. Dunque $k = 7 \cdot h + 3$. Dunque $x = 13\,k + 1 = 13(7h + 3) + 1 = 91\,h + 40$. Dunque il resto cercato è 40.

4. Raccolta di alcuni esercizi tratti da compiti d'esame.

Attenzione: questi sono alcuni esercizi d'esame, sugli argomenti di questa dispensa. Non sono una selezione di quelli che ritengo più significativi, ma solamente quelli tratti dagli appelli di cui sono in possesso del file sorgente. Siete quindi invitati a cercare di risolvere gli esercizi, su questi argomenti, tratti dai TUTTI gli esami degli anni passati (oltre agli esercizi assegnati, naturalmente).

Esercizio 4.1. Determinare gli interi x fra 0 e 200 che soddisfano

$$\begin{cases} x \equiv 3 \pmod{7}, \\ x \equiv 1 \pmod{13}. \end{cases}$$

La prima equazione ci dice che $x = 3 + 7k$ per un certo $k \in \mathbb{Z}$. Sostituendo nella seconda equazione troviamo che $3 + 7k \equiv 1 \pmod{13}$ e quindi $7k \equiv -2 \pmod{13}$.

Usando l'algoritmo euclideo (oppure con dei tentavi mirati) si trova che 2 è l'inverso moltiplicativo di 7 (mod 13). Moltiplicando per 2 si trova quindi che $k \equiv 2 \cdot 7k \equiv -2 \cdot 2 = -4 \pmod{13}$. In altre parole, si ha che $k = -4 + 13m$ per un certo $m \in \mathbb{Z}$. Sostituendo questo nella formula di x troviamo che $x = 3 + 7(-4 + 13m) = -25 + 91m$ per un certo $m \in \mathbb{Z}$.

Per $m = 1$ si ha che $x = 66$ e per $m = 2$ si ha che $x = 157$. Queste sono le uniche soluzioni $0 \leq x \leq 200$.

Esercizio 4.2. *Determinare tutti gli $x \in \mathbb{Z}$ tali che*

$$\begin{cases} 3x \equiv 6 \pmod{12}, \\ x \equiv 4 \pmod{15}. \end{cases}$$

La prima congruenza del sistema è equivalente alla congruenza $x \equiv 2 \bmod 4$, ed il sistema è equivalente al sistema

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 4 \pmod{15}. \end{cases}$$

Poiché $mcd(4, 15) = 1$, il Teorema Cinese del Resto ci assicura che il sistema ammette soluzioni. Ci dice inoltre che tali soluzioni sono della forma $x = x_0 + n60$, al variare di $n \in \mathbb{Z}$. Calcolo delle soluzioni (per sostituzione):

le soluzioni della prima congruenza del sistema sono date da $x = 2 + 4k$, al variare di $k \in \mathbb{Z}$. Sostituendo tali soluzioni nella seconda congruenza, troviamo la congruenza in k

$$4k \equiv 2 \bmod 15.$$

Poiché $mcd(4, 15) = 1$ divide 15, questa congruenza (e il sistema di congruenze originale) ammette soluzioni.

Per determinarle, calcoliamo innanzitutto $N, M \in \mathbb{Z}$ tali che $4N + 15M = 1 = mcd(4, 15)$: ad esempio $N = 4$ ed $M = -1$. (In questo caso N, M si vedono ad occhio; altrimenti si può usare l'algoritmo euclideo). Ne segue che $k = 8$ è una soluzione particolare della congruenza $4k \equiv 2 \bmod 15$, la cui soluzione generale è data da $k = 8+n15$, al variare di $n \in \mathbb{Z}$. Sostituendo i valori di k trovati nella soluzione generale della prima congruenza, troviamo la soluzione generale del sistema:

$$x = 2 + 4(8 + n15) = 34 + 60n, \quad n \in \mathbb{Z}.$$

Esercizio 4.3. *Sia $\mathcal{S}$ l'insieme dei numeri interi che divisi per 11 danno resto 1 e che divisi per 13 danno resto 5.*

(a) Determinare $\mathcal{S}$.

(b) Determinare tutti gli elementi $n \in \mathcal{S}$ tali che $0 \leq n \leq 99$.

(a) L'insieme $\mathcal{S}$ è formato dai numeri interi $x \in \mathbb{Z}$ che soddisfano il sistema di congruenze

$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 5 \pmod{13}. \end{cases}$$

Osserviamo che il sistema è compatibile e che la soluzione generale è della forma

$$x = x_0 + K143, \quad K \in \mathbb{Z}, \ 143 = 11 \cdot 13,$$

dove x_0 è una qualunque soluzione particolare del sistema. Dunque resta da calcolare una soluzione particolare x_0. Le soluzioni della prima congruenza sono date da

$$x = 1 + k11, \quad k \in \mathbb{Z}. \tag{$*$}$$

Sostituendo queste soluzioni nella seconda congruenza del sistema, troviamo la congruenza in k

$$11k \equiv 4 \bmod 13. \tag{$**$}$$

Una soluzione particolare della (**) sostituita in (*) dà una soluzione particolare del sistema. Determiniamo innanzitutto due interi $m, n \in \mathbb{Z}$ tali che $11n + 13m = 1$. Mediante l'agoritmo euclideo, troviamo ad esempio $n = 6, m = -5$. Dopodiché $N = 24, M = -20$ soddisfano $11N + 13M = 4$. La corrispondente soluzione particolare della (**) è data da $k_0 = 24$ che sostituita nella (*) ci dà $x_0 = 265$. (b) In questo caso non ci sono elementi $n \in \mathcal{S}$ tali che $0 \leq n \leq 99$.

Esercizio 4.4. *Sia $\mathbb{Z}_{91}$ l'anello delle classi resto (o classi di congruenza) modulo 91 e sia $\mathbb{Z}_{91}^*$ il sottoinsieme delle classi che ammettono inverso moltiplicativo. Determinare se $\overline{7}$ e $\overline{8}$ appartengono a $\mathbb{Z}_{91}^*$; in caso affermativo, calcolarne l'inverso in $\mathbb{Z}_{91}$.* Poiché $91 = 7 \times 13$ e

$mcd(7, 91) = 13 \neq 1$, la classe resto $\overline{7}$ non ammette inverso moltiplicativo in $\mathbb{Z}_{91}$ e dunque non appartiene a $\mathbb{Z}_{91}^*$. Si ha invece $mcd(8, 91) = 1$, e quindi $\overline{8} \in \mathbb{Z}_{91}^*$. Per calcolare l'inverso di $\overline{8}$, dobbiamo determinare un $x \in \mathbb{Z}$ tale che

$$8x + N91 = 1, \quad \text{per qualche } N \in \mathbb{Z}.$$

Tali interi x, N esistono perché $mcd(8, 91) = 1$ e si possono calcolare con l'algoritmo euclideo:

$$1 \cdot 91 + 0 \cdot 8 = 91$$

$$0 \cdot 91 + 1 \cdot 8 = 8$$

$$1 \cdot 91 + (-11) \cdot 8 = 3, \quad 91 = 8 \cdot 11 + 3$$

$$(-2) \cdot 91 + 23 \cdot 8 = 2, \quad 8 = 3 \cdot 2 + 2$$

$$3 \cdot 91 + (-34) \cdot 8 = 1, \quad 3 = 2 \cdot 1 + 1$$

Dal calcolo troviamo $x = -34$, per cui l'inverso cercato è

$$\overline{8}^{-1} = \overline{x} = \overline{57} \in \mathbb{Z}_{91}^*.$$

Esercizio 4.5. Determinare la classe di congruenza modulo 15 dell'intero

$$1234^{1234} + 5678^{5678}$$

Esercizio 4.6. a) Stabilire se le seguenti equazioni hanno soluzioni intere e, in caso affermativo, determinarle tutte:
$117\,x + 213\,y = -12$, $\qquad 117\,x + 213\,y = 4$
b) Determinare tutti i numeri naturali k, compresi tra 1 e 213, tali che $117\,k \equiv -12 \pmod{213}$.

SOLUZIONE. a) Con l'algoritmo euclideo si trova che $mcd(117, 213) = 3$ e che $213 \cdot 11 + 117 \cdot (-20) = 3$. Dunque, moltiplicando per -4: $213 \cdot (-44) + 117 \cdot 80 = -12$. Dunque $(80, -44)$ è una soluzione intera della prima equazione. Le altre sono (vedi teoria) tutte e sole le coppie della forma $(80 + \frac{213}{3}k, -44 - \frac{117}{3}) = (80 + 71k, -44 - 39k)$, per ogni $k \in \mathbf{Z}$.
La seconda equazione non ha soluzioni intere perchè $mcd(117, 213) = 3$ non divide 4.

b) La congruenza $117\,x \equiv -12 \pmod{213}$ è equivalente a $39\,x \equiv -4 \pmod{71}$. Poichè 39 e -4 sono coprimi, la soluzione è unica modulo 71. Dunque le soluzioni intere sono $80 + 71k$, per ogni $k \in \mathbf{Z}$. I numeri di questa forma compresi tra 1 e 213 sono: 9, 80, 151.

Esercizio 4.7. Determinare tutti i numeri interi $x \in \mathbf{Z}$ tali che $\begin{cases} x \equiv -12 \pmod 5 \\ 6x \equiv 4 \pmod 8 \\ 4x \equiv 3 \pmod 9 \end{cases}$.

Soluzione. L'equazione $4x \equiv 3 \pmod 9$ ha come soluzione $x \equiv 3 \pmod 9$.

L'equazione $6x \equiv 4 \pmod 8$ è equivalente a $3x \equiv 2 \pmod 4$ e ha come soluzione $x \equiv 2 \pmod 4$. Dunque il sistema è equivalente a

$$\begin{cases} x \equiv -2 \pmod 5 \\ x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 9 \end{cases}$$

la cui soluzione è unica modulo 180. Con facili calcoli si perrviene alla soluzione generale $X = 138 + 180k$, per ogni $k \in \mathbf{R}$.

Esercizio 4.8. Calcolare il resto della divisione per 99 del numero $863945^{3215452}$.

Soluzione. Per il teorema cinese sei resti, è sufficiente trovare il numero x tale che $0 \leq x < 99$ tale che

$$\begin{cases} x \equiv 863945^{321545^2} \pmod 9 \\ x \equiv 863945^{321545^2} \pmod{11} \end{cases}$$

Osserviamo che

$$863945^{321545^2} \equiv (-1)^{321545^2} \equiv -1 \pmod 9$$

(la prima congruenza segue dal fatto un numero positivo è congruente, modulo 9, alla somma delle sue cifre decimali e la seconda dal fatto che 321545^2 è dispari). Inoltre

$$863945^{321545^2} \equiv 5^{321545^2} \equiv 5^{5^2} \equiv 5^5 \equiv 1 \pmod{11}$$

(la prima congruenza segue dal fatto che un numero positivo è congruente alla somma alternata delle sue cifre decimali, la seconda e la terza dal Teorema di Fermat perchè $321545^2 \equiv 5^2 \equiv 5 \pmod{10}$.) Dunque si deve risolvere il sistema $\begin{cases} x \equiv -1 \pmod 9 \\ x \equiv 1 \pmod{11} \end{cases}$, la cui più piccola soluzione positiva è 89. Dunque il resto cercato è 89.

Esercizio 4.9. Determinare tutti gli $x \in \mathbf{Z}$ tali che $\begin{cases} x \equiv 58^{193} \pmod{55} \\ 2x \equiv 6 \pmod 8 \end{cases}$

Soluzione. Innanzitutto si osservi che la seconda equazione è equivalente a: $x \equiv 3 \pmod 4$. Dunque, per il Teorema Cinese dei Resti, la soluzione è unica modulo $55 \cdot 4 = 220$.

Si ha che $58 \equiv 3 \pmod{55}$. Per il teorema cinese dei resti, l'equazione $x \equiv 3^{193} \pmod{55}$ èd equivalente al sistema $\begin{cases} x \equiv 3^{193} \pmod 5 \\ x \equiv 3^{193} \pmod{11} \end{cases}$. Poichè, $193 \equiv 1 \pmod 4$, per il Teorema di Fermat, $3^{193} \equiv 3 \pmod 5$. Allo stesso modo, $3^{193} \equiv 3^3 \equiv 5 \pmod{11}$. In conclusione, il sistema è equivalente a: $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod 4 \end{cases}$. Si trova che la soluzione è $x = 203 + 220k$, $k \in \mathbf{Z}$.

Esercizio 4.10. Determinare, se esistono, tutte le soluzioni intere, comprese tra -700 e 700, delle seguenti congruenze:

(a) $414x \equiv 2 \pmod{662}$; (b) $414x \equiv -11 \pmod{662}$; (c) $414x \equiv -8 \pmod{662}$

Soluzione. Con l'algoritmo euclideo si vede che: (i) $mcd(662, 414) = 2$ e inoltre che: (ii) $2 = 662 \cdot (-5) + 414 \cdot 8$.

Da (ii) si deduce che sia (a) che (c) hanno soluzioni intere, uniche $\pmod{331}$, mentre (b) non ha soluzioni.

(a) Riducendo l'uguaglianza (ii) $\pmod{662}$ si vede che $x = 8$ è una soluzione. Quindi tutte le soluzioni intere sono: $8 + 331k$, $k \in \mathbf{Z}$. Quelle comprese tra -700 e 700 sono: -654, -323, 8, 339, 670.

(c) Poichè, come risulta da (a), $414 \cdot 8 \equiv 2 \pmod{662}$ si ha, moltiplicando per -4, che $414 \cdot (-32) \equiv -8 \pmod{662}$. Dunque le soluzioni intere sono $-32 + 331k$, $k \in \mathbf{Z}$. Quelle tra -700 e 700 sono: -694, -363, -32, 299, 630.

Esercizio 4.11. Per ciascuna delle seguenti congruenze/sistemi di congruenze, determinare tutti gli $x \in \mathbb{Z}$ che le verificano: (a) $34x \equiv 4 \pmod{74}$, (b) $34x \equiv 21 \pmod{74}$, (c) $\begin{cases} 34x \equiv 4 \pmod{74} \\ x \equiv 2 \pmod{3} \end{cases}$.

Soluzione. (b) Non ha soluzione perchè 21, essendo dispari, non è multiplo di $mcd(34, 74)$.

(a) $34x \equiv 4 \pmod{74}$ è equivalente a

$$17x \equiv 2 \pmod{37}$$

che ha soluzione unica $\pmod{37}$, perchè $mcd(17, 37) = 1$.

Con l'algoritmo euclideo si trova: $1 = 37 \cdot 6 + 17 \cdot (-13)$. Quindi $17 \cdot (-13) \equiv 1 \pmod{37}$. Moltiplicando per 2: $17 \cdot (-26) \equiv 2 \pmod{37}$. Dunque le soluzioni sono tutti i numeri interi congruenti $\pmod{37}$ a -26, dunque anche a 11, quindi sono i numeri interi

$$11 + 37k, \qquad \text{per ogni } k \in \mathbf{Z}.$$

(c) Per il punto (a)

$$\begin{cases} 34x \equiv 4 \pmod{74} \\ x \equiv 2 \pmod{3} \end{cases} \quad \Leftrightarrow \quad \begin{cases} x \equiv 11 \pmod{37} \\ x \equiv 2 \pmod{3} \end{cases}$$

Poichè $mcd(37, 3) = 1$ sappiamo già, per il teorema cinese dei resti, che le soluzioni esistono, uniche modulo $111 (= 37.3)$. Dalla prima equazione si ha

$$x = 11 + 37k, \qquad k \in \mathbf{Z}. \tag{1}$$

Sostituendo nella seconda: $11 + 37k \equiv 2 \pmod{3}$ cioè, riducendo modulo 3:

$$k \equiv 0 \pmod{3},$$

cioè $k = 3h$, $h \in \mathbf{Z}$. Dunque, sostituendo nella (1):

$$x = 11 + 111h, \qquad h \in \mathbf{Z}.$$

Esercizio 4.12. Calcolare il resto della divisione di $7^{(7^7)}$ per 19. Osserviamo che 19 è un numero primo e che dunque, grazie al piccolo teorema di Fermat, abbiamo $7^{\phi(19)} = 1$. Rimane quindi da calcolare la classe di congruenza di 7^7 modulo $\phi(19) = 18$. Ora, $7^3 \equiv 1 \pmod{18}$, quindi $7^7 \equiv 7 \pmod{18}$. Rimane da calcolare la classe di congruenza di 7^7 modulo 19. Ora, $7^3 \equiv 1 \pmod{19}$, quindi $7^7 \equiv 7 \pmod{19}$.

Esercizio 4.13. Sia $\mathbf{Z}_{15}^*$ il gruppo moltiplicativo di $\mathbf{Z}_{15}$. Si consideri la relazione R su $\mathbf{Z}_{15}^*$ così definita: $\bar{a}\, R\, \bar{b}$ se e solo se $\bar{a} = \bar{b}$ o $\bar{a} = \bar{b}^{-1}$.

(a) Dimostrare che R è una relazione di equivalenza

(b) Determinare tutte le classi di equivalenza.

Soluzione. (a) Riflessività: $\bar{a} = \bar{a}$. Quindi $\bar{a}\, R\, \bar{a}$, per ogni $\bar{a} \in \mathbf{Z}_{15}^*$.
Simmetria: se $\bar{a} = \bar{b}$, allora $\bar{b} = \bar{a}$. Se $\bar{a} = \bar{b}^{-1}$, allora $\bar{b} = \bar{a}^{-1}$. Dunque, in ogni caso, se $\bar{a}\, R\, \bar{b}$ allora $\bar{b}\, R\, \bar{a}$.
Transitività: se $\bar{a} = \bar{b}$ e $\bar{b} = \bar{c}$, allora $\bar{a} = \bar{c}$; se $\bar{a} = \bar{b}$ e $\bar{b} = \bar{c}^{-1}$ allora $\bar{a} = \bar{c}^{-1}$; se $\bar{a} = \bar{b}^{-1}$ e $\bar{b} = \bar{c}$: si ha anche che $\bar{b}^{-1} = \bar{c}^{-1}$, e quindi che $\bar{a} = \bar{c}^{-1}$. Se $\bar{a} = \bar{b}^{-1}$ e $\bar{b} = \bar{c}^{-1}$: si ha anche che $\bar{b}^{-1} = \bar{c}$, e quindi $\bar{a} = \bar{c}$.

(b) Ricordiamo che $\mathbf{Z}_{15}^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, 1\bar{1}, 1\bar{3}, 1\bar{4}\}$. Si vede facilmente che $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{8}$, $\bar{4}^{-1} = \bar{4}$, $\bar{7}^{-1} = 1\bar{3}$, $1\bar{1}^{-1} = 1\bar{1}$, $1\bar{3}^{-1} = 1\bar{3}$. Dunque le calssi di equivalenza sono sei, e precisamente: $\{\bar{1}\}$, $\{\bar{2}, \bar{8}\}$, $\{\bar{4}\}$, $\{\bar{7}, 1\bar{3}\}$, $\{1\bar{1}\}$, $\{1\bar{3}\}$.

Esercizio 4.14. Sia $\mathbf{Z}_7^*$ il gruppo moltiplicativo dei resti non nulli modulo 7.

(a) Dimostrare che $\overline{2} \in \mathbf{Z}_7^*$ è un quadrato. In altre parole, dimostrare che esiste $\overline{a} \in \mathbf{Z}_7^*$ tale che $\overline{a}^2 = \overline{2}$ in $\mathbf{Z}_7^*$.

(b) Dimostrare che $\overline{3} \in \mathbf{Z}_7^*$ non è un quadrato.

(c) Per $\overline{a}, \overline{b} \in \mathbf{Z}_7^*$ definiamo la relazione $\overline{a} \sim \overline{b}$ quando $\overline{a} \cdot \overline{b}$ è un quadrato. Dimostrare che si tratta di una relazione di equivalenza.

(d) Quante classi di equivalenza ci sono? noindent Abbiamo che $3^2 \equiv 2 \pmod 7$ e quindi la parte (a) è chiara.

Per dimostrare (b) calcoliamo tutti i quadrati modulo 7. Osservando che $4 \equiv -3 \pmod 7$, $5 \equiv -2 \pmod 7$ e $6 \equiv -1 \pmod 7$, troviamo che i quadrati in $\mathbf{Z}_7^*$ sono $(\pm 1)^2 \equiv 1 \pmod 7$, $(\pm 2)^2 \equiv 4 \pmod 7$ e $(\pm 3)^2 \equiv 2 \pmod 7$. Il sottoinsieme dei quadrati è quindi uguale a $\{\overline{1}, \overline{2}, \overline{4}\} \subset \mathbf{Z}_7^*$. Siccome $\overline{3}$ non appartiene a questo sottoinsieme, $\overline{3}$ non è un quadrato.

Siccome $\overline{a} \cdot \overline{a} = \overline{a}^2$ è sempre un quadrato, la relazione è riflessiva. Se $\overline{a} \cdot \overline{b}$ è un quadrato, anche $\overline{b} \cdot \overline{a}$ lo è, perché $\overline{b} \cdot \overline{a} = \overline{a} \cdot \overline{b}$. La relazione è quindi simmetrica. Finalmente, se $\overline{a} \cdot \overline{b}$ e $\overline{b} \cdot \overline{c}$ sono quadrati, anche il prodotto $\overline{a} \cdot \overline{b}^2 \cdot \overline{c}$ lo è. Moltiplicando per il quadrato dell'inverso di $\overline{b}$ segue che anche $\overline{a} \cdot \overline{c}$ è un quadrato. Questo implica la transitività della relazione. Si tratta quindi di una relazione di equivalenza.

Ci sono due classi di equivalenza: i quadrati $\{\overline{1}, \overline{2}, \overline{4}\}$ e i non quadrati $\{\overline{3}, \overline{5}, \overline{6}\}$.